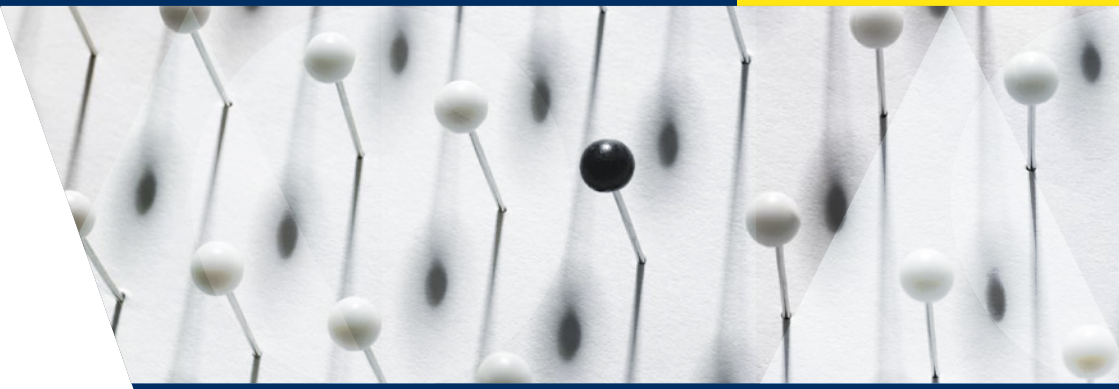
PRIROČNIK



Priročnik o evropskem pravu varstva osebnih podatkov

Izdaja iz leta 2018

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Rokopis tega priročnika je bil dokončan aprila 2018.

Posodobitve bodo v prihodnosti na voljo na spletišču Agencije EU za temeljne pravice (FRA) na spletnem naslovu fra.europa.eu, spletišču Sveta Evrope na naslovu coe.int/dataprotection, spletišču Evropskega sodišča za človekove pravice na spletnem naslovu echr.coe.int pod zavihkom „Sodna praksa“ in spletišču Evropskega nadzornika za varstvo podatkov na spletnem naslovu edps.europa.eu.

Fotografija (na naslovnici in v notranjosti): © iStockphoto

Veliko dodatnih informacij o Evropski uniji je na voljo na internetu (http://europa.eu).

Luxembourg: Urad za publikacije Evropske unije, 2021

Svet Evrope:	ISBN 978-92-871-9815-0		
FRA – Print:	ISBN 978-92-9474-788-4	doi:10.2811/903991	TK-05-17-225-SL-C
FRA – PDF:	ISBN 978-92-9474-785-3	doi:10.2811/972846	TK-05-17-225-SL-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Priročnik o evropskem pravu varstva osebnih podatkov

Izdaja iz leta 2018

Predgovor

Naše družbe so vse bolj digitalizirane. Hitrost tehnološkega razvoja in način obdelave osebnih podatkov vplivata na nas vsak dan in na najrazličnejše načine. Pred kratkim sta bila pregledana pravna okvira Evropske unije (EU) in Sveta Evrope, ki zagotavljata varstvo zasebnosti in osebnih podatkov.

Evropa je na področju varstva osebnih podatkov vodilna v svetu. Standardi EU za varstvo osebnih podatkov temeljijo na Konvenciji Sveta Evrope št. 108, instrumentih EU (vključno s Splošno uredbo o varstvu podatkov in direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja) ter zadevni sodni praksi Evropskega sodišča za človekove pravice in Sodišča Evropske unije.

Reforme na področju varstva osebnih podatkov, ki jih izvajata EU in Svet Evrope, so obsežne in včasih zapletene ter na najrazličnejše načine vplivajo na posameznike in podjetja. Namen tega priročnika je ozaveščati in izboljšati poznavanje predpisov o varstvu osebnih podatkov, zlasti med nespecializiranimi pravnimi delavci, ki se pri delu srečujejo z vprašanji varstva osebnih podatkov.

Ta priročnik je pripravila Agencija EU za temeljne pravice (FRA) v sodelovanju s Svetom Evrope (skupaj s sodnim tajništvom Evropskega sodišča za človekove pravice) in uradom Evropskega nadzornika za varstvo podatkov. Gre za posodobljeno izdajo priročnika iz leta 2014 in je del serije pravnih priročnikov, ki jih skupaj pripravljata FRA in Svet Evrope.

Za koristne povratne informacije o osnutku tega priročnika se zahvaljujemo organom za varstvo podatkov Belgije, Estonije, Francije, Gruzije, Irske, Italije, Madžarske, Monaka, Švice in Združenega kraljestva. Zahvaljujemo se tudi oddelkoma Evropske komisije za varstvo osebnih podatkov ter za mednarodni pretok podatkov in varstvo podatkov. Za dokumentacijsko podporo pri pripravi tega priročnika pa se zahvaljujemo Sodišču Evropske unije. Na koncu se zahvaljujemo tudi Informacijskemu pooblaščencu Republike Slovenije za podporo pri revidiranju slovenskega prevoda priročnika.

Christos Giakoumopoulos

Generalni direktor za človekove pravice in pravno državo pri Svetu Evrope

Giovanni Buttarelli

Evropski nadzornik za varstvo podatkov

Michael O'Flaherty

Direktor Agencije Evropske unije za temeljne pravice

Kazalo

Okrajšave in kratice

CCTV	televizija zaprtega kroga (videonadzor)
CETS	Zbirka pogodb Sveta Evrope
CIS	carinski informacijski sistem
C-SIS	centralni schengenski informacijski sistem
EFSA	Evropska agencija za varnost hrane
EFTA	Evropsko združenje za prosto trgovino
EGP	Evropski gospodarski prostor
EJT	Evropsko javno tožilstvo
EKČP	Evropska konvencija o človekovih pravicah
ENISA	Agencija Evropske unije za kibernetsko varnost
ENVP	Evropski nadzornik za varstvo podatkov
EOVP	Evropski odbor za varstvo podatkov
ES	Evropska skupnost
ESČP	Evropsko sodišče za človekove pravice
ESMA	Evropski organ za vrednostne papirje in trge
eTEN	vseevropska telekomunikacijska omrežja
EU	Evropska unija
eu-LISA	Agencija EU za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice
EuroPriSe	Evropski pečat zaupnosti
FRA	Agencija Evropske unije za temeljne pravice
GPS	globalni sistem za določanje položaja
IKT	informacijska in komunikacijska tehnologija
Konvencija št. 108	Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Svet Evrope). Odbor ministrov Sveta Evrope je na svojem 128. zasedanju v Helsingørju na Danskem (17. in 18. maj 2018) sprejel Protokol o spremembi (CETS št. 223) Konvencije št. 108 (v nadaljnjem besedilu: posodobljena Konvencija št. 108). Sklicevanja na posodobljeno Konvencijo št. 108 se nanašajo na Konvencijo, kakor je bila spremenjena s Protokolom CETS št. 223.

Listina	Listina Evropske unije o temeljnih pravicah
MPDPP	Mednarodni pakt o državljanskih in političnih pravicah
N-SIS	nacionalni schengenski informacijski sistem
NVO	nevladna organizacija
OECD	Organizacija za gospodarsko sodelovanje in razvoj
PDEU	Pogodba o delovanju Evropske unije
PEU	Pogodba o Evropski uniji
PIN	osebna identifikacijska številka
PNR	evidenca podatkov o potnikih
SDČP	Splošna deklaracija človekovih pravic
SEPA	enotno območje plačil v eurih
SEU	Sodišče Evropske unije (pred decembrom 2009 se je imenovalo Sodišče Evropskih skupnosti – SES)
SIS	schengenski informacijski sistem
SUVP	Splošna uredba o varstvu podatkov
SWIFT	Združenje za svetovne finančne telekomunikacije med bankami
UL	Uradni list
VIS	vizumski informacijski sistem
ZN	Združeni narodi

Kako uporabljati priročnik?

V tem priročniku so opisani pravni standardi v zvezi z varstvom osebnih podatkov, ki sta jih določila Evropska unija (EU) in Svet Evrope. Namenjen je delavcem v pravni stroki, ki niso specializirani za varstvo osebnih podatkov, vključno z odvetniki, sodniki in drugimi pravnimi delavci ter uslužbencem drugih organov, kot so nevladne organizacije (NVO), ki se lahko srečujejo s pravnimi vprašanji, povezanimi z varstvom osebnih podatkov.

Priročnik je prva referenčna točka o zadevnem pravu EU in Evropski konvenciji o človekovih pravicah (EKČP) in o Konvenciji Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108) in drugih instrumentih Sveta Evrope.

Na začetku vsakega poglavja je preglednica zakonskih določb v zvezi s temami, obravnavanimi v zadevnem poglavju. Preglednice, ki zajemajo pravni sistem Sveta Evrope in EU, vključujejo izbrano sodno prakso Evropskega sodišča za človekove pravice (ESČP) in Sodišča Evropske unije (SEU). Zadevni predpisi pravnih redov, ki se uporabljata v Evropi, so nato navedeni po vrstnem redu, kot se uporabljajo na posameznem področju. Bralec tako lahko vidi, v čem oba pravna sistema sovpadata in v čem se razlikujeta. Uporabniki naj bi tako lažje poiskali ključne informacije, ki se nanašajo na njihov primer, zlasti če se zanje uporablja samo pravo Sveta Evrope. Zaradi jedrnatosti predstavitve vsebine poglavja se lahko vrstni red tem v preglednici nekoliko razlikuje od vrstnega reda tem v besedilu poglavja. Priročnik vsebuje tudi kratek pregled okvira Združenih narodov.

Za delavce v pravni stroki iz držav, ki niso članice EU, vendar so članice Sveta Evrope ter pogodbenice EKČP in Konvencije št. 108, so informacije v zvezi z njihovo državo navedene v razdelkih, ki se nanašajo na Svet Evrope. Ti delavci morajo poleg tega upoštevati, da se pravila EU o varstvu osebnih podatkov od sprejetja Splošne uredbe o varstvu podatkov (SUVP) uporabljajo za organizacije in druge subjekte, ki niso ustanovljeni v EU, če obdelujejo osebne podatke ter ponujajo blago in storitve posameznikom, na katere se nanašajo osebni podatki, v Uniji ali spremljajo vedenje takih posameznikov.

Delavci v pravni stroki iz držav članic EU bodo morali uporabljati oba razdelka, saj sta za te države zavezujoča oba pravna reda. Opozoriti je treba, da so reforme in posodobitev pravil o varstvu osebnih podatkov v Evropi, ki so se izvajale v okviru Sveta Evrope (posodobljena Konvencija št. 108, kakor je bila spremenjena s Protokolom

CETS št. 223) in EU (sprejetje SUVP in Direktive (EU) 2016/680), potekale vzporedno. Regulativni organi v obeh pravnih sistemih so si nadvse prizadevali za zagotavljanje doslednosti in skladnosti med zadevnima pravnima okviroma. Reforme so tako privedle do večje usklajenosti med pravom Sveta Evrope o varstvu osebnih podatkov in zadevnim pravom EU. Za vse, ki o neki temi potrebujejo več informacij, je v razdelku Dodatna literatura na voljo seznam bolj specializiranega gradiva. Informacije v zvezi z določbami Konvencije št. 108 in njenega dodatnega protokola iz leta 2001, ki se uporabljajo do začetka veljavnosti protokola o spremembi, so na voljo v izdaji tega priročnika iz leta 2014.

Pravo Sveta Evrope je predstavljeno s kratkimi sklicevanji na izbrane zadeve ESČP. Te so bile izbrane iz številnih sodb in odločb ESČP, ki se nanašajo na vprašanja varstva osebnih podatkov.

Zadevno pravo EU sestavljajo sprejeti zakonodajni akti, zadevne določbe Pogodb in Listine Evropske unije o temeljnih pravicah, kot se razlagajo v sodni praksi SEU. Poleg tega so v priročniku navedena mnenja in smernice, ki jih je sprejela Delovna skupina iz člena 29, posvetovalni organ, ki je bil v skladu z direktivo o varstvu osebnih podatkov odgovoren za strokovno svetovanje državam članicam EU in ki ga je 25. maja 2018 nadomestil Evropski odbor za varstvo podatkov (EOVP). Pomemben vpogled v razlago prava EU so tudi mnenja Evropskega nadzornika za varstvo podatkov, ki so zato vključena v ta priročnik.

Zadeve, ki so opisane ali navedene v tem priročniku, so primeri iz obsežnega korpusa sodne prakse ESČP in SEU. S smernicami na koncu tega priročnika si lahko bralci pomagajo pri iskanju sodne prakse na spletu. Navedena sodna praksa SEU se nanaša na prej veljavno direktivo o varstvu osebnih podatkov, vendar se razlage SEU še naprej uporabljajo za ustrezne pravice in obveznosti, določene s SUVP.

Poleg tega so v besedilnih poljih z modrim ozadjem navedene praktične ponazoritve hipotetičnih scenarijev. Te so namenjene za dodatno ponazoritev uporabe evropskih pravil o varstvu osebnih podatkov v praksi, zlasti če ni na voljo specifična zadevna sodna praksa ESČP ali SEU. V drugih besedilnih poljih, tj. s sivim ozadjem, pa so navedeni primeri iz drugih virov, ki niso sodna praksa ESČP in SEU, na primer zakonodaja in mnenja, ki jih je izdala Delovna skupina iz člena 29.

Na začetku priročnika je na kratko opisana vloga dveh pravnih sistemov, kot je določena z EKČP in pravom EU (poglavje 1). V poglavjih od 2 do 8 se obravnavajo naslednja vprašanja:

- izrazi s področja varstva osebnih podatkov;
- ključna načela evropskega prava o varstvu osebnih podatkov;
- pravila evropskega prava o varstvu osebnih podatkov;
- neodvisen nadzor;
- pravice posameznikov, na katere se nanašajo osebni podatki, in njihovo uveljavljanje;
- čezmejni prenosi in pretoki osebnih podatkov;
- varstvo osebnih podatkov v okviru policije in kazenskega pravosodja;
- druga evropska pravila o varstvu osebnih podatkov na specifičnih področjih;
- sodobni izzivi v zvezi z varstvom osebnih podatkov.

1

Okvir in ozadje evropskega prava o varstvu osebnih podatkov

EU	Obravnavane teme	Svet Evrope
Pravica do varstva podatkov		
Pogodba o delovanju Evropske unije, člen 16 Listina Evropske unije o temeljnih pravicah (Listina), člen 8 (pravica do varstva osebnih podatkov) Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31), v veljavi do maja 2018 (v nadaljnjem besedilu: direktiva o varstvu osebnih podatkov) Okvirni sklep Sveta 2008/977/PNZ o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (UL L 350, 30.12.2008, str. 60), v veljavi do maja 2018 Uredba (EU) 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1)		EKČP, člen 8 (pravica do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja) Posodobljena Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (posodobljena Konvencija št. 108)

EU	Obravnavane teme	Svet Evrope
Direktiva (EU) 2016/680 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89) (v nadaljnjem besedilu: direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja) Direktiva 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37) Uredba (ES) št. 45/2001 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1) (v nadaljnjem besedilu: uredba o varstvu osebnih podatkov v institucijah EU)		
Omejitve pravice do varstva osebnih podatkov		
Listina, člen 52(1) SUVP, člen 23 SEU, združeni zadevi C-92/09 in C-93/09, *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen* (veliki senat), 2010		EKČP, člen 8(2) Posodobljena Konvencija št. 108, člen 11 ESČP, združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 2008
Uravnoteženje pravic		
SEU, združeni zadevi C-92/09 in C-93/09, *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen* (veliki senat), 2010	**Splošno**	

EU	Obravnavane teme	Svet Evrope
SEU, C-73/07, *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy in Satamedia Oy* (veliki senat), 2008 SEU, C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), 2014	**Svoboda izražanja**	ESČP, *Axel Springer AG proti Nemčiji* (veliki senat), pritožba št. 39954/08, 2012 ESČP, *Mosley proti Združenemu kraljestvu*, pritožba št. 48009/08, 2011 ESČP, *Bohlen proti Nemčiji*, pritožba št. 53495/09, 2015
SEU, C-28/08 P, *Evropska komisija proti The Bavarian Lager Co. Ltd.* (veliki senat), 2010 SEU, *ClientEarth in PAN Europe proti EFSA*, C-615/13 P, 2015	**Dostop do dokumentov**	ESČP, *Magyar Helsinki Bizottság proti Madžarski* (veliki senat), pritožba št. 18030/11, 2016
SUVP, člen 90	**Poklicna skrivnost**	ESČP, *Pruteanu proti Romuniji*, pritožba št. 30181/05, 2015
SUVP, člen 91	**Svoboda vere ali prepričanja**	
	Svoboda umetnosti in znanosti	ESČP, *Vereinigung Bildender Künstler proti Avstriji*, pritožba št. 68354/01, 2007
SEU, C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU* (veliki senat), 2008	**Varstvo lastnine**	
SEU, C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), 2014 SEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju*, 2017	**Ekonomske pravice**	

1.1 Pravica do varstva osebnih podatkov

Ključni poudarki

- Pravica do varstva pred zbiranjem in uporabo osebnih podatkov je na podlagi člena 8 EKČP sestavni del pravice do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja.
- Konvencija Sveta Evrope št. 108 je prvi mednarodni pravno zavezujoči instrument, v katerem je izrecno obravnavano varstvo osebnih podatkov. V zvezi z njo je potekal proces posodobitve, ki je bil zaključen s sprejetjem Protokola CETS št. 223 o spremembi.
- Varstvo osebnih podatkov je v pravu EU priznano kot posebna temeljna pravica. Potrjena je v členu 16 Pogodbe o delovanju EU in členu 8 Listine EU o temeljnih pravicah.
- Varstvo osebnih podatkov je bilo v pravu EU prvič urejeno leta 1995 z direktivo o varstvu osebnih podatkov.
- Zaradi hitrega tehnološkega razvoja je EU leta 2016 sprejela novo zakonodajo, da bi pravila o varstvu osebnih podatkov prilagodila digitalni dobi. S SUVP, ki se je začela uporabljati maja 2018, je bila direktiva o varstvu osebnih podatkov razveljavljena.
- EU je skupaj s SUVP sprejela zakonodajo o obdelavi osebnih podatkov, ki jo izvajajo državni organi za namene kazenskega pregona. V Direktivi (EU) 2016/680 so določena pravila o varstvu osebnih podatkov in načela varstva osebnih podatkov, s katerimi je urejena obdelava osebnih podatkov za namene preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ali izvrševanja kazenskih sankcij.

1.1.1 Pravica do spoštovanja zasebnega življenja in pravica do varstva osebnih podatkov: kratek uvod

Čeprav sta pravica do spoštovanja zasebnega življenja in pravica do varstva osebnih podatkov tesno povezani, sta ločeni pravici. Pravica do zasebnosti, ki se v evropskem pravu imenuje pravica do spoštovanja zasebnega življenja, je bila v mednarodnem pravu človekovih pravic prvič določena v Splošni deklaraciji človekovih pravic (SDČP), ki je bila sprejeta leta 1948, in sicer kot ena od temeljnih zaščitenih človekovih pravic. Kmalu po sprejetju SDČP je to pravico potrdila tudi Evropa, in sicer v Evropski konvenciji o človekovih pravicah (EKČP), ki je pravno zavezujoča za njene pogodbenice in je bila sestavljena leta 1950. EKČP določa, da ima vsakdo pravico do spoštovanja svojega zasebnega in družinskega življenja, doma in dopisovanja.

Poseganje javnih organov v to pravico je prepovedano, razen če je to določeno z zakonom, če sledi pomembnim in zakonitim javnim interesom ter če je nujno v demokratični družbi.

SDČP in EKČP sta bili sprejeti veliko pred razvojem računalnikov in interneta ter pred vzponom informacijske družbe. Ti dosežki so prinesli precejšnje koristi posameznikom in družbi ter izboljšali kakovost življenja, učinkovitost in produktivnost, hkrati pa pomenijo nova tveganja za pravico do spoštovanja zasebnega življenja. Zaradi potrebe po posebnih pravilih, ki bi urejala zbiranje in uporabo osebnih podatkov, se je pojavil nov pojem zasebnosti, ki se v nekaterih jurisdikcijah imenuje informacijska zasebnost, v drugih pa pravica do samostojnega odločanja glede informacij.[1] Ta pojem je privedel do oblikovanja posebnih pravnih predpisov, s katerimi je zagotovljeno varstvo osebnih podatkov.

Varstvo osebnih podatkov v Evropi se je začelo v sedemdesetih letih prejšnjega stoletja, ko so nekatere države sprejele zakonodajo za nadzor obdelave osebnih podatkov, ki jo izvajajo javni organi in velika podjetja.[2] Na evropski ravni[3] so bili nato vzpostavljeni instrumenti za varstvo osebnih podatkov, ki se je z leti razvilo v posebno vrednoto, ki ni zajeta s pravico do spoštovanja zasebnega življenja. V pravnem redu EU je varstvo osebnih podatkov priznano kot temeljna pravica, ki je ločena od temeljne pravice do spoštovanja zasebnega življenja. S to ločitvijo se poraja vprašanje, kakšni so razmerje in razlike med tema pravicama.

Pravica do spoštovanja zasebnega življenja in pravica do varstva osebnih podatkov sta tesno povezani. Cilj obeh je zaščititi podobne vrednote, tj. neodvisnost in človekovo dostojanstvo posameznikov, in sicer tako, da jim zagotavljata osebno sfero, v kateri lahko svobodno razvijajo svojo osebnost, razmišljajo in oblikujejo svoja

1 Nemško zvezno ustavno sodišče je pravico do samostojnega odločanja glede informacij potrdilo v sodbi iz leta 1983 v zadevi (*Volkszählungsurteil)*, BVerfGE Bd. 65, oddelek 1 in naslednji. Menilo je, da samostojno odločanje glede informacij izhaja iz temeljne pravice do spoštovanja osebnosti, ki je zaščitena z nemško ustavo. ESČP je v sodbi iz leta 2017 potrdilo, da člen 8 EKČP določa pravico do neke oblike samostojnega odločanja glede informacij. Glej ESČP, *Satakunnan Markkinapörssi Oy in Satamedia Oy proti Finski* (veliki senat), pritožba št. 931/13, 27. junij 2017, točka 137.

2 Nemška zvezna dežela Hessen je leta 1970 sprejela prvi zakon o varstvu osebnih podatkov, ki se je uporabljal le v tej deželi. Švedska je leta 1973 sprejela prvi nacionalni zakon o varstvu osebnih podatkov na svetu. Do konca osemdesetih let prejšnjega stoletja je zakonodajo o varstvu osebnih podatkov sprejelo tudi več drugih evropskih držav (Francija, Nemčija, Nizozemska in Združeno kraljestvo).

3 Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108) je bila sprejeta leta 1981. EU je prvi celoviti instrument za varstvo osebnih podatkov sprejela leta 1995, in sicer Direktivo 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.

mnenja. Zato sta nujen pogoj za uresničevanje drugih temeljnih svoboščin, kot so svoboda izražanja, svoboda mirnega zbiranja in združevanja ter svoboda vere.

Zadevni pravici se razlikujeta po formulaciji in obsegu. Pravica do spoštovanja zasebnega življenja zajema splošno prepoved poseganja, pri čemer se zanjo uporabljajo nekatera merila javnega interesa, na podlagi katerih je lahko v nekaterih primerih poseganje upravičeno. Varstvo osebnih podatkov je sodobna in aktivna pravica,[4] s katero se vzpostavi sistem nadzora in ravnotežja za zaščito posameznikov vedno, kadar se obdelujejo njihovi osebni podatki. Obdelava mora biti v skladu z bistvenima elementoma varstva osebnih podatkov, in sicer neodvisnim nadzorom in spoštovanjem pravic posameznika, na katerega se nanašajo osebni podatki.[5]

V členu 8 Listine EU o temeljnih pravicah (v nadaljnjem besedilu: Listina) je ne le potrjena pravica do varstva osebnih podatkov, temveč so opredeljene tudi temeljne vrednote, povezane s to pravico. Ta člen določa, da je treba osebne podatke obdelovati pošteno, za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom. Posamezniki morajo imeti pravico dostopa do svojih osebnih podatkov in pravico zahtevati, da se ti podatki popravijo, spoštovanje te pravice pa mora nadzirati neodvisen organ.

Pravico do varstva osebnih podatkov je treba spoštovati vedno, kadar se obdelujejo osebni podatki, zato je ta pravica širša od pravice do spoštovanja zasebnega življenja. Pri vsaki obdelavi osebnih podatkov je treba zagotoviti ustrezno varstvo. Varstvo osebnih podatkov zadeva vse vrste osebnih podatkov in obdelave podatkov, ne glede na razmerje in vpliv na zasebnost. Kot je razvidno iz primerov v nadaljevanju, lahko obdelava osebnih podatkov pomeni tudi kršitev pravice do zasebnega življenja, vendar ni treba dokazati posega v zasebno življenje, da se uporabijo pravila o varstvu osebnih podatkov.

Pravica do zasebnosti se nanaša na primere, v katerih je ogrožen zasebni interes ali zasebno življenje posameznika. Kot je pojasnjeno v tem priročniku, se v sodni praksi pojem zasebno življenje razlaga široko, tako da zajema intimne okoliščine, občutljive

4 Generalna pravobranilka E. Sharpston je v svojih sklepnih predlogih v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen* obravnavani zadevi opisala kot zadevi, ki vključujeta dve pravici: „klasično“ pravico do varstva zasebnosti in „sodobnejšo“ pravico, tj. pravico do varstva osebnih podatkov. Glej SEU, *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, združeni zadevi C-92/09 in C-93/02, *sklepni predlogi generalne pravobranilke E. Sharpston* z dne 17. junija 2010, točka 71.

5 Hustinx, P., spletišče ENVP, zavihek Govori in članki, *Pravo EU o varstvu osebnih podatkov: pregled Direktive 95/46/ES in predlagane splošne uredbe o varstvu podatkov*, julij 2013.

ali zaupne informacije, informacije, ki bi lahko vplivale na to, kako javnost dojema posameznika, ter celo vidike poklicnega življenja posameznika in njegovega vedenja v javnosti. Kljub temu je presoja, ali je prišlo do posega v zasebno življenje, odvisna od okoliščin in dejstev posamezne zadeve.

V nasprotju s tem bi lahko vsako dejanje, ki vključuje obdelavo osebnih podatkov, spadalo na področje uporabe pravil o varstvu osebnih podatkov in sprožilo uporabo pravice do varstva osebnih podatkov. Če na primer delodajalec evidentira podatke o imenih zaposlenih in prejemkih, ki so jim izplačani, zgolj evidentiranja teh podatkov ni mogoče šteti za poseg v zasebno življenje. Da je do takega posega prišlo, pa bi bilo mogoče trditi, če bi na primer delodajalec osebne podatke zaposlenih prenesel tretjim osebam. Delodajalci morajo vselej ravnati v skladu s pravili o varstvu osebnih podatkov, saj evidentiranje podatkov o zaposlenih pomeni obdelavo osebnih podatkov.

Primer: SEU je bilo v zadevi *Digital Rights Ireland*[6] zaprošeno, naj odloči o veljavnosti Direktive 2006/24/ES glede na temeljni pravici do varstva osebnih podatkov in spoštovanja zasebnega življenja, določeni v Listini EU o temeljnih pravicah. V skladu s to direktivo so morali ponudniki javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij telekomunikacijske podatke državljanov hraniti za obdobje do dveh let, da bi zagotovili, da so ti podatki na voljo za namene preprečevanja, preiskovanja in pregona hudih kaznivih dejanj. Ta ukrep se je nanašal le na metapodatke, podatke o lokaciji in podatke, potrebne za določitev naročnika ali uporabnika, ni pa se uporabljal za vsebino elektronskih komunikacij.

SEU je menilo, da ta direktiva pomeni poseganje v temeljno pravico do varstva osebnih podatkov, „ker določa obdelavo osebnih podatkov“.[7] Poleg tega je ugotovilo, da direktiva posega v pravico do spoštovanja zasebnega življenja.[8] Na podlagi vseh osebnih podatkov, ki so se hranili v skladu z njo in do katerih bi lahko dostopali pristojni organi, bi bilo mogoče „izpeljati zelo natančne ugotovitve o zasebnem življenju oseb, katerih podatki so bili

6 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim* in Kärntner Landesregierung in drugi (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014.

7 Prav tam, točka 36.

8 Prav tam, točke 32–35.

shranjeni, kot so vsakodnevne navade, kraji stalnega ali začasnega prebivališča, dnevne ali druge poti, dejavnosti, socialni odnosi in socialna okolja, ki jih obiskujejo".[9] Poseganje v zadevni pravici je bilo občutno in posebej resno.

SEU je Direktivo 2006/24/ES razglasilo za neveljavno, pri čemer je ugotovilo, da je, čeprav direktiva sledi zakonitemu cilju, poseganje v pravici do varstva osebnih podatkov in zasebnega življenja resno ter ni omejeno na to, kar je nujno potrebno.

1.1.2 Mednarodni pravni okvir: Združeni narodi

V okviru Združenih narodov varstvo osebnih podatkov ni priznano kot temeljna pravica, čeprav je v mednarodnem pravnem redu pravica do zasebnosti že dolgo uveljavljena temeljna pravica. Pravica posameznika, da svoje zasebno življenje varuje pred vmešavanjem drugih, zlasti države, je bila v mednarodnem instrumentu prvič določena v členu 12 SDČP o spoštovanju zasebnega in družinskega življenja.[10] Čeprav je SDČP nezavezujoča deklaracija, ima pomemben status kot temeljni instrument mednarodnega prava človekovih pravic in je vplivala na razvoj drugih instrumentov o človekovih pravicah v Evropi. Mednarodni pakt o državljanskih in političnih pravicah (MPDPP) je začel veljati leta 1976. V njem je določeno, da se nikomur ne sme nihče samovoljno ali nezakonito vmešavati v zasebno življenje, v stanovanje ali dopisovanje ali nezakonito napadati njegovo čast in ugled. MPDPP je mednarodna pogodba, ki svojih 169 pogodbenic zavezuje k spoštovanju in zagotavljanju uresničevanja državljanskih pravic posameznikov, vključno z zasebnostjo.

Združeni narodi so od leta 2013 sprejeli dve resoluciji o vprašanjih zasebnosti – o „pravici do zasebnosti v digitalni dobi"[11] – kot odgovor na razvoj novih tehnologij in razkritja o množičnem nadzoru, ki se izvaja v nekaterih državah (Snowdnova razkritja). V njiju so odločno obsodili množični nadzor in poudarili vpliv, ki bi ga lahko imel tak nadzor na temeljni pravici do zasebnosti in svobode izražanja ter na delovanje dinamične in demokratične družbe. Čeprav resoluciji nista pravno zavezujoči, sta spodbudili pomembno mednarodno politično razpravo na visoki ravni o zasebnosti, novih tehnologijah in nadzoru. Privedli sta tudi do vzpostavitve položaja posebnega poročevalca za pravico do zasebnosti, pooblaščenega za spodbujanje in ščitenje

9 Prav tam, točka 27.

10 Združeni narodi (ZN), Splošna deklaracija človekovih pravic, 10. december 1948.

11 Glej ZN, Generalna skupščina, Resolucija o pravici do zasebnosti v digitalni dobi, A/RES/68/167, New York, 18. december 2013, in ZN, Generalna skupščina, Revidirani osnutek resolucije o pravici do zasebnosti v digitalni dobi, A/C.3/69/L.26/Rev.1, New York, 19. november 2014.

te pravice. Posebne naloge poročevalca vključujejo zbiranje informacij o nacionalnih praksah in izkušnjah v zvezi z zasebnostjo in izzivi, ki izhajajo iz novih tehnologij, izmenjavo in spodbujanje najboljših praks ter opredelitev morebitnih ovir.

Prvotne resolucije so se osredotočale na negativne učinke množičnega nadzora in na odgovornost držav članic, da omejijo pooblastila obveščevalnih organov, novejše resolucije pa odražajo ključne novosti razprav o zasebnosti, ki potekajo v Združenih narodih.[12] V resolucijah, sprejetih leta 2016 in 2017, je ponovno potrjena potreba po omejitvi pooblastil obveščevalnih agencij, množični nadzor pa se v njih obsoja. Vendar je v njiju tudi izrecno navedeno, da lahko vse večja sposobnost podjetij, da zbirajo, obdelujejo in uporabljajo osebne podatke, pomeni tveganje za uveljavljanje pravice do zasebnosti v digitalni dobi. V resolucijah se poleg na odgovornost državnih organov opozarja tudi na odgovornost zasebnega sektorja, da spoštuje človekove pravice, pri čemer so podjetja pozvana, naj uporabnike obveščajo o zbiranju, uporabi, izmenjavi in hrambi osebnih podatkov ter vzpostavijo pregledne politike obdelave.

1.1.3 Evropska konvencija o človekovih pravicah

Svet Evrope je bil ustanovljen po drugi svetovni vojni, da bi povezal evropske države ter spodbujal načela pravne države, demokracije, človekovih pravic in družbenega razvoja. Zato je leta 1950 sprejel Evropsko konvencijo o človekovih pravicah (EKČP), ki je začela veljati leta 1953.

Pogodbenice imajo mednarodno obveznost, da upoštevajo EKČP. Vse države članice Sveta Evrope so EKČP že vključile v nacionalno zakonodajo ali jo začele izvajati, kar pomeni, da morajo ravnati v skladu z njenimi določbami. Pogodbenice morajo pri izvajanju vseh dejavnosti ali pooblastil spoštovati pravice, določene v konvenciji. To vključuje dejavnosti, ki se izvajajo zaradi nacionalne varnosti. Evropsko sodišče za človekove pravice (ESČP) je v prelomnih sodbah obravnavalo dejavnosti države na občutljivih področjih prava in prakse v zvezi z nacionalno varnostjo.[13] Sodišče je brez oklevanja potrdilo, da dejavnosti nadzora pomenijo poseg v pravico do spoštovanja zasebnega življenja.[14]

12 ZN, Generalna skupščina, Revidirani osnutek resolucije o pravici do zasebnosti v digitalni dobi, A/C.3/71/L.39/Rev.1, New York, 16. november 2016; ZN, Svet za človekove pravice, The right to privacy in the digital age (Pravica do zasebnosti v digitalni dobi), A/HRC/34/L.7/Rev.1, 22. marec 2017.

13 Glej na primer ESČP, *Klass in drugi proti Nemčiji*, pritožba št. 5029/71, 6. september 1978; ESČP, *Rotaru proti Romuniji* (veliki senat), pritožba št. 28341/95, 4. maj 2000, in ESČP, *Szabó in Vissy proti Madžarski*, pritožba št. 37138/14, 12. januar 2016.

14 Prav tam.

Da bi pogodbenice izpolnjevale svoje obveznosti na podlagi EKČP, je bilo leta 1959 v Strasbourgu v Franciji ustanovljeno Evropsko sodišče za človekove pravice (ESČP). To sodišče zagotavlja, da države izpolnjujejo obveznosti na podlagi konvencije, in sicer z obravnavanjem pritožb posameznikov, skupin posameznikov, nevladnih organizacij ali pravnih oseb, ki trdijo, da je bila kršena konvencija. ESČP obravnava tudi meddržavne sodne postopke, ki jih ena ali več držav članic Sveta Evrope sproži zoper drugo državo članico.

Svet Evrope ima od leta 2018 47 pogodbenic, od tega jih je 28 tudi držav članic EU. Ni nujno, da je pritožnik pred ESČP državljan ene od pogodbenic, morajo pa biti za obravnavo domnevnih kršitev pristojna sodišča ene od pogodbenic.

Pravica do varstva osebnih podatkov spada med pravice, varovane s členom 8 EKČP, s katerim je zagotovljena pravica do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja, določa pa tudi pogoje, pod katerimi so dovoljene omejitve te pravice.[15]

ESČP je obravnavalo že veliko zadev, ki so se nanašale na vprašanja varstva osebnih podatkov. Ta vključujejo prestrezanje komunikacij,[16] različne oblike nadzora, ki ga izvajajo organizacije iz zasebnega in javnega sektorja,[17] in varstvo pred hrambo osebnih podatkov s strani javnih organov.[18] Spoštovanje zasebnega življenja ni absolutna pravica, saj bi lahko uveljavljanje pravice do zasebnosti ogrozilo druge pravice, kot sta svoboda izražanja in dostop do informacij, ter obratno. Zato si Sodišče prizadeva najti ravnotežje med različnimi zadevnimi pravicami. Pojasnilo je, da se morajo države na podlagi člena 8 EKČP ne le vzdržati ukrepov, s katerimi bi lahko bila kršena ta pravica po konvenciji, ampak so jim v nekaterih okoliščinah naložene tudi pozitivne obveznosti za dejavno zagotavljanje učinkovitega spoštovanja zasebnega in družinskega življenja.[19] Številne od teh zadev so podrobneje opisane v ustreznih poglavjih.

15 Svet Evrope, Evropska konvencija o človekovih pravicah, CETS št. 005, 1950.

16 Glej na primer ESČP, *Malone proti Združenemu kraljestvu*, pritožba št. 8691/79, 2. avgust 1984; ESČP, *Copland proti Združenemu kraljestvu*, pritožba št. 62617/00, 3. april 2007, in ESČP, *Mustafa Sezgin Tanrıkulu proti Turčiji*, pritožba št. 27473/06, 18. julij 2017.

17 Glej na primer ESČP, *Klass in drugi proti Nemčiji*, pritožba št. 5029/71, 6. september 1978, in ESČP, *Uzun proti Nemčiji*, pritožba št. 35623/05, 2. september 2010.

18 Glej na primer ESČP, *Roman Zakharov proti Rusiji* (veliki senat), pritožba št. 47143/06, 4. december 2015, in ESČP, *Szabó in Vissy proti Madžarski*, pritožba št. 37138/14, 12. januar 2016.

19 Glej na primer ESČP, *I proti Finski*, pritožba št. 20511/03, 17. julij 2008, in ESČP, *K. U. proti Finski*, pritožba št. 2872/02, 2. december 2008.

1.1.4 Konvencija Sveta Evrope št. 108

S pojavom informacijske tehnologije v šestdesetih letih prejšnjega stoletja je vse bolj naraščala potreba po podrobnejših pravilih, s katerimi bi posameznikom zagotovili varstvo njihovih osebnih podatkov. Odbor ministrov Sveta Evrope je do sredine sedemdesetih let prejšnjega stoletja sprejel več resolucij o varstvu osebnih podatkov, v katerih se je skliceval na člen 8 EKČP.[20] Leta 1981 je bila na voljo za podpis Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108)[21]. Ta je bila in je še vedno edini pravno zavezujoči mednarodni instrument na področju varstva osebnih podatkov.

Konvencija št. 108 se uporablja za vse vrste obdelave osebnih podatkov v zasebnem in javnem sektorju, tudi za obdelavo osebnih podatkov v pravosodju in policiji. Posameznike varuje pred zlorabami, ki lahko spremljajo obdelavo osebnih podatkov, hkrati pa naj bi bil z njo urejen tudi čezmejni prenos osebnih podatkov. Kar zadeva obdelavo osebnih podatkov, se načela, določena v njej, nanašajo zlasti na pošteno in zakonito zbiranje ter avtomatsko obdelavo osebnih podatkov, ki so shranjeni za določene zakonite namene. To pomeni, da osebni podatki ne bi smeli biti namenjeni uporabi, ki ni združljiva s temi nameni, niti se hraniti dlje, kot je potrebno. Zadevna načela se nanašajo tudi na kakovost osebnih podatkov, in sicer morajo ti biti primerni, ustrezni in ne pretirani (sorazmernost) ter točni.

Konvencija določa jamstva glede obdelave osebnih podatkov in obveznosti glede varnosti podatkov, poleg tega pa tudi prepoveduje (če ni ustreznih pravnih jamstev) obdelavo občutljivih podatkov o posamezniku, na primer o njegovi rasi, političnem prepričanju, zdravju, veroizpovedi, spolnem življenju ali kazenski evidenci.

Konvencija določa tudi, da ima posameznik pravico vedeti, da se podatki o njem shranjujejo, in po potrebi zahtevati njihov popravek. Omejitve pravic, določenih v konvenciji, so dovoljene samo, če so ogroženi višji interesi, na primer varnost ali obramba države. Konvencija poleg tega določa prosti pretok osebnih podatkov med pogodbenicami in tudi nekaj omejitev glede prenosa v države, katerih pravna ureditev ne zagotavlja ustreznega varstva.

20 Svet Evrope, Odbor ministrov (1973), Resolucija št. (73) 22 o varstvu zasebnosti posameznikov na področju elektronskih bank podatkov v zasebnem sektorju, 26. september 1973; Svet Evrope, Odbor ministrov (1974), Resolucija št. (74) 29 o varstvu zasebnosti posameznikov na področju elektronskih bank podatkov v javnem sektorju, 20. september 1974.

21 Svet Evrope, Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, CETS št. 108, 1981.

Opozoriti je treba, da je Konvencija št. 108 za države, ki so jo ratificirale, zavezujoča. V zvezi z njo ne velja sodni nadzor ESČP, vendar pa se upošteva v njegovi sodni praksi, in sicer v okviru člena 8 EKČP. Sodišče že dolga leta razsoja, da je varstvo osebnih podatkov pomemben del pravice do spoštovanja zasebnega življenja (člen 8), pri čemer se pri presoji, ali je prišlo do posega v to temeljno pravico, opira na načela iz Konvencije št. 108.[22]

Da bi se natančneje izoblikovala splošna načela in pravila, določena v Konvenciji št. 108, je Odbor ministrov Sveta Evrope sprejel več priporočil, ki pa niso pravno zavezujoča. Ta priporočila so vplivala na razvoj prava o varstvu osebnih podatkov v Evropi. Tako je bil na primer dolga leta v Evropi edini instrument, ki je zagotavljal smernice o uporabi osebnih podatkov v policijskem sektorju, Priporočilo o uporabi osebnih podatkov v policijskem sektorju.[23] Načela iz tega priporočila, ki se med drugim nanašajo na sredstva za hrambo podatkovnih datotek in potrebo po izvajanju jasnih pravil o osebah, ki lahko dostopajo do teh datotek, so bila nadalje razvita in upoštevana v poznejši zakonodaji EU.[24] V novejših priporočilih so obravnavani izzivi digitalne dobe, na primer v zvezi z obdelavo osebnih podatkov v okviru zaposlitve (glej poglavje 9).

Konvencijo št. 108 so ratificirale vse države članice EU. Leta 1999 so bile predlagane spremembe Konvencije št. 108, da bi lahko njena pogodbenica postala tudi EU, vendar niso nikoli začele veljati.[25] Leta 2001 je bil sprejet Dodatni protokol h Konvenciji št. 108, s katerim so bile uvedene določbe o čezmejnem prenosu podatkov v države, ki niso pogodbenice, t. i. tretje države, in o obvezni ustanovitvi nacionalnih nadzornih organov za varstvo osebnih podatkov.[26]

H Konvenciji št. 108 lahko pristopijo tudi države, ki niso članice Sveta Evrope. Možnost, da se konvencija uveljavi kot splošni standard, in njena odprtost sta podlaga za spodbujanje varstva osebnih podatkov na svetovni ravni. H Konvenciji št. 108 je do

22 Glej na primer ESČP, *Z proti Finski*, pritožba št. 22009/93, 25. februar 1997.

23 Svet Evrope, Odbor ministrov (1987), Priporočilo Rec(87)15 državam članicam, ki ureja uporabo osebnih podatkov v policijskem sektorju, Strasbourg, 17. september 1987.

24 Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

25 Svet Evrope, Spremembe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (CETS št. 108), ki jih je Odbor ministrov sprejel v Strasbourgu 15. junija 1999.

26 Svet Evrope, Dodatni protokol h Konvenciji o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov v zvezi z nadzornimi organi in čezmejnim prenosom podatkov, CETS št. 181, 2001. S posodobitvijo Konvencije št. 108 se ta protokol ne uporablja več, saj so bile njegove določbe posodobljene in vključene v posodobljeno Konvencijo št. 108.

zdaj pristopilo 51 držav pogodbenic. Med njimi so vse države članice Sveta Evrope (47 držav), Urugvaj, ki je kot prva neevropska država k njej pristopil avgusta 2013, ter Mavricij, Senegal in Tunizija, ki so k njej pristopili leta 2016 in 2017.

Konvencija je bila pred kratkim posodobljena. V okviru javnega posvetovanja, izvedenega leta 2011, sta bila potrjena dva glavna cilja posodobitve: okrepiti varstvo zasebnosti na digitalnem področju in utrditi mehanizem spremljanja na podlagi konvencije. Proces posodobitve, ki je bil osredotočen na ta cilja, je bil dokončan s sprejetjem Protokola o spremembi Konvencije št. 108 (Protokol CETS št. 223). Delo je potekalo vzporedno z drugimi reformami mednarodnih instrumentov za varstvo osebnih podatkov in skupaj z reformo pravil EU o varstvu osebnih podatkov, ki se je začela leta 2012. Regulativni organi na ravni Sveta Evrope in ravni EU so si nadvse prizadevali za zagotavljanje doslednosti in skladnosti med zadevnima pravnima okviroma. Posodobljena različica ohranja splošnost in prožnost konvencije, okrepljen je tudi njen potencial univerzalnega instrumenta s področja prava o varstvu osebnih podatkov. V njej so ponovno potrjena in utrjena pomembna načela, posameznikom so zagotovljene nove pravice, obenem pa se povečujejo obveznosti subjektov, ki obdelujejo osebne podatke, s čimer je zagotovljena večja odgovornost. Posamezniki, katerih osebni podatki se obdelujejo, imajo na primer pravico, da se seznanijo z razlogi za tako obdelavo osebnih podatkov in da tej obdelavi ugovarjajo. Da bi omejili povečano uporabo oblikovanja profilov v spletnem svetu, je v konvenciji določena tudi pravica posameznika, da zanj ne veljajo odločitve, ki temeljijo zgolj na avtomatizirani obdelavi, ne da bi bila upoštevana njegova stališča. Izvajanje konvencije, ki ga v praksi zagotavljajo neodvisni nadzorni organi v državah pogodbenicah, je osrednjega pomena za učinkovito izvajanje pravil o varstvu osebnih podatkov. V posodobljeni konvenciji je zato poudarjeno, da je treba nadzornim organom dodeliti učinkovita pooblastila in naloge ter da morajo biti ti organi pri opravljanju svojih nalog dejansko neodvisni.

1.1.5 Pravo Evropske unije o varstvu osebnih podatkov

Pravo EU sestavljata primarna in sekundarna zakonodaja EU. Pogodbi, in sicer Pogodbo o Evropski uniji (PEU) in Pogodbo o delovanju Evropske unije (PDEU), so ratificirale vse države članice EU; Pogodbi tvorita primarno zakonodajo EU. Uredbe, direktive in sklepe EU sprejemajo institucije EU, ki so tako pristojnost dobile na podlagi Pogodb; ti instrumenti sestavljajo sekundarno zakonodajo EU.

Varstvo osebnih podatkov v primarni zakonodaji EU

Prvotne pogodbe Evropskih skupnosti niso vsebovale sklicevanja na človekove pravice ali njihovo varstvo, saj je bila Evropska gospodarska skupnost prvotno predvidena kot regionalna organizacija, osredotočena na gospodarsko povezovanje in vzpostavitev skupnega trga. Temeljno načelo, na katerem sta temeljila ustanovitev in razvoj Evropskih skupnosti, je načelo prenosa pristojnosti, ki velja še danes. V skladu s tem načelom EU deluje le v mejah pristojnosti, ki so jih s Pogodbama EU nanjo prenesle države članice. V nasprotju z instrumenti Sveta Evrope v Pogodbah EU niso določene izrecne pristojnosti glede zadev v zvezi s temeljnimi pravicami.

Ker pa so bile SEU predložene zadeve, v katerih so stranke zatrjevale, da so jim bile kršene človekove pravice na področjih, zajetih s pravom EU, je SEU zagotovilo pomembno razlago Pogodb. Da bi posameznikom zagotovilo varstvo, je temeljne pravice vključilo med tako imenovana splošna načela evropskega prava. Po mnenju SEU je v teh splošnih načelih upoštevana vsebina varstva človekovih pravic, vključena v nacionalne ustave in pogodbe o človekovih pravicah, zlasti EKČP. SEU je navedlo, da bo zagotavljalo skladnost prava EU s temi načeli.

EU je leta 2000 ob priznavanju, da bi lahko njene politike vplivale na človekove pravice, in v prizadevanju, da bi se državljani počutili bližje EU, razglasila Listino Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina). Ta vsebuje najrazličnejše civilne, politične, ekonomske in socialne pravice evropskih državljanov, saj združuje ustavne tradicije in mednarodne obveznosti, ki so skupne državam članicam. Pravice, opisane v Listini, so razdeljene na šest poglavij: dostojanstvo, svoboščine, enakost, solidarnost, pravice državljanov in sodno varstvo.

Listina, ki je bila prvotno samo politični dokument, je postala pravno zavezujoča[27] kot primarna zakonodaja EU (glej člen 6(1) PEU) ob začetku veljavnosti Lizbonske pogodbe 1. decembra 2009.[28] Določbe Listine veljajo za institucije in organe EU, ki morajo pri izpolnjevanju svojih dolžnosti spoštovati v njih navedene pravice. Določbe Listine so zavezujoče tudi za države članice, ko izvajajo pravo EU.

Z Listino ni zagotovljeno le spoštovanje zasebnega in družinskega življenja (člen 7), ampak je določena tudi pravica do varstva osebnih podatkov (člen 8). Raven tega varstva je z njo izrecno povzdignjena na raven temeljne pravice v pravu EU. To pravico morajo zagotavljati in spoštovati institucije in organi EU, kar velja tudi za države

27 EU (2012), Listina Evropske unije o temeljnih pravicah (UL C 326, 26.10.2012, str. 391).

28 Glej prečiščeni različici Pogodbe o Evropski uniji (UL C 326, 26.10.2012, str. 13) in Pogodbe o delovanju Evropske unije (PDEU) (UL C 326, 26.10.2012, str. 47).

članice, ko izvajajo pravo Unije (člen 51 Listine). Člen 8 Listine, ki je bil izoblikovan več let po sprejetju direktive o varstvu osebnih podatkov, je treba razumeti kot izraz predhodno veljavne zakonodaje EU o varstvu osebnih podatkov. V Listini tako pravica do varstva osebnih podatkov ni samo izrecno navedena v členu 8(1), ampak je v členu 8(2) navedeno tudi sklicevanje na ključna načela varstva osebnih podatkov. Ne nazadnje mora v skladu s členom 8(3) Listine izvajanje teh načel nadzorovati neodvisen organ.

Sprejetje Lizbonske pogodbe je mejnik v razvoju prava o varstvu osebnih podatkov, ne le zato, ker je z njo Listina dobila status zavezujočega pravnega dokumenta na ravni primarne zakonodaje, temveč tudi, ker je v njej določena pravica do varstva osebnih podatkov. Ta pravica je izrecno določena v členu 16 PDEU, in sicer v delu Pogodbe, v katerem so opredeljena splošna načela EU. Člen 16 je tudi nova pravna podlaga, ki EU podeljuje pristojnost za sprejemanje zakonodaje o varstvu osebnih podatkov. To je pomemben korak, saj so pravila EU o varstvu osebnih podatkov, zlasti direktiva o varstvu osebnih podatkov, sprva temeljila na pravni podlagi notranjega trga in potrebi po približevanju nacionalnih zakonov, da ne bi bil oviran prosti pretok osebnih podatkov v EU. Člen 16 PDEU zdaj zagotavlja neodvisno pravno podlago za sodoben in celovit pristop k varstvu osebnih podatkov, ki zajema vse zadeve v pristojnosti EU, vključno s policijskim in pravosodnim sodelovanjem v kazenskih zadevah. Ta člen poleg tega določa, da morajo upoštevanje pravil o varstvu osebnih podatkov, ki so bila sprejeta na njegovi podlagi, nadzirati neodvisni nadzorni organi. Člen 16 PDEU je bil pravna podlaga za sprejetje celovite reforme pravil o varstvu osebnih podatkov leta 2016, tj. SUVP in direktive o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja (glej v nadaljevanju).

Splošna uredba o varstvu podatkov

Od leta 1995 do maja 2018 je bil glavni pravni instrument EU za varstvo podatkov Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (direktiva o varstvu osebnih podatkov).[29] Sprejeta je bila leta 1995, ko je več držav članic že sprejelo nacionalne zakone o varstvu osebnih podatkov,[30] nastala pa je iz potrebe po uskladitvi teh zakonov za zagotavljanje visoke ravni varstva in

29 Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

30 Nemška zvezna dežela Hessen je leta 1970 sprejela prvi zakon o varstvu osebnih podatkov, ki se je uporabljal le v tej deželi. Švedska je leta 1973 sprejela *Datalagen*, Nemčija je leta 1976 sprejela *Bundesdatenschutzgesetz*, Francija pa je leta 1977 sprejela *Loi relatif à l'informatique, aux fichiers et aux libertés*. V Združenem kraljestvu je bil leta 1984 sprejet *Data Protection Act*, Nizozemska pa je leta 1989 sprejela *Wet Persoonregistraties*.

prostega pretoka osebnih podatkov med državami članicami. Za prosti pretok blaga, kapitala, storitev in ljudi na notranjem trgu je bil potreben prosti prenos podatkov, ki je bil uresničljiv samo, če so se lahko države članice oprle na enotno visoko raven varstva osebnih podatkov.

V direktivi o varstvu osebnih podatkov so bila upoštevana načela varstva osebnih podatkov, ki so bila že vključena v nacionalne zakone in Konvencijo št. 108, pri čemer je bilo več teh načel v njej razširjenih. Navedena direktiva izhaja iz možnosti iz člena 11 Konvencije št. 108, da se instrumenti varstva nadgradijo. Zlasti uvedba neodvisnega nadzora v direktivo kot instrumenta za izboljšanje upoštevanja pravil o varstvu osebnih podatkov se je izkazala za pomemben prispevek k učinkovitemu delovanju evropskega prava o varstvu osebnih podatkov. Ta značilnost je bila zato leta 2001 z Dodatnim protokolom h Konvenciji št. 108 vključena v pravo Sveta Evrope. To ponazarja tesno medsebojno povezanost in pozitivno vplivanje teh dveh instrumentov skozi leta.

Z direktivo o varstvu osebnih podatkov je bil v EU vzpostavljen podroben in celovit sistem varstva osebnih podatkov. Ker pa se v skladu s pravnim sistemom EU direktive ne uporabljajo neposredno, jih je treba prenesti v nacionalno zakonodajo držav članic. Neizogibno je, da imajo države članice diskrecijsko pravico pri prenosu njihovih določb. Čeprav naj bi se z navedeno direktivo zagotovila popolna uskladitev[31] (in polna raven varstva), so bile v praksi njene določbe v nacionalno zakonodajo držav članic prenesene različno. To je privedlo do oblikovanja različnih pravil o varstvu osebnih podatkov v EU, saj so se v nacionalnih zakonodajah opredelitve in pravila razlagali različno. Tudi ravni izvrševanja in strogost sankcij so se po državah članicah razlikovale. Odkar je bila sredi devetdesetih let prejšnjega stoletja pripravljena zadevna direktiva, so se na področju informacijske tehnologije zgodile bistvene spremembe. Vsi ti razlogi so spodbudili reformo zakonodaje EU o varstvu osebnih podatkov.

Na podlagi reforme je bila aprila 2016 po letih burnih razprav sprejeta SUVP. Razprave o potrebi po posodobitvi pravil EU o varstvu osebnih podatkov so se začele leta 2009, ko je Komisija začela javno posvetovanje o prihodnjem pravnem okviru za temeljno pravico do varstva osebnih podatkov. Komisija je predlog uredbe objavila januarja 2012, s čimer se je začel dolgotrajen zakonodajni postopek pogajanj med Evropskim parlamentom in Svetom EU. Ko je bila SUVP sprejeta, je bilo v njej

31 SEU, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, združeni zadevi C-468/10 in C-469/10, 24. november 2011, točka 29.

določeno dveletno prehodno obdobje. V celoti se je začela uporabljati 25. maja 2018, ko je bila razveljavljena direktiva o varstvu osebnih podatkov.

S sprejetjem SUVP leta 2016 je bila zakonodaja EU o varstvu osebnih podatkov posodobljena, s čimer je postala primerna za varstvo temeljnih pravic v okviru gospodarskih in družbenih izzivov digitalne dobe. V SUVP so ohranjena in dodatno razvita temeljna načela in pravice posameznikov, na katere se nanašajo osebni podatki, iz direktive o varstvu osebnih podatkov. Poleg tega so bile s to uredbo uvedene nove obveznosti, v skladu s katerimi morajo organizacije izvajati vgrajeno in privzeto varstvo osebnih podatkov, v nekaterih okoliščinah imenovati pooblaščeno osebo za varstvo podatkov, spoštovati novo pravico do prenosljivosti osebnih podatkov in upoštevati načelo odgovornosti. V skladu s pravom EU se uredbe uporabljajo neposredno, zato jih ni treba prenesti v nacionalno zakonodajo. SUVP tako določa enoten sklop pravil o varstvu osebnih podatkov v EU. To ustvarja usklajena pravila o varstvu osebnih podatkov v EU in vzpostavlja okolje pravne varnosti, od katerega imajo lahko koristi gospodarski subjekti in posamezniki, in sicer kot posamezniki, na katere se nanašajo osebni podatki.

Čeprav se SUVP uporablja neposredno, se od držav članic pričakuje, da bodo posodobile veljavno nacionalno zakonodajo o varstvu osebnih podatkov, da bo v celoti usklajena z zadevno uredbo, pri čemer je v njeni uvodni izjavi 10 državam članicam podeljena tudi diskrecijska pravica za sprejetje podrobnih določb. Glavna pravila in načela, določena v tej uredbi, in široke pravice, ki jih ta zagotavlja posameznikom, sestavljajo velik del priročnika in so pojasnjeni v naslednjih poglavjih. Uredba vključuje celovita pravila o ozemeljski veljavnosti. Uporablja se za podjetja, ustanovljena v EU, pa tudi za upravljavce in obdelovalce, ki niso ustanovljeni v EU in ki v EU ponujajo blago ali storitve posameznikom, na katere se nanašajo osebni podatki, ali spremljajo njihovo vedenje. Ker ima več čezmorskih tehnoloških podjetij ključni delež na evropskem trgu in več milijonov strank v EU, je treba za zagotavljanje varstva posameznikov in enakih konkurenčnih pogojev poskrbeti, da se za te organizacije uporabljajo pravila EU o varstvu osebnih podatkov.

Varstvo osebnih podatkov na področju kazenskega pregona – Direktiva (EU) 2016/680

Razveljavljena direktiva o varstvu osebnih podatkov je zagotavljala celovito ureditev varstva osebnih podatkov. Ta ureditev se je dodatno okrepila s sprejetjem SUVP. Čeprav je bilo področje uporabe razveljavljene direktive o varstvu osebnih podatkov obsežno, je bilo omejeno na dejavnosti, ki spadajo na področje notranjega trga, in

dejavnosti javnih organov, ki niso organi kazenskega pregona. Zato je bilo potrebno sprejetje posebnih instrumentov, da bi dosegli potrebno jasnost in ravnovesje med varstvom osebnih podatkov in drugimi zakonitimi interesi ter se uspešno spoprijemali z izzivi, ki so v posameznih sektorjih še posebej pomembni. To velja za pravila, s katerimi je urejena obdelava osebnih podatkov, ki jo izvajajo organi kazenskega pregona.

Prvi pravni instrument EU, ki je urejal to področje, je bil Okvirni sklep Sveta 2008/977/PNZ o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah. Njegova pravila so se uporabljala samo za policijske in pravosodne podatke, ki so se izmenjevali med državami članicami. Iz njegovega področja uporabe je bila izključena nacionalna obdelava osebnih podatkov, ki jo izvajajo organi kazenskega pregona.

Ta položaj je bil izboljšan z Direktivo (EU) 2016/680 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov[32] (direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja). S to direktivo, ki je bila sprejeta vzporedno s SUVP, je bil razveljavljen Okvirni sklep Sveta 2008/977/PNZ in vzpostavljen celovit sistem varstva osebnih podatkov v okviru kazenskega pregona, pri čemer so v njej upoštevane tudi posebnosti obdelave osebnih podatkov, povezane z javno varnostjo. Medtem ko so v SUVP določena splošna pravila za varstvo posameznikov pri obdelavi njihovih osebnih podatkov in za zagotavljanje prostega pretoka takih podatkov v EU, pa so v navedeni direktivi določena posebna pravila za varstvo osebnih podatkov na področju pravosodnega sodelovanja v kazenskih zadevah in policijskega sodelovanja. Kadar pristojni organ obdeluje osebne podatke za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, se uporablja Direktiva (EU) 2016/680. Če pristojni organi obdelujejo osebne podatke za namene, ki niso navedeni zgoraj, se uporablja splošna ureditev v skladu s SUVP. V nasprotju s področjem uporabe svojega predhodnika (Okvirni sklep Sveta 2008/977/PNZ) področje uporabe Direktive (EU) 2016/680 zajema tudi obdelavo osebnih podatkov, ki jo izvajajo organi kazenskega pregona na nacionalni ravni, in ni omejeno na izmenjave takih podatkov med državami članicami. Poleg tega je cilj

32 Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

navedene direktive doseči ravnovesje med pravicami posameznikov in zakonitimi cilji obdelave, povezane z varnostjo.

V navedeni direktivi so zato navedeni pravica do varstva osebnih podatkov in temeljna načela, s katerimi bi morala biti zajeta obdelava osebnih podatkov, pri čemer se v njej dosledno upoštevajo pravila in načela iz SUVP. Pravice posameznikov in obveznosti, ki so naložene upravljavcem, na primer v zvezi z varnostjo osebnih podatkov, vgrajenim in privzetim varstvom osebnih podatkov ter kršitvami varnosti osebnih podatkov, so podobne pravicam in obveznostim iz SUVP. V navedeni direktivi so poleg tega upoštevani resni nastajajoči tehnološki izzivi, ki bi lahko imeli posebej obremenjujoč vpliv na posameznike, kot je uporaba tehnik oblikovanja profilov s strani organov kazenskega pregona, pri čemer se v njej ti izzivi poskušajo tudi obravnavati. Načeloma je treba prepovedati sprejemanje odločitev izključno na podlagi avtomatizirane obdelave, vključno z oblikovanjem profilov.[33] Ob tem odločitve ne smejo temeljiti na občutljivih podatkih. Za ta načela veljajo nekatere izjeme, določene v navedeni direktivi. Poleg tega taka obdelava ne sme povzročiti diskriminacije nobene osebe.[34]

Direktiva vsebuje tudi pravila za zagotavljanje odgovornosti upravljavcev. Ti morajo imenovati pooblaščeno osebo za varstvo podatkov, ki spremlja skladnost s pravili o varstvu osebnih podatkov, obvešča subjekt in zaposlene, ki izvajajo obdelavo, o njihovih obveznostih ter jim svetuje o njih in sodeluje z nadzornim organom. Obdelava osebnih podatkov v policijskem sektorju in sektorju kazenskega pravosodja je zdaj pod nadzorom neodvisnih nadzornih organov. Tako splošna pravna ureditev za varstvo osebnih podatkov kot posebna ureditev za varstvo osebnih podatkov na področju kazenskega pregona in kazenskih zadev morata izpolnjevati zahteve iz Listine EU o temeljnih pravicah.

Posebna ureditev za varstvo osebnih podatkov v okviru policijskega in pravosodnega sodelovanja, vzpostavljena z direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, je podrobno opisana v poglavju 8.

33 Direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, člen 11(1).

34 Prav tam, člen 11(2) in (3).

Direktiva o zasebnosti in elektronskih komunikacijah

Posebna pravila o varstvu osebnih podatkov se je zdelo potrebno opredeliti tudi za sektor elektronskih komunikacij. Zaradi razvoja interneta ter fiksne in mobilne telefonije je bilo treba zagotoviti, da se bodo spoštovale pravice uporabnikov do zasebnosti in zaupnosti. V Direktivi 2002/58/ES[35] o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) so določena pravila o varnosti osebnih podatkov v teh omrežjih, uradnem obveščanju o kršitvah varnosti osebnih podatkov in zaupnosti komunikacij.

V zvezi z varnostjo morajo ponudniki elektronskih komunikacijskih storitev med drugim zagotoviti, da je dostop do osebnih podatkov omejen izključno na pooblaščene osebe, in sprejeti ukrepe za preprečevanje uničenja, izgube ali nenamernega poškodovanja osebnih podatkov.[36] V primeru posebnega tveganja za kršitev varnosti javnega komunikacijskega omrežja morajo ponudniki o zadevnem tveganju obvestiti naročnike.[37] Če kljub varnostnim ukrepom, ki se izvajajo, pride do kršitve varnosti, morajo ponudniki o kršitvi varnosti osebnih podatkov uradno obvestiti pristojni nacionalni organ, ki je odgovoren za izvajanje in izvrševanje navedene direktive. Ponudniki morajo v nekaterih primerih o kršitvah varnosti osebnih podatkov uradno obvestiti tudi posameznike, in sicer če je verjetno, da bo kršitev škodljivo vplivala na njihove osebne podatke in zasebnost.[38] Zaupnost komunikacij pomeni, da je načeloma prepovedano poslušanje, prisluškovanje, shranjevanje ali kateri koli način nadzora ali prestrezanja komunikacij in metapodatkov. Direktiva prepoveduje tudi neželena sporočila, razen če uporabniki privolijo v njihovo prejemanje, ter vsebuje pravila o shranjevanju piškotkov na računalnikih in napravah. Te temeljne negativne obveznosti jasno kažejo, da je zaupnost komunikacij tesno povezana z varstvom pravice do spoštovanja zasebnega življenja iz člena 7 Listine in pravice do varstva osebnih podatkov iz člena 8 Listine.

Komisija je januarja 2017 objavila predlog uredbe o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij, s katero naj bi se nadomestila Direktiva o zasebnosti in elektronskih komunikacijah. Cilj reforme je uskladiti pravila, ki urejajo elektronske komunikacije, z novo ureditvijo varstva

35 Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

36 Direktiva o zasebnosti in elektronskih komunikacijah, člen 4(1).

37 Prav tam, člen 4(2).

38 Prav tam, člen 4(3).

osebnih podatkov, vzpostavljeno na podlagi SUVP. Nova uredba se bo neposredno uporabljala v vsej EU; vsi posamezniki bodo uživali enako raven varstva svojih elektronskih komunikacij, telekomunikacijski operaterji in podjetja pa bodo imeli koristi od jasnosti, pravne varnosti in enotnega sklopa pravil v vsej EU. Predlagana pravila o zaupnosti elektronskih komunikacij se bodo uporabljala tudi za nove ponudnike elektronskih komunikacijskih storitev, ki niso zajeti z Direktivo o zasebnosti in elektronskih komunikacijah. Ta je zajemala le ponudnike tradicionalnih telekomunikacijskih storitev. Storitve OTT, kot so Skype, WhatsApp, Facebook Messenger in Viber, za pošiljanje sporočil ali klicanje, ki se množično uporabljajo, bodo spadale na področje uporabe nove uredbe ter bodo morale izpolnjevati njene zahteve glede varstva osebnih podatkov, zasebnosti in varnosti. V času objave tega priročnika je zakonodajni postopek o pravilih o zasebnosti in elektronskih komunikacijah še vedno potekal.

Uredba (ES) št. 45/2001

Ker se je direktiva o varstvu osebnih podatkov lahko uporabljala le za države članice EU, je bil potreben dodaten pravni instrument, s katerim bi se varstvo pri obdelavi osebnih podatkov uvedlo tudi v institucijah in organih EU. To nalogo izpolnjuje Uredba (ES) št. 45/2001 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (uredba o varstvu osebnih podatkov v institucijah EU).[39]

V Uredbi (ES) št. 45/2001 so dosledno upoštevana načela splošne ureditve EU o varstvu osebnih podatkov in z njo se ta načela uporabljajo tudi za obdelavo osebnih podatkov, ki jo izvajajo institucije in organi EU pri opravljanju svojih nalog. Z njo je bil poleg tega vzpostavljen neodvisen nadzorni organ za spremljanje uporabe njenih določb, in sicer Evropski nadzornik za varstvo podatkov (ENVP). Dolžnost ENVP, ki ima nadzorna pooblastila, je spremljati obdelavo osebnih podatkov v institucijah in organih EU ter obravnavati in preiskovati pritožbe zaradi domnevnih kršitev pravil o varstvu osebnih podatkov. ENVP poleg tega svetuje institucijam in organom EU o vseh zadevah v zvezi z varstvom osebnih podatkov, ki segajo od predlogov za novo zakonodajo do oblikovanja notranjih predpisov v zvezi z obdelavo osebnih podatkov.

39 Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

Evropska komisija je januarja 2017 predstavila predlog nove uredbe o obdelavi osebnih podatkov v institucijah EU, s katero bo razveljavljena sedanja uredba. Kot pri reformi Direktive o zasebnosti in elektronskih komunikacijah bodo v okviru reforme Uredbe (ES) št. 45/2001 posodobljena njena pravila, ki bodo usklajena z novo ureditvijo varstva osebnih podatkov, vzpostavljeno na podlagi SUVP.

Vloga SEU

SEU je pristojno za ugotavljanje, ali država članica izpolnjuje svoje obveznosti v skladu s pravom EU o varstvu osebnih podatkov, in razlago zakonodaje EU, da bi zagotovilo njeno učinkovito in enotno uporabo v vseh državah članicah. Odkar je bila leta 1995 sprejeta direktiva o varstvu osebnih podatkov, se je izoblikovala obsežna sodna praksa, ki pojasnjuje področje uporabe in pomen načel varstva osebnih podatkov ter temeljne pravice do varstva osebnih podatkov iz člena 8 Listine. Čeprav je bila zadevna direktiva razveljavljena in je zdaj v veljavi nov pravni instrument, tj. SUVP, je obstoječa sodna praksa še vedno ustrezna in veljavna za razlago in uporabo načel EU o varstvu osebnih podatkov, saj so v SUVP ohranjena temeljna načela direktive o varstvu osebnih podatkov in njeni pojmi.

1.2 Omejitve pravice do varstva osebnih podatkov

Ključni poudarki

- Pravica do varstva osebnih podatkov ni absolutna; mogoče jo je omejiti, če je to potrebno zaradi cilja splošnega interesa ali zaščite pravic in svoboščin drugih.
- Pogoji za omejitev pravic do spoštovanja zasebnega življenja in varstva osebnih podatkov so navedeni v členu 8 EKČP in členu 52(1) Listine. Oblikovani so bili na podlagi sodne prakse ESČP in SEU ter se v skladu z njo tudi razlagajo.
- V skladu s pravom Sveta Evrope o varstvu osebnih podatkov obdelava osebnih podatkov pomeni zakonito poseganje v pravico do spoštovanja zasebnega življenja in se lahko izvaja le, če:
  - je določena z zakonom,
  - uresničuje zakonit cilj,
  - spoštuje bistvo temeljnih pravic in svoboščin ter

  - je v demokratični družbi nujna in sorazmerna za dosego zakonitega cilja.
- V pravnem redu EU se uporabljajo podobni pogoji za omejevanje uresničevanja temeljnih pravic, ki so zaščitene z Listino. Omejevanje temeljnih pravic, vključno s pravico do varstva osebnih podatkov, je lahko zakonito le, če:
  - je določeno z zakonom,
  - spoštuje bistveno vsebino zadevne pravice,
  - je ob upoštevanju načela sorazmernosti potrebno in
  - uresničuje cilj splošnega interesa, ki ga priznava EU, ali je potrebno zaradi zaščite pravic drugih.

Temeljna pravica do varstva osebnih podatkov iz člena 8 Listine ni absolutna, „temveč jo je treba obravnavati glede na vlogo, ki jo ima v družbi".[40] V členu 52(1) Listine je tako določeno, da se uresničevanje pravic, kot sta pravici iz členov 7 in 8 Listine, lahko omeji, če so te omejitve predpisane z zakonom, če spoštujejo bistvo teh pravic in svoboščin ter če so – ob upoštevanju načela sorazmernosti – potrebne in dejansko ustrezajo ciljem splošnega interesa, ki jih priznava EU, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.[41] Podobno je v sistemu EKČP varstvo osebnih podatkov zagotovljeno s členom 8, uresničevanje te pravice pa je mogoče omejiti, če je to potrebno za doseganje zakonitega cilja. V tem razdelku so obravnavani pogoji za poseganje v skladu z EKČP, kot se razlagajo v sodni praksi ESČP, in pogoji za zakonite omejitve v skladu s členom 52 Listine.

1.2.1 Zahteve za upravičeno poseganje na podlagi EKČP

Obdelava osebnih podatkov lahko pomeni poseganje v pravico posameznika, na katerega se nanašajo osebni podatki, do spoštovanja zasebnega življenja, ki je zaščitena s členom 8 EKČP.[42] Kot je pojasnjeno zgoraj (glej razdelek 1.1.1 in razdelek 1.1.4), v nasprotju s pravnim redom EU varstvo osebnih podatkov v EKČP ni potrjeno kot posebna temeljna pravica. Namesto tega je varstvo osebnih podatkov del pravic, varovanih v okviru pravice do spoštovanja zasebnega življenja. Zato na področje

40 Glej na primer SEU, *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen* (veliki senat), združeni zadevi C-92/09 in C-93/09, 9. november 2010, točka 48.

41 Prav tam, točka 50.

42 ESČP, združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 8. december 2008, točka 67.

uporabe člena 8 EKČP ne more spadati vsako dejanje, ki vključuje obdelavo osebnih podatkov. Da bi se uporabil člen 8 EKČP, je treba najprej ugotoviti, ali je bil ogrožen zasebni interes ali zasebno življenje osebe. ESČP v svoji sodni praksi pojem zasebno življenje obravnava široko, tako da zajema tudi vidike poklicnega življenja in vedenja v javnosti. Razsodilo je tudi, da je varstvo osebnih podatkov pomemben del pravice do spoštovanja zasebnega življenja. Kljub širokí razlagi pojma zasebno življenje pa vse vrste obdelave same po sebi ne bi ogrozile pravic, zaščitenih na podlagi člena 8 EKČP.

Če ESČP meni, da zadevno dejanje obdelave vpliva na pravico posameznikov do spoštovanja zasebnega življenja, bo proučilo, ali je poseg upravičen. Pravica do spoštovanja zasebnega življenja ni absolutna pravica, temveč jo je treba uravnotežiti in uskladiti z drugimi zakonitimi interesi in pravicami, bodisi drugih oseb (zasebni interesi) bodisi družbe kot celote (javni interesi).

V nadaljevanju so navedeni kumulativni pogoji, pod katerimi bi lahko poseganje bilo upravičeno.

Določenost z zakonom

V skladu s sodno prakso ESČP je poseganje določeno z zakonom, če temelji na določbi nacionalnega zakona, ki ima določene značilnosti. Zakon mora biti dostopen zadevnim osebam in imeti predvidljive učinke.[43] Predpis je predvidljiv, če je opredeljen dovolj natančno, da lahko vsak posameznik (če je treba, ob ustreznem nasvetu) usmerja svoje ravnanje.[44] Poleg tega je stopnja natančnosti, ki se v zvezi s tem zahteva za posamezen zakon, odvisna od zadevne vsebine.[45]

43 ESČP, *Amann proti Švici* (veliki senat), pritožba št. 27798/95, 16. februar 2000, točka 50; glej tudi ESČP, *Kopp proti Švici*, pritožba št. 23224/94, 25. marec 1998, točka 55, in ESČP, *Iordachi in drugi proti Moldaviji*, pritožba št. 25198/02, 10. februar 2009, točka 50.

44 ESČP, *Amann proti Švici* (veliki senat), pritožba št. 27798/95, 16. februar 2000, točka 56; glej tudi ESČP, *Malone proti Združenemu kraljestvu*, pritožba št. 8691/79, 2. avgust 1984, točka 66, in ESČP, združene zadeve *Silver in drugi proti Združenemu kraljestvu*, pritožbe št. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 in 7113/75, 25. marec 1983, točka 88.

45 ESČP, *The Sunday Times proti Združenemu kraljestvu*, pritožba št. 6538/74, 26. april 1979, točka 49; glej tudi ESČP, združene zadeve *Silver in drugi proti Združenemu kraljestvu*, pritožbe št. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 in 7113/75, 25. marec 1983, točka 88.

Primeri: v zadevi *Rotaru proti Romuniji*[46] je pritožnik trdil, da je bila kršena njegova pravica do spoštovanja zasebnega življenja, saj je romunska obveščevalna služba vodila in uporabljala dosje z njegovimi osebnimi podatki. ESČP je ugotovilo, da v nacionalnem zakonu, ki je sicer omogočal zbiranje in evidentiranje informacij, ki vplivajo na nacionalno varnost, ter njihovo arhiviranje v tajnih dosjejih, niso bile določene omejitve za izvajanje teh pooblastil, ki je bilo prepuščeno presoji organov. V nacionalnem zakonu na primer niso bili opredeljeni vrsta informacij, ki se lahko obdelujejo, kategorije ljudi, proti katerim je dovoljeno sprejeti nadzorne ukrepe, okoliščine, v katerih je mogoče take ukrepe sprejeti, ali postopki, ki jih je treba upoštevati. Sodišče je zato ugotovilo, da nacionalni zakon ni izpolnjeval zahteve glede predvidljivosti na podlagi člena 8 EKČP in da je bil ta člen kršen.

V zadevi *Taylor-Sabori proti Združenemu kraljestvu*[47] je bil pritožnik tarča policijskega nadzora. Policija je uporabila klon pritožnikovega pozivnika in tako prestrezala sporočila, ki so mu bila poslana. Pritožnik je bil nato aretiran in obdolžen zarote pri dobavi nadzorovane droge. Dokazi tožilstva zoper njega so deloma temeljili na zapisih sporočil pozivnika, ki jih je policija sproti prepisovala. Vendar britanska zakonodaja v času sojenja pritožniku ni vsebovala določb, s katerimi bi bilo urejeno prestrezanje sporočil, poslanih prek zasebnih telekomunikacijskih sistemov. Poseganje v njegove pravice torej ni bilo določeno z zakonom. ESČP je ugotovilo, da je bil kršen člen 8 EKČP.

Zadeva *Vukota-Bojić proti Švici*[48] se je nanašala na tajni nadzor, ki so ga nad vlagateljico zahtevka za denarno nadomestilo iz naslova socialnega zavarovanja izvajali zasebni detektivi, ki jih je najela njena zavarovalnica. ESČP je menilo, da je nadzorni ukrep, ki je predmet pritožbe, sicer odredila zasebna zavarovalnica, da pa je navedeno družbo država pooblastila, da zagotavlja pravice iz obveznega zdravstvenega zavarovanja in pobira zavarovalne premije. Država se svojih dolžnosti po konvenciji ne more razbremeniti tako, da jih prenese na zasebnopravne subjekte ali fizične osebe. V nacionalnem pravu je treba zagotoviti zadostne zaščitne ukrepe pred zlorabami, da bi bilo poseganje v pravice iz člena 8 EKČP „določeno z zakonom“. ESČP je v obravnavani

46 ESČP, *Rotaru proti Romuniji* (veliki senat), pritožba št. 28341/95, 4. maj 2000, točka 57; glej tudi ESČP, *Association for European Integration and Human Rights in Ekimdzhiev proti Bolgariji*, pritožba št. 62540/00, 28. junij 2007; ESČP, *Shimovolos proti Rusiji*, pritožba št. 30194/09, 21. junij 2011, in ESČP, *Vetter proti Franciji*, pritožba št. 59842/00, 31. maj 2005.

47 ESČP, *Taylor-Sabori proti Združenemu kraljestvu*, pritožba št. 47114/99, 22. oktober 2002.

48 ESČP, *Vukota-Bojić proti Švici*, pritožba št. 61838/10, 18. oktober 2016, točka 77.

zadevi ugotovilo, da je bil kršen člen 8 EKČP, saj v nacionalnem pravu nista bila dovolj jasno opredeljena obseg in način izvajanja diskrecijske pravice, podeljene zavarovalnicam, ki delujejo kot javni organi v zavarovalnih sporih, da izvajajo tajni nadzor nad zavarovanimi osebami. Nacionalno pravo zlasti ni vključevalo zadostnih zaščitnih ukrepov pred zlorabami.

Uresničevanje zakonitega cilja

Zakoniti cilj je lahko eden od navedenih javnih interesov ali varstvo pravic in svoboščin drugih. V skladu s členom 8(2) EKČP so zakoniti cilji, s katerimi je mogoče upravičiti poseganje, interesi državne varnosti, javne varnosti ali ekonomske blaginje države, preprečevanje nereda ali kaznivega dejanja, zavarovanje zdravja ali morale ter varstvo pravic in svoboščin drugih ljudi.

Primer: v zadevi *Peck proti Združenemu kraljestvu*[49] je pritožnik na ulici poskušal storiti samomor z rezanjem žil na zapestjih, pri čemer se ni zavedal, da ga snema videonadzorna kamera. Policija, ki je spremljala nadzorne kamere, ga je rešila in videoposnetek pozneje posredovala medijem, ki so ga objavili, ne da bi zakrili pritožnikov obraz. ESČP je ugotovilo, da ni bilo ustreznih ali zadostnih upravičenih razlogov za neposredno razkritje posnetka javnosti, ne da bi organi pridobili pritožnikovo privolitev ali prikrili njegovo identiteto. Ugotovilo je, da je bil kršen člen 8 EKČP.

Nujnost v demokratični družbi

Stališče ESČP je, da pojem nujnosti pomeni, da poseganje temelji na pomembni družbeni potrebi in zlasti da je sorazmerno z uresničevanjem zakonitega cilja.[50] ESČP pri presoji, ali je ukrep potreben za obravnavo pomembne družbene potrebe, prouči njegovo ustreznost in primernost glede na zastavljeni cilj. V ta namen lahko upošteva, ali se s posegom poskuša obravnavati vprašanje, ki bi lahko, če ne bi bilo obravnavano, škodljivo vplivalo na družbo, ali so na voljo dokazi, da bi se s posegom tak škodljiv učinek lahko ublažil, in katera so širša družbena stališča o zadevnem vprašanju.[51] Če bi varnostne službe zbirale in hranile osebne podatke o določenih posa-

49 ESČP, *Peck proti Združenemu kraljestvu*, pritožba št. 44647/98, 28. januar 2003, točka 85.

50 ESČP, *Leander proti Švedski*, pritožba št. 9248/81, 26. marec 1987, točka 58.

51 Delovna skupina za varstvo podatkov iz člena 29 (2014), *Mnenje št. 1/2014 o uporabi konceptov nujnosti in sorazmernosti ter varstva podatkov v sektorju kazenskega pregona*, WP 211, Bruselj, 27. februar 2014, str. 7 in 8.

meznikih, za katere je bilo ugotovljeno, da so povezani s terorističnimi gibanji, bi to bil poseg v pravico teh posameznikov do spoštovanja zasebnega življenja, ki pa bi temeljil na resni in pomembni družbeni potrebi, in sicer nacionalni varnosti in boju proti terorizmu. Da bi poseg veljal za nujnega, mora biti tudi sorazmeren. V sodni praksi ESČP se sorazmernost obravnava v okviru pojma nujnosti. V skladu z načelom sorazmernosti poseg v pravice, zaščitene v skladu z EKČP, ne sme presegati tistega, kar je potrebno za izpolnitev zakonitega cilja. Pomembni dejavniki, ki jih je treba upoštevati pri preizkusu sorazmernosti, so obseg posega, zlasti število prizadetih oseb, in zaščitni ukrepi ali opozorila, ki so vzpostavljena za omejitev obsega posega ali njegovega škodljivega učinka na pravice posameznikov.[52]

Primer: v zadevi *Khelili proti Švici*[53] je policija med kontrolo ugotovila, da ima pritožnica pri sebi vizitke, na katerih je pisalo: „Prijetna, čedna ženska v poznih tridesetih bi rada spoznala moškega, s katerim bi šla na pijačo ali se z njim občasno družila. Tel. št. […]“. Pritožnica je trdila, da jo je policija po tem odkritju vnesla v svojo evidenco kot prostitutko, čeprav je ta poklic vztrajno zanikala. Zahtevala je, naj se beseda „prostitutka“ izbriše iz policijske računalniške evidence. ESČP je načeloma potrdilo, da je lahko hramba osebnih podatkov posameznika z utemeljitvijo, da bi lahko ta oseba storila še eno kaznivo dejanje, v določenih okoliščinah sorazmerna. Vendar se je trditev o nezakoniti prostituciji v pritožničini zadevi zdela preveč nejasna in splošna ter ni bila podprta s konkretnimi dokazi, saj še nikoli ni bila obsojena zaradi nezakonite prostitucije, zato ni bilo mogoče šteti, da izhaja iz pomembne družbene potrebe v smislu člena 8 EKČP. Ker bi morali organi dokazati točnost podatkov, shranjenih o pritožnici, in ker je šlo za resno poseganje v pravico pritožnice, je Sodišče razsodilo, da večletna hramba besede „prostitutka“ v policijskih spisih ni nujna v demokratični družbi. Ugotovilo je, da je bil kršen člen 8 EKČP.

Primer: v združenih zadevah *S. in Marper proti Združenemu kraljestvu*[54] sta bila pritožnika aretirana in obdolžena kaznivih dejanj. Policija jima je odvzela prstne odtise in vzorce DNK, kot je bilo določeno v zakonu o policiji in dokazih v kazenskih postopkih (Police and Criminal Evidence Act). Pritožnika nista bila nikoli spoznana za kriva: eden je bil oproščen na sodišču, kazenski postopek

52 Prav tam, str. 9–11.

53 ESČP, *Khelili proti Švici*, pritožba št. 16188/07, 18. oktober 2011.

54 ESČP, združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 4. december 2008.

zoper drugega pa je bil ustavljen. Policija je kljub temu v podatkovni zbirki imela in hranila njune prstne odtise, profil DNK in celične vzorce, pri čemer je bila časovno neomejena hramba dovoljena z nacionalno zakonodajo. Čeprav je Združeno kraljestvo trdilo, da hramba prispeva k identifikaciji prihodnjih storilcev kaznivih dejanj ter s tem uresničuje zakoniti cilj preprečevanja in odkrivanja kaznivih dejanj, je ESČP menilo, da je poseganje v pravico pritožnikov do spoštovanja zasebnega življenja neupravičeno. Opozorilo je, da mora biti v skladu s temeljnimi načeli varstva osebnih podatkov hramba osebnih podatkov sorazmerna glede na namen zbiranja in da mora biti obdobje hrambe omejeno. Sodišče je pritrdilo, da lahko razširitev podatkovne zbirke, ki poleg profilov DNK obsojenih oseb vključuje tudi zadevne profile vseh posameznikov, ki so bili osumljeni, ne pa spoznani za krive, prispeva k odkrivanju in preprečevanju kaznivih dejanj v Združenem kraljestvu. Vendar je bilo osuplo nad vsesplošno in neselektivno naravo pristojnosti za hrambo.[55]

Glede na obsežno količino genskih in zdravstvenih informacij, ki jih vsebujejo celični vzorci, je bil poseg v pravico pritožnikov do zasebnega življenja še posebej moteč. Prijetim osebam je bilo mogoče odvzeti prstne odtise in vzorce ter jih za nedoločen čas hraniti v policijski podatkovni zbirki, in sicer ne glede na vrsto in težo kaznivega dejanja ter celo za manjše kršitve, ki se ne kaznujejo z zaporno kaznijo. Poleg tega so bile možnosti oproščenih posameznikov, da se njihovi osebni podatki odstranijo iz podatkovne zbirke, omejene. Nazadnje je ESČP posebno pozornost namenilo dejstvu, da je bil eden od pritožnikov ob prijetju star enajst let. Hramba osebnih podatkov mladoletnika, ki ni bil obsojen, je lahko še posebej škodljiva zaradi njegove ranljivosti ter pomena njegovega razvoja in vključevanja v družbo.[56] Sodišče je soglasno odločilo, da takšna hramba pomeni nesorazmeren poseg v pravico do zasebnega življenja, ki ga v demokratični družbi ni mogoče šteti za nujnega.

Primer: ESČP je v zadevi *Leander proti Švedski*[57] razsodilo, da tajni nadzor nad kandidati za delovna mesta, ki so pomembna za državno varnost, sam po sebi ni v nasprotju z zahtevo po nujnosti v demokratični družbi. Glede na posebne zaščitne ukrepe, ki so v nacionalni zakonodaji določeni za zaščito interesov posameznika, na katerega se nanašajo osebni podatki – na primer nadzor, ki

55 Prav tam, točka 119.

56 Prav tam, točka 124.

57 ESČP, *Leander proti Švedski*, pritožba št. 9248/81, 26. marec 1987, točki 59 in 67.

ga izvajata parlament in varuh človekovih pravic –, je ugotovilo, da švedski sistem nadzora nad zaposlenimi izpolnjuje zahteve iz člena 8(2) EKČP. Tožena država je glede na široko polje proste presoje, ki ga ima na voljo, upravičeno menila, da v pritožnikovem primeru interesi nacionalne varnosti prevladajo nad interesi posameznika. Sodišče je ugotovilo, da člen 8 EKČP ni bil kršen.

1.2.2 Pogoji za zakonito omejevanje na podlagi Listine EU o temeljnih pravicah

Listina se po zgradbi in besedilu razlikuje od EKČP. V Listini ni sklicevanja na posega-nje v zagotovljene pravice, temveč vsebuje določbo o omejitvah izvajanja pravic in svoboščin, priznanih z Listino.

V skladu s členom 52(1) so omejitve izvajanja pravic in svoboščin, priznanih z Listino, torej tudi izvajanja pravice do varstva osebnih podatkov, dopustne samo, če:

- so predpisane z zakonom;
- spoštujejo bistveno vsebino pravice do varstva osebnih podatkov;
- so ob upoštevanju načela sorazmernosti potrebne[58] ter
- ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali so potrebne zaradi zaščite pravic in svoboščin drugih.

Ker je varstvo osebnih podatkov v pravnem redu EU ločena in samostojna temeljna pravica, zaščitena v skladu s členom 8 Listine, vsaka obdelava osebnih podatkov že sama po sebi pomeni poseg v to pravico. Ni pomembno, ali so zadevni osebni po-datki povezani z zasebnim življenjem posameznika, ali so občutljivi oziroma ali so imeli posamezniki, na katere se nanašajo, zato kakršne koli nevšečnosti. Da bi bil poseg zakonit, mora izpolnjevati vse pogoje iz člena 52(1) Listine.

58 V zvezi s presojo potrebnosti ukrepov, s katerimi se omeji temeljna pravica do varstva osebnih podatkov, glej ENVP (2017), Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, Bruselj, 11. april 2017.

Določenost z zakonom

Omejitve pravice do varstva osebnih podatkov morajo biti predpisane z zakonom. Ta zahteva pomeni, da morajo omejitve temeljiti na pravni podlagi, ki je ustrezno dostopna in predvidljiva ter opredeljena dovolj natančno, da lahko posamezniki razumejo svoje obveznosti in prilagodijo svoje ravnanje. V pravni podlagi je treba poleg tega jasno opredeliti obseg in način izvajanja tega pooblastila, danega pristojnim organom, da se posameznikom zagotovi ustrezno varstvo pred samovoljnim poseganjem. Ta razlaga je podobna zahtevi po zakonitem poseganju iz sodne prakse ESČP,[59] pri čemer je bilo predlagano, da je treba izrazu „predpisano z zakonom", uporabljenemu v Listini, podeliti podoben obseg, kot ga ima ta izraz v okviru EKČP.[60] Sodna praksa ESČP in zlasti pojem kakovost zakona, ki ga je z leti razvilo to sodišče, je pomemben dejavnik, ki ga mora SEU upoštevati pri razlagi področja uporabe člena 52(1) Listine.[61]

Spoštovanje bistvene vsebine pravice

V pravnem redu EU morajo vse omejitve temeljnih pravic, zaščitenih z Listino, spoštovati bistveno vsebino teh pravic. To pomeni, da omejitve, ki so tako obsežne in moteče, da z njimi temeljna pravica ostane brez svoje osnovne vsebine, ne morejo biti upravičene. Če je ogroženo bistvo pravice, je treba omejitev šteti za nezakonito, pri čemer ni treba nadalje presojati, ali se z njo uresničuje cilj v splošnem interesu ter ali izpolnjuje merili potrebnosti in sorazmernosti.

Primer: zadeva *Schrems*[62] se je nanašala na varstvo posameznikov pri prenosu njihovih osebnih podatkov v tretje države, v tem primeru Združene države Amerike. M. Schrems, avstrijski državljan, ki je več let uporabljal družbeno omrežje Facebook, je pri irskem nadzornem organu za varstvo podatkov vložil pritožbo, v kateri je nasprotoval prenosu svojih osebnih podatkov od Facebookove irske hčerinske družbe družbi Facebook Inc. in na

59 ENVP (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Bruselj, 11. april 2017, str. 4; glej tudi SEU, *Mnenje Sodišča 1/15 (veliki senat)* z dne 26. julija 2017.

60 SEU, *Tele2 Sverige AB proti Post- och telestyrelsen* in *Secretary of State for the Home Department proti Tomu Watsonu in drugim*, združeni zadevi C-203/15 in C-698/15, sklepni predlogi generalnega pravobranilca Henrika Saugmandsgaarda Øeja z dne 19. julija 2016, točka 140.

61 SEU, *Scarlet Extended SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, sklepni predlogi generalnega pravobranilca Pedra Cruza Villalóna z dne 14. aprila 2011, točka 100.

62 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015.

njene strežnike v ZDA, na katerih se obdelujejo. Trdil je, da glede na razkritja ameriškega žvižgača Edwarda Snowdna iz leta 2013 v zvezi z dejavnostmi nadzora, ki jih izvajajo obveščevalne službe ZDA, pravo in praksa te države ne zagotavljata zadostne zaščite osebnih podatkov, ki se prenašajo na ozemlje ZDA. Snowden je razkril, da Agencija za nacionalno varnost neposredno vdira v strežnike družb, kot je Facebook, ter da lahko bere vsebino klepetov in zasebnih sporočil.

Prenos podatkov v ZDA je temeljil na odločbi Komisije o primernosti zaščite, ki je bila sprejeta leta 2000, s katero je bil dovoljen prenos podatkov družbam iz ZDA, ki so samocertificirale, da bodo varovale osebne podatke, prenesene iz EU, in ravnale v skladu s tako imenovanimi načeli varnega pristana. Ko je bila zadeva predložena SEU, je to proučilo veljavnost odločbe Komisije glede na Listino. Opozorilo je, da varstvo temeljnih pravic v EU zahteva, da se odstopanja od teh pravic in njihove omejitve določijo v mejah tega, kar je nujno potrebno. SEU je menilo, da ureditev, ki javnim organom omogoča splošen dostop do vsebine elektronskih komunikacij, „pomeni poseg v bistvo temeljne pravice do spoštovanja zasebnega življenja, zagotovljene v členu 7 Listine“. Zadevni pravici bi bilo odvzeto bistvo, če bi lahko javni organi ZDA naključno dostopali do komunikacij brez kakršne koli objektivne utemeljitve iz konkretnih razlogov državne varnosti ali preprečevanja kriminalitete, ne da bi bili v zvezi s temi dejavnostmi nadzora določeni ustrezni in preverljivi zaščitni ukrepi pred zlorabo pooblastil.

Poleg tega je SEU ugotovilo, da „ureditev, ki ne določa nobene možnosti, da bi posameznik lahko uporabil pravna sredstva za pridobitev dostopa do osebnih podatkov, ki se nanj nanašajo, ali dosegel popravo ali izbris takih podatkov“, ni skladna s temeljno pravico do učinkovitega sodnega varstva (člen 47 Listine). Odločba o varnem pristanu zato ni zagotavljala, da je raven varstva temeljnih pravic v ZDA v bistvenem enaka ravni, ki je zagotovljena v EU na podlagi Direktive 95/46 v povezavi z Listino. SEU je posledično zadevno odločbo razveljavilo.[63]

63 Odločitev SEU, da razveljavi Odločbo Komisije 520/2000/ES, je temeljila tudi na drugih razlogih, ki bodo obravnavani v drugih razdelkih tega priročnika. Menilo je zlasti, da so z odločbo nezakonito omejena pooblastila nacionalnih nadzornih organov za varstvo podatkov. Poleg tega v okviru sistema varnega pristana niso bila na voljo pravna sredstva za posameznike, ki bi želeli dostopati do osebnih podatkov, ki se nanje nanašajo, in/ali doseči njihov popravek ali izbris. Zato je to pomenilo tudi poseg v bistvo temeljne pravice do učinkovitega sodnega varstva iz člena 47 Listine.

Primer: SEU je v zadevi *Digital Rights Ireland*[64] proučilo skladnost Direktive 2006/24/ES (direktiva o hrambi podatkov) s členoma 7 in 8 Listine. V skladu z navedeno direktivo so morali ponudniki elektronskih komunikacijskih storitev podatke o prometu in lokaciji hraniti najmanj šest mesecev in največ 24 mesecev ter pristojnim nacionalnim organom omogočiti dostop do teh podatkov za namene preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj. Direktiva ni omogočala hrambe vsebine elektronskih komunikacij. SEU je ugotovilo, da so podatki, ki so jih morali ponudniki hraniti v skladu z direktivo, vključevali podatke, potrebne za sledenje in določitev vira in cilja komunikacije, datum, čas in trajanje komunikacije, kličočo telefonsko številko, klicane telefonske številke in IPnaslove. Na podlagi vseh teh podatkov „je mogoče izpeljati zelo natančne ugotovitve o zasebnem življenju oseb, katerih podatki so bili shranjeni, kot so vsakodnevne navade, kraji stalnega ali začasnega prebivališča, dnevne ali druge poti, dejavnosti, socialni odnosi in socialna okolja, ki jih obiskujejo".

Zato je hramba osebnih podatkov v skladu z direktivo pomenila posebej resno poseganje v pravici do zasebnosti in varstva osebnih podatkov. Vendar je SEU menilo, da poseg ni posegal v bistveno vsebino teh pravic. Kar zadeva pravico do zasebnosti, njena bistvena vsebina ni bila ogrožena, saj direktiva ni omogočala seznanjanja s samo vsebino elektronskih komunikacij kot tako. Poleg tega ni bila ogrožena niti bistvena vsebina pravice do varstva osebnih podatkov, saj so morali ponudniki elektronskih storitev v skladu z zadevno direktivo spoštovati nekatera načela varstva osebnih podatkov in varnosti osebnih podatkov ter v ta namen izvajati ustrezne tehnične in organizacijske ukrepe.

Potrebnost in sorazmernost

Člen 52(1) Listine določa, da so ob upoštevanju načela sorazmernosti omejitve uresničevanja temeljnih pravic in svoboščin, ki jih priznava Listina, dovoljene samo, če so potrebne.

Omejitev je lahko **potrebna**, če je treba sprejeti ukrepe za cilj javnega interesa, ki se uresničuje, vendar potrebnost, kot jo razlaga SEU, pomeni tudi, da morajo biti sprejeti ukrepi manj moteči v primerjavi z drugimi možnostmi za doseganje istega cilja. SEU

64 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim in Kärntner Landesregierung in drugi (veliki senat)*, združeni zadevi C-293/12 in C-594/12, 8. april 2014.

v zvezi z omejitvami pravic do spoštovanja zasebnega življenja in varstva osebnih podatkov uporablja strog preizkus potrebnosti, pri čemer meni, da je treba odstopanja in omejitve uporabljati le, če je to nujno potrebno. Če se šteje, da je omejitev nujno potrebna, je treba oceniti tudi, ali je sorazmerna.

Sorazmernost pomeni, da bi morale prednosti, ki izhajajo iz omejitve, prevladati nad pomanjkljivostmi, ki jih omejitev povzroči v zvezi z uveljavljanjem zadevnih temeljnih pravic.[65] Da bi zmanjšali pomanjkljivosti in tveganja v zvezi z uživanjem pravic do zasebnosti in varstva osebnih podatkov, je pomembno, da omejitve vključujejo ustrezne zaščitne ukrepe.

Primer: SEU je v združenih zadevah *Volker und Markus Schecke*[66] ugotovilo, da sta Svet in Komisija z določitvijo obveznosti objave osebnih podatkov vseh fizičnih oseb, ki so upravičene do sredstev iz določenih kmetijskih skladov, ne da bi se pri tem opravilo razlikovanje glede na ustrezna merila, kot so obdobja, v katerih so navedene osebe prejemale tako pomoč, pogostost ali vrsta in višina take pomoči, presegla meje, ki jih določa načelo sorazmernosti.

SEU je zato menilo, da je treba za neveljavne razglasiti nekatere določbe Uredbe Sveta (ES) št. 1290/2005, Uredbo (ES) št. 259/2008 pa v celoti.[67]

Primer: SEU je v zadevi *Digital Rights Ireland*[68] menilo, da poseg v pravico do zasebnosti, ki je bil povzročen z direktivo o hrambi podatkov, ni ogrozil bistvene vsebine te pravice, saj je bila z njo prepovedana hramba vsebine elektronskih komunikacij. Vendar je ugotovilo, da je zadevna direktiva nezdružljiva s členoma 7 in 8 Listine, zato jo je razglasilo za neveljavno. Če bi se združili vsi podatki o prometu in lokaciji, bi jih bilo mogoče analizirati in iz njih izpeljati natančne ugotovitve o zasebnem življenju oseb, zato je to pomenilo resen poseg v navedeno pravico. SEU je upoštevalo, da je bilo

65 ENVP (2017), *Nabor orodij za presojo potrebnosti*, str. 5.

66 SEU, *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen* (veliki senat), združeni zadevi C-92/09 in C-93/09, 9. november 2010, točki 89 in 86.

67 Uredba Sveta (ES) št. 1290/2005 z dne 21. junija 2005 o financiranju skupne kmetijske politike (UL L 209, 11.8.2005, str. 1); Uredba Komisije (ES) št. 259/2008 z dne 18. marca 2008 o podrobnih pravilih za uporabo Uredbe Sveta (ES) št. 1290/2005 glede objavljanja informacij o upravičencih do sredstev iz Evropskega kmetijskega jamstvenega sklada (EKJS) in Evropskega kmetijskega sklada za razvoj podeželja (EKSRP) (UL L 76, 19.3.2008, str. 28).

68 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim in Kärntner Landesregierung in drugi* (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014, točka 39.

treba v skladu z zadevno direktivo hraniti vse metapodatke v zvezi s fiksno telefonijo, mobilno telefonijo, dostopom do interneta, internetno elektronsko pošto in internetno telefonijo, pri čemer se je ta direktiva nanašala na vsa sredstva elektronske komunikacije, katerih uporaba je v vsakdanjem življenju ljudi zelo razširjena. Pomenila je poseg, ki je v praksi vplival na celotno evropsko prebivalstvo. Glede na obseg in resnost tega posega bi lahko bila hramba podatkov o prometu in lokaciji po mnenju SEU upravičena le za namene boja proti hudim kaznivim dejanjem. Poleg tega v tej direktivi niso bila določena objektivna merila, ki bi zagotavljala, da je dostop pristojnih nacionalnih organov do hranjenih podatkov omejen na to, kar je nujno potrebno. Direktiva ni vsebovala niti vsebinskih niti postopkovnih pogojev, s katerimi bi bila urejena dostop nacionalnih organov do hranjenih podatkov in njihova uporaba, ki nista bila odvisna od predhodnega nadzora, ki bi ga opravilo sodišče ali drug neodvisen organ.

SEU je do podobnega zaključka prišlo v združenih zadevah *Tele2 Sverige AB proti Post- och telestyrelsen* in *Secretary of State for the Home Department proti Tomu Watsonu in drugim*.[69] Ti sta se nanašali na hrambo podatkov o prometu in lokaciji vseh naročnikov in registriranih uporabnikov v zvezi z vsemi elektronskimi sredstvi ter vseh metapodatkov, in sicer brez „razlikovanja, omejitve ali izjeme glede na cilj, ki se ga poskuša doseči".[70] V obravnavani zadevi hramba podatkov o osebi ni bila pogojena s tem, da je oseba bodisi neposredno ali posredno povezana s hudimi kaznivimi dejanji bodisi da so njene komunikacije pomembne za nacionalno varnost. Ker ni bilo zahtevane povezave med hranjenimi podatki in grožnjo za javno varnost oziroma ker ni bilo omejitev v zvezi z obdobjem ali geografskim območjem, je SEU ugotovilo, da nacionalna zakonodaja presega meje tistega, kar je nujno potrebno za boj proti hudim kaznivim dejanjem.[71]

Podoben pristop v zvezi s potrebnostjo je uporabil Evropski nadzornik za varstvo podatkov v dokumentu o naboru orodij za presojo potrebnosti.[72] Cilj tega nabora orodij je olajšati presojo skladnosti predlaganih ukrepov s pravom EU o varstvu osebnih

69 SEU, *Tele2 Sverige AB proti Post- och telestyrelsen* in *Secretary of State for the Home Department proti Tomu Watsonu in drugim* (veliki senat), združeni zadevi C-203/15 in C-698/15, 21. december 2016, točki 105 in 106.

70 Prav tam, točka 105.

71 Prav tam, točka 107.

72 ENVP (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Bruselj, 11. april 2017.

podatkov. Oblikovan je bil, da bi se zagotovila boljša usposobljenost oblikovalcev politik in zakonodajalcev EU, odgovornih za pripravo ali skrben pregled ukrepov, ki vključujejo obdelavo osebnih podatkov ter omejujejo pravico do varstva osebnih podatkov ter druge pravice in svoboščine, določene v Listini.

Cilji splošnega interesa

Da bi bila omejitev uresničevanja pravic, priznanih z Listino, upravičena, mora dejansko ustrezati ciljem splošnega interesa, ki jih priznava Unija, ali biti potrebna zaradi zaščite pravic in svoboščin drugih. Kar zadeva potrebo po varstvu pravic in svoboščin drugih, je pravica do varstva osebnih podatkov pogosto povezana z drugimi temeljnimi pravicami. V razdelku 1.3 je na voljo podrobna analiza takih povezav. Kar zadeva cilje splošnega interesa, ti vključujejo splošne cilje EU iz člena 3 Pogodbe o Evropski uniji (PEU), kot so krepitev miru in blaginje njenih narodov, spodbujanje socialne pravičnosti in varstva ter vzpostavitev območja svobode, varnosti in pravice, na katerem je v povezavi z ustreznimi ukrepi glede preprečevanja kriminala in boja proti njemu zagotovljeno prosto gibanje oseb, ter druge cilje in interese, ki so zaščiteni s posebnimi določbami Pogodb.[73] V zvezi s tem je v SUVP natančneje določen člen 52(1) Listine: v členu 23(1) zadevne uredbe je navedena vrsta ciljev splošnega interesa, ki se pri omejevanju pravic posameznikov štejejo za zakonite, če omejitev spoštuje bistvo pravice do varstva osebnih podatkov ter je potrebna in sorazmerna. Med cilji javnega interesa, ki so navedeni v tem členu, so državna varnost in obramba, preprečevanje kaznivih dejanj, zaščita pomembnih gospodarskih in finančnih interesov EU ali držav članic ter javno zdravje in socialna varnost.

Cilj splošnega interesa, ki se uresničuje z omejitvijo, je treba opredeliti in pojasniti dovolj podrobno, saj se bo potrebnost omejitve presojala ob upoštevanju navedenega. Nujen je jasen in podroben opis cilja omejitve in predlaganih ukrepov, da se lahko presodi, ali je omejitev potrebna.[74] Med ciljem, ki se uresničuje, ter potrebnostjo in sorazmernostjo omejitve je tesna povezava.

Primer: zadeva *Schwarz proti Stadt Bochum*[75] se je nanašala na omejitve pravice do spoštovanja zasebnega življenja in pravice do varstva osebnih podatkov, ki izhajajo iz odvzema prstnih odtisov in njihovega shranjevanja pri

73 Pojasnila k Listini o temeljnih pravicah (UL C 303, 14.12.2007, str. 17–35).

74 ENVP (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Bruselj, 11. april 2017, str. 4.

75 SEU, *Michael Schwarz proti Stadt Bochum*, C-291/12, 17. oktober 2013.

izdaji potnih listov s strani držav članic.[76] Tožeča stranka je pri Stadt Bochum (mesto Bochum) zaprosila za izdajo potnega lista, pri čemer je odklonila odvzem prstnih odtisov, zato je Stadt Bochum njeno prošnjo za izdajo potnega lista zavrnilo. Tožeča stranka je nato pri nemškem sodišču vložila tožbo, da bi se ji potni list izdal brez odvzema prstnih odtisov. Nemško sodišče je zadevo predložilo SEU, in sicer je spraševalo, ali je treba člen 1(2) Uredbe (ES) št. 2252/2004 o standardih za varnostne značilnosti in biometrične podatke v potnih listih in potovalnih dokumentih, ki jih izdajo države članice, šteti za veljaven.

SEU je poudarilo, da so prstni odtisi **osebni podatki**, saj objektivno vsebujejo edinstvene informacije o fizičnih osebah in omogočajo njihovo natančno identifikacijo, odvzem prstnih odtisov in njihovo shranjevanje pa pomenita obdelavo. Navedena obdelava, ki je določena v členu 1(2) Uredbe (ES) št. 2252/2004, pomeni kršitev pravic do spoštovanja zasebnega življenja in varstva osebnih podatkov.[77] Vendar člen 52(1) Listine dopušča omejitve pri uresničevanju teh pravic, če so te omejitve predpisane z zakonom, če spoštujejo bistveno vsebino teh pravic, če so ob upoštevanju načela sorazmernosti potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali so potrebne zaradi zaščite pravic in svoboščin drugih.

SEU je v obravnavani zadevi najprej ugotovilo, da je treba omejitev, ki izhaja iz odvzema prstnih odtisov in njihovega shranjevanja pri izdaji potnih listov, šteti za **predpisano z zakonom**, saj sta ti dejanji določeni s členom 1(2) Uredbe (ES) št. 2252/2004. Drugič, cilj navedene uredbe je preprečiti ponarejanje potnih listov in njihovo zlorabo. Zato je bil vzpostavljen člen 1(2), katerega cilj je med drugim preprečevati nezakonit vstop oseb na ozemlje Unije, kar pomeni, da se s tem členom uresničuje cilj splošnega interesa, ki ga priznava Unija. Tretjič, iz dokazov, ki so bili na voljo SEU, ni bilo razvidno – poleg tega ni bilo niti zatrjevano –, da omejitve pri uresničevanju zadevnih pravic v obravnavani zadevi ne bi spoštovale bistvene vsebine teh pravic. Četrtič, za shranjevanje prstnih odtisov na zelo varnem pomnilniškem mediju, določenem z navedeno določbo, je potrebna vrhunska tehnologija. Tako shranjevanje lahko zmanjša tveganje ponarejanja potnih listov in olajša delo organov, ki so zadolženi za preverjanje verodostojnosti potnih listov na mejah EU. Dejstvo, da zadevni način preverjanja ni povsem zanesljiv, ni odločilno. Čeprav ta način

76 Prav tam, točke 33–36.

77 Prav tam, točke 27–30.

ne izključuje povsem sprejetja nepooblaščenih oseb, zadostuje, da znatno znižuje tveganje za tako sprejetje. Glede na navedeno je SEU ugotovilo, da se lahko z odvzemom prstnih odtisov in njihovim shranjevanjem, določenima v členu 1(2) Uredbe (ES) št. 2252/2004, dosežejo cilji, ki jim sledi zadevna uredba, in s tem tudi cilj preprečevanja nezakonitega vstopa na ozemlje EU.[78]

SEU je nato proučilo **potrebnost** take obdelave, pri čemer je ugotovilo, da odvzem sestoji le iz odvzema odtisa dveh prstov, ki sta poleg tega običajno izpostavljena pogledu drugih, tako da ne gre za intimno dejanje. To dejanje ravno tako zadevni osebi ne povzroča posebnega fizičnega ali psihičnega nelagodja, tako kot slikanje obraza. Poleg tega je treba poudariti, da je bilo v postopku pred SEU kot edina dejanska alternativa odvzemu prstnih odtisov navedeno slikanje očesne šarenice. Vendar nikjer v spisu, predloženem zadevnemu sodišču, ni bilo navedeno, da bi ta postopek manj posegal v pravici, priznani s členoma 7 in 8 Listine, kot odvzem prstnih odtisov. Glede učinkovitosti teh dveh načinov tudi ni sporno, da stopnja tehnološke dovršenosti načina, ki temelji na prepoznavanju očesne šarenice, ne dosega stopnje tehnološke dovršenosti načina, ki temelji na prstnih odtisih, poleg tega je prepoznavanje očesne šarenice trenutno občutno dražji postopek od postopka primerjanja prstnih odtisov in je zato manj primeren za splošno uporabo. Posledično SEU ni bilo seznanjeno z obstojem ukrepov, ki bi lahko dovolj učinkovito prispevali k cilju zaščite potnih listov pred zlorabo in ki bi obenem pomenili manjši poseg v pravici, priznani s členoma 7 in 8 Listine, kot je poseg, povzročen z načinom, ki temelji na prstnih odtisih.[79]

SEU je navedlo, da člen 4(3) Uredbe (ES) št. 2252/2004 izrecno določa, da se lahko prstni odtisi uporabijo samo za preverjanje verodostojnosti potnega lista in identitete njegovega imetnika, medtem ko člen 1(2) navedene uredbe določa shranjevanje prstnih odtisov le v potnem listu, ki ostaja v izključni posesti imetnika tega potnega lista. Uredba zato ne zagotavlja pravne podlage za centralizirano shranjevanje podatkov, zbranih na njeni osnovi, ali za uporabo teh podatkov v druge namene kot za preprečevanje nezakonitega vstopa oseb na ozemlje EU.[80] Glede na vse zgornje ugotovitve je SEU ugotovilo, da preizkus predloženega vprašanja ni pokazal ničesar, kar bi vplivalo na veljavnost člena 1(2) Uredbe (ES) št. 2252/2004.

78 Prav tam, točke 35–45.

79 Prav tam, točke 46–53.

80 Prav tam, točke 56–61.

Razmerje med Listino in EKČP

Člen 52(1) Listine o pogojih za zakonite omejitve pravic kljub drugačnemu besedilu spominja na člen 8(2) EKČP o pravici do spoštovanja zasebnega življenja. SEU in ESČP se v svoji sodni praksi pogosto sklicujeta na sodbe drug drugega v okviru stalnega medsebojnega dialoga, s katerim si prizadevata za usklajeno razlago pravil o varstvu osebnih podatkov. Člen 52(3) Listine se glasi: „Kolikor ta listina vsebuje pravice, ki ustrezajo pravicam, zagotovljenim z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin, sta vsebina in obseg teh pravic enaka kot vsebina in obseg pravic, ki ju določa navedena konvencija." Vendar člen 8 Listine ne ustreza neposredno nobenemu od členov EKČP.[81] Člen 52(3) Listine se nanaša na vsebino in obseg pravic, zaščitenih z vsakim od zadevnih dveh pravnih redov, ne pa na pogoje za njihovo omejitev. Vendar pa lahko SEU glede na širši okvir dialoga in sodelovanja z ESČP v svojih analizah upošteva merila za zakonito omejitev v skladu s členom 8 EKČP, kot jih razlaga ESČP. Možno je tudi obratno, in sicer da se ESČP sklicuje na pogoje za zakonito omejitev v skladu z Listino. Vsekakor bi bilo treba upoštevati tudi, da v EKČP ni popolnega ustreznika členu 8 Listine, ki bi zadeval varstvo osebnih podatkov ter zlasti pravice posameznika, na katerega se nanašajo osebni podatki, zakonite razloge za obdelavo in nadzor, ki ga izvaja neodvisni organ. Nekateri elementi člena 8 Listine temeljijo na sodni praksi ESČP, ki je bila oblikovana na podlagi člena 8 EKČP in se nanaša na Konvencijo št. 108.[82] S to povezavo je zagotovljeno, da se lahko SEU in ESČP v zadevah v zvezi z varstvom osebnih podatkov opirata na sodno prakso drug drugega.

1.3 Povezava z drugimi pravicami in zakonitimi interesi

Ključni poudarki

- Pravica do varstva osebnih podatkov je pogosto povezana z drugimi pravicami, kot sta svoboda izražanja ter pravica do prejemanja in prenašanja informacij.
- Ta povezava je pogosto ambivalentna: medtem ko je v nekaterih primerih pravica do varstva osebnih podatkov v nasprotju s posamezno drugo pravico, je lahko v drugih primerih z njo dejansko zagotovljeno spoštovanje iste posamezne pravice. To na primer velja za svobodo izražanja, saj je poklicna skrivnost del pravice do spoštovanja zasebnega življenja.

81 ENVP (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Bruselj, 11. april 2017, str. 6.

82 Pojasnila k Listini o temeljnih pravicah (UL C 303, 14.12.2007, str. 17), člen 8.

- Eno od meril, ki se uporabljajo za presojo zakonitosti omejitve pravice do varstva osebnih podatkov, je potreba po varstvu pravic in svoboščin drugih.
- Če so ogrožene različne pravice, jih morajo sodišča uravnotežiti, da bi jih lahko uskladila.
- Države članice morajo v skladu s SUVP pravico do varstva osebnih podatkov usklajevati s svobodo izražanja in obveščanja.
- Države članice lahko poleg tega v nacionalnem pravu sprejmejo posebna pravila za uskladitev pravice do varstva osebnih podatkov z dostopom javnosti do uradnih dokumentov in obveznostmi varovanja poklicne skrivnosti.

Pravica do varstva osebnih podatkov ni absolutna pravica; pogoji za zakonito omejitev te pravice so podrobneje opisani zgoraj. Eno od meril za zakonite omejitve pravic, priznanih s pravom Sveta Evrope in pravom EU, je, da je poseg v varstvo osebnih podatkov potreben za varstvo pravic in svoboščin drugih. Kadar je varstvo osebnih podatkov povezano z drugimi pravicami, sta ESČP in SEU že večkrat navedla, da je pri uporabi in razlagi člena 8 EKČP in člena 8 Listine nujno uravnoteženje z drugimi pravicami.[83] Kako to ravnotežje doseči, bo ponazorjeno z več pomembnimi primeri.

Poleg uravnoteženja, ki ga izvedeta ti sodišči, lahko države članice po potrebi sprejmejo zakonodajo, s katero pravico do varstva osebnih podatkov uskladijo z drugimi pravicami. Zato je v SUVP določenih več področij nacionalnega odstopanja.

Kar zadeva svobodo izražanja, morajo države članice v skladu s SUVP z zakonom usklajevati „pravico do varstva osebnih podatkov na podlagi te uredbe s pravico do svobode izražanja in obveščanja, vključno z obdelavo v novinarske namene ali zaradi akademskega, umetniškega ali književnega izražanja“.[84] Države članice lahko sprejmejo tudi zakone za uskladitev varstva osebnih podatkov z dostopom javnosti do uradnih dokumentov in obveznostmi varovanja poklicne skrivnosti, ki je zaščitena kot oblika pravice do spoštovanja zasebnega življenja.[85]

83 ESČP, združeni zadevi *Von Hannover proti Nemčiji (št. 2)* (veliki senat), pritožbi št. 40660/08 in 60641/08, 7. februar 2012; SEU, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, združeni zadevi C-468/10 in C-469/10, 24. november 2011, točka 48, in SEU, *Productores de Música de España (Promusicae) proti Telefónica de España SAU* (veliki senat), C-275/06, 29. januar 2008, točka 68.

84 SUVP, člen 85.

85 Prav tam, člena 86 in 90.

1.3.1 Svoboda izražanja

Ena od pravic, ki je tesno povezana s pravico do varstva osebnih podatkov, je pravica do svobodnega izražanja.

Svoboda izražanja je varovana s členom 11 Listine (Svoboda izražanja in obveščanja). Ta pravica vključuje „svobodo mnenja ter sprejemanja in širjenja vesti ali idej brez vmešavanja javnih organov in ne glede na državne meje". Svoboda obveščanja v skladu s členom 11 Listine in členom 10 EKČP varuje ne le pravico do širjenja vesti, temveč tudi pravico do njihovega *sprejemanja*.

Omejitve svobode izražanja morajo biti v skladu z zgoraj opisanimi merili iz člena 52(1) Listine. Poleg tega člen 11 ustreza členu 10 EKČP. V skladu s členom 52(3) Listine sta, če ta vsebuje pravice, ki ustrezajo pravicam, zagotovljenim z EKČP, „vsebina in obseg teh pravic enaka kot vsebina in obseg pravic, ki ju določa navedena konvencija". Omejitve, ki jih je mogoče zakonito določiti v zvezi s pravico, zagotovljeno s členom 11 Listine, zato ne smejo presegati omejitev iz člena 10(2) EKČP, kar pomeni, da morajo biti določene z zakonom in nujne v demokratični družbi „za varovanje ugleda ali pravic drugih ljudi". Take pravice zajemajo zlasti pravico do spoštovanja zasebnega življenja in pravico do varstva osebnih podatkov.

Razmerje med varstvom osebnih podatkov in svobodo izražanja je urejeno s členom 85 SUVP z naslovom Obdelava ter svoboda izražanja in obveščanja. Ta člen določa, da države članice usklajujejo pravico do varstva osebnih podatkov s pravico do svobode izražanja in obveščanja. Izjeme in odstopanja od posebnih poglavij SUVP se določijo zlasti v novinarske namene ali zaradi akademskega, umetniškega ali književnega izražanja, če so potrebni za uskladitev pravice do varstva osebnih podatkov s svobodo izražanja in obveščanja.

Primer: SEU je bilo v zadevi *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy in Satamedia Oy*[86] zaprošeno, naj opredeli razmerje med varstvom osebnih podatkov in svobodo tiska.[87] Obravnavati je moralo razširjanje davčnih podatkov o približno 1,2 milijona fizičnih oseb, zakonito

86 SEU, *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy in Satamedia Oy* (veliki senat), C-73/07, 16. december 2008, točke 56, 61 in 62.

87 Zadeva se je nanašala na razlago člena 9 direktive o varstvu osebnih podatkov – zdaj nadomeščenega s členom 85 SUVP –, ki se je glasil: „Države članice določijo izjeme ali odstopanja od določb tega poglavja, poglavja IV in poglavja VI za obdelavo osebnih podatkov, ki se izvaja zgolj v novinarske namene ali zaradi umetniškega ali literarnega izražanja samo, če so potrebna za uskladitev pravice do zasebnosti s predpisi, ki urejajo svobodo izražanja."

pridobljenih od finskih davčnih organov, ki ga je prek sporočil SMS izvajala neka družba. Finski nadzorni organ za varstvo podatkov je izdal odločbo, s katero je od zadevne družbe zahteval, naj preneha razširjati te podatke. Družba je to odločbo izpodbijala pri nacionalnem sodišču, ki je SEU zaprosilo za pojasnitev glede razlage direktive o varstvu osebnih podatkov. SEU je moralo zlasti preveriti, ali je treba obdelavo osebnih podatkov, ki so jih davčni organi dali na voljo, da bi uporabnikom mobilnih telefonov omogočili prejemanje davčnih podatkov o drugih posameznikih, šteti za dejavnost, ki se opravlja zgolj v novinarske namene. Po tem, ko je ugotovilo, da se dejavnosti zadevne družbe štejejo za „obdelavo osebnih podatkov" v smislu člena 3(1) direktive o varstvu osebnih podatkov, je analiziralo člen 9 navedene direktive (o obdelavi osebnih podatkov in svobodi izražanja). Najprej je opozorilo na pomen pravice do svobodnega izražanja v vsaki demokratični družbi in razsodilo, da je treba pojme v zvezi z navedeno pravico, na primer pojem novinarstva, razlagati široko. Nato je ugotovilo, da je treba izjeme in omejitve pravice do varstva osebnih podatkov – za uravnoteženje obeh temeljnih pravic – uporabljati samo, če je to najnujneje potrebno. SEU je v teh okoliščinah ugotovilo, da je mogoče dejavnosti, ki sta jih zadevni družbi izvajali v zvezi s podatki iz dokumentov, ki so v skladu z nacionalno zakonodajo javni, opredeliti kot „dejavnosti novinarstva", če je njihov cilj razkritje informacij, mnenj ali idej javnosti, ne glede na sredstvo, ki se uporablja za njihov prenos. Odločilo je tudi, da te dejavnosti niso pridržane medijem in se lahko opravljajo s pridobitnim namenom. Vendar je nacionalnemu sodišču prepustilo, naj ugotovi, ali to drži glede na dejstva v obravnavani zadevi.

Isto zadevo je obravnavalo tudi ESČP po tem, ko je nacionalno sodišče na podlagi smernic SEU odločilo, da je odločba nadzornega organa, s katero je ta zahteval prenehanje objave vseh davčnih podatkov, upravičen poseg v svobodo izražanja družbe. ESČP je ta pristop potrdilo.[88] Ugotovilo je, da čeprav je prišlo do poseganja v pravico zadevnih družb do širjenja vesti, je bilo to v skladu z zakonom, je uresničevalo zakonit cilj in bilo nujno v demokratični družbi.

Sodišče je opozorilo na merila sodne prakse, ki bi morala nacionalne organe in ESČP usmerjati pri uravnoteževanju svobode izražanja s pravico do spoštovanja zasebnega življenja. Če gre za politični govor ali razpravo o zadevi

88 ESČP, *Satakunnan Markkinapörssi Oy in Satamedia Oy proti Finski* (veliki senat), pritožba št. 931/13, 27. junij 2017.

v javnem interesu, je malo možnosti za omejitev pravice do sprejemanja in širjenja vesti, saj ima javnost pravico, da je obveščena, in je to bistvena pravica v demokratični družbi.[89] Vendar v zvezi s časopisnimi članki, katerih edini cilj je potešiti radovednost določenega kroga bralcev glede podrobnosti o zasebnem življenju posameznika, ni mogoče šteti, da prispevajo k razpravi v javnem interesu. Cilj odstopanja od pravil o varstvu osebnih podatkov v novinarske namene je novinarjem omogočiti, da dostopajo do osebnih podatkov, jih zbirajo in obdelujejo, da lahko opravljajo novinarske dejavnosti. Zato je bilo v javnem interesu, da se družbama pritožnicama zagotovi dostop do velikih količin zadevnih davčnih podatkov ter da se jima omogoči njihovo zbiranje in obdelava. Sodišče je nasprotno ugotovilo, da ni bilo javnega interesa za masovno razširjanje takih neobdelanih podatkov v časopisih v nespremenjeni obliki in brez analitičnega prispevka. Davčni podatki so radovednim članom javnosti morda omogočili, da so posameznike razvrščali glede na njihov ekonomski položaj in potešili žejo javnosti po informacijah o zasebnem življenju drugih. Tega ni mogoče šteti za prispevek k razpravi v javnem interesu.

Primer: SEU je v zadevi *Google Spain*[90] obravnavalo, ali bi morala družba Google zastarele informacije o finančnih težavah pritožnika izbrisati s seznama zadetkov iskanja. Kadar je bilo v iskalniku Google opravljeno iskanje z vnosom pritožnikovega imena, so bile med rezultati iskanja povezave na stare časopisne članke, v katerih je bila omenjena pritožnikova povezava s stečajnim postopkom. Pritožnik je menil, da je to kršitev njegovih pravic do spoštovanja zasebnega življenja in varstva osebnih podatkov, saj je bil postopek končan pred več leti, zato je njegovo omenjanje brezpredmetno.

SEU je najprej pojasnilo, da je mogoče z internetnimi iskalniki in rezultati iskanja sestaviti podroben profil posameznika. Glede na vse bolj digitalizirano družbo je zahteva po točnosti osebnih podatkov in tem, da njihova objava ne presega tega, kar je potrebno, tj. zagotavljanja informacij javnosti, bistvenega pomena za zagotavljanje visoke ravni varstva osebnih podatkov za posameznike. „[U]pravljavec tega iskalnika, ki je odgovoren za to obdelavo, [mora] v okviru svoje odgovornosti, pristojnosti in zmožnosti zagotoviti, da ta obdelava izpolnjuje zahteve“ prava EU, da imajo lahko vzpostavljena

89 Prav tam, točka 169.

90 SEU, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), C-131/12, 13. maj 2014, točke 81–83.

pravna jamstva polni učinek. To pomeni, da pravica do izbrisa osebnih podatkov, ko obdelava ni več potrebna ali so ti podatki zastareli, zajema tudi iskalnike, za katere je bilo ugotovljeno, da so upravljavci, ne le obdelovalci (glej razdelek 2.3.1).

V zvezi s tem, ali bi morala družba Google odstraniti povezave, ki se nanašajo na pritožnika, je SEU menilo, da imajo posamezniki pod določenimi pogoji pravico, da zahtevajo izbris osebnih podatkov iz zadetkov iskanja na internetnem iskalniku. Ta pravica se lahko uveljavlja, kadar so podatki v zvezi s posameznikom netočni, neprimerni, neustrezni ali pretirani glede na namene obdelave osebnih podatkov. SEU je navedlo, da ta pravica ni absolutna, temveč da jo je treba uravnotežiti z drugimi pravicami, zlasti interesom in pravico širše javnosti, da ima dostop do zadevnih informacij. V zvezi z vsakim zahtevkom za izbris je treba opraviti presojo za vsak primer posebej, da se doseže ravnotežje med temeljnima pravicama do varstva osebnih podatkov in spoštovanja zasebnega življenja posameznika, na katerega se nanašajo osebni podatki, na eni strani ter zakonitimi interesi vseh internetnih uporabnikov na drugi strani. SEU je zagotovilo smernice o dejavnikih, ki jih je treba upoštevati pri izvedbi uravnoteženja. Zlasti pomemben dejavnik je narava zadevnih informacij. Če so informacije občutljive z vidika zasebnega življenja posameznika in če ni javnega interesa za njihovo razpoložljivost, bi pravici do varstva osebnih podatkov in zasebnosti prevladali nad pravico širše javnosti do dostopa do informacij. Če se nasprotno zdi, da je posameznik, na katerega se nanašajo osebni podatki, javna osebnost ali da je narava zadevnih informacij taka, da upravičuje odobritev dostopa širše javnosti do takih informacij, je poseg v temeljni pravici do varstva osebnih podatkov in zasebnosti upravičen.

Delovna skupina iz člena 29 je na podlagi te sodbe SEU sprejela smernice o njenem izvajanju. Te smernice vključujejo seznam skupnih meril, ki jih morajo nadzorni organi uporabljati pri obravnavi pritožb v zvezi z zahtevki posameznikov za izbris, v njih pa so na voljo tudi napotki za nadzorne organe glede tega uravnoteženja pravic.[91]

91 Delovna skupina za varstvo podatkov iz člena 29, *Guidelines on the implementation of the CJEU judgment on „Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12* (Smernice za izvajanje sodbe SEU v zadevi Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu, C-131/12), WP 225, Bruselj, 2014.

ESČP je v zvezi z uskladitvijo pravice do varstva osebnih podatkov s pravico do svobodnega izražanja izdalo več prelomnih sodb.

Primer: ESČP je v zadevi *Axel Springer AG proti Nemčiji*[92] menilo, da sodna odredba, s katero je bila tožeči družbi prepovedana objava članka o aretaciji in obsodbi znanega igralca, pomeni kršitev člena 10 EKČP. Opozorilo je na merila, ki so določena v njegovi sodni praksi in jih je treba upoštevati pri uravnoteženju pravice do svobodnega izražanja s pravico do spoštovanja zasebnega življenja:

- ali je bil dogodek, na katerega se je objavljeni članek nanašal, v splošnem interesu;
- ali je bila zadevna oseba javna osebnost;
- kako so bile informacije pridobljene in ali so bile zanesljive.

ESČP je ugotovilo, da sta bila prijetje igralca in njegova obsodba sodno ugotovljeni javni dejstvi, zato sta bila v javnem interesu, da je bil igralec dovolj znan, da ga je bilo mogoče šteti za javno osebnost, ter da je informacije zagotovilo državno tožilstvo, zato stranki nista oporekali njihovi točnosti. Prepovedi objave, naložene družbi, zato niso bile razumno sorazmerne z zakonitim ciljem varstva pritožnikovega zasebnega življenja. Sodišče je ugotovilo, da je bil kršen člen 10 EKČP.

Primer: zadeva *Couderc in Hachette Filipacchi Associés proti Franciji*[93] se je nanašala na objavo intervjuja z go. Costa v francoskem tedniku, v katerem je trdila, da je monaški princ Albert oče njenega sina. V intervjuju sta bila opisana tudi razmerje ge. Costa s princem in njegov odziv na rojstvo otroka, objavljene so bile tudi fotografije princa z otrokom. Princ Albert je zoper založniško družbo sprožil postopek zaradi kršitve njegove pravice do varstva zasebnega življenja. Francoska sodišča so menila, da je bila z objavo članka princu Albertu povzročena nepopravljiva škoda, ter odločila, da mora založniška družba plačati odškodnino in na naslovnici revije objaviti podrobnosti o sodbi.

92 ESČP, *Axel Springer AG proti Nemčiji* (veliki senat), pritožba št. 39954/08, 7. februar 2012, točki 90 in 91.

93 ESČP, *Couderc in Hachette Filipacchi Associés proti Franciji* (veliki senat), pritožba št. 40454/07, 10. november 2015.

Založniki revije so vložili pritožbo pri ESČP, v kateri so trdili, da sodba francoskih sodišč pomeni neupravičen poseg v njihovo pravico do svobode izražanja. ESČP je moralo pravico princa Alberta do spoštovanja zasebnega življenja uravnotežiti s pravico založnikov do svobodnega izražanja in pravico širše javnosti do obveščenosti. Pomembna dejavnika sta bila tudi pravica ge. Costa, da svojo zgodbo deli z javnostjo, in interes otroka, da se uradno ugotovi razmerje oče-otrok.

ESČP je menilo, da je objava intervjuja pomenila poseg v zasebno življenje princa, in je nato proučilo, ali je bil ta poseg potreben. Menilo je, da se je objava nanašala na javno osebnost in zadevo v javnem interesu, saj je bilo v interesu državljanov Monaka, da so seznanjeni z obstojem prinčevega otroka, saj je prihodnost nasledstvene monarhije „neločljivo povezana z obstojem potomstva" in je zato stvar javnega interesa.[94] Sodišče je poleg tega ugotovilo, da je članek ge. Costa in njenemu otroku omogočil uveljavljanje njune pravice do svobodnega izražanja. Nacionalna sodišča niso ustrezno upoštevala načel in meril, ki so se oblikovala s sodno prakso ESČP, v zvezi z uravnoteženjem pravice do spoštovanja zasebnega življenja in pravice do svobodnega izražanja. Ugotovilo je, da je Francija kršila člen 10 EKČP o svobodi izražanja.

V sodni praksi ESČP je eno od ključnih meril v zvezi z uravnoteženjem teh pravic prav to, ali zadevno izražanje pripomore k razpravi, ki je v splošnem javnem interesu.

Primer: v zadevi *Mosley proti Združenemu kraljestvu*[95] je nacionalni tednik objavil intimne fotografije pritožnika, znane osebnosti, ki je pozneje uspešno vložil civilno tožbo zoper založnika in prejel odškodnino. Čeprav mu je bila dodeljena denarna odškodnina, se je pritožil, da ostaja žrtev kršitve pravice do zasebnosti, ker pred objavo zadevnih fotografij ni imel možnosti zahtevati sodne odredbe, saj ne obstajajo pravne zahteve, v skladu s katerimi bi ga časopis moral predhodno obvestiti o objavi.

ESČP je opozorilo, da čeprav se je tako gradivo na splošno razširjalo za razvedritev in ne toliko za izobraževanje, je bilo nedvomno varovano s členom 10 EKČP, nad katerim pa bi lahko prevladale zahteve iz člena 8 EKČP, če

94 Prav tam, točke 104–116.

95 ESČP, *Mosley proti Združenemu kraljestvu*, pritožba št. 48009/08, 10. maj 2011, točki 129 in 130.

so bile informacije zasebne in intimne ter ni bilo javnega interesa za njihovo razširjanje. Vendar je bilo treba še posebej skrbno proučiti omejitve, ki bi lahko delovale kot oblika cenzure pred objavo. ESČP je zaradi odvračilnega učinka, ki bi ga lahko povzročila zahteva po predhodnem obveščanju, dvomov o njegovi učinkovitosti in širokega polja proste presoje na tem področju ugotovilo, da na podlagi člena 8 EKČP ni potreben obstoj pravno zavezujoče zahteve po predhodnem obveščanju. Sodišče je zato ugotovilo, da člen 8 EKČP ni bil kršen.

Primer: v zadevi *Bohlen proti Nemčiji*[96] je pritožnik, znan pevec in umetniški producent, izdal avtobiografijo, pozneje pa je bil zaradi sodnih odločb iz nje prisiljen odstraniti nekatere odlomke. Zgodba je bila pritegnila veliko pozornost nacionalnih medijev, neka tobačna družba pa je začela humorno oglaševalsko kampanjo, ki se je nanašala na zadevni dogodek in v kateri je uporabila pritožnikovo ime brez njegove privolitve. Pritožnik je od oglaševalske družbe neuspešno zahteval odškodnino, pri čemer je trdil, da so bile kršene njegove pravice na podlagi člena 8 EKČP. ESČP je navedlo merila, na katerih temelji uravnoteženje pravice do spoštovanja zasebnega življenja in pravice do svobode izražanja, in ugotovilo, da člen 8 EKČP ni bil kršen. Pritožnik je bil javna osebnost, oglas pa se ni nanašal na podrobnosti o njegovem zasebnem življenju, temveč na javni dogodek, ki je že bil deležen medijske pozornosti in o katerem se je javno razpravljalo. Poleg tega je bil oglas humorne narave in ni vseboval ničesar, kar bi bilo za pritožnika ponižujoče ali negativno.

Primer: v zadevi *Biriuk proti Litvi*[97] je pritožnica pred ESČP trdila, da Litva ni izpolnila svoje obveznosti glede zagotovitve spoštovanja njene pravice do zasebnega življenja, saj so ji nacionalna sodišča, ki so obravnavala zadevo, kljub temu, da je časopis z velikim krogom bralcev huje kršil njeno zasebnost, prisodila smešno nizek znesek odškodnine za premoženjsko škodo. Nacionalna sodišča so pri dodeljevanju odškodnine za nepremoženjsko škodo uporabila določbe nacionalne zakonodaje o obveščanju javnosti, v skladu s katerimi je bila določena nizka zgornja meja za nepremoženjsko škodo, ki jo povzročijo mediji z nezakonitim javnim razširjanjem informacij o zasebnem življenju posameznika. Zadeva je izhajala iz objave članka na naslovnici

96 ESČP, *Bohlen proti Nemčiji*, pritožba št. 53495/09, 19. februar 2015, točke 45–60.

97 ESČP, *Biriuk proti Litvi*, pritožba št. 23373/03, 25. november 2008.

največjega litovskega dnevnika, v katerem je bilo navedeno, da je pritožnica okužena z virusom HIV. V članku se je kritiziralo tudi vedenje pritožnice in se spraševalo o njenih moralnih merilih.

ESČP je opozorilo, da je varstvo osebnih podatkov, zlasti zdravstvenih podatkov, temeljnega pomena za pravico do spoštovanja zasebnega življenja v skladu z EKČP. Zaupnost zdravstvenih podatkov je zlasti pomembna, saj lahko njihovo razkritje (v obravnavani zadevi okužba pritožnice z virusom HIV) bistveno vpliva na zasebno in družinsko življenje posameznika, pa tudi na njegov zaposlitveni položaj in vključenost v družbo. Sodišče je poseben pomen pripisalo dejstvu, da je glede na poročanje časopisa informacije o pritožničini okužbi z virusom HIV zagotovilo zdravstveno osebje bolnišnice, ki je s tem očitno kršilo obveznost zdravniške molčečnosti. Poseganje v pravico pritožnice do zasebnega življenja zato ni bilo zakonito.

Članek je bil objavljen v tiskanem mediju, svoboda izražanja pa je prav tako temeljna pravica v skladu z EKČP. Vendar je Sodišče pri proučevanju, ali je bila objava tovrstnih informacij o pritožnici utemeljena z obstojem javnega interesa, ugotovilo, da je bil glavni namen objave povečati prodajo časopisa s potešitvijo radovednosti bralcev. V zvezi s takim namenom ni bilo mogoče šteti, da prispeva k razpravi v splošnem interesu družbe. Ker je šlo za primer nezaslišane zlorabe svobode tiska, so stroge omejitve pri nadomestitvi škode in nizek znesek odškodnine za nepremoženjsko škodo, določen v nacionalnem pravu, pomenili, da Litva ni izpolnila svoje pozitivne obveznosti glede varstva pritožničine pravice do zasebnega življenja. ESČP je ugotovilo, da je bil kršen člen 8 EKČP.

Pravica do svobode izražanja in pravica do varstva osebnih podatkov nista vedno v nasprotju. V nekaterih primerih učinkovito varstvo osebnih podatkov zagotavlja svobodo izražanja.

Primer: SEU je v zadevi *Tele2 Sverige* navedlo, da je poseg, povzročen z Direktivo 2006/24/ES (direktiva o hrambi podatkov) v temeljne pravice iz členov 7 in 8 Listine, „širok in ga je treba obravnavati kot posebno resnega. Okoliščina, da se hramba podatkov izvede, ne da bi bili uporabniki elektronskih komunikacijskih storitev o tem obveščeni, lahko pri zadevnih osebah povzroči občutek, da se njihovo zasebno življenje stalno nadzoruje". SEU je tudi ugotovilo, da bi lahko splošna hramba podatkov o prometu in podatkov o lokaciji vplivala na uporabo elektronskih komunikacijskih sredstev in, „posledično, na njihovo uresničevanje svobode izražanja, zagotovljene s členom 11 Listine".[98] Pravila o varstvu osebnih podatkov, v skladu s katerimi so potrebni strogi zaščitni ukrepi za zagotavljanje, da se hramba osebnih podatkov ne izvaja na splošno, v tem smislu navsezadnje prispevajo k uresničevanju svobode izražanja.

Kar zadeva pravico do prejemanja informacij, ki je prav tako del svobode izražanja, je zavedanje, kako pomembna je preglednost javne uprave za delovanje demokratične družbe, vse večje. Preglednost je cilj v splošnem interesu, s katerim bi se zato lahko upravičilo poseganje v pravico do varstva osebnih podatkov, če je to potrebno in sorazmerno, kot je pojasnjeno v razdelku 1.2. Pravica do dostopa do dokumentov javnih organov se zato v zadnjih dveh desetletjih priznava kot pomembna pravica vsakega državljana EU in vseh fizičnih ali pravnih oseb, ki prebivajo v državi članici ali imajo v njej registrirani sedež.

V skladu s pravom Sveta Evrope se je mogoče sklicevati na načela, vključena v Priporočilo o dostopu do uradnih dokumentov, po katerem so se zgledovali pisci Konvencije o dostopu do uradnih dokumentov (Konvencija št. 205).[99]

V okviru prava EU je pravica do dostopa do dokumentov zagotovljena z Uredbo (ES) št. 1049/2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (uredba o dostopu do dokumentov).[100] S členom 42 Listine in čle-

98 SEU, *Tele2 Sverige AB proti Post- och telestyrelsen* in *Secretary of State for the Home Department proti Tomu Watsonu in drugim* (veliki senat), združeni zadevi C-203/15 in C-698/15, 21. december 2016, točki 37 in 101, in SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim* in Kärntner Landesregierung in drugi (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014, točka 28.

99 Svet Evrope, Odbor ministrov (2002), Priporočili R (81) 19 in Rec(2002)2 državam članicam o dostopu do uradnih dokumentov, 21. februar 2002; Svet Evrope, Konvencija o dostopu do uradnih dokumentov, CETS št. 205, 18. junij 2009. Konvencija še ni začela veljati.

100 Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (UL L 145, 31.5.2001, str. 43).

nom 15(3) PDEU je bila ta pravica do dostopa razširjena na „dokument[e] institucij, organov, uradov in agencij Unije, ne glede na nosilec dokumenta“.

S to pravico bi se lahko poseglo v pravico do varstva osebnih podatkov, če bi se z dostopom do dokumenta razkrili osebni podatki drugih oseb. Člen 86 SUVP jasno določa, da lahko javni organ oziroma telo v skladu s pravom Unije[101] ali pravom države članice razkrije osebne podatke iz uradnih dokumentov, s katerimi razpolaga, da se uskladi dostop javnosti do uradnih dokumentov s pravico do varstva osebnih podatkov v skladu z navedeno uredbo.

Zahteve za dostop do dokumentov ali informacij javnih organov je zato morda treba uravnotežiti s pravico oseb, katerih osebne podatke vsebujejo zahtevani dokumenti, do varstva osebnih podatkov.

Primer: SEU je moralo v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*[102] odločiti o sorazmernosti objave – zahtevane z zakonodajo EU – imen upravičencev do kmetijskih subvencij EU in zneskov, ki so jih prejeli. Namen objave je bil povečati preglednost in prispevati k temu, da upravni organi javna sredstva uporabljajo primerno. Več upravičencev je izpodbijalo sorazmernost te objave.

SEU je poudarilo, da pravica do varstva osebnih podatkov ni absolutna, in navedlo, da spletna objava poimenskih podatkov o upravičencih do sredstev iz dveh skladov kmetijske pomoči EU in točnih zneskih, ki so jih prejeli, na splošno pomeni poseganje v njihovo zasebno življenje, natančneje v varstvo njihovih osebnih podatkov.

SEU je ugotovilo, da je tako poseganje v člena 7 in 8 Listine določeno z zakonom in da izpolnjuje cilj v splošnem interesu, ki ga priznava EU, in sicer povečanje preglednosti porabe sredstev Skupnosti. Vendar je odločilo, da poimenska objava posameznikov, upravičencev do kmetijske pomoči EU iz obeh skladov, in natančnih zneskov, ki so jih prejeli, pomeni nesorazmeren ukrep in glede na člen 52(1) Listine ni upravičena. Menilo je, da je v demokratični družbi pomembno, da so davkoplačevalci obveščeni o porabi javnih sredstev. Ker pa ni „mogoče določiti, da ima cilj preglednosti samodejno prednost pred

101 Člen 42 Listine, člen 15(3) PDEU in Uredba (ES) št. 1049/2001.

102 SEU, *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen* (veliki senat), združeni zadevi C-92/09 in C-93/09, 9. november 2010, točke 47–52, 58, 66–67, 75, 86 in 92.

pravico do varstva osebnih podatkov",[103] morajo institucije EU interes Unije za preglednost uravnotežiti z omejitvijo uresničevanja pravic do zasebnosti in varstva osebnih podatkov, ki so jo upravičenci utrpeli zaradi objave.

SEU je menilo, da institucije EU tega uravnoteženja niso izvedle ustrezno, saj je bilo mogoče predvideti ukrepe, ki bi manj posegali v temeljne pravice posameznikov, obenem pa učinkovito prispevali k cilju preglednosti, ki se je uresničeval z objavo. Namesto splošne objave, ki vpliva na vse upravičence ter v okviru katere se za vsakega od njih navedejo njihovo ime in natančni zneski, ki so jih prejeli, bi se lahko na primer med upravičenci razlikovalo glede na ustrezna merila, kot so obdobja, v katerih so prejemali sredstva, pogostost sredstev ali njihova višina in vrsta.[104] SEU je zato razglasilo delno ničnost zakonodaje EU o objavi informacij v zvezi z upravičenci do sredstev iz evropskih kmetijskih skladov.

Primer: SEU je v zadevi *Rechnungshof proti Österreichischer Rundfunk in drugim*[105] proučilo združljivost nekaterih avstrijskih zakonov s pravom EU o varstvu osebnih podatkov. V skladu z zadevno zakonodajo je moral državni organ zbirati in sporočati podatke o dohodkih zaradi objave imen in dohodkov zaposlenih pri različnih javnih subjektih v letnem poročilu, ki je na voljo širši javnosti. Nekateri posamezniki svojih podatkov niso želeli sporočiti, pri čemer so se sklicevali na varstvo osebnih podatkov.

SEU se je v svojem mnenju opiralo na varstvo temeljnih pravic kot splošno načelo prava EU in člen 8 EKČP, pri čemer je opozorilo, da Listina takrat ni bila zavezujoča. Menilo je, da zbiranje podatkov v zvezi s poklicnimi dohodki posameznikov, zlasti za njihovo posredovanje tretjim osebam, spada na področje uporabe pravice do spoštovanja zasebnega življenja in pomeni kršitev te pravice. Ta poseg bi lahko bil upravičen, če bi bil določen z zakonom, uresničeval zakonit cilj in bil nujen v demokratični družbi za izpolnitev tega cilja. SEU je ugotovilo, da je avstrijska zakonodaja uresničevala zakonit cilj, in sicer ohranjati višino plač javnih uslužbencev v razumnih mejah, kar je dejavnik, ki je povezan tudi z ekonomsko blaginjo države. Vendar je bilo treba

103 Prav tam, točka 85.

104 Prav tam, točka 89.

105 SEU, *Rechnungshof proti Österreichischer Rundfunk in drugim* in *Christa Neukomm in Joseph Lauermann proti Österreichischer Rundfunk*, združene zadeve C-465/00, C-138/01 in C-139/01, 20. maj 2003.

interes Avstrije po zagotavljanju najbolj smotrne uporabe javnih sredstev uravnotežiti z resnostjo posega v pravico zadevnih oseb do spoštovanja njihovega zasebnega življenja.

Čeprav je SEU preverjanje, ali je objava podatkov o dohodku posameznikov potrebna in sorazmerna s ciljem, ki se uresničuje z zakonodajo, prepustilo nacionalnemu sodišču, ga je pozvalo, naj prouči, ali takega cilja ne bi bilo mogoče enako učinkovito doseči z manj motečimi sredstvi. To bi bilo na primer mogoče tako, da bi se osebni podatki posredovali le javnim nadzornim organom, ne pa širši javnosti.

V poznejših zadevah je postalo jasno, da je za uravnoteženje med varstvom osebnih podatkov in dostopom do dokumentov potrebna podrobna analiza za vsak primer posebej. Nobena pravica ne more samodejno prevladati nad drugo. SEU je imelo v dveh zadevah priložnost za razlago pravice do dostopa do dokumentov, ki vsebujejo osebne podatke.

Primer: SEU je v zadevi *Evropska komisija proti Bavarian Lager*[106] opredelilo obseg varstva osebnih podatkov v okviru dostopa do dokumentov institucij EU ter razmerje med Uredbo (ES) št. 1049/2001 (uredba o dostopu do dokumentov) in Uredbo (ES) št. 45/2001 (uredba o varstvu osebnih podatkov v institucijah EU). Družba Bavarian Lager, ustanovljena leta 1992, v Združeno kraljestvo uvaža ustekleničeno nemško pivo, predvsem za točilnice. Naletela pa je na težave, ker je bila britanska zakonodaja *de facto* bolj naklonjena nacionalnim proizvajalcem. Evropska komisija je v odgovor na pritožbo družbe Bavarian Lager začela postopek proti Združenemu kraljestvu zaradi neizpolnitve obveznosti, na podlagi česar je Združeno kraljestvo sporne določbe spremenilo in jih uskladilo s pravom EU. Družba Bavarian Lager je nato Komisijo poleg drugih dokumentov zaprosila za kopijo zapisnika sestanka, ki so se ga udeležili predstavniki Komisije, britanskih organov in združenja *Confédération des Brasseurs du Marché Commun* (CBMC). Komisija se je strinjala, da bo razkrila nekatere dokumente v zvezi s sestankom, vendar je pet imen, navedenih v zapisniku, izbrisala, saj sta dve osebi izrecno nasprotovali razkritju svoje identitete, s preostalimi tremi pa ni mogla navezati stika. Z odločbo z dne 18. marca 2004 je zavrnila novo prošnjo družbe Bavarian

106 SEU, *Evropska komisija proti The Bavarian Lager Co. Ltd.*(veliki senat), C-28/08 P, 29. junij 2010.

Lager za pridobitev celotnega zapisnika sestanka, pri čemer se je sklicevala zlasti na varstvo zasebnosti navedenih oseb, ki je zagotovljeno z uredbo o varstvu osebnih podatkov v institucijah EU.

Ker družba Bavarian Lager s tem ni bila zadovoljna, je vložila tožbo pri Sodišču prve stopnje. To sodišče je odločbo Komisije s sodbo z dne 8. novembra 2007 v zadevi *The Bavarian Lager Co. Ltd proti Komisiji Evropskih skupnosti* (T-194/04) razglasilo za nično, pri čemer je ugotovilo, da zgolj vnos imen zadevnih oseb na seznam prisotnih, ki so se sestanka udeležili v imenu organa, ki so ga zastopali, ne pomeni poseganja v zasebnost in nikakor ne ogroža zasebnega življenja navedenih oseb.

SEU je sodbo prvostopenjskega sodišča na podlagi pritožbe Komisije razveljavilo. Ugotovilo je, da se z uredbo o dostopu do dokumentov „uvaja posebn[a] ureditev in krepi varstvo osebe, katere osebni podatki bi se v nekaterih primerih lahko posredovali javnosti". Po mnenju SEU postanejo določbe uredbe o varstvu osebnih podatkov v institucijah EU v celoti upoštevne, če se poskuša s prošnjo na podlagi uredbe o dostopu do dokumentov pridobiti dostop do dokumentov, ki vsebujejo osebne podatke. SEU je nato ugotovilo, da je Komisija upravičeno zavrnila prošnjo za dostop do celotnega zapisnika sestanka iz oktobra 1996. Ker pet udeležencev navedenega sestanka ni dalo privolitve, je Komisija ustrezno spoštovala obveznost javnosti, tako da je razkrila različico zadevnega dokumenta, v katerem so bila njihova imena izbrisana.

SEU je poleg tega menilo, da „ker družba Bavarian Lager ni predložila nobene izrecne in zakonite utemeljitve niti nobenega prepričljivega argumenta, da bi dokazala potrebo po posredovanju teh osebnih podatkov, Komisija ni mogla pretehtati različnih interesov zadevnih strank. Poleg tega ni mogla preveriti, ali ni nobenega razloga, iz katerega bi se morda poseglo v zakonite interese posameznika, na katerega se nanašajo osebni podatki", kot se zahteva z uredbo o varstvu osebnih podatkov v institucijah EU.

Primer: SEU je v zadevi *Client Earth in PAN Europe proti EFSA*[107] proučilo, ali je bila odločitev Evropske agencije za varnost hrane (EFSA), da pritožnicama zavrne poln dostop do dokumentov, potrebna za zaščito pravic do

107 SEU, *ClientEarth in Pesticide Action Network Europe (PAN Europe) proti Evropski agenciji za varno hrano in Evropski komisiji*, C-615/13 P, 16. julij 2015.

zasebnosti in varstva osebnih podatkov oseb, na katere so se dokumenti nanašali. Dokumenti so se nanašali na osnutek smernic, ki ga je delovna skupina agencije EFSA pripravila v sodelovanju z zunanjimi strokovnjaki za dajanje fitofarmacevtskih proizvodov v promet. EFSA je pritožnicama najprej odobrila delni dostop, zavrnila pa je dostop do nekaterih delovnih različic osnutka smernic. Pozneje je odobrila dostop do osnutka, ki je vključeval posamezne pripombe zunanjih strokovnjakov, vendar je prikrila imena strokovnjakov, pri čemer se je sklicevala na člen 4(1)(b) Uredbe (ES) št. 45/2001 o obdelavi osebnih podatkov v institucijah in organih Skupnosti ter potrebo po varstvu zasebnosti zunanjih strokovnjakov. Splošno SEU je na prvi stopnji potrdilo odločbo agencije EFSA.

SEU je na podlagi pritožbe pritožnic razveljavilo sodbo prvostopenjskega sodišča. Ugotovilo je, da je bil prenos osebnih podatkov v tem primeru potreben, da bi se preverila nepristranskost vsakega od zunanjih strokovnjakov pri opravljanju njihovih znanstvenih nalog in zagotovila preglednost postopka odločanja pri agenciji EFSA. Po mnenju SEU agencija EFSA ni navedla, kako bi razkritje imen zunanjih strokovnjakov, ki so podali posebne pripombe k osnutku smernic, poseglo v zakonite interese strokovnjakov. Splošna trditev, da bi razkritje pomenilo nevarnost posega v zasebno življenje, ne zadostuje, če ni podprta z dokazi, ki se nanašajo na posamezni primer.

V skladu s tema sodbama je za poseg v pravico do varstva osebnih podatkov v okviru dostopa do dokumentov potreben konkreten in utemeljen razlog. Pravica do dostopa do dokumentov ne more samodejno prevladati nad pravico do varstva osebnih podatkov.[108]

Ta pristop je podoben pristopu ESČP v zvezi z zasebnostjo in dostopom do dokumentov, kot je razvidno iz naslednje sodbe. ESČP je v sodbi v zadevi *Magyar Helsinki* navedlo, da s členom 10 EKČP posamezniku ni dodeljena pravica dostopa do informacij, ki jih hranijo javni organi, niti ni v skladu z njim vladi treba takih informacij posredovati posamezniku. Vendar bi lahko taka pravica ali obveznost nastala, prvič, če bi posredovanje informacij odredilo sodišče s pravnomočno odločbo, in, drugič, kadar je dostop do informacij ključen za to, da posameznik uresničuje svojo pravico do svobodnega izražanja, zlasti pravice do sprejemanja in širjenja vesti, in kadar bi

108 Vendar glej tudi podrobne preudarke v: ENVP (2011), *Dostop javnosti do dokumentov, ki vsebujejo osebne podatke, po odločitvi Sodišča v zadevi Bavarian Lager*, Bruselj, 24. marec 2011.

zavrnitev dostopa do informacij pomenila poseg v navedeno pravico.[109] Ali in v kolikšnem obsegu zavrnitev dostopa do informacij pomeni poseg v pritožnikovo svobodo izražanja, je treba ugotoviti za vsak primer posebej in ob upoštevanju konkretnih okoliščin, med drugim: (i) namena zahteve po informacijah, (ii) vrste zahtevanih informacij, (iii) vloge pritožnika ter (iv) tega, ali so bile informacije pripravljene in na voljo.

Primer: v zadevi *Magyar Helsinki Bizottság proti Madžarski*[110] je pritožnica, nevladna organizacija za človekove pravice, od policije zahtevala informacije v zvezi z delom zagovornikov po uradni dolžnosti, ki jih je potrebovala za dokončanje študije o delovanju sistema zagovornikov po uradni dolžnosti na Madžarskem. Policija je predložitev teh informacij zavrnila, češ da gre za osebne podatke, ki niso javnega značaja. ESČP je ob upoštevanju zgornjih meril menilo, da je prišlo do poseganja v pravico, varovano s členom 10 EKČP. Natančneje, pritožnica je želela uveljavljati pravico do širjenja vesti o zadevi v javnem interesu, zato je v ta namen zahtevala dostop do informacij, ki so bile potrebne za uveljavljanje njene pravice do svobode izražanja. Informacije o imenovanju zagovornikov po javni dolžnosti so bile v javnem interesu. Ni bilo razloga za dvom, da je zadevna raziskava vključevala informacije, v zvezi s katerimi se je pritožnica zavezala, da jih bo posredovala javnosti, in ki jih je javnost imela pravico prejeti. Sodišče se je tako prepričalo, da je pritožnica dostop do zahtevanih informacij potrebovala za izpolnitev naloge. Poleg tega so bile informacije pripravljene in na voljo.

ESČP je ugotovilo, da je zavrnitev dostopa do informacij v navedenem primeru posegla v samo bistvo svobode sprejemanja vesti. Pri oblikovanju te ugotovitve je proučilo zlasti namen zahtevanih informacij in njihov prispevek k pomembni javni razpravi, vrsto zahtevanih informacij in to, ali so bile v javnem interesu, ter vlogo, ki jo ima pritožnica v obravnavani zadevi v družbi.

Sodišče je v obrazložitvi navedlo, da se je študija, ki jo je opravila zadevna nevladna organizacija, nanašala na delovanje pravosodja in pravico do poštenega sojenja, ki je v skladu z EKČP bistvena pravica. Ker zahtevane informacije niso vključevale podatkov, ki bi presegali meje javne sfere, pravice zadevnih posameznikov, na katere se nanašajo osebni podatki (zagovornikov

109 ESČP, *Magyar Helsinki Bizottság proti Madžarski* (veliki senat), pritožba št. 18030/11, 8. november 2016, točka 148.

110 Prav tam, točke 181 in 187–200.

po uradni dolžnosti), do zasebnosti ne bi bile ogrožene, če bi policija pritožnici zagotovila dostop do informacij. Informacije, ki jih je zahtevala pritožnica, so bile statistične narave in so se nanašale na to, kolikokrat je bil zagovornik po uradni dolžnosti imenovan za zastopanje obtožencev v javnih kazenskih postopkih.

Sodišče je menilo, da bi bilo treba glede na to, da je bil cilj študije prispevati k pomembni razpravi o zadevi v javnem interesu, vsakršne omejitve v zvezi s predlagano publikacijo nevladne organizacije skrbno proučiti. Zadevne informacije so bile v javnem interesu, saj javni interes zajema zadeve, ki bi lahko sprožile precejšnje polemike, se nanašajo na pomembno družbeno vprašanje ali vključujejo težavo, s katero bi javnost hotela biti seznanjena.[111] Zato bi zagotovo zajemal razpravo o delovanju pravosodja in poštenem sojenju, kar je bila tema pritožničine študije. ESČP, ki je uravnotežilo različne zadevne pravice in upoštevalo načelo sorazmernosti, je menilo, da je prišlo do neupravičene kršitve pravic pritožnice v skladu s členom 10 EKČP.

1.3.2 Poklicna skrivnost

V skladu z nacionalnim pravom lahko za nekatere komunikacije velja obveznost varovanja poklicne skrivnosti. Varovanje poklicne skrivnosti se lahko razume kot posebna etična dolžnost, iz katere izhaja pravna obveznost, neločljivo povezana z nekaterimi poklici in funkcijami, ki temeljijo na zaupanju. Osebe in institucije, ki opravljajo te funkcije, ne smejo razkriti zaupnih informacij, ki jih prejmejo med opravljanjem svojih nalog. Varovanje poklicne skrivnosti zlasti velja za zdravstveni poklic ter sporazumevanje med odvetnikom in stranko, v številnih jurisdikcijah pa je priznana tudi obveznost varovanja poklicne skrivnosti v finančnem sektorju. Varovanje poklicne skrivnosti ni temeljna pravica, temveč je zaščiteno kot oblika pravice do spoštovanja zasebnega življenja. SEU je na primer menilo, da je v nekaterih primerih „namreč lahko potrebna prepoved razkritja nekaterih informacij, ki so opredeljene kot zaupne, zato da se ohrani temeljna pravica podjetja do spoštovanja zasebnega življenja iz člena 8 [EKČP] […] in iz člena 7 Listine“.[112] Tudi ESČP je bilo zaprošeno, naj odloči, ali omejitve varovanja poklicne skrivnosti pomenijo kršitev člena 8 EKČP, kot je ponazorjeno s primeroma v spodnjem besedilnem polju.

111 Prav tam, točka 156.

112 Splošno sodišče, *Pilkington Group Ltd proti Evropski komisiji*, T-462/12 R, sklep predsednika z dne 11. marca 2013, točka 44.

Primer: v zadevi *Pruteanu proti Romuniji*[113] je bil pritožnik odvetnik gospodarske družbe, ki ji je bilo zaradi domnevnih goljufij prepovedano opravljati bančne transakcije. Romunska sodišča so med preiskavo zadeve organom kazenskega pregona odobrila, da v določenem obdobju prestrezajo in snemajo telefonske pogovore partnerjev družbe. Posnetki in prestrezanja so vključevali tudi komunikacije zadevnega partnerja s pritožnikom, svojim odvetnikom.

A. Pruteanu je trdil, da je šlo za poseg v njegovo pravico do spoštovanja zasebnega življenja in dopisovanja. ESČP je v svoji sodbi poudarilo status in pomen razmerja med odvetnikom in njegovo stranko. S prestrezanjem pogovorov med odvetnikom in njegovo stranko je nedvomno prišlo do posega v obveznost varovanja poklicne skrivnosti, ki je temelj razmerja med njima. V takem primeru se je lahko odvetnik pritožil tudi zaradi poseganja v svojo pravico do spoštovanja zasebnega življenja in dopisovanja. ESČP je ugotovilo, da je bil kršen člen 8 EKČP.

Primer: v zadevi *Brito Ferrinho Bexiga Villa-Nova proti Portugalski*[114] pritožnica, odvetnica, davčnim organom ni želela razkriti svojih osebnih bančnih izpiskov, pri čemer se je sklicevala na poklicno in bančno tajnost. Tožilstvo je začelo preiskavo zaradi davčne goljufije in predlagalo, naj se dolžnost varovanja poklicne tajnosti ne upošteva. Nacionalna sodišča so odredila, da se pravila o varovanju poklicne in bančne tajnosti v tem primeru ne upoštevajo, saj so menila, da javni interes prevlada nad zasebnimi interesi pritožnice.

Ko je bila zadeva predložena ESČP, je to menilo, da dostop do bančnih izpiskov pritožnice pomeni poseg v njeno pravico do spoštovanja poklicne tajnosti, ki spada v okvir zasebnega življenja. Poseg je imel pravno podlago, saj je temeljil na zakoniku o kazenskem postopku in se je z njim uresničeval zakonit cilj. Vendar je ESČP po proučitvi potrebnosti in sorazmernosti posega opozorilo na dejstvo, da je bil postopek za razrešitev dolžnosti varovanja tajnosti izveden brez sodelovanja pritožnice ali njene vednosti. Pritožnica tako ni mogla predložiti svojih trditev. In čeprav je bilo v nacionalnem pravu določeno, da se je treba v takem postopku posvetovati z odvetniškim združenjem, ni bilo z njim opravljeno nikakršno posvetovanje. Poleg tega pritožnica ni imela ne možnosti, da bi učinkovito izpodbijala razrešitev dolžnosti varovanja tajnosti,

113 ESČP, *Pruteanu proti Romuniji*, pritožba št. 30181/05, 3. februar 2015.

114 ESČP, *Brito Ferrinho Bexiga Villa-Nova proti Portugalski*, pritožba št. 69436/10, 1. december 2015.

ne pravnega sredstva za izpodbijanje zadevnega ukrepa. ESČP je ugotovilo, da je bil zaradi pomanjkanja procesnih jamstev in učinkovitega sodnega nadzora nad ukrepom, s katerim se je odredila razrešitev dolžnosti varovanja tajnosti, kršen člen 8 EKČP.

Povezava med obveznostjo varovanja poklicne skrivnosti in varstvom osebnih podatkov je pogosto protislovna. Po eni strani pravila in zaščitni ukrepi glede varstva osebnih podatkov, določeni v zakonodaji, pripomorejo k zagotavljanju varovanja poklicne skrivnosti. S pravili, v skladu s katerimi morajo upravljavci in obdelovalci izvajati učinkovite ukrepe za zagotavljanje varnosti osebnih podatkov, se med drugim na primer želi preprečiti izgubo zaupnosti osebnih podatkov, zaščitenih s poklicno skrivnostjo. Poleg tega SUVP omogoča obdelavo zdravstvenih podatkov, ki so posebna vrsta osebnih podatkov, ki jih je treba strožje varovati, vendar jo pogojuje z obstojem ustreznih in posebnih ukrepov za zaščito pravic posameznikov, na katere se nanašajo osebni podatki, zlasti varovanja poklicne skrivnosti.[115]

Po drugi strani se lahko z obveznostmi varovanja poklicne skrivnosti, ki so v zvezi z nekaterimi osebnimi podatki naložene upravljavcem in obdelovalcem, omejijo pravice posameznikov, na katere se nanašajo osebni podatki, zlasti pravica do sprejemanja vesti. Čeprav SUVP vsebuje izčrpen seznam z informacijami, ki jih je načeloma treba zagotoviti posamezniku, na katerega se nanašajo osebni podatki, kadar ti niso bili pridobljeni od njega, se ta zahteva po razkritju ne uporablja, kadar morajo osebni podatki ostati zaupni zaradi obveznosti varovanja poklicne skrivnosti v skladu z nacionalnim pravom ali pravom EU.[116]

V SUVP je določeno, da lahko države članice z zakonom sprejmejo posebna pravila glede varovanja poklicne skrivnosti ali druge enakovredne obveznosti varovanja skrivnosti, če je to potrebno zaradi uskladitve pravice do varstva osebnih podatkov z obveznostjo varovanja poklicne skrivnosti.[117]

SUVP določa, da lahko države članice sprejmejo posebna pravila o pooblastilih nadzornih organov v zvezi z upravljavci ali obdelovalci, za katere velja obveznost varovanja poslovne skrivnosti. Ta posebna pravila se nanašajo na pooblastilo za pridobitev dostopa do prostorov upravljavca ali obdelovalca, do njegove opreme za obdelavo osebnih podatkov in do osebnih podatkov, ki jih hrani, če so bili taki osebni

115 SUVP, člen 9(2)(h) in (3).

116 Prav tam, člen 14(5)(d).

117 Prav tam, uvodna izjava 164 in člen 90.

podatki prejeti v okviru dejavnosti, za katero velja obveznost varovanja skrivnosti. Nadzorni organi, pooblaščeni za varstvo osebnih podatkov, morajo zato spoštovati obveznosti varovanja poklicne skrivnosti, ki zavezujejo upravljavce in obdelovalce. Poleg tega dolžnost varovanja poklicne skrivnosti velja tudi za člane samih nadzornih organov, in sicer med njihovim mandatom in po njem. Člani in osebje nadzornih organov se lahko med opravljanjem svojih nalog seznanijo z zaupnimi informacijami. Člen 54(2) zadevne uredbe jasno določa, da v zvezi s takimi zaupnimi informacijami zanje velja dolžnost varovanja poklicne skrivnosti.

Države članice morajo v skladu s SUVP Komisijo uradno obvestiti o pravilih, ki jih sprejmejo za uskladitev varstva osebnih podatkov in načel, določenih v zadevni uredbi, z obveznostjo varovanja poklicne skrivnosti.

1.3.3 Svoboda vere in prepričanja

Svoboda vere in prepričanja je zaščitena na podlagi člena 9 EKČP (svoboda mišljenja, vesti in vere) in člena 10 Listine EU o temeljnih pravicah. Osebni podatki, ki razkrivajo verska ali filozofska prepričanja, se v skladu s pravom EU in pravom Sveta Evrope štejejo za občutljive podatke, zato za njihovo obdelavo in uporabo velja okrepljeno varstvo.

Primer: pritožnik v zadevi *Sinak Işik proti Turčiji*[118] je bil član alevitske verske skupnosti, na katere vero so vplivali sufizem in druga predislamska verovanja, pri čemer jo nekateri učenjaki štejejo za posebno vero, drugi pa za del islamske vere. Pritožnik se je pritožil, ker je bil v njegovi osebni izkaznici proti njegovi volji v okvirčku o veroizpovedi namesto „alevizem“ naveden „islam“. Nacionalna sodišča so zavrnila njegovo zahtevo po spremembi navedbe veroizpovedi v njegovi osebni izkaznici v „alevizem“, ker naj bi ta beseda označevala podskupino v islamu, ne pa posebne vere. Nato je vložil pritožbo pri ESČP, v kateri je trdil, da je moral razkriti svojo veroizpoved, čeprav je temu nasprotoval, saj je bila navedba veroizpovedi v osebni izkaznici obvezna, kar je v nasprotju z njegovo pravico do svobode vere in vesti, zlasti ker je bila navedba „islam“ v njegovi osebni izkaznici napačna.

118 ESČP, *Sinan Işık proti Turčiji*, pritožba št. 21924/05, 2. februar 2010.

ESČP je opozorilo, da verska svoboda pomeni svobodo izražanja svoje vere skupaj z drugimi, javno in v krogu oseb, ki si delijo isto vero, pa tudi posamezno in zasebno. V skladu s takrat veljavno nacionalno zakonodajo so morali posamezniki imeti pri sebi osebno izkaznico, ki jo je bilo treba predložiti na zahtevo katerega koli javnega organa ali zasebnega podjetja in v kateri je morala biti navedena njihova veroizpoved. V okviru te obveznosti ni bilo priznano, da je s pravico do izražanja vere dodeljena tudi nasprotna pravica, tj. pravica, da posamezniku ni treba razkriti svojih prepričanj. Čeprav je vlada trdila, da je bila nacionalna zakonodaja spremenjena, tako da so posamezniki lahko zahtevali, da se okence o veroizpovedi v osebni izkaznici pusti prazno, je Sodišče menilo, da bi lahko že samo dejstvo, da je bilo treba zaprositi za izbris navedbe veroizpovedi, pomenilo razkritje informacij o njihovem odnosu do vere. Če imajo osebne izkaznice okence o veroizpovedi, bi to, da bi to ostalo neizpolnjeno, poleg tega imelo poseben pomen, saj bi imetniki osebne izkaznice brez informacije o veroizpovedi izstopali glede na tiste, ki imajo v osebni izkaznici navedeno veroizpoved. ESČP je ugotovilo, da je nacionalna zakonodaja v nasprotju s členom 9 EKČP.

Za delovanje cerkva in verskih združenj ali skupnosti je lahko potrebna obdelava osebnih podatkov članov, da se omogočita komunikacija in organizacija dejavnosti v okviru zadevne skupine vernikov. Cerkve in verska združenja zato pogosto izvajajo pravila v zvezi z obdelavo osebnih podatkov. Kadar so v skladu s členom 91 SUVP ta pravila celovita, lahko veljajo še naprej, če so usklajena z določbami navedene uredbe. Cerkve in verska združenja, ki uporabljajo taka pravila, mora nadzirati neodvisen nadzorni organ, ki je lahko poseben organ zanje, če izpolnjuje zahteve iz SUVP za take organe.[119]

Verske organizacije lahko obdelujejo osebne podatke iz več razlogov, na primer da vzdržujejo stike s svojimi verniki ali sporočajo informacije o verskih ali dobrodelnih prireditvah in praznovanjih, ki se organizirajo. V nekaterih državah morajo cerkve voditi registre svojih članov iz davčnih razlogov, saj lahko članstvo v verskih organizacijah vpliva na davke, ki jih morajo plačati posamezniki. Vsekakor so v skladu z evropskim pravom podatki, ki razkrivajo verska prepričanja, občutljivi podatki, zato morajo biti cerkve odgovorne za ravnanje s takimi podatki in njihovo obdelavo, zlasti ker se informacije, ki jih obdelujejo verske organizacije, pogosto nanašajo na otroke, starejše ali druge ranljive člane družbe.

119 SUVP, člen 91(2).

1.3.4 Svoboda umetnosti in znanosti

Še ena pravica, ki jo je treba uravnotežiti s pravicama do spoštovanja zasebnega življenja in varstva osebnih podatkov, je svoboda umetnosti in znanosti, ki je izrecno varovana s členom 13 Listine EU o temeljnih pravicah. Ta pravica je izpeljana predvsem iz pravice do svobode misli in izražanja ter jo je treba uveljavljati ob upoštevanju člena 1 Listine (človekovo dostojanstvo). ESČP meni, da je svoboda umetnosti varovana s členom 10 EKČP.[120] Tudi pravica, zagotovljena s členom 13 Listine, je lahko predmet omejitev v skladu s členom 52(1) Listine, ki se lahko prav tako razlagajo v duhu člena 10(2) EKČP.[121]

Primer: avstrijska sodišča so v zadevi *Vereinigung bildender Künstler proti Avstriji*[122] združenju, ki je vložilo pritožbo, prepovedala nadaljnje razstavljanje slike, ki je vsebovala fotografije glav več javnih osebnosti v spolnih položajih. Avstrijski poslanec, čigarfotografija je bila uporabljena na sliki, je sprožil postopek zoper združenje, ki je vložilo pritožbo, da bi dosegel sodno prepoved razstavljanja slike. Nacionalno sodišče je izdalo sodno prepoved. ESČP je opozorilo, da se člen 10 EKČP uporablja tudi za sporočanje idej, ki državo ali del prebivalstva žalijo, pretresejo ali vznemirijo. Kdor ustvarja, izvaja, razširja ali razstavlja umetniška dela, prispeva k izmenjavi idej in stališč, država pa ne sme neupravičeno kratiti njegove svobode izražanja. Ker je bila slika kolaž in so bile uporabljene samo fotografije glav oseb, njihova telesa pa so bila naslikana nerealistično in karikirano, tako da njihov namen očitno ni bilo izražanje resničnosti ali celo namigovanje nanjo, je ESČP še navedlo, da skoraj ni mogoče, da bi se slika nanašala na podrobnosti iz zasebnega življenja upodobljene osebe, temveč se verjetneje navezuje na njen javni ugled kot politika in da mora upodobljena oseba na tej funkciji pokazati večjo strpnost do kritike. ESČP je ob tehtanju različnih zadevnih interesov ugotovilo, da neomejena prepoved nadaljnjega razstavljanja slike ni sorazmerna. Ugotovilo je, da je bil kršen člen 10 EKČP.

V evropskem pravu o varstvu osebnih podatkov je priznana tudi posebna vrednost, ki jo ima za družbo znanost. S SUVP in posodobljeno Konvencijo št. 108 je dovoljena hramba osebnih podatkov za daljša obdobja, če se bodo osebni podatki obdelovali izključno v znanstveno- ali zgodovinskoraziskovalne namene. Poleg tega se

120 ESČP, *Müller in drugi proti Švici*, pritožba št. 10737/84, 24. maj 1988.

121 Pojasnila k Listini o temeljnih pravicah (UL C 303, 4.12.2007, str. 17).

122 ESČP, *Vereinigung bildender Künstler proti Avstriji*, pritožba št. 68354/01, 25. januar 2007, točki 26 in 34.

ne glede na prvotni namen posebne dejavnosti obdelave poznejša uporaba osebnih podatkov za znanstvene raziskave ne šteje za nezdružljiv namen.[123] Hkrati je treba uvesti ustrezne zaščitne ukrepe za tako obdelavo, da se zaščitijo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. EU ali države članice lahko določijo odstopanja od pravic posameznika, na katerega se nanašajo osebni podatki, na primer pravice do dostopa, popravka, omejitve obdelave in ugovora, in sicer v zvezi z obdelavo njegovih osebnih podatkov za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene (glej tudi razdelek 6.1 in razdelek 9.4).

1.3.5 Varstvo intelektualne lastnine

Pravica do varstva lastnine je določena v členu 1 Protokola št. 1 k EKČP in členu 17(1) Listine EU o temeljnih pravicah. Pomemben vidik lastninske pravice, ki je zlasti pomemben za varstvo osebnih podatkov, je varstvo intelektualne lastnine, ki je izrecno navedeno v členu 17(2) Listine. Pravni red EU vsebuje več direktiv, katerih namen je učinkovito varstvo intelektualne lastnine, zlasti avtorske pravice. Intelektualna lastnina se ne nanaša samo na literarno in umetniško lastnino, ampak tudi na patentne pravice, pravice blagovne znamke in sorodne pravice.

Kot je jasno razvidno iz sodne prakse SEU, je treba varstvo temeljne lastninske pravice uravnotežiti z varstvom drugih temeljnih pravic, zlasti pravice do varstva osebnih podatkov.[124] Institucije za varstvo avtorske pravice so že večkrat zahtevale, naj ponudniki dostopa do interneta razkrijejo identiteto uporabnikov spletnih platform za izmenjavo datotek. Take platforme uporabnikom spleta pogosto omogočajo brezplačen prenos glasbenih del, tudi če so ta zaščitena z avtorsko pravico.

Primer: v zadevi *Promusicae proti Telefónica de España*[125] španski ponudnik dostopa do interneta, družba Telefónica, združenju Promusicae, nepridobitnemu združenju glasbenih producentov ter založnikov glasbenih in avdiovizualnih posnetkov, ni razkrila osebnih podatkov nekaterih oseb, ki jim je zagotavljala dostop do interneta. Združenje Promusicae si je prizadevalo za razkritje informacij, da bi lahko sprožilo civilni postopek zoper navedene

123 SUVP, člen 5(1)(b); posodobljena Konvencija št. 108, člen 5(4)(b).

124 SEU, *Productores de Música de España (Promusicae) proti Telefónica de España SAU* (veliki senat), C-275/06, 29. januar 2008, točke 62–68.

125 Prav tam, točki 54 in 60.

osebe, ki naj bi uporabljale program za izmenjavo datotek, ki je omogočal dostop do zvočnih zapisov, katerih pravice materialnega izkoriščanja so imeli člani združenja Promusicae.

Špansko sodišče je zadevo predložilo SEU, pri čemer mu je postavilo vprašanje, ali je treba v skladu s pravom Skupnosti take osebne podatke posredovati v okviru civilnih postopkov, da bi se zagotovilo učinkovito varstvo avtorske pravice. Sklicevalo se je na direktive 2000/31/ES, 2001/29/ES in 2004/48/ES v povezavi s členoma 17 in 47 Listine. SEU je ugotovilo, da navedene tri direktive in tudi Direktiva o zasebnosti in elektronskih komunikacijah (Direktiva 2002/58/ES) državam članicam ne preprečujejo, da bi določile obveznost razkritja osebnih podatkov v okviru civilnih postopkov in tako zagotovile učinkovito varstvo avtorske pravice.

SEU je poudarilo, da se v zadevi zato postavlja vprašanje potrebne uskladitve zahtev, povezanih z varstvom temeljnih pravic, in sicer pravice do spoštovanja zasebnega življenja ter pravic do varstva lastnine in učinkovitega pravnega sredstva.

Ugotovilo je, da „morajo države članice ob prenosu zgoraj navedenih direktiv paziti, da se oprejo na razlago teh direktiv, ki omogoča zagotovitev pravilnega ravnovesja med različnimi temeljnimi pravicami, varovanimi s pravnim redom Skupnosti. Organi in sodišča držav članic morajo ob uporabi ukrepov za prenos teh direktiv ne zgolj razlagati nacionalno pravo v skladu z direktivami, temveč tudi paziti, da se ne opirajo na tako razlago besedila teh direktiv, ki bi bila v nasprotju s temeljnimi pravicami ali z drugimi splošnimi načeli prava Skupnosti, kot je načelo sorazmernosti“.[126]

Primer: zadeva *Bonnier Audio AB in drugi proti Perfect Communication Sweden AB*[127] se je nanašala na ravnotežje med pravicami intelektualne lastnine in varstvom osebnih podatkov. Tožeče stranke, pet založniških podjetij, ki imajo avtorske pravice na 27 zvočnih knjigah, so začele postopek pred švedskim sodiščem, ker naj bi bile njihove avtorske pravice kršene zaradi uporabe strežnika FTP (protokol za prenos datotek, ki omogoča izmenjavo datotek in prenos podatkov prek interneta). Tožeče stranke so zahtevale,

126 Prav tam, točki 65 in 68; glej tudi SEU *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) proti Netlog NV*, C-360/10, 16. februar 2012.

127 SEU, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB proti Perfect Communication Sweden AB*, C-461/10, 19. april 2012.

naj ponudnik internetnih storitev razkrije ime in naslov osebe, ki uporablja IP-naslov, s katerega naj bi bile prenesene zadevne datoteke. Ponudnik internetnih storitev, družba ePhone, je temu nasprotoval in trdil, da je to v nasprotju z Direktivo 2006/24/ES (direktive o hrambi podatkov, ki je bila razveljavljena leta 2014).

Švedsko sodišče je zadevo predložilo SEU z vprašanjem, ali Direktiva 2006/24/ES nasprotuje uporabi nacionalne določbe na podlagi člena 8 Direktive 2004/48/ES (direktiva o uveljavljanju pravic intelektualne lastnine), ki omogoča izdajo odredbe, v skladu s katero morajo ponudniki internetnih storitev imetnikom avtorske pravice posredovati informacije o naročnikih, katerih IP-naslovi naj bi bili uporabljeni pri kršitvah. Vprašanje je temeljilo na domnevi, da je predlagatelj odredbe kršitev avtorske pravice izkazal za verjetno in da je ukrep sorazmeren.

SEU je poudarilo, da se Direktiva 2006/24/ES nanaša izključno na obdelavo in hrambo podatkov, ki jih pridobivajo ponudniki elektronskih komunikacijskih storitev za namen preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, in na posredovanje teh podatkov pristojnim nacionalnim organom. Nacionalna določba, s katero je bila prenesena direktiva o uveljavljanju pravic intelektualne lastnine, je zunaj področja uporabe Direktive 2006/24/ES, zato ji navedena direktivane nasprotuje.[128]

Kar zadeva razkritje zadevnega imena in naslova, ki so ga predlagale pritožnice, je SEU menilo, da tako dejanje pomeni obdelavo osebnih podatkov in spada na področje uporabe Direktive 2002/58/ES (Direktiva o zasebnosti in elektronskih komunikacijah). Ugotovilo je tudi, da je razkritje teh podatkov predlagano v okviru civilnega postopka v korist imetnika avtorske pravice, da se zagotovi učinkovito varstvo avtorske pravice, in da zato glede na predmet spada tudi na področje uporabe Direktive 2004/48/ES.[129]

SEU je ugotovilo, da je treba direktivi 2002/58/ES in 2004/48/ES razlagati tako, da ne nasprotujeta nacionalni zakonodaji, kot je ta v postopku v glavni stvari, ker ta zakonodaja omogoča nacionalnemu sodišču, pri katerem je

128 Prav tam, točki 40 in 41.

129 Prav tam, točke 52–54. Glej tudi SEU, *Productores de Música de España (Promusicae) proti Telefónica de España SAU* (veliki senat), C-275/06, 29. januar 2008, točka 58.

vložena prošnja za odredbo o razkritju osebnih podatkov, da glede na okoliščine vsakega primera in ob ustreznem upoštevanju zahtev, ki izhajajo iz načela sorazmernosti, pretehta obstoječe nasprotne interese.

1.3.6 Varstvo osebnih podatkov in gospodarski interesi

V digitalni dobi ali dobi masovnih podatkov so podatki opisani kot „nova nafta" gospodarstva za spodbujanje inovativnosti in ustvarjalnosti.[130] Številna podjetja so vzpostavila trdne poslovne modele, ki temeljijo na obdelavi podatkov, pri čemer taka obdelava pogosto vključuje osebne podatke. Nekatera podjetja morda menijo, da bi lahko posamezna pravila v zvezi z varstvom osebnih podatkov v praksi privedla do pretirano obremenjujočih obveznosti, ki bi lahko vplivale na njihove gospodarske interese. Zato se poraja vprašanje, ali bi bilo mogoče z gospodarskimi interesi upravljavcev in obdelovalcev ali širše javnosti upravičiti omejitev pravice do varstva osebnih podatkov.

Primer: SEU je v sodbi v zadevi *Google Spain*[131] odločilo, da imajo posamezniki pod določenimi pogoji pravico zahtevati, da iskalniki odstranijo zadetke iskanja s seznama zadetkov. V obrazložitvi je opozorilo na dejstvo, da je mogoče z uporabo iskalnikov in seznama zadetkov iskanja sestaviti podroben profil posameznika. Te informacije se lahko z več vidikov nanašajo na zasebno življenje posameznika in jih brez iskalnika ne bi bilo mogoče zlahka najti ali povezati. Zadevna obdelava podatkov je zato pomenila potencialno resno poseganje v temeljni pravici posameznikov, na katere se nanašajo osebni podatki, do zasebnosti in varstva osebnih podatkov.

SEU je nato proučilo, ali bi poseganje lahko bilo upravičeno. V zvezi z gospodarskim interesom upravljavca iskalnika pri obdelavi je navedlo, da poseganje „ne more biti upravičeno zgolj zaradi gospodarskega interesa, ki ga ima upravljavec iskalnika pri tej obdelavi", ter da temeljne pravice v smislu

130 Glej na primer *Financial Times* (2016), „Data is the new oil... who's going to own it?" (Podatki so nova nafta ... Kdo si jih bo lastil?), 16. november 2016.

131 SEU, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), C-131/12, 13. maj 2014.

členov 7 in 8 Listine „na splošno“ prevladajo nad takim gospodarskim interesom in interesom širše javnosti, da navedeno informacijo najde z iskanjem na podlagi imena posameznika, na katerega se nanašajo osebni podatki.[132]

Eden od ključnih vidikov zakonodaje EU o varstvu podatkov je posameznikom zagotoviti večji nadzor nad njihovimi osebnimi podatki. Za digitalno dobo je značilno neravnovesje med močjo gospodarskih subjektov, ki obdelujejo velike količine osebnih podatkov in imajo dostop do njih, in zmožnostjo posameznikov, ki jim ti osebni podatki pripadajo, da svoje informacije nadzorujejo. SEU pri usklajevanju varstva osebnih podatkov in gospodarskih interesov, kot so interesi tretjih oseb v zvezi z delniškimi družbami in družbami z omejeno odgovornostjo, obravnava vsak primer posebej, kot je razvidno iz sodbe v zadevi *Manni*.

Primer: zadeva *Manni*[133] se je nanašala na vključitev osebnih podatkov posameznika v javni register družb. S. Manni je zahteval, naj gospodarska zbornica v Lecceju izbriše njegove osebne podatke iz navedenega registra, saj je ugotovil, da je potencialnim strankam iz registra razvidno, da je bil upravitelj družbe, zoper katero je bil pred več kot desetimi leti uveden stečajni postopek. Zaradi teh informacij so si potencialne stranke oblikovale predsodke, kar bi lahko negativno vplivalo na njegove poslovne interese.

SEU je bilo zaprošeno, naj odloči, ali je v tem primeru v pravu EU priznana pravica do izbrisa. Pri sprejemanju odločitve je pravila EU o varstvu osebnih podatkov in poslovni interes S. Mannija za izbris informacij o stečaju njegovega nekdanjega podjetja uravnotežilo z javnim interesom za dostop do teh informacij. Ustrezno je upoštevalo dejstvo, da je objava v javnem registru družb določena z zakonom, zlasti z direktivo EU, katere cilj je zagotavljati lažji dostop tretjih oseb do informacij o družbah. Objava je bila pomembna za varovanje interesov tretjih oseb, ki morda želijo poslovati s posamezno družbo, saj je edino jamstvo, ki ga delniške družbe in družbe z omejeno odgovornostjo zagotavljajo tretjim osebam, njihovo premoženje. Zato „mora objava tretjim osebam omogočati, da se seznanijo z osnovnimi dokumenti zadevne družbe in drugimi informacijami v zvezi z družbo, zlasti s podatki o osebah, ki so pooblaščene za zastopanje in sprejemanje obveznosti v imenu družbe“.[134]

132 Prav tam, točki 81 in 97.

133 SEU, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju*, C-398/15, 9. marec 2017.

134 Prav tam, točka 49.

Glede na pomen zakonitega cilja, ki se uresničuje z registrom, je SEU menilo, da S. Manni nima pravice doseči izbrisa svojih osebnih podatkov, saj potreba po zaščiti interesov tretjih oseb v razmerju do delniških družb in družb z omejeno odgovornostjo ter po zagotovitvi pravne varnosti, poštenih poslovnih transakcij in pravilnega delovanja notranjega trga prevlada nad njegovimi pravicami v skladu z zakonodajo o varstvu osebnih podatkov. To še zlasti velja, ker se posamezniki, ki se odločijo, da bodo sodelovali pri gospodarski izmenjavi prek delniške družbe ali družbe z omejeno odgovornostjo, zavedajo, da so zavezani objaviti podatke v zvezi s svojo identiteto in funkcijami v tej družbi.

Čeprav je SEU ugotovilo, da v tem primeru ni razlogov za dosego izbrisa, je priznalo obstoj pravice do ugovora obdelavi, pri čemer je navedlo, da „ni mogoče izključiti, da lahko pride do posebnih položajev, v katerih je iz zakonitih in nujnih razlogov, povezanih s konkretnim primerom zadevne osebe, izjemoma upravičeno, da je dostop do osebnih podatkov, ki se nanašajo nanjo in so vpisani v register, ko preteče dovolj časa [...], omejen na tretje osebe, ki izkažejo poseben interes za vpogled v te podatke“.[135]

SEU je navedlo, da morajo nacionalna sodišča na podlagi vseh upoštevnih okoliščin posameznika za vsak primer posebej presoditi, ali obstajajo zakoniti in nujni razlogi, na podlagi katerih bi lahko bilo izjemoma upravičeno, da se omeji dostop tretjih oseb do osebnih podatkov v registru družb. Vendar je pojasnilo, da v primeru S. Mannija samega dejstva, da razkritje njegovih osebnih podatkov v registru domnevno vpliva na njegove stranke, ni mogoče šteti za tak zakonit in nujen razlog. Njegove potencialne stranke imajo zakonit interes, da razpolagajo z informacijami o stečaju njegovega prejšnjega podjetja.

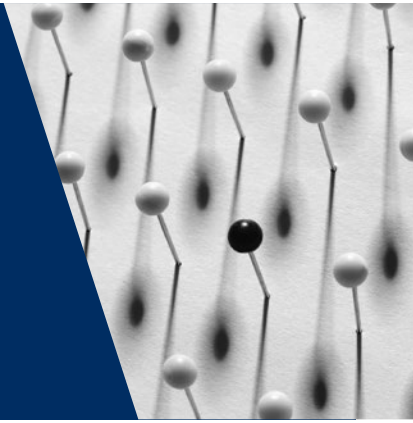
Poseganje v temeljni pravici S. Mannija in drugih oseb, vključenih v register, do spoštovanja zasebnega življenja in varstva osebnih podatkov, zagotovljeni s členoma 7 in 8 Listine, je bilo v splošnem interesu ter potrebno in sorazmerno.

SEU je zato v zadevi *Manni* odločilo, da pravici do varstva osebnih podatkov in zasebnosti ne prevladata nad interesom tretjih oseb za dostop do informacij v registru družb v zvezi z delniškimi družbami in družbami z omejeno odgovornostjo.

135 Prav tam, točka 60.

2

Izrazi s področja varstva osebnih podatkov



EU	Obravnavane teme	Svet Evrope
Osebni podatki		
SUVP, člen 4(1) SUVP, člen 4(5) in člen 5(1)(e) SUVP, člen 9 SEU, združeni zadevi C-92/09 in C-93/09, *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*(veliki senat), 2010 SEU, C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU* (veliki senat), 2008 SEU, C-70/10, *Scarlet Extended SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 SEU, C-582/14, *Patrick Breyer proti Bundesrepublik Deutschland*, 2016 SEU, združeni zadevi C-141/12 in C-372/12, *YS proti Minister voor Immigratie, Integratie en Asiel in Minister voor Immigratie, Integratie en Asiel proti M in S*, 2014	**Pravna opredelitev varstva osebnih podatkov**	Posodobljena Konvencija št. 108, člen 2(a) ESČP, *Bernh Larsen Holding AS in drugi proti Norveški*, pritožba št. 24117/08, 2013 ESČP, *Uzun proti Nemčiji*, pritožba št. 35623/05, 2010 ESČP, *Amann proti Švici* (veliki senat), pritožba št. 27798/95, 2000
SEU, C-101/01, *Kazenski postopek proti Bodil Lindqvist*, 2003	**Posebne kategorije osebnih podatkov (občutljivi podatki)**	Posodobljena Konvencija št. 108, člen 6(1)

EU	Obravnavane teme	Svet Evrope
SEU, C-434/16, *Peter Nowak proti Data Protection Commissioner*, 2017	Anonimizirani in psevdonimizirani osebni podatki	Posodobljena Konvencija št. 108, člen 5(4)(e) Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 50
Obdelava osebnih podatkov		
SUVP, člen 4(2) SEU, C-212/13, *František Ryneš proti Úřad pro ochranu osobních údajů*, 2014 SEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju*, 2017 SEU, C-101/01, *Kazenski postopek proti Bodil Lindqvist*, 2003 SEU, C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), 2014	Opredelitev pojmov	Posodobljena Konvencija št. 108, člen 2(b) in (c)
Uporabniki osebnih podatkov		
SUVP, člen 4(7) SEU, C-212/13, *František Ryneš proti Úřad pro ochranu osobních údajů*, 2014 SEU, C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), 2014	Upravljavec	Posodobljena Konvencija 108, člen 2(d) Priporočilo o oblikovanju profilov, člen 1(g)*
SUVP, člen 4(8)	Obdelovalec	Posodobljena Konvencija št. 108, člen 2(f) Priporočilo o oblikovanju profilov, člen 1(h)
SUVP, člen 4(9)	Uporabnik	Posodobljena Konvencija št. 108, člen 2(e)
SUVP, člen 4(10)	Tretja oseba	
Privolitev		
SUVP, člen 4(11) in člen 7 SEU, C-543/09, *Deutsche Telekom AG proti Bundesrepublik Deutschland*, 2011 SEU, C-536/15, *Tele2 (Netherlands) BV in drugi proti Autoriteit Consument en Markt (ACM)*, 2017	Opredelitev in zahteve za veljavno privolitev	Posodobljena Konvencija št. 108, člen 5(2) Priporočilo o zdravstvenih podatkih, člen 6, in različna poznejša priporočila ESČP, *Elberte proti Latviji*, pritožba št. 61243/08, 2015

*Opomba: *Svet Evrope, Odbor ministrov, Priporočilo Rec(2010)13 državam članicam o varstvu posameznikov v zvezi z avtomatsko obdelavo osebnih podatkov pri oblikovanju profilov (priporočilo o oblikovanju profilov), 2010.*

2.1 Osebni podatki

Ključni poudarki

- Podatki so osebni, če se nanašajo na določeno ali določljivo osebo, to je posameznika, na katerega se nanašajo osebni podatki.
- Pri ugotavljanju, ali je posameznik določljiv, bi bilo treba upoštevati vsa sredstva – kot je na primer izločitev –, za katera se razumno pričakuje, da jih bo upravljavec ali druga oseba uporabila za neposredno ali posredno identifikacijo posameznika.
- Avtentikacija pomeni dokazati, da ima določena oseba določeno istovetnost in/ali da je pooblaščena za izvajanje nekaterih dejavnosti.
- V posodobljeni Konvenciji št. 108 in pravu EU o varstvu osebnih podatkov so navedene posebne kategorije podatkov, t. i. občutljivi osebni podatki, za katere se zahteva okrepljeno varstvo, zato zanje velja posebna pravna ureditev.
- Podatki so anonimizirani, če se ne nanašajo več na določenega ali določljivega posameznika.
- Psevdonimizacija je ukrep, s katerim osebnih podatkov ni mogoče pripisati posamezniku, na katerega se nanašajo, brez dodatnih informacij, ki se hranijo ločeno. Ključ, ki omogoča ponovno identifikacijo posameznikov, na katere se nanašajo osebni podatki, je treba hraniti ločeno in na varnem. Psevdonimizirani podatki so še vedno osebni podatki. V pravu EU se pojem psevdonimizirani podatki ne uporablja.
- Načela in pravila o varstvu osebnih podatkov se ne uporabljajo v zvezi z anonimiziranimi podatki, uporabljajo pa se za psevdonimizirane podatke.

2.1.1 Glavni vidiki pojma osebnih podatkov

V pravu EU in **pravu Sveta Evrope** so osebni podatki opredeljeni kot informacije v zvezi z določenim ali določljivim posameznikom.[136] Nanašajo se na informacije o osebi, katere istovetnost je bodisi očitna bodisi jo je mogoče vsaj ugotoviti na podlagi dodatnih informacij. Pri ugotavljanju, ali je posameznik določljiv, bi bilo treba upoštevati vsa sredstva – kot je na primer izločitev –, za katera se razumno pričakuje, da jih bo upravljavec ali druga oseba uporabila za neposredno ali posredno identifikacijo posameznika, na podlagi katere lahko neko osebo obravnava drugače od drugih.[137]

136 SUVP, člen 4(1); posodobljena Konvencija št. 108, člen 2(a).

137 SUVP, uvodna izjava 26.

Če se obdelujejo podatki o taki osebi, se ta oseba imenuje „posameznik, na katerega se nanašajo osebni podatki“.

Posameznik, na katerega se nanašajo osebni podatki

V skladu s pravom EU so posamezniki edini upravičenci do varstva osebnih podatkov[138], z evropskim pravom o varstvu osebnih podatkov pa so zaščitene le žive osebe.[139] V SUVP so osebni podatki opredeljeni kot katera koli informacija v zvezi z določenim ali določljivim posameznikom.

Tudi **pravo Sveta Evrope**, zlasti posodobljena Konvencija št. 108, vključuje sklicevanje na varstvo posameznikov pri obdelavi njihovih osebnih podatkov. Tudi v njej izraz osebni podatki pomeni vse informacije, ki se nanašajo na določenega ali določljivega posameznika. Ta posameznik, kot je opredeljen v SUVP in posodobljeni Konvenciji št. 108, se v pravu o varstvu osebnih podatkov imenuje posameznik, na katerega se nanašajo osebni podatki.

Nekaj varstva se zagotavlja tudi pravnim osebam. Sodna praksa ESČP vključuje sodbe o pritožbah pravnih oseb, ki so trdile, da so jim bile kršene pravice do varstva pred uporabo njihovih osebnih podatkov na podlagi člena 8 EKČP. Člen 8 EKČP zajema pravico do spoštovanja zasebnega in družinskega življenja ter do doma in dopisovanja. Sodišče lahko zato zadeve prouči na podlagi pravice do spoštovanja doma in dopisovanja, ne more pa jih obravnavati na podlagi pravice do zasebnega življenja.

Primer: zadeva *Bernh Larsen Holding AS in drugi proti Norveški*[140] se je nanašala na pritožbo, ki so jo tri norveška podjetja vložila v zvezi z odločbo davčnega organa, s katero jim je bilo naloženo, da morajo davčnim revizorjem predložiti kopijo vseh podatkov na računalniškem strežniku, ki so ga uporabljala skupaj.

138 Prav tam, člen 1.

139 Prav tam, uvodna izjava 27. Glej tudi Delovna skupina za varstvo podatkov iz člena 29, *Mnenje 4/2007 o pojmu osebnih podatkov*, WP 136, 20. junij 2007, str. 22.

140 ESČP, *Bernh Larsen Holding AS in drugi proti Norveški*, pritožba št. 24117/08, 14. marec 2013. Glej tudi ESČP, *Liberty in drugi proti Združenemu kraljestvu*, pritožba št. 58243/00, 1. julij 2008.

ESČP je ugotovilo, da obveznost, naložena tožečim podjetjem, pomeni poseganje v njihovi pravici do spoštovanja doma in dopisovanja na podlagi člena 8 EKČP. Vendar je Sodišče ugotovilo tudi, da so imeli davčni organi učinkovite in ustrezne zaščitne ukrepe pred zlorabami: tožeča podjetja so bila obveščena dovolj zgodaj; navzoča so bila med posredovanjem na kraju samem in so lahko izrazila stališča, gradivo pa naj bi se po končani davčni reviziji uničilo. V takih okoliščinah je bilo doseženo pravično ravnovesje med pravico tožečih podjetij do spoštovanja doma in dopisovanja ter njihovim interesom za varovanje zasebnosti zaposlenih na eni strani in javnim interesom za zagotovitev učinkovitega pregleda zaradi davčne revizije na drugi strani. Sodišče je ugotovilo, da člen 8 EKČP ni bil kršen.

Varstvo osebnih podatkov se **v skladu s posodobljeno Konvencijo št. 108** nanaša predvsem na varstvo fizičnih oseb, vendar lahko pogodbenice varstvo osebnih podatkov v svojem nacionalnem pravu razširijo tudi na pravne osebe, kot so podjetja in združenja. V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je navedeno, da se lahko v nacionalnem pravu zaščitijo zakoniti interesi pravnih oseb z razširitvijo področja uporabe konvencije na take akterje.[141] **Pravo EU o varstvu osebnih podatkov** ne zajema obdelave osebnih podatkov, ki se nanašajo na pravne osebe, in zlasti ne zadeva podjetij, ki so ustanovljena kot pravne osebe, vključno z imenom in obliko pravne osebe in njenimi kontaktnimi podatki.[142] Vendar se z Direktivo o zasebnosti in elektronskih komunikacijah varujejo zaupnost komunikacij in zakoniti interesi pravnih oseb v zvezi s čedalje večjo zmogljivostjo samodejnega shranjevanja in obdelave osebnih podatkov, ki se nanašajo na naročnike in uporabnike.[143] Podobno je tudi v osnutku uredbe o zasebnosti in elektronskih komunikacijah varstvo razširjeno na pravne osebe.

Primer: SEU je v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*[144] s sklicevanjem na objavo osebnih podatkov o upravičencih do kmetijske pomoči razsodilo, da se lahko „pravne osebe v zvezi s takim poimenskim navajanjem [...] sklicujejo na varstvo iz členov 7 in 8 Listine le, če je iz imena pravne osebe razvidna ena ali več fizičnih oseb.

141 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 30.

142 SUVP, uvodna izjava 14.

143 Direktiva o zasebnosti in elektronskih komunikacijah, uvodna izjava 7 in člen 1(2).

144 SEU, *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen* (veliki senat), združeni zadevi C-92/09 in C-93/09, 9. november 2010, točka 53.

[...] [S]poštovanje pravice do zasebnega življenja v zvezi z obravnavo osebnih podatkov, ki jo določata člena 7 in 8 Listine, [se] nanaša na vsako informacijo o določeni ali določljivi fizični osebi [...].“[145]

SEU je z uravnoteženjem interesa EU za zagotavljanje preglednosti pri dodeljevanju pomoči na eni strani ter temeljnih pravic do zasebnosti in varstva osebnih podatkov posameznikov, ki so prejeli pomoč, na drugi strani ugotovilo, da je poseganje v ti temeljni pravici nesorazmerno. Menilo je, da bi bilo mogoče cilj glede preglednosti učinkovito doseči z ukrepi, ki manj posegajo v pravice zadevnih posameznikov. Ko pa je proučevalo sorazmernost objave informacij o pravnih osebah, ki so prejele pomoč, pa je prišlo do drugačne ugotovitve in odločilo, da taka objava ne presega meja načela sorazmernosti. Navedlo je, da je „[t]eža kršitve pravice do varstva osebnih podatkov [...] namreč pri pravnih osebah drugačna kot pri fizičnih osebah“.[146] Pri pravnih osebah so obveznosti glede objave podatkov, ki se nanašajo nanje, velike. SEU je menilo, da bi obveznost nacionalnih organov, da pred objavo podatkov za vsako pravno osebo upravičenko preverijo, ali njeni podatki označujejo katero koli povezano fizično osebo, zanje pomenila nerazumno upravno breme. Zato je z zakonodajo, v skladu s katero se zahteva splošna objava podatkov o pravnih osebah, vzpostavljeno pravično ravnovesje med zadevnimi nasprotujočimi si interesi.

Vrsta podatkov

Osebni podatek je lahko kakršna koli vrsta informacije, če se nanaša na določeno ali določljivo osebo.

Primer: ocena delovne uspešnosti zaposlenega, ki jo izvede nadrejeni in je shranjena v osebnem spisu zaposlenega, je osebni podatek o zaposlenem. To velja, čeprav lahko deloma ali v celoti izraža samo osebno mnenje nadrejenega, na primer: „zaposleni ni predan svojemu delu“, ne pa neizpodbitnih dejstev, na primer: „zaposleni je bil v zadnjih šestih mesecih pet tednov odsoten z dela“.

145 Prav tam, točki 52 in 53.

146 Prav tam, točka 87.

Osebni podatki vključujejo informacije, ki se nanašajo na zasebno življenje osebe, kar vključuje tudi poklicne dejavnosti, in informacije o njenem javnem življenju.

ESČP je v zadevi *Amann*[147] pojem osebni podatki razlagalo, kot da ni omejen na zadeve iz zasebnega življenja posameznika. Ta pomen pojma osebni podatki je pomemben tudi za SUVP.

Primer: SEU je v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*[148] navedlo, da „[v] zvezi s tem dejstvo, da se objavljeni podatki nanašajo na poklicne dejavnosti, ni pomembno [...]. Evropsko sodišče za človekove pravice je ob razlagi člena 8 EKČP v zvezi s tem presodilo, da se pojem ‚zasebnost' ne sme razlagati restriktivno in da ‚načeloma poklicnih dejavnosti ni mogoče izključiti [...] iz pojma ‚zasebnosti''."

Primer: SEU je v združenih zadevah *YS proti Minister voor Immigratie, Integratie en Asiel* in *Minister voor Immigratie, Integratie en Asiel proti M in S*[149] navedlo, da pravna analiza iz predloga odločbe službe za priseljevanje in naturalizacijo, ki obravnava prošnje za izdajo dovoljenja za prebivanje, sama po sebi ni osebni podatek, čeprav lahko vsebuje nekatere osebne podatke.

V sodni praksi ESČP o členu 8 EKČP je potrjeno, da je včasih težko popolnoma razlikovati med zadevami zasebnega in poklicnega življenja.[150]

Primer: v zadevi *Bărbulescu proti Romuniji*[151] je bil pritožnik odpuščen, ker je v nasprotju z internimi pravili med delovnim časom uporabljal delodajalčev internet. Delodajalec je nadzoroval njegovo komunikacijo, pri čemer je bila v nacionalnem postopku predložena evidenca komunikacije, v kateri so bila povsem zasebna sporočila. ESČP, ki je ugotovilo, da zadeva spada na področje uporabe člena 8 EKČP, ni odgovorilo na vprašanje, ali so omejevalni predpisi delodajalca pritožniku dopuščali primerno raven zasebnosti, vsekakor pa je

147 Glej ESČP, *Amann proti Švici* (veliki senat), pritožba št. 27798/95, 16. februar 2000, točka 65.

148 SEU, *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen* (veliki senat), združeni zadevi C-92/09 in C-93/09, 9. november 2010, točka 59.

149 SEU, *YS proti Minister voor Immigratie, Integratie en Asiel* in *Minister voor Immigratie, Integratie en Asiel proti M in S*, združeni zadevi C-141/12 in C-372/12, 17. julij 2014, točka 39.

150 Glej na primer ESČP, *Rotaru proti Romuniji* (veliki senat), pritožba št. 28341/95, 4. maj 2000, točka 43, in ESČP, *Niemietz proti Nemčiji*, pritožba št. 13710/88, 16. december 1992, točka 29.

151 ESČP, *Bărbulescu proti Romuniji* (veliki senat), pritožba št. 61496/08, 5. september 2017, točka 121.

ugotovilo, da navodila delodajalca ne morejo povsem prepovedati zasebnega družbenega življenja na delovnem mestu. Kar zadeva vsebino zadeve, je bilo treba pogodbenicam podeliti široko polje proste presoje pri ocenjevanju potrebe po vzpostavitvi pravnega okvira, ki bi urejal pogoje, v katerih bi lahko delodajalec urejal nepoklicno komunikacijo zaposlenih – elektronsko ali drugo – na delovnem mestu. Kljub temu bi morali nacionalni organi zagotoviti, da ukrepe za nadzor dopisovanja in drugih oblik komunikacije, ki jih uvede delodajalec, in sicer ne glede na njihov obseg in trajanje, spremljajo ustrezni in zadostni zaščitni ukrepi pred zlorabo. Načelo sorazmernosti in procesna jamstva, ki preprečujejo samovoljnost, so bistvena, pri čemer je ESČP opredelilo več dejavnikov, ki bi jih bilo treba upoštevati v okoliščinah obravnavane zadeve. Ti dejavniki so se med drugim nanašali na obseg nadzora, ki ga je uvedel delodajalec, in stopnjo posega v zasebnost delavca, posledice nadzora za zaposlenega ter to, ali so bili sprejeti ustrezni zaščitni ukrepi. Poleg tega bi morali nacionalni organi zagotoviti, da ima delavec, čigar komunikacija se je nadzirala, dostop do pravnega sredstva pred sodnim organom, ki je pristojen, da vsaj vsebinsko odloča, kako so bila upoštevana navedena merila in ali so bili izpodbijani ukrepi zakoniti. ESČP je v tem primeru ugotovilo kršitev člena 8 EKČP, saj nacionalni organi niso zagotovili ustreznega varstva pritožnikove pravice do spoštovanja zasebnega življenja in dopisovanja ter posledično niso vzpostavili pravičnega ravnotežja med zadevnimi interesi.

V skladu s pravom EU in **pravom Sveta Evrope** informacije vsebujejo podatke o osebi, če je:

- posameznik v teh informacijah določen ali je z njimi določljiv ali
- mogoče posameznika, ki sicer ni določen, s temi informacijami izločiti tako, da je mogoče z dodatnim raziskovanjem ugotoviti, kdo je posameznik, na katerega se nanašajo osebni podatki.

Obe vrsti informacij sta z evropskim pravom o varstvu osebnih podatkov varovani enako. Za neposredno ali posredno določljivost posameznikov je potrebno stalno ocenjevanje, pri čemer je treba „upoštevati razpoložljivo tehnologijo in tehnološki razvoj v času obdelave“.[152] ESČP je večkrat navedlo, da je pojem osebni podatki

152 SUVP, uvodna izjava 26.

v okviru EKČP enak kot v Konvenciji št. 108, zlasti v zvezi s pogojem, da se podatki nanašajo na določene ali določljive osebe.[153]

SUVP določa, da je določljiv posameznik tisti, ki „ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika".[154] Za določitev so torej potrebni elementi, s katerimi je oseba opisana tako, da jo je mogoče razlikovati od vseh drugih oseb in je prepoznavna kot posameznik. Dober primer takega opisnega elementa je ime osebe, s katerim lahko neposredno določimo osebo. V nekaterih primerih imajo lahko tudi drugi atributi podoben učinek kot ime, zaradi katerih je oseba posredno določljiva. Telefonska številka, številka socialnega zavarovanja in registrska številka vozila so primeri informacij, na podlagi katerih je posameznik določljiv. Poleg tega je atribute, kot so računalniške datoteke, piškotki in orodja za nadzor spletnega prometa, mogoče uporabiti za izločitev posameznikov na podlagi določitve njihovega vedenja in navad. Kot je pojasnjeno v mnenju Delovne skupine iz člena 29, „[n]e da bi nas sploh zanimala ime in naslov posameznika, je mogoče razvrstiti to osebo na podlagi socio-ekonomskih, psiholoških, filozofskih ali drugih meril in ji pripisati določene odločitve, saj njena stična točka (računalnik) ne zahteva več nujno razkritja njene identitete v ožjem smislu".[155] Opredelitev osebnih podatkov v pravu Sveta Evrope in pravu EU je dovolj široka, da zajema vse možnosti identifikacije (in zato vse stopnje določljivosti).

Primer: SEU je v zadevi *Promusicae proti Telefónica de España*[156] navedlo, da „ni sporno, da posredovanje imen in naslovov določenih uporabnikov [določene spletne platforme za izmenjavo datotek] [...] vključuje uporabo osebnih podatkov, to je podatkov o določenih ali določljivih fizičnih osebah, v skladu z opredelitvijo iz člena 2(a) Direktive 95/46 [zdaj člen 4(1) SUVP] [...]. To posredovanje informacij, ki so po mnenju Promusicae shranjene pri Telefónica – čemur slednja ne ugovarja –, pomeni obdelavo osebnih podatkov [...]."[157]

153 Glej ESČP, *Amann proti Švici* (veliki senat), pritožba št. 27798/95, 16. februar 2000, točka 65.

154 SUVP, člen 4(1).

155 Delovna skupina za varstvo podatkov iz člena 29, *Mnenje 4/2007 o pojmu osebnih podatkov*, WP 136, 20. junij 2007, str. 13.

156 SEU, *Productores de Música de España (Promusicae) proti Telefónica de España SAU* (veliki senat), C-275/06, 29. januar 2008, točka 45.

157 Prej Direktiva 95/46/ES, člen 2(b), zdaj SUVP, člen 4(2).

Primer: zadeva *Scarlet Extended SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] se je nanašala na zavrnitev ponudnika internetnih storitev Scarlet, da namesti sistem za filtriranje elektronskih komunikacij v obliki programske opreme za izmenjavo datotek, katerega namen je preprečiti izmenjavo datotek, ki pomeni kršitev avtorske pravice, ki jo nadzira SABAM, družba za upravljanje, ki zastopa avtorje, skladatelje in založnike glasbenih del. SEU je odločilo, da so IP-naslovi uporabnikov „varovani osebni podatki, saj omogočajo natančno identifikacijo teh uporabnikov".

Ker veliko imen ni unikatnih, so lahko za ugotovitev istovetnosti osebe potrebni dodatni atributi, da osebe ne bi zamenjali s kom drugim. Za identifikacijo posameznika, na katerega se nanašajo osebni podatki, je včasih treba združiti neposredne in posredne atribute. Pogosto se uporabljata datum in kraj rojstva. Poleg tega so bile za boljše razlikovanje med državljani v nekaterih državah uvedene osebne identifikacijske številke. Osebni podatki so lahko preneseni davčni podatki,[159] podatki o prosilcu za dovoljenje za prebivanje, vsebovani v upravnem dokumentu,[160] ter dokumenti v zvezi z bančnimi in fiduciarnimi razmerji[161]. Biometrični podatki, na primer prstni odtisi, digitalne fotografije ali slike šarenice, podatki o lokaciji in spletni atributi se v tehnološki dobi vse bolj uporabljajo za identifikacijo oseb.

Vendar za uporabo evropskega prava o varstvu osebnih podatkov ni potrebna dejanska identifikacija osebe, na katero se nanašajo osebni podatki; zadostuje že, da je zadevna oseba določljiva. Oseba se šteje za določljivo, če je na voljo dovolj elementov, na podlagi katerih je mogoče osebo neposredno ali posredno identificirati.[162] V skladu z uvodno izjavo 26 SUVP je odločilnega pomena, ali se pričakuje, da bodo imeli predvidljivi uporabniki informacij na voljo sredstva za identifikacijo in bodo ta sredstva uporabili, to vključuje informacije, ki jih hranijo tretji uporabniki (glej razdelek 2.3.2).

158 SEU, *Scarlet Extended SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, 24. november 2011, točka 51.

159 SEU, *Smaranda Bara in drugi proti Președintele Casei Naționale de Asigurări de Sănătate in drugim*, C-201/14, 1. oktobra 2015.

160 SEU, *YS proti Minister voor Immigratie, Integratie en Asiel* in *Minister voor Immigratie, Integratie en Asiel proti M in S*, združeni zadevi C-141/12 in C-372/12, 17. julij 2014.

161 ESČP, *M. N. in drugi proti San Marinu*, pritožba št. 28005/12, 7. julij 2015.

162 SUVP, člen 4(1).

Primer: lokalni organ se odloči, da bo zbiral podatke o avtomobilih, ki po lokalnih cestah vozijo prehitro. Avtomobile fotografira, s čimer se samodejno zabeležita čas in kraj, nato pa podatke posreduje pristojnemu organu, da lahko oglobi vse, ki so prekoračili omejitev hitrosti. Posameznik, na katerega se nanašajo osebni podatki, vloži pritožbo, v kateri trdi, da lokalni organ za tako zbiranje podatkov nima pravne podlage v zakonodaji o varstvu osebnih podatkov. Lokalni organ trdi, da ne zbira osebnih podatkov. Registrske tablice so po njegovem mnenju anonimne. Lokalni organ nima zakonske pristojnosti za dostop do splošnega registra vozil, da bi ugotovil identiteto lastnika vozila ali voznika.

Ta obrazložitev ni v skladu z uvodno izjavo 26 SUVP. Ker je očitni namen zbiranja podatkov ugotoviti identiteto prehitrih voznikov in jih oglobiti, je mogoče predvideti, da se jih bo poskušalo identificirati. Čeprav lokalni organi nimajo neposredno na voljo sredstev za identifikacijo, bodo podatke posredovali pristojnemu organu, tj. policiji, ki taka sredstva ima. V uvodni izjavi 26 je izrecno predviden scenarij, po katerem lahko tudi nadaljnji uporabniki podatkov in ne samo njihovi neposredni uporabniki poskušajo ugotoviti identiteto posameznika. V skladu z uvodno izjavo 26 je dejanje lokalnega organa zbiranje podatkov o določljivih osebah, zato je potrebna pravna podlaga v zakonodaji o varstvu podatkov.

Da „bi ugotovili, ali se za ta sredstva lahko razumno pričakuje, da bodo uporabljena za identifikacijo posameznika, bi bilo treba upoštevati vse objektivne dejavnike, kot so stroški identifikacije in čas, potreben zanjo, ter pri tem upoštevati razpoložljivo tehnologijo in tehnološki razvoj v času obdelave“.[163]

Primer: SEU je v zadevi *Breyer proti Bundesrepublik Deutschland*[164] obravnavalo pojem posredne določljivosti posameznikov, na katere se nanašajo osebni podatki. Zadeva se je nanašala na dinamične IP-naslove, tj. naslove, ki se spreminjajo ob vsaki povezavi z internetom. Na spletiščih nemških zveznih služb so se evidentirali in hranili dinamični IP-naslovi za preprečevanje kibernetskih napadov in sprožitev kazenskega postopka, če bi to bilo potrebno. Le ponudnik internetnih storitev, ki ga je uporabljal P. Breyer, je imel dodatne informacije, potrebne za njegovo identifikacijo.

163 Prav tam, uvodna izjava 26.

164 SEU, *Patrick Breyer proti Bundesrepublik Deutschland*, C-582/14, 19. oktober 2016, točki 47 in 48.

SEU je menilo, da dinamični IP-naslov, ki ga ponudnik storitev spletnih medijev zabeleži ob dostopu neke osebe do spletišča, ki ga ta ponudnik daje na voljo javnosti, pomeni osebni podatek, pri čemer ima le tretja oseba – v tem primeru ponudnik internetnih storitev – dodatne podatke, ki so potrebni za identifikacijo zadevne osebe.[165] Ugotovilo je, da „ni nujno, da se vse informacije, ki omogočajo identifikacijo posameznika, na katerega se nanašajo osebni podatki, znajdejo v rokah samo ene osebe", da bi se informacije štele za osebne podatke. Uporabniki dinamičnih IP-naslovov, ki jih je evidentiral ponudnik internetnih storitev, se lahko v nekaterih okoliščinah, na primer v okviru kazenskega postopka v primeru kibernetskih napadov, identificirajo s pomočjo drugih oseb.[166] Kadar ima ponudnik „na voljo pravna sredstva, ki mu omogočajo identifikacijo posameznika, na katerega se nanašajo osebni podatki, z dodatnimi informacijami, ki jih ima na voljo ponudnik [internetnih storitev] tega posameznika", to pomeni „sredstvo, za katero se razumno pričakuje, da se bo uporabilo za identifikacijo posameznika, na katerega se nanašajo osebni podatki", je menilo SEU. Taki podatki se zato štejejo za osebne podatke.

V okviru prava Sveta Evrope se določljivost razume podobno. Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108 vključuje podoben opis: pojem določljiv se ne nanaša le na posameznikovo civilno ali pravno identiteto kot tako, temveč tudi na tisto, na podlagi česar bi bilo neko osebo mogoče individualizirati ali izločiti od drugih oseb in jo posledično morda drugače obravnavati. Ta individualizacija bi se lahko na primer izvedla z izrecnim sklicevanjem na osebo ali na napravo oziroma kombinacijo naprav (računalnik, mobilni telefon, fotoaparat, igralne naprave itd.) na podlagi identifikacijske številke, psevdonima, biometričnih ali genskih podatkov, podatkov o lokaciji, IP-naslova ali drugega identifikatorja.[167] Posameznik se ne šteje za določljivega, če je za njegovo identifikacijo potrebnega nerazumno veliko časa, napora ali sredstev. To bi na primer veljalo, kadar bi bili za identifikacijo posameznika, na katerega se nanašajo osebni podatki, potrebni preveč zapleteni, dolgotrajni in dragi postopki. O tem, ali je potrebnega nerazumno veliko časa, napora ali sredstev, je treba presojati za vsak primer posebej, pri čemer se upoštevajo dejavniki, kot so

165 Prej veljavna Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, člen 2(a).

166 SEU, *Scarlet Extended SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, 24. november 2011, točki 47 in 48.

167 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 18.

namen obdelave, stroški in koristi identifikacije, vrsta upravljavca in uporabljena tehnologija.[168]

Kar zadeva obliko, v kateri se osebni podatki hranijo ali uporabljajo, je treba opozoriti, da ta za uporabo prava o varstvu osebnih podatkov ni pomembna. Osebne podatke lahko vsebujejo pisna ali govorna sporočila in slike[169], vključno s posnetki videonadzornih kamer (CCTV)[170], ali zvok.[171] Tudi elektronsko zabeležene informacije in informacije na papirju so lahko osebni podatki. Celo celični vzorci človeškega tkiva, v katerih je zapisana DNK osebe, so lahko viri, iz katerih je mogoče pridobiti biometrične podatke,[172] če se podatki nanašajo na podedovane ali pridobljene genetske značilnosti posameznika, dajejo edinstvene informacije o njegovem zdravju ali fiziologiji in so rezultat analize biološkega vzorca zadevnega posameznika.[173]

Anonimizacija

V skladu z načelom omejitve hrambe iz SUVP in posodobljene Konvencije št. 108 (ki je podrobneje obravnavano v poglavju 3) je treba osebne podatke hraniti „v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo“.[174] Če bi upravljavec želel hraniti osebne podatke po tem, ko niso več potrebni in ne izpolnjujejo več svojega prvotnega namena, bi jih bilo treba izbrisati ali anonimizirati.

Postopek anonimizacije podatkov pomeni, da so iz niza osebnih podatkov odstranjeni vsi identifikacijski elementi, tako da posameznik, na katerega se nanašajo osebni podatki, ni več določljiv.[175] Delovna skupina iz člena 29 je v Mnenju št. 5/2014

168 Prav tam, točka 17.

169 ESČP, *Von Hannover proti Nemčiji*, pritožba št. 59320/00, 24. junij 2004; ESČP, *Sciacca proti Italiji*, pritožba št. 50774/99, 11. januar 2005, in SEU, *František Ryneš proti Úřad pro ochranu osobních údajů*, C-212/13, 11. december 2014.

170 ESČP, *Peck proti Združenemu kraljestvu*, pritožba št. 44647/98, 28. januar 2003, in ESČP, *Köpke proti Nemčiji*, pritožba št. 420/07, sklep z dne 5. oktobra 2010, in ENVP, *Smernice ENVP za videonadzor*, 2010.

171 ESČP, *P. G. in J. H. proti Združenemu kraljestvu*, pritožba št. 44787/98, 25. september 2001, točki 59 in 60, in ESČP, *Wisse proti Franciji*, pritožba št. 71611/01, 20. december 2005 (francoska jezikovna različica).

172 Glej Delovna skupina za varstvo podatkov iz člena 29 (2007), *Mnenje 4/2007 o pojmu osebnih podatkov*, WP 136, 20. junij 2007, str. 9; Svet Evrope, Priporočilo Rec(2006)4 Odbora ministrov državam članicam o raziskavah bioloških materialov človeškega izvora, 15. marec 2006.

173 SUVP, člen 4(13).

174 Prav tam, člen 5(1)(e); posodobljena Konvencija št. 108, člen 5(4)(e).

175 SUVP, uvodna izjava 26.

analizirala učinkovitost in omejitve različnih anonimizacijskih tehnik.[176] Priznala je potencialno vrednost takih tehnik, vendar je poudarila, da nekatere tehnike ne delujejo nujno v vseh primerih. Da bi našli najboljšo rešitev v danih okoliščinah, bi bilo treba za vsak primer posebej določiti ustrezen postopek anonimizacije. Ne glede na uporabljeno tehniko je treba identifikacijo nepreklicno preprečiti. To pomeni, da v anonimiziranih podatkih ne sme ostati noben element, na podlagi katerega bi bilo mogoče ob razumnem naporu znova ugotoviti identiteto zadevne osebe ali oseb.[177] Tveganje ponovne identifikacije se lahko oceni z upoštevanjem časa, napora ali sredstev, potrebnih glede na naravo podatkov, okvir njihove uporabe, razpoložljive tehnologije, ki so na voljo za ponovno identifikacijo, in povezane stroške.[178]

Ko so osebni podatki uspešno anonimizirani, niso več osebni podatki, zato se zanje ne uporablja več zakonodaja o varstvu osebnih podatkov.

V SUVP je določeno, da oseba ali organizacija, ki upravlja obdelavo osebnih podatkov, ne sme biti zavezana k ohranitvi, pridobitvi ali obdelavi dodatnih informacij, da bi identificirala posameznika, na katerega se nanašajo osebni podatki, samo zaradi zagotavljanja skladnosti z zadevno uredbo. Vendar ima to pravilo pomembno izjemo: kadar koli posameznik, na katerega se nanašajo osebni podatki, upravljavcu za namene uveljavljanja pravic do dostopa, popravka, izbrisa, omejitve obdelave in prenosljivosti podatkov predloži dodatne informacije, ki omogočajo njegovo identifikacijo, postanejo podatki, ki so bili predhodno anonimizirani, spet osebni podatki.[179]

Psevdonimizacija

Osebni podatki vsebujejo atribute, kot so ime, datum rojstva, spol in naslov ali drugi elementi, ki bi lahko privedli do identifikacije. Postopek psevdonimizacije osebnih podatkov pomeni, da se ti atributi nadomestijo s psevdonimom.

V **pravu EU** je psevdonimizacija opredeljena kot „obdelav[a] osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi

176 Delovna skupina za varstvo podatkov iz člena 29 (2014), *Mnenje št. 5/2014 o anonimizacijskih tehnikah*, WP 216, 10. april 2014.

177 SUVP, uvodna izjava 26.

178 Svet Evrope, Posvetovalni odbor po Konvenciji št. 108 (2017), *Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov*, 23. januar 2017, točka 6.2.

179 SUVP, člen 11.

za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku".[180] Psevdonimizirani podatki so v nasprotju z anonimiziranimi podatki še vedno osebni podatki, zato zanje velja zakonodaja o varstvu osebnih podatkov. Psevdonimizacija ni izvzeta iz področja uporabe SUVP, čeprav se lahko z njo zmanjšajo varnostna tveganja za posameznike, na katere se nanašajo osebni podatki.

V SUVP različne uporabe psevdonimizacije štejejo kot ustrezen tehnični ukrep za izboljšanje varstva osebnih podatkov, pri čemer je psevdonimizacija posebej navedena v zvezi z zasnovo in varnostjo obdelave osebnih podatkov.[181] Je tudi ustrezen zaščitni ukrep, ki bi ga bilo mogoče uporabiti za obdelavo osebnih podatkov za namene, ki niso nameni, za katere so bili osebni podatki prvotno zbrani.[182]

Psevdonimizacija v pravni opredelitvi posodobljene Konvencije **Sveta Evrope** št. 108 ni izrecno navedena. Vendar je v pojasnjevalnem poročilu k tej konvenciji jasno navedeno, da „uporaba psevdonima ali katerega koli drugega digitalnega identifikatorja/digitalne identitete ne privede do anonimizacije podatkov, saj je lahko posameznik, na katerega se nanašajo osebni podatki, še vedno določljiv ali individualiziran".[183] Eden od načinov psevdonimizacije osebnih podatkov je šifriranje podatkov. Ko so osebni podatki psevdonimizirani, povezava z identiteto obstaja v obliki psevdonima in ključa za dešifriranje. Brez tega ključa je psevdonimizirane podatke težko razvozlati, vendar je ponovna identifikacija zlahka mogoča za vse, ki imajo pravico uporabljati ta ključ. Zlasti je treba preprečiti, da bi šifrirne ključe uporabljale nepooblaščene osebe. Zato se psevdonimizirani podatki štejejo za osebne podatke, zajete s posodobljeno Konvencijo št. 108.[184]

Avtentikacija

S tem postopkom lahko oseba dokaže, da ima določeno identiteto in/ali da je pooblaščena za izvajanje določenih dejanj, na primer za vstop na varovano območje ali dvig denarja z bančnega računa. Avtentikacijo je mogoče izvesti s primerjavo biometričnih podatkov, na primer fotografije ali prstnih odtisov v potnem listu, s podatki, s katerimi se oseba predstavi na primer med kontrolo priseljevanja,[185] ali

180 Prav tam, člen 4(5).

181 Prav tam, člen 25(1).

182 Prav tam, člen 6(4).

183 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 18.

184 Prav tam.

185 Prav tam, točki 56 in 57.

z zahtevanjem informacij, ki bi jih morala poznati samo oseba z določeno identiteto ali dovoljenjem, na primer osebne identifikacijske številke (PIN) ali gesla, lahko pa tudi z zahtevanjem predložitve določenega predmeta, ki bi ga morala imeti izključno oseba z določeno identiteto ali dovoljenjem, na primer posebne čipne kartice ali ključa bančnega sefa. Poleg gesel ali čipnih kartic so elektronski podpisi – včasih skupaj s številkami PIN – še posebej primeren instrument za identifikacijo in avtentikacijo osebe v elektronskih komunikacijah.

2.1.2 Posebne vrste osebnih podatkov

V okviru **prava EU** in **prava Sveta Evrope** obstajajo posebne vrste osebnih podatkov, ki lahko glede na svojo naravo pomenijo tveganje za posameznike, na katere se nanašajo, zato je zanje potrebno okrepljeno varstvo. Za take podatke velja načelo prepovedi, njihova obdelava pa je zakonita le na podlagi omejenega števila pogojev.

V okviru posodobljene Konvencije št. 108 (člen 6) in SUVP (člen 9) se za občutljive podatke štejejo naslednje vrste podatkov:

- osebni podatki, ki razkrivajo rasno ali etnično poreklo;
- osebni podatki, ki razkrivajo politično mnenje in versko ali drugo prepričanje, vključno s filozofskim;
- osebni podatki, ki razkrivajo članstvo v sindikatu;
- genski in biometrični podatki, ki se obdelujejo za namene identifikacije osebe;
- osebni podatki v zvezi z zdravjem, spolnim življenjem ali spolno usmerjenostjo.

Primer: zadeva *Bodil Lindqvist*[186] se je nanašala na navedbo več oseb na spletni strani, pri čemer je bila njihova prepoznavnost omogočena z navedbo imena ali z drugimi sredstvi, na primer z navedbo telefonske številke ali informacij v zvezi s preživljanjem prostega časa. SEU je navedlo, da „je navedba, da si je oseba poškodovala nogo in je delno odsotna z dela zaradi bolezni, osebni podatek v zvezi z zdravjem".[187]

186 SEU, *Kazenski postopek proti Bodil Lindqvist*, C-101/01, 6. november 2003, točka 51.

187 Prej Direktiva 95/46/ES, člen 8(1), zdaj SUVP, člen 9(1).

Osebni podatki v zvezi s kazenskimi obsodbami in prekrški

V posodobljeni Konvenciji št. 108 so osebni podatki v zvezi s prekrški, kazenskimi postopki in obsodbami ter povezanimi varnostnimi ukrepi uvrščeni na seznam posebnih vrst osebnih podatkov.[188] V okviru SUVP osebni podatki v zvezi s kazenskimi obsodbami in prekrški ali povezanimi varnostnimi ukrepi kot taki niso navedeni na seznamu posebnih vrst osebnih podatkov, vendar so obravnavani v posebnem členu. Člen 10 SUVP določa, da se obdelava takih podatkov izvaja le „pod nadzorom uradnega organa ali če obdelavo dovoljuje pravo Unije ali pravo države članice, ki zagotavlja ustrezne zaščitne ukrepe za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki". Celoviti registri z informacijami o kazenskih obsodbah se lahko po drugi strani vodijo samo pod nadzorom posebnih uradnih organov.[189] V EU je obdelava osebnih podatkov v okviru kazenskega pregona urejena s posebnim pravnim instrumentom, in sicer z Direktivo (EU) 2016/680.[190] V njej so določena posebna pravila za varstvo osebnih podatkov, ki so za pristojne organe zavezujoča, kadar osebne podatke obdelujejo za namene preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj (glej razdelek 8.2.1).

2.2 Obdelava osebnih podatkov

Ključni poudarki

- Pojem obdelava osebnih podatkov se nanaša na vsako dejanje, ki se izvede v zvezi z osebnimi podatki.
- Pojem obdelava zajema avtomatizirano in neavtomatizirano obdelavo.
- V okviru prava EU se obdelava nanaša tudi na ročno obdelavo v strukturiranih zbirkah.
- V okviru prava Sveta Evrope je mogoče pomen izraza obdelava z nacionalnim pravom razširiti tako, da vključuje ročno obdelavo.

188 Posodobljena Konvencija št. 108, člen 6(1).

189 SUVP, člen 10.

190 Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

2.2.1 Pojem obdelave osebnih podatkov

Pojem obdelave osebnih podatkov je **po pravu EU in po pravu Sveta Evrope** izčrpen: „‚obdelava [osebnih podatkov]' pomeni vsako dejanje [...], kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje"[191] osebnih podatkov. S posodobljeno Konvencijo št. 108 je bila v opredelitev zadevnega pojma dodana hramba osebnih podatkov.[192]

Primer: v zadevi *František Ryneš*[193] je F. Ryneš z domačim videonadzornim sistemom, ki ga je namestil zaradi varovanja premoženja, posnel dva posameznika, ki sta razbila okna njegove hiše. SEU je odločilo, da video nadzor, ki vključuje snemanje in shranjevanje osebnih podatkov, pomeni avtomatsko obdelavo osebnih podatkov, ki spada v okvir prava EU o varstvu osebnih podatkov.

Primer: v zadevi *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju*[194] je S. Manni zahteval izbris svojih osebnih podatkov iz registra bonitetne družbe, saj so ga ti povezovali s stečajem nepremičninske družbe, kar je negativno vplivalo na njegov ugled. SEU je menilo, da „organ, ki je odgovoren za vodenje registra, s tem, da navedene informacije vpiše v register in jih hrani ter po potrebi posreduje tretjim, izvaja ‚obdelavo osebnih podatkov', zaradi česar je ‚upravljavec'".

Primer: delodajalci zbirajo in obdelujejo podatke o svojih zaposlenih, vključno z informacijami o njihovih plačah. Pravna podlaga za zakonitost takega početja je pogodba o zaposlitvi.

Delodajalci morajo podatke o plačah svojih zaposlenih posredovati davčnim organom. Tudi to posredovanje podatkov je obdelava v smislu tega pojma v posodobljeni Konvenciji št. 108 in SUVP. Vendar pravna podlaga za tako

191 SUVP, člen 4(2). Glej tudi posodobljeno Konvencijo št. 108, člen 2(b).

192 Posodobljena Konvencija št. 108, člen 2(b).

193 SEU, *František Ryneš proti Úřad pro ochranu osobních údajů*, C-212/13, 11. december 2014, točka 25.

194 SEU, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju*, C-398/15, 9. marec 2017, točka 35.

razkritje ni pogodba o zaposlitvi. Za obdelavo, pri kateri delodajalec podatke o plači posreduje davčnim organom, je potrebna dodatna pravna podlaga. Ta pravna podlaga je običajno vključena v določbe nacionalne davčne zakonodaje. Prenos osebnih podatkov bi se brez takih določb – in če ne bi bilo drugih zakonitih razlogov za obdelavo – štel za nezakonito obdelavo.

2.2.2 Avtomatizirana obdelava osebnih podatkov

Varstvo osebnih podatkov na podlagi posodobljene Konvencije št. 108 in SUVP se v celoti uporablja za avtomatizirano obdelavo podatkov.

V skladu s **pravom EU** se avtomatizirana obdelava osebnih podatkov nanaša na dejanja, ki se izvajajo v zvezi z osebnimi podatki „v celoti ali delno [...] z avtomatiziranimi sredstvi".[195] Posodobljena Konvencija št. 108 vključuje podobno opredelitev.[196] V praksi to pomeni, da za vsako obdelavo osebnih podatkov z avtomatiziranimi sredstvi, na primer z osebnim računalnikom, mobilno napravo ali usmerjevalnikom, veljajo pravila EU in Sveta Evrope o varstvu osebnih podatkov.

Primer: zadeva *Bodil Lindqvist*[197] se je nanašala na navedbo več oseb na spletni strani po imenu ali kako drugače, na primer z njihovo telefonsko številko ali informacijami v zvezi s preživljanjem prostega časa. SEU je menilo, da je „postopek navedbe različnih oseb na spletni strani, pri čemer je njihova prepoznavnost omogočena z navedbo imena ali z drugimi sredstvi, na primer z navedbo telefonske številke ali informacij v zvezi z njihovimi delovnimi razmerami in preživljanjem prostega časa, ‚obdelava osebnih podatkov v celoti ali delno z avtomatskimi sredstvi'" v smislu člena 3(1) Direktive 95/46/ES.[198]

Primer: v zadevi *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji González*[199] je M. Costeja González zahteval odstranitev ali spremembo povezave med njegovim imenom v iskalniku Google in dvema spletnima stranema časopisa, na katerih je

195 SUVP, člen 2(1) in člen 4(2).

196 Posodobljena Konvencija št. 108, člen 2(b) in (c); Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 21.

197 SEU, *Kazenski postopek proti Bodil Lindqvist*, C-101/01, 6. november 2003, točka 27.

198 SUVP, člen 2(1).

199 SEU, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji González* (veliki senat), C-131/12, 13. maj 2014.

bilo objavljeno obvestilo o nepremičninski dražbi v zvezi s postopkom izvršbe zaradi neplačila socialnih prispevkov. SEU je navedlo, „da s tem, da na internetu samodejno, konstantno in sistematično preiskuje na njem objavljene informacije, družba, ki upravlja iskalnik, ‚zbira' take podatke, ki jih nato s svojimi programi za indeksiranje ‚išče', ‚beleži' in ‚ureja', ‚shranjuje' na svoje strežnike in, če je treba, ‚posreduje' in ‚razpolaga [daje na voljo]' svojim uporabnikom v obliki seznamov zadetkov iskanja".[200] Ugotovilo je, da taka dejanja pomenijo „obdelavo", „pri čemer ni pomembno, da družba, ki upravlja iskalnik, uporablja enake postopke tudi za druge vrste informacij in ne razlikuje med temi informacijami in osebnimi podatki".

2.2.3 Neavtomatizirana obdelava osebnih podatkov

Varstvo osebnih podatkov je treba zagotavljati tudi pri ročni obdelavi osebnih podatkov.

Varstvo osebnih podatkov v **okviru prava EU** nikakor ni omejeno na avtomatizirano obdelavo osebnih podatkov. V skladu s tem se varstvo osebnih podatkov v okviru prava EU nanaša na obdelavo osebnih podatkov v ročni zbirki, to pomeni v posebej strukturirani papirni zbirki.[201] Strukturirana zbirka je zbirka, v kateri je niz osebnih podatkov razvrščen, kar pomeni, da so ti podatki dostopni glede na določena merila. Če na primer delodajalec vodi papirno zbirko z naslovom Dopust zaposlenih, ki vsebuje vse podatke o dopustu, ki so ga zaposleni vzeli v prejšnjem letu, in je razvrščena po abecednem vrstnem redu, je ta zbirka ročna zbirka, za katero se uporabljajo pravila EU o varstvu osebnih podatkov. Razlog za to razširitev varstva osebnih podatkov je, da:

- je mogoče papirno zbirko strukturirati tako, da je iskanje informacij hitro in preprosto, ter
- je mogoče s shranjevanjem osebnih podatkov v strukturirani papirni zbirki zlahka zaobiti omejitve, ki so z zakonom predpisane za avtomatizirano obdelavo osebnih podatkov.[202]

200 Prav tam, točka 28.

201 SUVP, člen 2(1).

202 SUVP, uvodna izjava 15.

V okviru **prava Sveta Evrope** je v opredelitvi pojma avtomatizirana obdelava priznano, da so lahko med dejanji avtomatizirane obdelave potrebne nekatere faze ročne uporabe osebnih podatkov.[203] Člen 2(c) posodobljene Konvencije št. 108 določa, da če se avtomatizirana obdelava ne uporablja, obdelava osebnih podatkov pomeni dejanje ali niz dejanj, opravljenih v zvezi z osebnimi podatki v okviru strukturiranega niza takih podatkov, ki so dostopni ali jih je mogoče priklicati glede na specifična merila.

2.3 Uporabniki osebnih podatkov

Ključni poudarki

- Kdor določi sredstva in namene obdelave osebnih podatkov drugih, je v skladu z zakonodajo o varstvu osebnih podatkov „upravljavec"; če tako odločitev skupaj sprejme več oseb, so te lahko „skupni upravljavci".
- „Obdelovalec" je fizična ali pravna oseba, ki obdeluje osebne podatke v imenu upravljavca.
- Obdelovalec postane upravljavec, če sam določi sredstva in namene obdelave osebnih podatkov.
- „Uporabnik" je oseba, ki so ji osebni podatki razkriti.
- „Tretja oseba" je fizična ali pravna oseba, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec ali oseba, ki je pooblaščena za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca.
- Privolitev kot pravna podlaga za obdelavo osebnih podatkov mora biti prostovoljno, informirano, konkretno in nedvoumno ravnanje v obliki jasnega pritrdilnega dejanja, iz katerega je mogoče sklepati na želje posameznika, s katerim izrazi strinjanje z obdelavo.
- Za obdelavo posebnih vrst podatkov na podlagi privolitve je potrebna izrecna privolitev.

2.3.1 Upravljavci in obdelovalci

Pri upravljavcih in obdelovalcih je najpomembneje, da so pravno zavezani k izpolnjevanju zadevnih obveznosti na podlagi zakonodaje o varstvu osebnih podatkov.

203 Posodobljena Konvencija št. 108, člen 2(b) in (c).

V zasebnem sektorju je to običajno fizična ali pravna oseba, v javnem sektorju pa organ. Med upravljavcem podatkov in obdelovalcem podatkov je pomembna razlika: prvi je fizična ali pravna oseba, ki določi namene in sredstva obdelave, drugi pa je fizična ali pravna oseba, ki osebne podatke obdeluje v imenu upravljavca in ob upoštevanju natančnih navodil. Načeloma mora upravljavec osebnih podatkov izvajati nadzor nad obdelavo in je zanjo odgovoren, tudi pravno. Vendar morajo obdelovalci v skladu s spremenjenimi pravili o varstvu osebnih podatkov zdaj izpolnjevati številne zahteve, ki se uporabljajo za upravljavce. V skladu s SUVP morajo obdelovalci na primer voditi evidenco vseh vrst dejavnosti obdelave za dokazovanje, da izpolnjujejo svoje obveznosti v skladu z navedeno uredbo.[204] Obdelovalci morajo poleg tega izvajati ustrezne tehnične in organizacijske ukrepe za zagotavljanje varnosti obdelave,[205] v nekaterih primerih imenovati pooblaščeno osebo za varstvo podatkov[206] in upravljavca uradno obvestiti o kršitvah varnosti osebnih podatkov.[207]

Ali ima oseba sposobnost odločanja ter določitve namena in sredstev obdelave, je odvisno od dejanskih elementov ali okoliščin primera. V skladu z opredelitvijo upravljavca iz SUVP je upravljavec lahko fizična ali pravna oseba ali katero koli drugo telo. Vendar je Delovna skupina iz člena 29 poudarila, da je za to, da bi se posameznikom zagotovil stalnejši referenčni subjekt za uveljavljanje njihovih pravic, „treba dati prednost stališču, da se za upravljavca šteje podjetje ali organ kot tak, ne pa konkretna oseba znotraj tega podjetja ali organa“.[208] Na primer, podjetje, ki prodaja zdravstveno opremo izvajalcem zdravstvene dejavnosti, je upravljavec, ki sestavi in vzdržuje distribucijski seznam v zvezi z vsemi izvajalci na določenem območju, ne pa vodja prodaje, ki ta seznam dejansko uporablja.

Primer: če oddelek družbe Sonček za trženje načrtuje obdelavo osebnih podatkov za tržno raziskavo, je upravljavec take obdelave podjetje Sonček, ne pa zaposleni v oddelku za trženje. Oddelek za trženje ne more biti upravljavec, saj nima ločene identitete.

Fizične osebe so lahko upravljavci v skladu s pravom EU in Sveta Evrope. Kadar pa fizične osebe osebne podatke o drugih obdelujejo v okviru popolnoma osebne ali

204 SUVP, člen 30(2).

205 Prav tam, člen 32.

206 Prav tam, člen 37.

207 Prav tam, člen 33(2).

208 Delovna skupina za varstvo podatkov iz člena 29 (2010), *Mnenje 1/2010 o pojmih „upravljavec“ in „obdelovalec“*, WP 169, Bruselj, 16. februar 2010.

domače dejavnosti, se zanje ne uporabljajo pravila iz SUVP in posodobljene Konvencije št. 108 ter se ne štejejo za upravljavce.[209] Posameznik, ki vodi svojo korespondenco, osebni dnevnik, v katerem so opisani dogodki s prijatelji in sodelavci, ter zdravstveno evidenco družinskih članov, je lahko izvzet iz pravil o varstvu osebnih podatkov, saj bi te dejavnosti lahko bile popolnoma osebne ali zgolj domače dejavnosti. V SUVP je poleg tega določeno, da bi osebne ali domače dejavnosti lahko vključevale tudi dejavnosti na družbenih omrežjih in na spletu, kadar se izvajajo v okviru tovrstnih dejavnosti.[210] Nasprotno se pravila o varstvu osebnih podatkov v celoti uporabljajo za upravljavce in obdelovalce, ki zagotavljajo sredstva za obdelavo osebnih podatkov za osebne ali domače dejavnosti (na primer platforme družbenih omrežij).[211]

Zaradi dostopa državljanov do interneta ter ker se lahko platforme za elektronsko trgovanje, družbena omrežja in blogerska spletna mesta uporabljajo za izmenjavo osebnih podatkov o sebi in drugih, je vse težje ločevati med osebno in neosebno obdelavo.[212] Ali so dejavnosti popolnoma osebne ali domače, je odvisno od okoliščin.[213] Dejavnosti, ki imajo poklicne ali komercialne vidike, ne morejo spadati v okvir izjeme obdelave za domače potrebe.[214] Če obseg in pogostost obdelave osebnih podatkov kažeta na poklicno dejavnost ali dejavnost s polnim delovnim časom, bi posameznik lahko štel za upravljavca. Poleg poklicne ali komercialne narave dejavnosti obdelave je treba upoštevati tudi, ali so osebni podatki dani na voljo velikemu številu oseb, ki so očitno zunaj zasebne sfere zadevnega posameznika. V sodni praksi na podlagi direktive o varstvu osebnih podatkov je bilo ugotovljeno, da se pravo o varstvu osebnih podatkov uporablja, če fizična oseba pri uporabi interneta na javnem spletišču objavi osebne podatke o drugih. SEU še ni odločalo o podobnih dejstvih na podlagi SUVP, ki zagotavlja več usmeritev glede tem, za katere bi bilo v skladu z izjemo obdelave za domače potrebe mogoče šteti, da ne spadajo na področje uporabe zakonodaje o varstvu osebnih podatkov, kot je uporaba družbenih medijev za osebne namene.

209 SUVP, uvodna izjava 18 in člen 2(2)(c); posodobljena Konvencija št. 108, člen 3(2).

210 SUVP, uvodna izjava 18.

211 Prav tam, uvodna izjava 18; Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 29.

212 Glej izjavo Delovne skupine iz člena 29 o razpravah v zvezi s svežnjem ukrepov za reformo varstva podatkov (2013), *Priloga 2: Predlogi in spremembe v zvezi z izvzetjem za osebne ali domače dejavnosti*, 27. februar 2013.

213 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 28.

214 Glej SUVP, uvodna izjava 18, in Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 27.

Primer: zadeva *Bodil Lindqvist*[215] se je nanašala na navedbo različnih oseb na spletni strani po imenu ali kako drugače, na primer z njihovo telefonsko številko ali informacijami v zvezi s preživljanjem prostega časa. SEU je menilo, da je „postopek navedbe različnih oseb na spletni strani, pri čemer je njihova prepoznavnost omogočena z navedbo imena ali z drugimi sredstvi, [...] ‚obdelava osebnih podatkov v celoti ali delno z avtomatskimi sredstvi'" v smislu člena 3(1) Direktive 95/46/ES.[216]

Taka obdelava osebnih podatkov ne spada med popolnoma osebne ali domače dejavnosti, ki so zunaj področja uporabe pravil EU o varstvu osebnih podatkov, saj je treba to izjemo „razlagati tako, da se nanaša samo na dejavnosti, ki se izvajajo v zasebnem in družinskem življenju posameznikov, kar očitno ne velja za obdelavo osebnih podatkov, ki vključuje njihovo objavo na spletu, s čimer ti postanejo dostopni neopredeljenemu številu oseb".[217]

SEU meni, da lahko zakonodaja EU o varstvu osebnih podatkov v nekaterih okoliščinah zajema tudi slikovne posnetke zasebno nameščene varnostne kamere.

Primer: v zadevi *František Ryneš*[218] je F. Ryneš z domačim videonadzornim sistemom (CCTV), ki ga je namestil zaradi varovanja premoženja, posnel dva posameznika, ki sta razbila okna njegove hiše. Posnetki so bili nato izročeni policiji in kot dokaz predloženi v kazenskem postopku.

SEU je navedlo, da „[č]e videonadzorni sistem [...] zajema, čeprav delno, javni prostor in je tako usmerjen iz zasebnega okolja tistega, ki tako opravi obdelavo podatkov, ga ni mogoče šteti za popolnoma ‚osebno ali domačo dejavnost' [...]".[219]

215 SEU, *Kazenski postopek proti Bodil Lindqvist*, C-101/01, 6. november 2003.

216 Prav tam, točka 27; prej Direktiva 95/46/ES, člen 3(1), zdaj SUVP, člen 2(1).

217 SEU, *Kazenski postopek proti Bodil Lindqvist*, C-101/01, 6. november 2003, točka 47.

218 SEU, *František Ryneš proti Úřad pro ochranu osobních údajů*, C-212/13, 11. december 2014, točka 33.

219 Prej Direktiva 95/46/ES, člen 3(2), druga alineja, zdaj SUVP, člen 2(2)(c).

Upravljavec

V okviru prava EU je upravljavec opredeljen kot oseba, ki „sam[a] ali skupaj z drugimi določa namene in sredstva obdelave [osebnih podatkov]“.[220] Upravljavec določi, zakaj in kako se bodo obdelovali osebni podatki.

V okviru prava Sveta Evrope je upravljavec v posodobljeni Konvenciji št. 108 opredeljen kot fizična ali pravna oseba, javni organ, služba, agencija ali drugo telo, ki ima samo ali skupaj z drugimi pooblastilo za odločanje v zvezi z obdelavo podatkov.[221] Tako pooblastilo za odločanje se nanaša na namene in sredstva obdelave, na vrste podatkov, ki se obdelujejo, in na dostop do podatkov.[222] Odločitev o tem, ali to pooblastilo izhaja iz pravnega imenovanja ali dejanskih okoliščin, je treba sprejeti za vsak primer posebej.[223]

Primer: v zadevi *Google Spain*[224] je španski državljan zahteval, naj se iz brskalnika Google izbriše povezava na star časopisni članek o njegovi finančni preteklosti.

SEU je bilo postavljeno vprašanje, ali je Google kot družba, ki upravlja iskalnik, tudi upravljavec podatkov v smislu člena 2(d) direktive o varstvu osebnih podatkov.[225] SEU je upoštevalo široko opredelitev pojma upravljavec, da bi se zagotovilo „učinkovito in popolno varstvo zadevnih oseb“.[226] Ugotovilo je, da družba, ki upravlja iskalnik, določa namene in sredstva zadevne dejavnosti ter da podatke, ki so jih izdajatelji spletnih mest vnesli na internetne strani, daje na voljo vsem internetnim uporabnikom, ki izvedejo iskanje na podlagi imena zadevne osebe.[227] Zato je odločilo, da družba Google lahko šteje za upravljavca.[228]

220 SUVP, člen 4(7).

221 Posodobljena Konvencija št. 108, člen 2(d).

222 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 22.

223 Prav tam.

224 SEU, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), C-131/12, 13. maj 2014.

225 SUVP, člen 4(7); SEU, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), C-131/12, 13. maj 2014, točka 21.

226 SEU, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), C-131/12, 13. maj 2014, točka 34.

227 Prav tam, točke 35–40.

228 Prav tam, točka 41.

Če je upravljavec ali obdelovalec ustanovljen zunaj EU, mora pisno imenovati predstavnika v EU.[229] V SUVP je poudarjeno, da mora biti predstavnik ustanovljen „v eni od držav članic, kjer so posamezniki, na katere se nanašajo osebni podatki, katerih osebni podatki se obdelujejo v zvezi s ponujanjem blaga ali storitev tem posameznikom ali katerih vedenje se spremlja".[230] Če predstavnik ni določen, se zoper samega upravljavca ali obdelovalca še vedno lahko uvedejo pravni ukrepi.[231]

Skupno upravljanje

SUVP določa, da se dva ali več upravljavcev, ki skupaj določijo namene in načine obdelave, štejejo za skupne upravljavce. To pomeni, da se skupaj odločijo za obdelavo osebnih podatkov za skupni namen.[232] V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je navedeno, da lahko tudi v **okviru Sveta Evrope** obstaja več upravljavcev ali skupno upravljanje.[233]

Delovna skupina iz člena 29 je poudarila, da ima lahko skupno upravljanje različne oblike in da sodelovanje različnih upravljavcev pri dejavnostih upravljanja ni nujno enakopravno.[234] Taka prožnost omogoča, da se upošteva vse večja zapletenost dejanskega stanja obdelave podatkov.[235] Da bi skupni upravljavci izpolnjevali obveznosti iz SUVP, morajo zato v posebnem sporazumu opredeliti svoje individualne odgovornosti.[236]

Skupno upravljanje privede do skupne odgovornosti za dejavnost obdelave.[237] V okviru **prava EU** to pomeni, da je lahko vsak upravljavec ali obdelovalec v celoti odgovoren za celotno škodo, nastalo zaradi obdelave v okviru skupnega upravljanja, da se zagotovi, da posameznik, na katerega se nanašajo osebni podatki, prejme učinkovito odškodnino.[238]

229 SUVP, člen 27(1).

230 Prav tam, člen 27(3).

231 Prav tam, člen 27(5).

232 Prav tam, člen 4(7) in člen 26.

233 Posodobljena Konvencija št. 108, člen 2(d); Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 22.

234 Delovna skupina za varstvo podatkov iz člena 29 (2010), *Mnenje 1/2010 o pojmih „upravljavec" in „obdelovalec"*, WP 169, Bruselj, 16. februar 2010, str. 18.

235 Prav tam.

236 SUVP, uvodna izjava 79.

237 Prav tam, točka 21.

238 Prav tam, člen 82(4).

Primer: pogost primer skupnega upravljanja je podatkovna zbirka, ki jo v zvezi s strankami, ki ne izpolnjujejo obveznosti, skupaj upravlja več kreditnih institucij. Ko oseba zaprosi za kreditno linijo pri banki, ki je eden od skupnih upravljavcev, banke preverijo podatkovno zbirko, da lahko sprejmejo informirano odločitev o kreditni sposobnosti prosilca.

V pravnih določbah ni izrecno navedeno, ali mora biti skupni namen pri skupnem upravljanju enak za vse upravljavce ali pa zadostuje že, da se njihovi nameni samo deloma prekrivajo. Zadevna sodna praksa na evropski ravni zaenkrat še ni na voljo. Delovna skupina iz člena 29 je v svojem mnenju o upravljavcih in obdelovalcih iz leta 2010 navedla, da so lahko skupnim upravljavcem skupni vsi nameni in sredstva obdelave, lahko pa jim je skupen le del namenov ali sredstev.[239] V prvem primeru bi bilo razmerje med njimi zelo tesno, v drugem pa manj povezano.

Delovna skupina iz člena 29 zagovarja širšo razlago pojma skupnega upravljanja, da bi se omogočilo nekaj prožnosti, ki je v trenutnih razmerah nujna, saj obdelava osebnih podatkov postaja vse bolj zapletena.[240] Stališče delovne skupine ponazarja zadeva, povezana z Združenjem za svetovne finančne telekomunikacije med bankami (SWIFT).

Primer: v t. i. zadevi SWIFT so evropske bančne institucije najele združenje SWIFT, prvotno kot obdelovalca, za prenos podatkov med bančnimi transakcijami. Združenje SWIFT je take podatke o bančnih transakcijah, shranjene v računalniškem storitvenem centru v Združenih državah, razkrilo ameriškemu ministrstvu za finance, ne da bi mu evropske bančne institucije, ki so z njim sodelovale, to izrecno naročile. Delovna skupina iz člena 29 je med oceno zakonitosti takega položaja ugotovila, da je treba evropske bančne institucije, ki so uporabljale združenje SWIFT, in samo združenje SWIFT šteti za skupne upravljavce, ki so evropskim strankam odgovorni za razkritje njihovih osebnih podatkov ameriškim organom.[241]

239 Delovna skupina za varstvo podatkov iz člena 29 (2010), *Mnenje 1/2010 o pojmih „upravljavec“ in „obdelovalec“*, WP 169, Bruselj, 16. februar 2010, str. 18.

240 Prav tam.

241 Delovna skupina za varstvo podatkov iz člena 29 (2006), *Mnenje 10/2006 o obdelavi osebnih podatkov Družbe za svetovne medbančne finančne telekomunikacije (SWIFT)*, WP 128, Bruselj, 22. november 2006.

Obdelovalec

Obdelovalec je v skladu s **pravom EU** opredeljen kot oseba, ki obdeluje osebne podatke v imenu upravljavca.[242] Dejavnosti, zaupane obdelovalcu, so lahko omejene na zelo specifično nalogo ali okvir, lahko pa so precej splošne in obsežne.

V skladu s **pravom Sveta Evrope** je pomen obdelovalca enak kot po pravu EU.[243]

Obdelovalci so poleg tega, da obdelujejo osebne podatke za druge, tudi samostojni upravljavci osebnih podatkov v zvezi z obdelavo, ki jo izvajajo za lastne namene, na primer v zvezi s svojimi zaposlenimi, prodajo in računovodstvom.

Primer: družba VednoNared je specializirana za obdelavo kadrovskih podatkov za druge družbe. V tej funkciji je družba VednoNared obdelovalec. Kadar pa družba VednoNared obdeluje osebne podatke o svojih zaposlenih, je upravljavec osebnih podatkov za namene izpolnjevanja svojih obveznosti kot delodajalec.

Razmerje med upravljavcem in obdelovalcem

Kot smo videli, je upravljavec opredeljen kot oseba, ki določi namene in sredstva obdelave. V SUVP je jasno navedeno, da lahko obdelovalec obdeluje osebne podatke samo po navodilih upravljavca, razen če to od njega zahteva pravo EU ali pravo države članice.[244] Pogodba med upravljavcem in obdelovalcem je bistven element njunega razmerja in je pravno zahtevana.[245]

Primer: direktor družbe Sonček odloči, naj družba Oblaček, ki je specializirana za hrambo podatkov v oblaku, upravlja podatke Sončkovih strank. Upravljavec ostaja družba Sonček, družba Oblaček pa je samo obdelovalec, saj lahko družba Oblaček v skladu s pogodbo podatke o strankah družbe Sonček uporablja samo za namene, ki jih določi slednja.

242 SUVP, člen 4(8).

243 Posodobljena Konvencija št. 108, člen 2(f).

244 SUVP, člen 29.

245 Prav tam, člen 28(3).

Če se pristojnost za določitev sredstev obdelave prenese na obdelovalca, mora imeti upravljavec vseeno možnost izvajati ustrezno stopnjo nadzora nad odločitvami obdelovalca v zvezi s sredstvi obdelave. Splošno odgovornost še vedno nosi upravljavec, ki mora obdelovalce nadzorovati in tako zagotoviti, da so njihove odločitve v skladu s pravom o varstvu osebnih podatkov in njegovimi navodili.

Če poleg tega obdelovalec ne upošteva pogojev za obdelavo osebnih podatkov, ki jih je določil upravljavec, obdelovalec postane upravljavec, vsaj kar zadeva kršitev navodil upravljavca. Obdelovalec tako najverjetneje postane upravljavec, ki ravna nezakonito. Posledično mora prvotni upravljavec pojasniti, kako je lahko obdelovalec kršil svoje pooblastilo.[246] Delovna skupina iz člena 29 v takih primerih praviloma predpostavlja, da gre za skupno upravljanje, saj se tako najbolje zavarujejo interesi posameznikov, na katere se nanašajo osebni podatki.[247]

Pojavijo se lahko tudi vprašanja glede porazdelitve odgovornosti, če je upravljavec malo podjetje, obdelovalec pa velika gospodarska družba, ki ima moč, da narekuje pogoje svojih storitev. Vendar Delovna skupina iz člena 29 v takih okoliščinah zagovarja stališče, da standarda odgovornosti ne bi smeli zniževati na podlagi gospodarskega neravnotežja in da je treba ohraniti razumevanje pojma upravljavec.[248]

Zaradi jasnosti in preglednosti morajo biti podrobnosti razmerja med upravljavcem in obdelovalcem določene v pisni pogodbi.[249] Pogodba mora vključevati zlasti vsebino, naravo, namen in trajanje obdelave, vrsto osebnih podatkov in kategorije posameznikov, na katere se nanašajo osebni podatki. V njej morajo biti določene tudi obveznosti in pravice upravljavca in obdelovalca, kot so zahteve glede zaupnosti in varnosti. Če take pogodbe ni, to pomeni kršitev obveznosti upravljavca, da zagotovi pisno dokumentacijo o vzajemnih odgovornostih, in lahko se naložijo sankcije. V primeru škode, ki nastane zaradi prekoračitve zakonitih navodil upravljavca ali njihove neizpolnitve, je lahko za škodo poleg upravljavca odgovoren tudi obdelovalec.[250] Obdelovalec mora voditi evidenco vseh vrst dejavnosti obdelave, ki jih izvaja v imenu

246 Prav tam, člen 82(2).

247 Delovna skupina za varstvo podatkov iz člena 29 (2010), *Mnenje 1/2010 o pojmih „upravljavec" in „obdelovalec"*, WP 169, Bruselj, 16. februar 2010, str. 25; Delovna skupina za varstvo podatkov iz člena 29 (2006), *Mnenje 10/2006 o obdelavi osebnih podatkov Družbe za svetovne medbančne finančne telekomunikacije (SWIFT)*, WP 128, Bruselj, 22. november 2006.

248 Delovna skupina za varstvo podatkov iz člena 29 (2010), *Mnenje 1/2010 o pojmih „upravljavec" in „obdelovalec"*, WP 169, Bruselj, 16. februar 2010, str. 24.

249 SUVP, člen 28(3) in (9).

250 Prav tam, člen 82(2).

upravljavca.[251] Nadzornemu organu je na zahtevo treba omogočiti dostop do teh evidenc, saj morata upravljavec in obdelovalec sodelovati z navedenim organom pri izvajanju njegovih nalog.[252] Upravljavci in obdelovalci se lahko tudi zavežejo odobrenemu kodeksu ravnanja ali izvajanju odobrenega mehanizma certificiranja, da dokažejo skladnost z zahtevami iz SUVP.[253]

Obdelovalci morda želijo nekatere naloge prenesti na druge podobdelovalce. To je zakonsko dopustno, če so med upravljavcem in obdelovalcem opredeljene ustrezne pogodbene določbe, vključno s tem, ali je dovoljenje upravljavca vedno nujno ali pa zadostuje že obveščanje. SUVP določa, da prvi obdelovalec še naprej v celoti odgovarja upravljavcu, če podobdelovalec ne izpolni svojih obveznosti varstva podatkov.[254]

V skladu s **pravom Sveta Evrope** je razlaga pojmov upravljavec in obdelovalec, kot sta pojasnjena zgoraj, v celoti upoštevna.[255]

2.3.2 Uporabniki in tretje osebe

Razlika med tema kategorijama oseb ali subjektov, ki sta bili uvedeni z direktivo o varstvu osebnih podatkov, izhaja predvsem iz njunega razmerja do upravljavca in posledično iz njunega pooblastila za dostop do osebnih podatkov, ki jih hrani upravljavec.

„Tretja oseba" se razlikuje od upravljavca in obdelovalca. V skladu s členom 4(10) SUVP tretja oseba pomeni „fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca". To pomeni, da se osebe, zaposlene pri organizaciji, ki je ločena od upravljavca – tudi če ta pripada isti skupini ali krovni družbi –, štejejo za tretje osebe (ali spadajo mednje). Nasprotno pa se podružnice banke, ki obdelujejo račune strank na podlagi neposrednega pooblastila svojega sedeža, ne bi štele za tretje osebe.[256]

251 Prav tam, člen 30(2).

252 Prav tam, člen 30(4) in člen 31.

253 Prav tam, člen 28(5) in člen 42(4).

254 Prav tam, člen 28(4).

255 Glej na primer posodobljeno Konvencijo št. 108, člen 2(b) in (f); Priporočilo o oblikovanju profilov, člen 1.

256 Delovna skupina za varstvo podatkov iz člena 29 (2010), *Mnenje 1/2010 o pojmih „upravljavec" in „obdelovalec"*, WP 169, Bruselj, 16. februar 2010, str. 28.

„Uporabnik" je širši pojem kot tretja oseba. Uporabnik v smislu člena 4(9) SUVP pomeni „fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne". Ta uporabnik je lahko oseba, ki ni povezana z upravljavcem ali obdelovalcem – to bi bila potem tretja oseba –, ali nekdo, ki je povezan z upravljavcem ali obdelovalcem, na primer zaposleni ali drug oddelek v isti družbi ali organu.

Razlikovanje med uporabniki in tretjimi osebami je pomembno samo zaradi pogojev za zakonito razkritje osebnih podatkov. Zaposleni pri upravljavcu ali obdelovalcu so lahko brez dodatnih pravnih zahtev uporabniki osebnih podatkov, če sodelujejo pri postopkih obdelave upravljavca ali obdelovalca. Nasprotno pa tretja oseba, ki je ločena od upravljavca ali obdelovalca, ni pooblaščena za uporabo osebnih podatkov, ki jih obdeluje upravljavec, razen če v posameznem primeru obstaja posebna pravna podlaga.

Primer: oseba, ki je zaposlena pri upravljavcu in uporablja osebne podatke v okviru nalog, ki ji jih je zaupal delodajalec, je uporabnik osebnih podatkov, vendar ni tretja oseba, saj uporablja podatke v imenu in po navodilih upravljavca. Če na primer delodajalec zaradi skorajšnjega ocenjevanja delovne uspešnosti kadrovski službi razkrije osebne podatke o svojih zaposlenih, je kadrovska služba uporabnik osebnih podatkov, saj so ji bili ti podatki razkriti v okviru obdelave za upravljavca.

Če pa organizacija podatke o svojih zaposlenih zagotovi družbi za usposabljanje, ki jih bo uporabila, da bo program usposabljanja prilagodila potrebam zaposlenih, je družba za usposabljanje tretja oseba. Razlog je v tem, da družba za usposabljanje nima posebne legitimnosti ali pooblastila (ki v primeru zaposlenih v kadrovski službi izhaja iz delovnega razmerja z upravljavcem) za obdelavo teh osebnih podatkov. Z drugimi besedami, družba za usposabljanje zadevnih podatkov ni prejela v okviru svojega delovnega razmerja z upravljavcem podatkov.

2.4 Privolitev

Ključna poudarka

- Privolitev kot pravna podlaga za obdelavo osebnih podatkov mora biti prostovoljno, informirano, konkretno in nedvoumno ravnanje v obliki jasnega pritrdilnega dejanja, iz katerega je mogoče sklepati na želje posameznika, s katerim izrazi strinjanje z obdelavo.
- Za obdelavo posebnih vrst osebnih podatkov je potrebna izrecna privolitev.

Kot bo podrobneje obravnavano v poglavju 4, je privolitev eden od šestih zakonitih razlogov za obdelavo osebnih podatkov. Privolitev pomeni „prostovoljno, konkretno, informirano in nedvoumno ravnanje […], iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki“.[257]

V **pravu EU** je opredeljenih več dejavnikov, na podlagi katerih je privolitev veljavna in katerih namen je zagotoviti, da se posamezniki, na katere se nanašajo osebni podatki, dejansko strinjajo z uporabo svojih osebnih podatkov.[258]

- Privolitev mora biti dana z jasnim pritrdilnim ravnanjem, ki pomeni, da je posameznik, na katerega se nanašajo osebni podatki, prostovoljno, konkretno, informirano in nedvoumno izrazil strinjanje z obdelavo svojih osebnih podatkov. Tako ravnanje je lahko dejanje ali izjava.

- Posameznik, na katerega se nanašajo osebni podatki, mora imeti pravico, da svojo privolitev kadar koli prekliče.

- V okviru pisne izjave, ki zajema tudi druge zadeve, kot so splošne pogoje, morajo biti zahteve za privolitev predložene v jasnem in preprostem jeziku ter v razumljivi in zlahka dostopni obliki, da se privolitev jasno razlikuje od drugih zadev; če je del te izjave v nasprotju s SUVP, ni zavezujoč.

Privolitev je v okviru prava o varstvu osebnih podatkov veljavna le, če so izpolnjene vse te zahteve. Odgovornost upravljavca je, da dokaže, da je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo svojih osebnih podatkov.[259]

257 SUVP, člen 4(11). Glej tudi posodobljeno Konvencijo št. 108, člen 5(2).

258 SUVP, člen 7.

259 Prav tam, člen 7(1).

Elementi veljavne privolitve so podrobneje obravnavani v razdelku 4.1.1 o zakonitih razlogih za obdelavo osebnih podatkov.

Konvencija št. 108 ne vsebuje opredelitve privolitve; to je prepuščeno nacionalnemu pravu. Vendar **po pravu Sveta Evrope** dejavniki veljavne privolitve ustrezajo tistim, ki so bili pojasnjeni zgoraj.[260]

Dodatne zahteve za veljavno privolitev na podlagi civilnega prava, na primer pravna sposobnost, se seveda uporabljajo tudi v okviru varstva osebnih podatkov, saj so take zahteve temeljni pravni pogoji. Neveljavna privolitev oseb, ki nimajo pravne sposobnosti, pomeni, da ni pravne podlage za obdelavo osebnih podatkov o takih osebah. V zvezi s pravno sposobnostjo mladoletnikov za sklepanje pogodb je v SUVP določeno, da njene določbe o minimalni starosti za pridobitev veljavne privolitve ne vplivajo na splošno pogodbeno pravo držav članic.[261]

Privolitev mora biti dana jasno, da ni nikakršnega dvoma o nameri posameznika, na katerega se nanašajo osebni podatki.[262] Če se nanaša na obdelavo občutljivih osebnih podatkov, mora biti nedvoumna in je lahko ustna ali pisna.[263] Pisna privolitev se lahko predloži z elektronskimi sredstvi.[264] V okviru **prava EU** in **prava Sveta Evrope** je treba strinjanje z obdelavo osebnih podatkov izraziti z izjavo ali jasnim pritrdilnim dejanjem.[265] Molk, vnaprej označena okenca, vnaprej izpolnjeni obrazci ali nedejavnost zato ne pomenijo privolitve.[266]

260 Posodobljena Konvencija št. 108, člen 5(2); Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točke 42–45.

261 SUVP, člen 8(3).

262 Prav tam, člen 6(1)(a) in člen 9(2)(a).

263 Prav tam, uvodna izjava 32.

264 Prav tam.

265 Prav tam, člen 4(11); Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 42.

266 SUVP, uvodna izjava 32; Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 42.

3

Ključna načela evropskega prava o varstvu osebnih podatkov

EU	Obravnavane teme	Svet Evrope
SUVP, člen 5(1)(a)	**Načelo zakonitosti**	Posodobljena Konvencija št. 108, člen 5(3)
SUVP, člen 5(1)(a)	**Načelo poštenosti**	Posodobljena Konvencija št. 108, člen 5(4)(a) ESČP, *K. H. in drugi proti Slovaški*, pritožba št. 32881/04, 2009
SUVP, člen 5(1)(a) SEU, C-201/14, *Smaranda Bara in drugi proti Președintele Casei Naționale de Asigurări de Sănătate in drugim*, 2015	**Načelo preglednosti**	Posodobljena Konvencija št. 108, člen 5(4)(a) in člen 8 ESČP, *Haralambie proti Romuniji*, pritožba št. 21737/03, 2009
SUVP, člen 5(1)(b)	**Načelo omejitve namena**	Posodobljena Konvencija št. 108, člen 5(4)(b)
SUVP, člen 5(1)(c) SEU, združeni zadevi C-293/12 in C-594/12, *Digital Rights Ireland* in Kärntner Landesregierung in drugi (veliki senat), 2014	**Načelo najmanjšega obsega podatkov**	Posodobljena Konvencija št. 108, člen 5(4)(c)
SUVP, člen 5(1)(d) SEU, C-553/07, *College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer*, 2009	**Načelo točnosti osebnih podatkov**	Posodobljena Konvencija št. 108, člen 5(4)(d)

EU	Obravnavane teme	Svet Evrope
SUVP, člen 5(1)(e) SEU, združeni zadevi C-293/12 in C-594/12, *Digital Rights Ireland* in Kärntner Landesregierung in drugi (veliki senat), 2014	**Načelo omejitve hrambe**	Posodobljena Konvencija št. 108, člen 5(4)(e) ESČP, združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 2008
SUVP, člen 5(1)(f) in člen 32	**Načelo varnosti (celovitosti in zaupnosti) podatkov**	Posodobljena Konvencija št. 108, člen 7
SUVP, člen 5(2)	**Načelo odgovornosti**	Posodobljena Konvencija št. 108, člen 10

Člen 5 SUVP določa načela, ki urejajo obdelavo osebnih podatkov. Ta načela zajemajo:

- zakonitost, poštenost in preglednost;
- omejitev namena;
- najmanjši obseg podatkov;
- točnost podatkov;
- omejitev hrambe;
- celovitost in zaupnost.

Ta načela so izhodišče za podrobnejše določbe v naslednjih členih navedene uredbe. Pojavijo se tudi v členih 5, 7, 8 in 10 posodobljene Konvencije št. 108. Vsa poznejša zakonodaja o varstvu osebnih podatkov na ravni Sveta Evrope in EU mora biti v skladu s temi načeli, upoštevati pa jih je treba tudi pri njeni razlagi. V skladu s pravom EU so omejitve načel obdelave dovoljene le, če ustrezajo pravicam in obveznostim iz členov 12 do 22SUVP, pri čemer morajo take omejitve spoštovati bistvo temeljnih pravic in svoboščin. Morebitne izjeme od teh ključnih načel in njihove omejitve se lahko določijo na ravni EU ali nacionalni ravni,[267] biti morajo določene z zakonom, imeti morajo zakonit cilj ter biti potrebni in sorazmerni ukrepi v demokratični družbi.[268] Izpolnjeni morajo biti vsi trije pogoji.

267 Posodobljena Konvencija št. 108, člen 11(1); SUVP, člen 23(1).

268 SUVP, člen 23(1).

3.1 Načela zakonitosti, poštenosti in preglednosti obdelave osebnih podatkov

Ključni poudarki

- Načela zakonitosti, poštenosti in preglednosti se uporabljajo za vsako obdelavo osebnih podatkov.
- V skladu s SUVP je za zakonitost potrebno vsaj eno od naslednjega:
  - privolitev posameznika, na katerega se nanašajo osebni podatki;
  - potrebnost za sklenitev pogodbe;
  - zakonska obveznost;
  - potrebnost za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge osebe;
  - potrebnost za opravljanje naloge v javnem interesu;
  - potrebnost zaradi zakonitih interesov upravljavca ali tretje osebe, če nad njimi ne prevladajo interesi in pravice posameznika, na katerega se nanašajo osebni podatki.
- Osebne podatke je treba obdelovati pošteno.
  - Posameznika, na katerega se nanašajo osebni podatki, je treba seznaniti s tveganjem, s čimer se zagotovi, da obdelava ne bo imela nepredvidljivih škodljivih učinkov.
- Osebne podatke je treba obdelovati pregledno.
  - Upravljavci morajo posameznike, na katere se nanašajo osebni podatki, med drugim obvestiti o namenu obdelave ter o identiteti in naslovu upravljavca.
  - Informacije o dejanjih obdelave je treba zagotoviti v jasnem in preprostem jeziku, da lahko posamezniki, na katere se nanašajo osebni podatki, zlahka razumejo zadevna pravila, tveganja, zaščitne ukrepe in pravice.
  - Posamezniki, na katere se nanašajo osebni podatki, imajo pravico dostopa do svojih podatkov, ne glede na to, kje se ti podatki obdelujejo.

3.1.1 Zakonitost obdelave

V skladu z **zakonodajo EU in Sveta Evrope o varstvu osebnih podatkov** je treba osebne podatke obdelovati zakonito.[269] Obdelava je zakonita, če je vanjo privolil posameznik, na katerega se nanašajo osebni podatki, ali če temelji na drugem zakonitem razlogu, določenem v zakonodaji o varstvu osebnih podatkov.[270] Člen 6(1) SUVP poleg privolitve vključuje pet zakonitih razlogov za obdelavo, in sicer je obdelava osebnih podatkov zakonita, kadar je potrebna za izvajanje pogodbe, za opravljanje naloge pri izvajanju javne oblasti, za izpolnitev zakonske obveznosti, zaradi zakonitih interesov upravljavca ali tretje osebe ali kadar je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki. To bo podrobneje obravnavano v razdelku 4.1.

3.1.2 Poštenost obdelave

V skladu z zakonodajo EU in Sveta Evrope o varstvu osebnih podatkov je treba osebne podatke obdelovati ne le zakonito, temveč tudi pošteno.[271] Z načelom poštene obdelave je urejeno predvsem razmerje med upravljavcem in posameznikom, na katerega se nanašajo osebni podatki.

Upravljavci bi morali posameznike, na katere se nanašajo osebni podatki, in širšo javnost obvestiti, da bodo osebne podatke obdelali zakonito in pregledno, poleg tega morajo biti zmožni dokazati, da so dejanja obdelave v skladu s SUVP. Dejanja obdelave se ne smejo izvajati na skrivaj, posamezniki, na katere se nanašajo osebni podatki, pa bi morali biti seznanjeni z morebitnimi tveganji. Poleg tega morajo upravljavci čim bolj upoštevati želje posameznika, na katerega se nanašajo osebni podatki, zlasti če je njegova privolitev pravna podlaga za obdelavo osebnih podatkov.

Primer: v zadevi *K. H. in drugi proti Slovaški*[272] so se pritožnice – romskega porekla – med nosečnostjo zdravile v dveh bolnišnicah na vzhodu Slovaške in so tam tudi rodile. Pozneje nobeni od njih kljub večkratnim poskusom ni več uspelo zanositi. Nacionalna sodišča so bolnišnicama naročila, naj pritožnicam in njihovim zastopnikom dovolijo vpogled v zdravstvene kartoteke in izdelavo

269 Posodobljena Konvencija št. 108, člen 5(3); SUVP, člen 5(1)(a).

270 Listina Evropske unije o temeljnih pravicah, člen 8(2); SUVP, uvodna izjava 40 in členi 6–9; posodobljena Konvencija št. 108, člen 5(2); Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 41.

271 SUVP, člen 5(1)(a); posodobljena Konvencija št. 108, člen 5(4)(a).

272 ESČP, *K. H. in drugi proti Slovaški*, pritožba št. 32881/04, 28. april 2009.

ročnih izpiskov, zavrnila pa so njihovo prošnjo za fotokopiranje dokumentacije, da bi se domnevno preprečile zlorabe. Pozitivne obveznosti države na podlagi člena 8 EKČP so nujno vključevale obveznost, da posameznicam, na katere so se nanašali osebni podatki, zagotovijo kopije njihovih zdravstvenih kartotek. Država bi morala zagotoviti možnosti za kopiranje osebnih kartotek ali po potrebi navesti prepričljive razloge za zavrnitev. Nacionalna sodišča so v primeru pritožnic prepoved kopiranja njihovih zdravstvenih kartotek utemeljila predvsem s potrebo po zaščiti zadevnih informacij pred zlorabo. Vendar ESČP ni razumelo, kako bi lahko pritožnice, ki jim je bil tako ali tako omogočen dostop do celotnih zdravstvenih kartotek, zlorabile informacije, ki se nanašajo na njih same. Poleg tega bi bilo mogoče tveganje take zlorabe preprečiti z drugimi sredstvi in ne tako, da se je pritožnicam prepovedalo kopiranje kartotek, na primer z omejitvijo kroga oseb s pravico do dostopa do kartotek. Država ni izkazala dovolj prepričljivih razlogov za to, da se je pritožnicam prepovedal učinkovit dostop do informacij v zvezi z njihovim zdravjem. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

V zvezi z internetnimi storitvami morajo sistemi za obdelavo podatkov omogočati, da posamezniki, na katere se nanašajo osebni podatki, dejansko razumejo, kaj se dogaja z njihovimi podatki. Načelo poštenosti vsekakor presega obveznosti glede preglednosti in bi ga bilo mogoče povezati tudi z etično obdelavo osebnih podatkov.

Primer: univerzitetni raziskovalni oddelek izvaja poskus, v okviru katerega se analizirajo spremembe razpoloženja pri 50 poskusnih osebah. Te morajo vsako uro ob določenem času v elektronski datoteki zabeležiti svoje misli. Zadevnih 50 oseb je dalo privolitev za ta konkretni projekt in univerzi za to specifično uporabo podatkov. Raziskovalni oddelek kmalu ugotovi, da bi bilo elektronsko beleženje misli zelo koristno za neki drug projekt, ki je osredotočen na duševno zdravje in ga usklajuje neka druga skupina. Čeprav bi lahko univerza kot upravljavec iste podatke uporabila za delo druge skupine, ne da bi sprejela nadaljnje ukrepe za zagotovitev zakonitosti obdelave teh podatkov, saj sta namena združljiva, je poskusne osebe v skladu s svojim kodeksom raziskovalne etike in načelom poštene obdelave obvestila ter jih zaprosila za novo privolitev.

3.1.3 Preglednost obdelave

V skladu z **zakonodajo EU in Sveta Evrope o varstvu osebnih podatkov** je treba osebne podatke obdelovati „na pregleden način v zvezi s posameznikom, na katerega se nanašajo".[273]

To načelo določa obveznost upravljavca, da sprejme vse ustrezne ukrepe za obveščanje posameznikov, na katere se nanašajo osebni podatki – ti so lahko uporabniki, stranke ali naročniki –, kako se uporabljajo njihovi osebni podatki.[274] Preglednost se lahko nanaša na informacije, ki so posamezniku dane pred začetkom obdelave,[275] informacije, ki bi morale biti med obdelavo zlahka dostopne posameznikom, na katere se nanašajo osebni podatki,[276] pa tudi na informacije, ki se zadevnim posameznikom predložijo na podlagi zahteve za dostop do osebnih podatkov.[277]

Primer: v zadevi *Haralambie proti Romuniji*[278] je bil pritožniku odobren dostop do informacij, ki jih je v zvezi z njim hranila tajna služba, šele pet let po vložitvi zahteve. ESČP je opozorilo, da imajo posamezniki, o katerih imajo javni organi osebne kartoteke, življenjski interes za to, da se jim omogoči dostop do teh kartotek. Dolžnost organov je, da zagotovijo učinkovit postopek za pridobitev dostopa do takih informacij. ESČP je menilo, da niti količina poslanih kartotek niti pomanjkljivosti sistema arhiviranja ne upravičujejo petletne zamude pri ugoditvi pritožnikovi prošnji za dostop do njegove kartoteke. Organi pritožniku niso zagotovili učinkovitega in dostopnega postopka, ki bi mu v razumnem času zagotovil dostop do osebne kartoteke. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Dejanja obdelave morajo biti posameznikom, na katere se nanašajo osebni podatki, razložena na lahko dostopen način, tako da razumejo, kaj se bo zgodilo z njihovimi podatki. To pomeni, da mora biti posameznik, na katerega se nanašajo osebni podatki, v času zbiranja osebnih podatkov seznanjen s konkretnim namenom obdelave

273 SUVP, člen 5(1)(a); posodobljena Konvencija št. 108, člen 5(4)(a) in člen 8.

274 SUVP, člen 12.

275 Prav tam, člena 13 in 14.

276 Delovna skupina za varstvo podatkov iz člena 29, *Mnenje št. 2/2017 o obdelavi podatkov pri delu*, WP 249, str. 25.

277 SUVP, člen 15.

278 ESČP, *Haralambie proti Romuniji*, pritožba št. 21737/03, 27. oktober 2009.

osebnih podatkov.[279] V skladu z načelom preglednosti obdelave je treba uporabljati jasen in preprost jezik.[280] Zadevni posamezniki morajo razumeti, katera so tveganja, pravila, zaščitni ukrepi in pravice v zvezi z obdelavo njihovih osebnih podatkov.[281]

V **pravu Sveta Evrope** je tudi določeno, da mora upravljavec posameznikom, na katere se nanašajo osebni podatki, obvezno proaktivno zagotoviti nekatere bistvene informacije. Informacije o imenu in naslovu upravljavca (ali soupravljavcev), pravni podlagi in namenih obdelave osebnih podatkov, vrstah osebnih podatkov, ki se obdelujejo, in uporabnikih ter načinih uveljavljanja pravic se lahko zagotovijo v kateri koli ustrezni obliki (na spletišču, s tehnološkimi orodji na osebnih napravah itd.), če so te informacije posamezniku, na katerega se nanašajo osebni podatki, pojasnjene pošteno in učinkovito. Predložene informacije bi morale biti zlahka dostopne, berljive, razumljive in prilagojene zadevnim posameznikom, na katere se nanašajo osebni podatki (po potrebi na primer v otroku razumljivem jeziku). Predložiti je treba tudi vse dodatne informacije, ki so potrebne za zagotavljanje poštene obdelave osebnih podatkov ali so koristne za ta namen, na primer informacije o obdobju hrambe, razlogih, na katerih temelji obdelava osebnih podatkov, ali prenosih osebnih podatkov uporabniku v drugi državi pogodbenici ali nepogodbenici (vključno z informacijami o tem, ali zadevna država nepogodbenica zagotavlja ustrezno raven varstva ali o ukrepih, ki jih je sprejel upravljavec za zagotavljanje take ustrezne ravni varstva osebnih podatkov).[282]

V skladu s pravico do dostopa[283] ima posameznik, na katerega se nanašajo osebni podatki, pravico, da ga upravljavec na zahtevo obvesti, ali se njegovi osebni podatki obdelujejo, in če se, da ga obvesti, kateri osebni podatki se tako obdelujejo.[284] Upravljavci ali obdelovalci morajo poleg tega v skladu s pravico do obveščenosti[285] proaktivno obveščati osebe, katerih osebni podatki se obdelujejo, o – med drugim – namenih, trajanju in načinih obdelave, in to načeloma pred začetkom obdelave.

279 SUVP, uvodna izjava 39.

280 Prav tam.

281 Prav tam.

282 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 68.

283 SUVP, člen 15.

284 Posodobljena Konvencija št. 108, člen 8 in člen 9(1)(b).

285 SUVP, člena 13 in 14.

Primer: zadeva *Smaranda Bara in drugi proti Preşidentele Casei Naţionale de Asigurări de Sănătate in drugim*[286] se je nanašala na prenos davčnih podatkov v zvezi z dohodkom samozaposlenih oseb iz nacionalne agencije davčne uprave v nacionalni zavod za zdravstveno zavarovanje v Romuniji, na podlagi katerega je bilo treba poravnati zaostale prispevke za zdravstveno zavarovanje. SEU je bilo zaprošeno, naj ugotovi, ali bi bilo treba posameznike, na katere se nanašajo osebni podatki, predhodno obvestiti o identiteti upravljavca osebnih podatkov in namenu prenosa osebnih podatkov, preden je te osebne podatke obdelal nacionalni zavod za zdravstveno zavarovanje. SEU je menilo, da je treba, kadar javni upravni organ države članice prenese osebne podatke drugemu javnemu upravnemu organu, ki te podatke nadalje obdeluje, o tem prenosu ali obdelavi obvestiti posameznike, na katere se nanašajo osebni podatki.

V nekaterih primerih so dovoljena odstopanja od obveznosti obveščanja posameznikov, na katere se nanašajo osebni podatki, o obdelavi osebnih podatkov, ki bodo podrobneje obravnavana v razdelku 6.1 o pravicah posameznika, na katerega se nanašajo osebni podatki.

3.2 Načelo omejitve namena

Ključni poudarki

- Namen obdelave osebnih podatkov mora biti določen pred začetkom obdelave.
- Osebnih podatkov ni mogoče nadalje obdelovati na način, ki ni združljiv s prvotnim namenom, čeprav so v SUVP predvidene izjeme od tega pravila, in sicer za namene arhiviranja v javnem interesu, znanstveno- ali zgodovinskoraziskovalne namene in statistične namene.
- Načelo omejitve namena v bistvu pomeni, da mora biti vsaka obdelava osebnih podatkov opravljena za točno določen namen in le za dodatne določene namene, ki so združljivi s prvotnim.

Načelo omejitve namena je eno od temeljnih načel evropskega prava o varstvu osebnih podatkov. Tesno je povezano s preglednostjo, predvidljivostjo in nadzorom uporabnikov: če je namen obdelave dovolj določen in jasen, posamezniki vedo, kaj

286 SEU, *Smaranda Bara in drugi proti Președintele Casei Naționale de Asigurări de Sănătate in drugim*, C-201/14, 1. oktober 2015, točke 28–46.

lahko pričakujejo, povečata se tudi preglednost in pravna varnost. Hkrati je treba jasno opisati namen, da se posameznikom, na katere se nanašajo osebni podatki, omogoči učinkovito uveljavljanje njihovih pravic, kot je pravica do ugovora obdelavi.[287]

V skladu s tem načelom mora biti vsaka obdelava osebnih podatkov opravljena za točno določen namen in le za dodatne določene namene, ki so združljivi s prvotnim.[288] Obdelava osebnih podatkov za nedoločene in/ali neomejene namene je zato nezakonita. Nezakonita je tudi obdelava osebnih podatkov brez določenega namena, ki temelji le na mnenju, da bodo lahko ti podatki v prihodnosti koristni. Zakonitost obdelave osebnih podatkov je odvisna od namena obdelave, ki mora biti izrecen, določen in zakonit.

Vsak novi namen obdelave osebnih podatkov, ki ni združljiv s prvotnim, mora imeti svojo pravno podlago in ne more temeljiti na dejstvu, da so bili osebni podatki prvotno pridobljeni ali obdelani za drug zakoniti namen. Zakonita obdelava je tako omejena na prvotno določen namen, za vsak nov namen obdelave pa je potrebna nova ločena pravna podlaga. Razkritje osebnih podatkov tretjim osebam za nov namen je na primer treba skrbno proučiti, saj je za tako razkritje verjetno potrebna dodatna pravna podlaga, ki se razlikuje od pravne podlage za zbiranje osebnih podatkov.

Primer: letalska družba od potnikov zbira podatke za rezervacijo, da lahko zagotovi ustrezno izvedbo leta. Potrebuje podatke o: številkah sedežev potnikov, posebnih fizičnih omejitvah, na primer potrebi po invalidskem vozičku, in posebnih zahtevah glede prehrane, na primer hrane halal ali košer. Če se od letalskih družb zahteva, naj podatke iz evidence podatkov o potnikih posredujejo organom za priseljevanje na namembnem letališču, se ti podatki tako uporabijo za nadzor nad priseljevanjem, ki se razlikuje od prvotnega namena zbiranja osebnih podatkov. Za prenos teh podatkov organu za priseljevanje se zato zahteva nova in ločena pravna podlaga.

Pri proučitvi obsega in omejitve določenega namena se v posodobljeni Konvenciji št. 108 in SUVP uporablja pojem združljivosti: uporaba podatkov za združljive namene je dovoljena na podlagi prvotne pravne podlage. Nadaljnja obdelava osebnih podatkov se zato ne sme izvajati na način, ki bi za posameznika, na katerega se nanašajo

287 Delovna skupina za varstvo podatkov iz člena 29 (2013), *Mnenje št. 3/2013 o omejitvi namena*, WP 203, 2. april 2013.

288 SUVP, člen 5(1)(b).

osebni podatki, bil nepričakovan, neustrezen ali sporen.[289] Upravljavec bi moral pri presoji, ali se lahko nadaljnja obdelava šteje za združljivo, (med drugim) upoštevati:

- „morebitno povezavo med prvotnimi nameni in nameni načrtovane nadaljnje obdelave;
- okoliščine, v katerih so bili osebni podatki zbrani, zlasti razumna pričakovanja posameznikov, na katere se nanašajo osebni podatki, o nadaljnji uporabi teh podatkov ob upoštevanju njihovega razmerja z upravljavcem;
- naravo osebnih podatkov;
- posledice načrtovane nadaljnje obdelave za te posameznike in
- obstoj ustreznih zaščitnih ukrepov, tako pri prvotnih kot načrtovanih nadaljnjih dejanjih obdelave."[290] To bi bilo na primer mogoče doseči s šifriranjem ali psevdonimizacijo.

Primer: družba Sonček pridobi osebne podatke o strankah v okviru upravljanja odnosov s strankami. Te podatke nato posreduje družbi za neposredno trženje, družbi Mesečina, ki želi te podatke uporabiti pri trženjskih kampanjah tretjih družb. Prenos osebnih podatkov, ki ga opravi družba Sonček, za trženje, ki ga izvajajo druge družbe, pomeni naknadno uporabo osebnih podatkov za nov namen, ki ni združljiv z upravljanjem odnosov s strankami, tj. s prvotnim namenom družbe Sonček za zbiranje podatkov o strankah. Za prenos osebnih podatkov družbi Mesečina je zato potrebna samostojna pravna podlaga.

Nasprotno pa se uporaba osebnih podatkov, pridobljenih v okviru upravljanja odnosov s strankami, za lastne potrebe trženja družbe Sonček, to je pošiljanje trženjskih sporočil njenim strankam za lastne izdelke, na splošno dopušča kot združljiv namen.

V SUVP in posodobljeni Konvenciji št. 108 je navedeno, da se „nadaljnja obdelava v namene arhiviranja v javnem interesu, v znanstveno- ali zgodovinskoraziskovalne

289 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 49.

290 SUVP, uvodna izjava 50 in člen 6(4); Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 49.

namene ali statistične namene“ *a priori* šteje za združljivo s prvotnim namenom.[291] Vendar pa je treba pri nadaljnji obdelavi osebnih podatkov sprejeti ustrezne zaščitne ukrepe, kot so anonimizacija, šifriranje ali psevdonimizacija podatkov ter omejitev dostopa do osebnih podatkov.[292] V SUVP je poleg tega navedeno, da „[k]adar je posameznik, na katerega se nanašajo osebni podatki, privolil ali če obdelava temelji na pravu Unije ali pravu države članice, kar je potreben in sorazmeren ukrep v demokratični družbi za varovanje zlasti pomembnih ciljev v splošnem javnem interesu, bi moralo biti upravljavcu dovoljeno, da nadalje obdeluje osebne podatke, ne glede na združljivost namenov“.[293] Pri nadaljnji obdelavi bi zato bilo treba posameznika, na katerega se nanašajo osebni podatki, obvestiti o namenih in njegovih pravicah, kot je pravica do ugovora.[294]

Primer: družba Sonček v okviru upravljanja odnosov s strankami zbira in hrani osebne podatke o svojih strankah. Nadaljnja uporaba teh podatkov s strani družbe Sonček za statistično analizo nakupovalnih navad njenih strank je dovoljena, ker se statistika šteje za združljiv namen. Dodatna pravna podlaga, na primer privolitev posameznikov, na katere se nanašajo osebni podatki, ni potrebna. Vendar če želi družba Sonček nadalje obdelati osebne podatke za statistične namene, mora uvesti ustrezne zaščitne ukrepe v zvezi s pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki. Tehnični in organizacijski ukrepi, ki jih mora izvajati družba Sonček, lahko vključujejo psevdonimizacijo.

291 SUVP, člen 5(1)(b); posodobljena Konvencija št. 108, člen 5(4)(b). Primer takih nacionalnih določb je avstrijski zakon o varstvu osebnih podatkov (*Datenschutzgesetz*), Zvezni uradni list I, št. 165/1999, točka 46.

292 SUVP, člen 6(4); posodobljena Konvencija št. 108, člen 5(4)(b); Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 50.

293 SUVP, uvodna izjava 50.

294 Prav tam.

3.3 Načelo najmanjšega obsega podatkov

Ključni poudarki

- Obdelava osebnih podatkov mora biti omejena na to, kar je potrebno za izpolnitev zakonitega cilja.
- Obdelava osebnih podatkov bi se morala izvajati le, če namena obdelave ni mogoče razumno uresničiti z drugimi sredstvi.
- Obdelava osebnih podatkov ne sme nesorazmerno posegati v zadevne interese, pravice in svoboščine.

Obdelujejo se samo osebni podatki, ki so ustrezni, relevantni in ne pretirani glede na namene, za katere se zbirajo in/ali nadalje obdelujejo.[295] Vrste osebnih podatkov, izbrane za obdelavo, morajo biti nujne za dosego izraženega skupnega cilja postopkov obdelave, upravljavec pa mora zbiranje osebnih podatkov strogo omejiti na informacije, ki so neposredno pomembne za konkretni namen obdelave.

Primer: SEU je v zadevi *Digital Rights Ireland*[296] proučilo veljavnost direktive o hrambi podatkov, katere cilj je bil uskladiti nacionalne določbe o hrambi osebnih podatkov, pridobljenih ali obdelanih z javno dostopnimi elektronskimi komunikacijskimi storitvami ali omrežji, za njihov morebitni prenos pristojnim organom za boj proti hudim kaznivim dejanjem, kot sta organizirani kriminal in terorizem. Ne glede na to, da se je to štelo za namen, ki dejansko izpolnjuje cilj splošnega interesa, pa se je za problematično štelo dejstvo, da ta direktiva na splošno zajema „vse osebe in vsa sredstva elektronske komunikacije ter vse podatke o prometu brez razlikovanja, omejitve ali izjeme v zvezi s ciljem boja proti hudim kaznivim dejanjem“.[297]

Poleg tega se je z uporabo posebne tehnologije za boljše varovanje zasebnosti včasih mogoče povsem izogniti uporabi osebnih podatkov ali uporabiti ukrepe za zmanjšanje sposobnosti pripisovanja osebnih podatkov posamezniku, na katerega

295 Posodobljena Konvencija št. 108, člen 5(4)(c); SUVP, člen 5(1)(c).

296 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim* in Kärntner Landesregierung in drugi (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014.

297 Prav tam, točki 44 in 57.

se nanašajo (na primer s psevdonimizacijo), s čimer se zagotovi spoštovanje zasebnosti. To je zlasti primerno za obsežnejše sisteme obdelave.

Primer: mestni svet rednim uporabnikom mestnega javnega prevoza za določeno pristojbino ponuja čipno kartico. Na površini kartice je izpisano ime uporabnika, ki je v elektronski obliki navedeno tudi v čipu kartice. Ob uporabi avtobusa ali tramvaja je treba čipno kartico približati čitalniku, nameščenemu na primer na avtobusih in tramvajih. Podatki, prebrani z napravo, se elektronsko preverijo v podatkovni zbirki, v kateri so imena ljudi, ki so kupili kartico za javni prevoz.

Načelo najmanjšega obsega podatkov s tem sistemom ni upoštevano optimalno: preverjanje, ali je posamezniku dovoljeno uporabljati prevozna sredstva, bi bilo mogoče izvesti, ne da bi se osebni podatki na čipni kartici primerjali s podatkovno zbirko. Zadostovala bi na primer posebna elektronska slika v čipu kartice, na primer črtna koda, tako da bi se s približanjem kartice čitalniku potrdilo, ali je kartica veljavna ali ne. Tak sistem ne bi beležil, kdo je uporabil določeno prevozno sredstvo in kdaj. To bi bila najboljša rešitev v smislu načela najmanjšega obsega podatkov, saj je treba v skladu z njim čim bolj zmanjšati zbiranje osebnih podatkov.

Člen 5(1) posodobljene Konvencije št. 108 vsebuje zahtevo po sorazmernosti pri obdelavi osebnih podatkov glede na zakoniti namen, ki se uresničuje. V vseh fazah obdelave je treba vzpostaviti pravično ravnotežje med vsemi zadevnimi interesi. To pomeni, da je treba osebne podatke, ki so ustrezni in relevantni, vendar bi pomenili nesorazmeren poseg v zadevne temeljne pravice in svoboščine, šteti za pretirane.[298]

298 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 52; SUVP, člen 5(1)(c).

3.4 Načelo točnosti osebnih podatkov

Ključni poudarki

- Upravljavec mora načelo točnosti osebnih podatkov upoštevati pri vseh dejanjih obdelave.
- Netočne osebne podatke je treba brez odlašanja izbrisati ali popraviti.
- Osebne podatke je morda treba redno pregledovati in posodabljati, da se zagotovi njihova točnost.

Upravljavec, ki hrani osebne podatke, lahko te podatke uporabi samo, če z razumno gotovostjo zagotovi, da so točni in posodobljeni.[299]

Obveznost zagotavljanja točnosti osebnih podatkov je treba razumeti v okviru namena obdelave osebnih podatkov.

Primer: SEU je v zadevi *Rijkeboer*[300] obravnavalo zahtevo nizozemskega državljana, da od lokalne uprave mesta Amsterdam prejme informacije o identiteti oseb, ki so jim bile v zadnjih dveh letih posredovane informacije, ki se nanašajo nanj in jih imajo lokalne občinske uprave, pa tudi informacije o vsebini razkritih osebnih podatkov. SEU je navedlo, da „pravica do spoštovanja zasebnosti pomeni, da se lahko posameznik, na katerega se osebni podatki nanašajo, prepriča, da je obdelava njegovih osebnih podatkov pravilna in zakonita, zlasti da so osnovni podatki, ki se nanašajo nanj, pravilni in da so posredovani pooblaščenim prejemnikom“. Nato se je sklicevalo na preambulo direktive o varstvu osebnih podatkov, ki določa, da morajo posamezniki, na katere se nanašajo osebni podatki, imeti pravico dostopa do svojih osebnih podatkov, da lahko preverijo, ali so pravilni.[301]

299 SUVP, člen 5(1)(d); posodobljena Konvencija št. 108, člen 5(4)(d).

300 SEU, *College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer*, C-553/07, 7. maj 2009.

301 Uvodna izjava 41 prej veljavne Direktive 95/46/ES.

Posodabljanje shranjenih osebnih podatkov pa je lahko celo zakonsko prepovedano, kadar je glavni namen shranjevanja podatkov dokumentiranje preteklega stanja dogodkov.

Primer: zdravstvene dokumentacije o operaciji ni dovoljeno spreminjati, tj. posodabljati, tudi če se ugotovitve, navedene v dokumentaciji, pozneje izkažejo za napačne. V takih okoliščinah se lahko dodajo le opombe k dokumentaciji, če so jasno označene kot naknadni vnosi.

Nasprotno sta lahko posodabljanje podatkov in redno preverjanje njihove točnosti v nekaterih primerih nujno potrebna zaradi škode, ki bi jo lahko utrpel posameznik, na katerega se nanašajo osebni podatki, če bi podatki ostali netočni.

Primer: če nekdo želi skleniti kreditno pogodbo z bančno ustanovo, bo banka običajno preverila kreditno sposobnost potencialne stranke. Zato so na voljo posebne podatkovne zbirke, ki vsebujejo podatke o preteklih posojilih fizičnih oseb. Če taka podatkovna zbirka vsebuje netočne ali zastarele podatke o posamezniku, lahko to privede do negativnih učinkov za to osebo. Upravljavci takih podatkovnih zbirk si morajo zato še posebej prizadevati za upoštevanje načela točnosti.

3.5 Načelo omejitve hrambe

Ključni poudarek

- Načelo omejitve hrambe pomeni, da je treba osebne podatke izbrisati ali anonimizirati takoj, ko niso več potrebni za namene, za katere so bili zbrani.

V skladu s členom 5(1)(e) SUVP in členom 5(4)(e) posodobljene Konvencije št. 108 morajo biti osebni podatki „hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo“. Ko so ti nameni izpolnjeni, je treba torej osebne podatke izbrisati ali anonimizirati. V ta namen „bi moral upravljavec določiti

roke za izbris ali občasno preverjanje" za zagotovitev, da se osebni podatki hranijo le toliko časa, kolikor je potrebno.[302]

ESČP je v združenih zadevah *S. in Marper* ugotovilo, da mora biti hramba osebnih podatkov v skladu s ključnimi načeli iz zadevnih instrumentov Sveta Evrope ter zakonodajo in prakso drugih pogodbenic sorazmerna glede na namen zbiranja in časovno omejena, zlasti v policijskem sektorju.[303]

> Primer: ESČP je v združenih zadevah *S. in Marper*[304] odločilo, da je neomejena hramba prstnih odtisov, celičnih vzorcev in profilov DNK zadevnih dveh pritožnikov nesorazmerna in nepotrebna v demokratični družbi, saj sta se kazenska postopka zoper zadevna pritožnika končala z oprostitvijo oziroma umikom tožbe.

Časovna omejitev hrambe osebnih podatkov velja samo za podatke, shranjene v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo. Zakonito shranjevanje osebnih podatkov, ki niso več potrebni, je torej mogoče z njihovo anonimizacijo.

Osebni podatki se lahko shranjujejo za daljše obdobje, če se bodo uporabljali zgolj za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene.[305] Pri trajni hrambi in uporabi osebnih podatkov je treba izvajati ustrezne tehnične in organizacijske ukrepe, da se zaščitijo pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki.

Posodobljena Konvencija št. 108 dopušča tudi izjeme od načela omejitve hrambe, če so določene z zakonom, spoštujejo bistvo temeljnih pravic in svoboščin ter so potrebne in sorazmerne za uresničevanje omejenega števila zakonitih ciljev.[306] Ti med drugim vključujejo nacionalno varnost, preiskovanje in pregon kaznivih dejanj,

302 SUVP, uvodna izjava 39.

303 ESČP, združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 4. december 2008; glej na primer tudi ESČP, *M. M. proti Združenemu kraljestvu*, pritožba št. 24029/07, 13. november 2012.

304 ESČP, združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 4. december 2008.

305 SUVP, člen 5(1)(e); posodobljena Konvencija št. 108, člen 5(4)(b) in člen 11(2).

306 Posodobljena Konvencija št. 108, člen 11(1); Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točke 91–98.

izvajanje kazenskih sankcij, zaščito posameznika, na katerega se nanašajo osebni podatki, ter varstvo pravic in temeljnih svoboščin drugih.

Primer: SEU je v zadevi *Digital Rights Ireland*[307] proučilo veljavnost direktive o hrambi podatkov, katere cilj je bil uskladiti nacionalne določbe o hrambi osebnih podatkov, pridobljenih ali obdelanih z javno dostopnimi elektronskimi komunikacijskimi storitvami ali omrežji, za boj proti hudim kaznivim dejanjem, kot sta organizirani kriminal in terorizem. V direktivi o hrambi podatkov je bilo določeno, da se podatki hranijo „najmanj šest mesecev, ne da bi se kakor koli razlikovalo med kategorijami podatkov, določenimi v členu 5 te direktive, glede na njihovo možno uporabnost za zastavljeni cilj ali glede na osebe, ki jih to zadeva".[308] SEU je poleg tega opozorilo, da v direktivi o hrambi podatkov ni objektivnih meril, na podlagi katerih bi bilo treba natančno določiti trajanje hrambe – ta lahko traja od najmanj šest mesecev do največ štiriindvajset mesecev –, da bi se zagotovila njena omejitev na to, kar je nujno potrebno.[309]

3.6 Načelo varnosti osebnih podatkov

Ključni poudarki

- Varnost in zaupnost osebnih podatkov sta ključnega pomena za preprečevanje škodljivih učinkov za posameznika, na katerega se nanašajo osebni podatki.
- Varnostni ukrepi so lahko tehnični in/ali organizacijski.
- Psevdonimizacija je proces, s katerim je mogoče zavarovati osebne podatke.
- Ustreznost varnostnih ukrepov je treba opredeliti za vsak primer posebej in jo redno pregledovati.

V skladu z načelom varnosti osebnih podatkov je treba pri obdelavi osebnih podatkov izvajati ustrezne tehnične in organizacijske ukrepe, s katerimi se zaščitijo pred nenamernim, nepooblaščenim ali nezakonitim dostopom, uporabo, spremembo,

307 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim in Kärntner Landesregierung in drugi* (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014.

308 Prav tam, točka 63.

309 Prav tam, točka 64.

razkritjem, izgubo, uničenjem ali poškodbo.[310] V SUVP je navedeno, da bi morala upravljavec in obdelovalec take ukrepe izvajati ob upoštevanju „najnovejšega tehnološkega razvoja in stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti".[311] Glede na okoliščine posameznega primera bi lahko ustrezni tehnični in organizacijski ukrepi vključevali na primer psevdonimizacijo in šifriranje osebnih podatkov in/ali redno testiranje in vrednotenje učinkovitosti ukrepov za zagotavljanje varnosti obdelave osebnih podatkov.[312]

Kot je pojasnjeno v razdelku 2.1.1, psevdonimizacija podatkov pomeni, da se atributi v osebnih podatkih – ki omogočajo identifikacijo posameznika, na katerega se nanašajo – nadomestijo s psevdonimom, pri čemer se ti identifikatorji v skladu s tehničnimi ali organizacijskimi ukrepi hranijo ločeno. Postopek psevdonimizacije se ne sme zamenjevati s postopkom anonimizacije, v okviru katerega so iz osebnih podatkov odstranjeni vsi identifikacijski elementi.

Primer: stavek „Charles Spencer, rojen 3. aprila 1967, je oče štirih otrok, dveh dečkov in dveh deklic" je na primer mogoče psevdonimizirati tako:

„C. S., 1967, je oče štirih otrok, dveh dečkov in dveh deklic", ali

„324 je oče štirih otrok, dveh dečkov in dveh deklic", ali

„YESz320l je oče štirih otrok, dveh dečkov in dveh deklic".

Uporabniki, ki dostopajo do teh psevdonimiziranih podatkov, v „324" ali „YESz3201" običajno ne morejo prepoznati „Charlesa Spencerja, rojenega 3. aprila 1967". Taki podatki so zato varnejši pred zlorabo.

Prvi primer pa je manj varen. Če se stavek „C. S., 1967, je oče štirih otrok, dveh dečkov in dveh deklic" uporabi v vasici, v kateri živi Charles Spencer, je g. Spencerja lažje prepoznati. Metoda psevdonimizacije lahko vpliva na učinkovitost varstva osebnih podatkov.

310 SUVP, uvodna izjava 39 in člen 5(1)(f); posodobljena Konvencija št. 108, člen 7.

311 SUVP, člen 32(1).

312 Prav tam.

Osebni podatki s šifriranimi ali ločeno hranjenimi atributi se velikokrat uporabljajo kot sredstvo za ohranitev tajnosti identitete oseb. To je zlasti koristno, kadar morajo upravljavci osebnih podatkov zagotoviti, da obravnavajo iste posameznike, na katere se nanašajo osebni podatki, vendar ne potrebujejo ali ne smejo poznati prave identitete teh posameznikov. Tako je na primer, če raziskovalec proučuje potek bolezni pri bolnikih, katerih identiteto pozna samo bolnišnica, v kateri se zdravijo in od katere raziskovalec dobi psevdonimizirane anamneze. Psevdonimizacija je torej pomembno orodje na področju tehnologije za boljše varovanje zasebnosti. Lahko je tudi pomemben dejavnik pri izvajanju vgrajene zasebnosti. To pomeni, da je varstvo osebnih podatkov vgrajeno v ogrodje sistemov za obdelavo osebnih podatkov.

V členu 25 SUVP, v katerem je obravnavano vgrajeno varstvo osebnih podatkov, je psevdonimizacija izrecno navedena kot primer ustreznega tehničnega in organizacijskega ukrepa, ki bi ga morali izvajati upravljavci, da bi upoštevali načela varstva osebnih podatkov in vključili potrebne zaščitne ukrepe. Upravljavci bodo s tem izpolnili zahteve navedene uredbe in zaščitili pravice posameznikov, na katere se nanašajo osebni podatki, pri obdelavi njihovih osebnih podatkov.

Zavezanost k odobrenemu kodeksu ravnanja ali izvajanje odobrenega mehanizma certificiranja lahko pripomore k izkazovanju izpolnjevanja zahteve glede varnosti obdelave.[313] Svet Evrope je v svojem mnenju o posledicah, ki jih ima obdelava evidenc podatkov o potnikih za varstvo osebnih podatkov, navedel tudi druge primere ustreznih varnostnih ukrepov za varstvo osebnih podatkov v sistemih evidenc podatkov o potnikih. Ti vključujejo hrambo osebnih podatkov v varnem prostoru, nadzor nad omejitvijo dostopa z večplastno prijavo in zaščito komunikacije osebnih podatkov z močnim šifriranjem.[314]

Primer: družbena omrežja in ponudniki elektronske pošte uporabnikom omogočajo, da dodajo dodatno plast varnosti osebnih podatkov storitvam, ki jim jih zagotavljajo, in sicer so v ta namen uvedli dvostopenjsko avtentikacijo. Uporabniki morajo poleg vnosa osebnega gesla opraviti dodatno prijavo, če želijo dostopati do osebnega računa. Dodatna prijava je lahko na primer vpis varnostne kode, poslane na številko mobilnega telefona, ki je povezana

313 Prav tam, člen 32(3).

314 Svet Evrope, Posvetovalni odbor po Konvenciji št. 108, *Mnenje o posledicah, ki jih ima obdelava evidenc podatkov o potnikih za varstvo podatkov*, T-PD(2016)18rev, 19. avgust 2016, str. 9.

z osebnim računom. Preverjanje v dveh korakih tako zagotavlja boljšo zaščito osebnih podatkov pred nepooblaščenim dostopom do osebnih računov z vdorom v informacijski sistem.

V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 so navedeni dodatni primeri ustreznih zaščitnih ukrepov, kot sta izvajanje obveznosti glede varovanja poklicne skrivnosti ali sprejetje ustreznih tehničnih varnostnih ukrepov, kot je šifriranje podatkov.[315] Upravljavec ali po potrebi obdelovalec bi moral pri sprejemanju konkretnih varnostnih ukrepov upoštevati več elementov, kot so vrsta in obseg osebnih podatkov, ki se obdelujejo, morebitne škodljive posledice za posameznike, na katere se nanašajo osebni podatki, in potreba po omejenem dostopu do osebnih podatkov.[316] Pri izvajanju ustreznih varnostnih ukrepov je treba upoštevati trenutne najsodobnejše metode za zagotavljanje varnosti osebnih podatkov in tehnike za njihovo obdelavo. Stroški takih ukrepov morajo biti sorazmerni z resnostjo in verjetnostjo morebitnih tveganj. Varnostne ukrepe je treba redno pregledovati, da jih je po potrebi mogoče posodabljati.[317]

V skladu s posodobljeno Konvencijo št. 108 in SUVP mora upravljavec v primeru kršitve varnosti osebnih podatkov, zaradi katere so ogrožene pravice in svoboščine posameznikov, o njej brez nepotrebnega odlašanja uradno obvestiti pristojni nadzorni organ.[318] Podobna obveznost sporočitve kršitve posamezniku, na katerega se nanašajo osebni podatki, se uporablja, če je verjetno, da bi kršitev lahko povzročila veliko tveganje za njegove pravice in svoboščine.[319] Posameznikom, na katere se nanašajo osebni podatki, je treba take kršitve sporočiti v jasnem in preprostem jeziku.[320] Če se obdelovalec seznani s kršitvijo varnosti osebnih podatkov, mora o tem nemudoma obvestiti upravljavca.[321] V nekaterih primerih se lahko uporabljajo izjeme od obveznosti obveščanja. Upravljavcu na primer ni treba obvestiti nadzornega organa, če „ni verjetno, da bi bile s kršitvijo varnosti osebnih podatkov ogrožene pravice in svoboščine posameznikov".[322] Posameznika, na katerega se nanašajo osebni podatki, prav tako ni treba obvestiti, če na podlagi izvedenih varnostnih ukrepov

315 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 56.

316 Prav tam, točka 62.

317 Prav tam, točka 63.

318 Posodobljena konvencija št. 108, člen 7(2); SUVP, člen 33(1).

319 Posodobljena Konvencija št. 108, člen 7(2); SUVP, člen 34(1).

320 SUVP, člen 34(2).

321 Prav tam, člen 33(1).

322 Prav tam, člen 33(1).

postanejo osebni podatki nerazumljivi nepooblaščenim osebam ali če je z naknadnimi ukrepi zagotovljeno, da se veliko tveganje verjetno ne bo več udejanjilo.[323] Če bi bil za sporočilo posamezniku, na katere se nanašajo osebni podatki, o kršitvi varnosti njihovih osebnih podatkov potreben nesorazmeren napor upravljavca, se lahko z javnim sporočilom ali podobnim ukrepom zagotovi, da so „posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni".[324]

3.7 Načelo odgovornosti

Ključni poudarki

- Odgovornost pomeni, da morajo upravljavci in obdelovalci v okviru dejavnosti obdelave dejavno in stalno izvajati ukrepe za spodbujanje in zagotavljanje varstva osebnih podatkov.
- Upravljavci in obdelovalci so odgovorni za skladnost dejavnosti obdelave s pravom o varstvu osebnih podatkov in izpolnjevanje svojih zadevnih obveznosti.
- Upravljavci morajo biti posameznikom, na katere se nanašajo osebni podatki, širši javnosti in nadzornim organom kadar koli zmožni dokazati, da upoštevajo določbe o varstvu osebnih podatkov. Tudi obdelovalci morajo izpolnjevati nekatere obveznosti, ki so strogo povezane z odgovorno obdelavo osebnih podatkov (na primer vodenje evidence o dejanjih obdelave in imenovanje pooblaščene osebe za varstvo podatkov).

V SUVP in posodobljeni Konvenciji št. 108 je določeno, da je upravljavec odgovoren za skladnost z načeli obdelave osebnih podatkov, opisanimi v tem poglavju, in da mora biti to skladnost tudi zmožen dokazati.[325] V ta namen mora izvajati ustrezne tehnične in organizacijske ukrepe.[326] Čeprav načelo odgovorne obdelave osebnih podatkov iz člena 5(2) SUVP velja le za upravljavce, se tudi od obdelovalcev pričakuje, da so odgovorni, saj morajo izpolnjevati več obveznosti, in da so tesno povezani z odgovorno obdelavo osebnih podatkov.

Zakonodaja EU in Sveta Evrope o varstvu osebnih podatkov poleg tega določa, da je upravljavec odgovoren za skladnost z načeli varstva osebnih podatkov,

323 Prav tam, člen 34(3)(a) in (b).

324 Prav tam, člen 34(3)(c).

325 Prav tam, člen 5(2); posodobljena Konvencija št. 108, člen 10(1).

326 SUVP, člen 24.

obravnavanih v razdelkih 3.1 do 3.6, in da bi moral biti to skladnost tudi zmožen dokazati.[327] Delovna skupina za varstvo podatkov iz člena 29 je poudarila, da „bi se vrsta postopkov in mehanizmov razlikovala glede na tveganja, ki jih pomenita obdelava in narava podatkov".[328]

Upravljavci lahko olajšajo izpolnjevanje te zahteve na različne načine, med drugim tako, da:

- evidentirajo dejavnosti obdelave osebnih podatkov in nadzornemu organu na zahtevo omogočijo dostop do evidence;[329]
- v nekaterih primerih imenujejo pooblaščeno osebo za varstvo podatkov, ki je vključena v vse zadeve v zvezi z varstvom osebnih podatkov;[330]
- izvedejo ocene učinka v zvezi z varstvom osebnih podatkov za tiste vrste obdelave, ki bi lahko povzročile veliko tveganje za pravice in svoboščine posameznikov;[331]
- zagotavljajo vgrajeno in privzeto varstvo osebnih podatkov;[332]
- izvajajo načine in postopke za uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki;[333]
- so zavezani k odobrenemu kodeksu ravnanja ali mehanizmom certificiranja.[334]

Načelo odgovornosti iz člena 5(2) SUVP sicer ne omenja izrecno obdelovalcev, vendar nekatere določbe, povezane z odgovornostjo, vsebujejo tudi obveznosti zanje, kot sta vodenje evidence dejavnosti obdelave in imenovanje pooblaščene osebe za varstvo podatkov za vse dejavnosti obdelave, pri katerih je to potrebno.[335] Obdelo-

327 Prav tam, člen 5(2); posodobljena Konvencija št. 108, člen 10(1).

328 Delovna skupina za varstvo podatkov iz člena 29, *Mnenje 3/2010 o načelu zanesljivega izvajanja*, WP 173, Bruselj, 13. julij 2010, točka 12.

329 SUVP, člen 30.

330 Prav tam, členi 37–39.

331 Prav tam, člen 35; posodobljena Konvencija št. 108, člen 10(2).

332 SUVP, člen 25; posodobljena Konvencija št. 108, člen 10(2) in (3).

333 Prav tam, člena 12 in 24.

334 Prav tam, člena 40 in 42.

335 Prav tam, člen 5(2) ter člena 30 in 37.

valci morajo poleg tega zagotoviti, da se izvajajo vsi potrebni ukrepi za zagotavljanje varnosti osebnih podatkov.[336] V pravno zavezujoči pogodbi med upravljavcem in obdelovalcem mora biti določeno, da obdelovalec pomaga upravljavcu pri izpolnjevanju nekaterih zahtev glede skladnosti, na primer pri izvajanju ocene učinka v zvezi z varstvom podatkov ali z obvestitvijo upravljavca o kršitvi varnosti osebnih podatkov po tem, ko se z njo seznani.[337]

Organizacija za gospodarsko sodelovanje in razvoj (OECD) je leta 2013 sprejela smernice o zasebnosti, v katerih je poudarjeno, da imajo upravljavci pomembno vlogo pri zagotavljanju varstva osebnih podatkov v praksi. Smernice vključujejo načelo odgovornosti, v skladu s katerim mora biti upravljavec osebnih podatkov odgovoren za upoštevanje ukrepov, s katerimi se uresničujejo zgoraj navedena vsebinska načela.[338]

Primer: načelo odgovornosti je poudarjeno z zakonodajnim primerom spremembe Direktive 2002/58/ES o zasebnosti in elektronskih komunikacijah iz leta 2009.[339] Člen 4 navedene direktive v svoji spremenjeni obliki določa obveznost izvajanja varnostne politike, in sicer da se „zagot[ovi] izvajanje varnostne politike pri obdelavi osebnih podatkov“. Kar zadeva varnostne določbe navedene direktive, se je zakonodajalec torej odločil, da je treba uvesti izrecno zahtevo po opredelitvi in izvajanju varnostne politike.

Po mnenju Delovne skupine za varstvo podatkov iz člena 29[340] je bistvo odgovornosti upravljavčeva obveznost, da:

- uvede ukrepe, s katerimi se (v običajnih okoliščinah) zagotovi, da se v okviru dejanj obdelave upoštevajo pravila o varstvu osebnih podatkov, ter

336 Prav tam, člen 28(3)(c).

337 Prav tam, člen 28(3)(f).

338 OECD, *Guidelines on governing the Protection of Privacy and transborder flows of personal data* (Smernice o varstvu zasebnosti in čezmejnem prenosu osebnih podatkov), 2013, člen 14.

339 Direktiva 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov (UL L 337, 18.12.2009, str. 11).

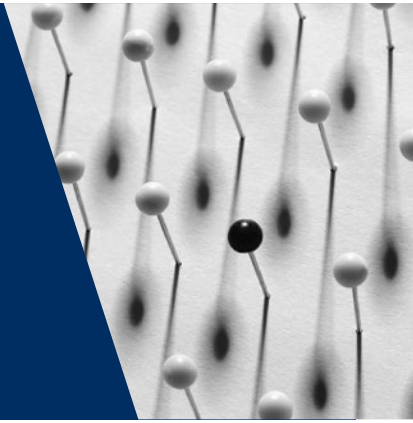
340 Delovna skupina za varstvo podatkov iz člena 29, *Mnenje 3/2010 o načelu zanesljivega izvajanja*, WP 173, Bruselj, 13. julij 2010.

- ima pripravljeno dokumentacijo, s katero lahko posameznikom, na katere se nanašajo osebni podatki, in nadzornim organom dokaže, kateri ukrepi so bili sprejeti za dosego skladnosti s pravili o varstvu osebnih podatkov.

Načelo odgovornosti torej pomeni, da morajo upravljavci dejavno dokazovati skladnost s predpisi in ne le čakati, da bodo posamezniki, na katere se nanašajo osebni podatki, ali nadzorni organi opozorili na pomanjkljivosti.

4

Pravila evropskega prava o varstvu osebnih podatkov



EU	Obravnavane teme	Svet Evrope
Pravila o zakoniti obdelavi osebnih podatkov		
SUVP, člen 6(1)(a) SEU, C-543/09, *Deutsche Telekom AG proti Bundesrepublik Deutschland*, 2011 SEU, C-536/15, zadevi *Tele2 (Netherlands) BV in drugi proti Autoriteit Consument en Markt (ACM)*, 2017	**Privolitev**	Priporočilo o oblikovanju profilov, člen 3(4)(b) in člen 3(6) Posodobljena Konvencija št. 108, člen 5(2)
SUVP, člen 6(1)(b)	**(Pred)pogodbeno razmerje**	Priporočilo o oblikovanju profilov, člen 3(4)(b)
SUVP, člen 6(1)(c)	**Zakonske obveznosti upravljavca**	Priporočilo o oblikovanju profilov, člen 3(4)(a)
SUVP, člen 6(1)(d)	**Življenjski interesi posameznika, na katerega se nanašajo osebni podatki**	Priporočilo o oblikovanju profilov, člen 3(4)(b)
SUVP, člen 6(1)(e) SEU, C-524/06, *Huber proti Bundesrepublik Deutschland* (veliki senat), 2008	**Javni interes in izvajanje javne oblasti**	Priporočilo o oblikovanju profilov, člen 3(4)(b)

EU	Obravnavane teme	Svet Evrope
SUVP, člen 6(1)(f) SEU, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde proti Rīgas pašvaldības SIA „Rīgas satiksme“*, 2017 SEU, združeni zadevi C-468/10 in C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, 2011	Zakoniti interesi drugih	Priporočilo o oblikovanju profilov, člen 3(4)(b) ESČP, *Y proti Turčiji*, pritožba št. 648/10, 2015
SUVP, člen 6(4)	Izjema od omejitve namena: nadaljnja obdelava za druge namene	Posodobljena Konvencija št. 108, člen 5(4)(b)
Pravila o zakoniti obdelavi občutljivih osebnih podatkov		
SUVP, člen 9(1)	Splošna prepoved obdelave	Posodobljena Konvencija št. 108, člen 6
SUVP, člen 9(2)	Izjeme od splošne prepovedi	Posodobljena Konvencija št. 108, člen 6
Pravila o varni obdelavi osebnih podatkov		
SUVP, člen 32	Obveznost zagotovitve varne obdelave	Posodobljena Konvencija št. 108, člen 7(1) ESČP, *I proti Finski*, pritožba št. 20511/03, 2008
SUVP, člen 28 in člen 32(1)(b)	Obveznost zaupnosti	Posodobljena Konvencija št. 108, člen 7(1)
SUVP, člen 34 Direktiva o zasebnosti in elektronskih komunikacijah, člen 4(2)	Obvestila o kršitvah varnosti osebnih podatkov	Posodobljena Konvencija št. 108, člen 7(2)
Pravila o odgovornosti in spodbujanju skladnosti		
SUVP, členi 12, 13 in 14	Preglednost na splošno	Posodobljena Konvencija št. 108, člen 8
SUVP, členi 37, 38 in 39	Pooblaščene osebe za varstvo podatkov	Posodobljena Konvencija št. 108, člen 10(1)
SUVP, člen 30	Evidenca dejavnosti obdelave	
SUVP, člena 35 in 36	Ocena učinka in predhodno posvetovanje	Posodobljena Konvencija št. 108, člen 10(2)

EU	Obravnavane teme	Svet Evrope
SUVP, člena 33 in 34	Obvestila o kršitvah varnosti osebnih podatkov	Posodobljena Konvencija št. 108, člen 7(2)
SUVP, člena 40 in 41	Kodeksi ravnanja	
SUVP, člena 42 in 43	Certificiranje	
Vgrajeno in privzeto varstvo osebnih podatkov		
SUVP, člen 25(1)	Vgrajeno varstvo osebnih podatkov	Posodobljena Konvencija št. 108, člen 10(2)
SUVP, člen 25(2)	Privzeto varstvo osebnih podatkov	Posodobljena Konvencija št. 108, člen 10(3)

Načela so nujno splošna. Njihova uporaba v konkretnih primerih je deloma odvisna od razlage in izbire sredstev. Po **pravu Sveta Evrope** je pogodbenicam posodobljene Konvencije št. 108 prepuščeno, da tako različno razlago pojasnijo v nacionalnem pravu. Položaj v **pravu EU** je drugačen: za uveljavitev varstva osebnih podatkov na notranjem trgu se je štelo, da so na ravni EU potrebna podrobnejša pravila za uskladitev ravni varstva osebnih podatkov v nacionalnih zakonodajah držav članic. SUVP na podlagi načel iz njenega člena 5 določa podrobna pravila, ki se neposredno uporabljajo v nacionalnem pravnem redu. V naslednjih opisih podrobnih pravil o varstvu osebnih podatkov na evropski ravni je zato obravnavano predvsem pravo EU.

4.1 Pravila o zakoniti obdelavi osebnih podatkov

Ključna poudarka

- Osebni podatki se lahko obdelujejo zakonito, če je izpolnjeno eno od naslednjih meril:
  - obdelava temelji na privolitvi posameznika, na katerega se nanašajo osebni podatki;
  - obdelava osebnih podatkov je nujna zaradi pogodbenega razmerja;
  - obdelava je nujna zaradi izpolnjevanja pravne obveznosti upravljavca;
  - obdelava osebnih podatkov posameznikov je nujna zaradi njihovih življenjskih interesov;
  - obdelava je potrebna za opravljanje naloge v javnem interesu;

  - razlog za obdelavo so zakoniti interesi upravljavcev ali tretjih oseb, vendar samo, če nad njimi ne prevladajo interesi ali temeljne pravice posameznikov, na katere se nanašajo osebni podatki.
- Za zakonito obdelavo občutljivih osebnih podatkov velja posebna, strožja ureditev.

4.1.1 Zakoniti razlogi za obdelavo osebnih podatkov

V poglavju II SUVP z naslovom Načela je določeno, da je treba pri vsaki obdelavi osebnih podatkov upoštevati, prvič, načela v zvezi s kakovostjo osebnih podatkov iz člena 5 navedene uredbe. Eno od načel je, da bi morali biti osebni podatki „obdelani zakonito, pošteno in na pregleden način". Drugič, da bi bili osebni podatki obdelani zakonito, mora biti obdelava v skladu z enim od zakonitih razlogov za zakonito obdelavo osebnih podatkov iz člena 6[341] za neobčutljive osebne podatke in člena 9 za posebne vrste osebnih podatkov (ali občutljive osebne podatke). Podobno je v poglavju II posodobljene Konvencije št. 108, v katerem so določena osnovna načela za varstvo osebnih podatkov, določeno, da mora biti obdelava osebnih podatkov sorazmerna glede na zakoniti cilj, ki se uresničuje, da bi bila zakonita.

Ne glede na zakonito podlago za obdelavo, na katero se sklicuje upravljavec za začetek dejanja obdelave osebnih podatkov, bo moral upravljavec uporabiti tudi zaščitne ukrepe, določene v okviru splošne pravne ureditve varstva osebnih podatkov.

Privolitev

V okviru prava Sveta Evrope je privolitev navedena v členu 5(2) posodobljene Konvencije št. 108. Sklicevanja nanjo so tudi v sodni praksi ESČP in več priporočilih Sveta Evrope.[342] **V okviru prava EU** je privolitev kot podlaga za zakonito obdelavo osebnih podatkov jasno določena v členu 6 SUVP, izrecno je navedena tudi v členu 8 Listine. Značilnosti veljavne privolitve so pojasnjene v opredelitvi privolitve v členu 4, pogoji za pridobitev veljavne privolitve so podrobneje opisani v členu 7, posebna pravila za privolitev otroka v zvezi s storitvami informacijske družbe pa v členu 8 SUVP.

341 SEU, *Rechnungshof proti Österreichischer Rundfunk in drugim* in *Christa Neukomm in Joseph Lauermann proti Österreichischer Rundfunk*, združene zadeve C-465/00, C-138/01 in C-139/01, 20. maj 2003, točka 65; SEU, *Heinz Huber proti Bundesrepublik Deutschland* (veliki senat), C-524/06, 16. december 2008, točka 48, in SEU, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, združeni zadevi C-468/10 in C-469/10, 24. november 2011, točka 26.

342 Glej na primer Svet Evrope, Odbor ministrov, Priporočilo Rec(2010)13 državam članicam o varstvu posameznikov v zvezi z avtomatsko obdelavo osebnih podatkov pri oblikovanju profilov, 2010, člen 3(4)(b).

Kot je pojasnjeno v razdelku 2.4, mora biti privolitev prostovoljna, informirana, konkretna in nedvoumna. Privolitev mora biti izjava ali jasno pritrdilno dejanje, s katerim se izrazi strinjanje z obdelavo, pri čemer ima oseba pravico, da svojo privolitev kadar koli prekliče. Upravljavci morajo voditi preverljivo evidenco privolitev.

Prostovoljna privolitev

V okviru posodobljene Konvencije **Sveta Evrope** št. 108 mora privolitev posameznika, na katerega se nanašajo osebni podatki, pomeniti svoboden izraz namerne izbire.[343] Prostovoljna privolitev je veljavna samo, če „ima posameznik, na katerega se osebni podatki nanašajo, resnično izbiro in če ne obstaja nevarnost zavajanja, ustrahovanja, prisiljevanja ali znatnih negativnih posledic, če posameznik ne da privolitve".[344] V zvezi s tem je v **pravu EU** določeno, da se privolitev ne šteje za prostovoljno, „če posameznik, na katerega se nanašajo osebni podatki, nima možnosti dejanske ali prostovoljne izbire ali privolitve ne more zavrniti ali preklicati brez škode".[345] V SUVP je poudarjeno, da se „[p]ri ugotavljanju, ali je bila privolitev dana prostovoljno, [...] med drugim zlasti upošteva, ali je izvajanje pogodbe, vključno z zagotavljanjem storitve, pogojeno s privolitvijo v obdelavo osebnih podatkov, ki ni potrebna za izvedbo zadevne pogodbe".[346] V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je navedeno, da se na posameznika, na katerega se nanašajo osebni podatki, ne sme izvajati nedopustno vplivanje ali pritisk (ki je lahko ekonomske ali druge narave), bodisi neposreden bodisi posreden, privolitev pa se ne bi smela šteti za prostovoljno, če posameznik, na katerega se nanašajo osebni podatki, nima možnosti dejanske izbire ali privolitve ne more zavrniti ali preklicati brez škode.[347]

Primer: nekatere občine v državi A so se odločile, da bodo razvile kartice za prebivalce z vgrajenim čipom. Za prebivalce pridobitev te elektronske kartice ni obvezna. Vendar prebivalci, ki niso imetniki te kartice, nimajo dostopa do več pomembnih upravnih storitev, kot so možnost spletnega plačevanja občinskih davkov, elektronskega vlaganja pritožb, na katere morajo zadevni

343 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 42.

344 Delovna skupina za varstvo podatkov iz člena 29 (2011), *Mnenje št. 15/2011 o opredelitvi privolitve*, WP 187, Bruselj, 13. julij 2011, str. 12.

345 SUVP, uvodna izjava 42.

346 Prav tam, člen 7(4).

347 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 42.

organi odgovoriti v treh dneh, in celo preskakovanja vrst, kupovanja vstopnic po znižani ceni ob obisku občinske koncertne dvorane in uporabe skenerjev pri vstopu v prostore.

V tem primeru obdelava osebnih podatkov, ki jo izvajajo občine, ne more temeljiti na privolitvi. Ker obstaja vsaj posreden pritisk na prebivalce, da pridobijo elektronsko kartico in privolijo v obdelavo, privolitev ni dana prostovoljno. Razvoj sistema elektronskih izkaznic, ki ga izvajajo občine, bi zato moral temeljiti na drugi zakoniti podlagi, ki bi upravičevala obdelavo. Občine bi se lahko na primer sklicevale na to, da je obdelava potrebna za izvajanje naloge v javnem interesu, kar je v skladu s členom 6(1)(e) SUVP zakonita podlaga za obdelavo.[348]

Prostovoljna privolitev bi lahko bila ogrožena tudi v položajih podrejenosti, kadar je med upravljavcem, ki mora dobiti privolitev, in posameznikom, na katerega se nanašajo osebni podatki in ki mora dati privolitev, precejšnje ekonomsko ali drugo neravnovesje.[349] Tipičen primer takih neravnovesij in podrejenosti je obdelava osebnih podatkov, ki jo v okviru delovnega razmerja izvaja delodajalec. Po mnenju Delovne skupine iz člena 29 „[z]aposleni glede na odvisnost, ki izhaja iz razmerja med delodajalcem in zaposlenim, skoraj nikoli niso v položaju, da bi lahko prostovoljno dali, zavrnili ali preklicali privolitev. Zaradi neravnotežja moči lahko zaposleni prostovoljno privolitev dajo le v izjemnih okoliščinah, ko sprejetje ali zavrnitev ponudbe nima prav nobenih posledic."[350]

Primer: veliko podjetje namerava izključno zaradi izboljšanja komunikacije znotraj podjetja ustvariti imenik, ki bo vseboval imena vseh zaposlenih, njihov položaj v podjetju in poslovni naslov. Vodja kadrovske službe predlaga,

348 Delovna skupina za varstvo podatkov iz člena 29 (2011), *Mnenje št. 15/2011 o opredelitvi privolitve*, WP 187, Bruselj, 13. julij 2011, str. 16. Dodatni primeri, v katerih obdelava osebnih podatkov ne more temeljiti na privolitvi, temveč je zanjo potrebna drugačna pravna podlaga za utemeljitev obdelave, so navedeni na straneh 14 in 17 zadevnega mnenja.

349 Glej tudi Delovna skupina za varstvo podatkov iz člena 29 (2001), *Opinion 8/2001 on the processing of personal data in the employment context* (Mnenje št. 8/2001 o obdelavi osebnih podatkov v okviru zaposlitve), WP 48, Bruselj, 13. september 2001; Delovna skupina za varstvo podatkov iz člena 29 (2005), *Delovni dokument o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995*, WP 114, Bruselj, 25. november 2005; Delovna skupina za varstvo podatkov iz člena 29 (2017), *Mnenje št. 2/2017 o obdelavi podatkov pri delu*, WP 249, Bruselj, 8. junij 2017.

350 Delovna skupina za varstvo podatkov iz člena 29, *Mnenje št. 2/2017 o obdelavi podatkov pri delu*, WP 249, Bruselj, 8. junij 2017.

naj se v imenik doda fotografija vsakega zaposlenega, da bo na sestankih lažje prepoznati sodelavce. Predstavniki zaposlenih zahtevajo, naj se to stori samo, če posamezni zaposleni v to privoli.

V takem primeru je treba privolitev zaposlenega priznati kot pravno podlago za obdelavo fotografij v imeniku, saj se zaposleni pri delodajalcu verjetno sploh ne bo znašel v nemilosti, če se ne bo strinjal z objavo svoje fotografije v imeniku.

Primer: podjetje A načrtuje sestanek med tremi od svojih zaposlenih in direktorji podjetja B, da bi razpravljali o morebitnem prihodnjem sodelovanju pri projektu. Sestanek bo potekal v prostorih podjetja B, ki od podjetja A zahteva, naj mu po elektronski pošti pošlje imena, življenjepise in fotografije udeležencev sestanka. Podjetje B trdi, da imena in fotografije udeležencev potrebuje, da bo varnostno osebje ob vhodu v stavbo lahko preverilo, ali gre za prave osebe, življenjepisi pa bodo direktorjem omogočili, da se bolje pripravijo na sestanek. V tem primeru prenos osebnih podatkov svojih zaposlenih, ki ga opravi podjetje A, ne more temeljiti na privolitvi. V zvezi s privolitvijo ni mogoče šteti, da bi bila „dana prostovoljno“, saj je mogoče, da se lahko zaposleni znajdejo v nemilosti, če prošnjo zavrnejo (tako bi jih na primer lahko drug sodelavec zamenjal ne le na sestanku, temveč tudi na splošno pri sodelovanju s podjetjem B in pri projektu). Obdelava mora zato temeljiti na drugi zakoniti podlagi.

To pa ne pomeni, da privolitev nikoli ne more biti veljavna v okoliščinah, ko bi zavrnitev privolitve imela nekatere negativne posledice. Če na primer zavrnitev pridobitve trgovske kartice zvestobe pomeni samo, da kupec ne bo upravičen do majhnega znižanja cene za določeno blago, bi lahko bila privolitev še vedno veljavna pravna podlaga za obdelavo osebnih podatkov kupcev, ki so privolili v pridobitev take kartice. Med podjetjem in kupcem ni podrejenosti, posledice zavrnitve pa za posameznika, na katerega se nanašajo osebni podatki, niso dovolj resne, da bi se onemogočila svobodna izbira (če je znižanje cene dovolj majhno, da ne vpliva na njegovo svobodno izbiro).

Če pa je blago ali storitve mogoče pridobiti le z razkritjem nekaterih osebnih podatkov upravljavcu ali nadalje tretjim osebam, privolitve posameznika, na katerega se nanašajo osebni podatki, da se razkrijejo njegovi podatki, ki niso potrebni za pogodbo, ni mogoče šteti za svobodno izbiro, zato na podlagi zakonodaje o varstvu

osebnih podatkov ni veljavna.[351] SUVP precej strogo prepoveduje povezovanje privolitve z zagotavljanjem blaga in storitev.[352]

Primer: soglasja, ki ga potniki dajo letalski družbi, da t. i. evidence podatkov o potnikih (tj. podatke o njihovi identiteti, prehranjevalnih navadah ali zdravstvenih težavah) posreduje organom za priseljevanje določene tuje države, ni mogoče šteti za veljavno privolitev na podlagi zakonodaje o varstvu osebnih podatkov, saj potniki nimajo izbire, če želijo obiskati to državo. Da bi se taki osebni podatki posredovali zakonito, je potrebna druga pravna podlaga, in ne privolitev, najverjetneje neki zakon.

Informirana privolitev

Posameznik, na katerega se nanašajo osebni podatki, mora imeti dovolj informacij, preden sprejme odločitev. Informirana privolitev običajno vključuje natančen in preprosto razumljiv opis vsebine, za katero je potrebna privolitev. Kot pojasnjuje Delovna skupina iz člena 29, mora privolitev temeljiti na presoji in razumevanju dejstev in posledic ravnanja posameznika, na katerega se nanašajo osebni podatki, s katerim ta privoli v obdelavo. Zato morajo biti „[z]adevnemu posamezniku […] jasno in razumljivo dane na voljo točne in popolne informacije o vseh pomembnih zadevah […], kot so narava obdelanih podatkov, nameni obdelave, prejemniki morebitnih prenosov in pravice posameznika, na katerega se nanašajo podatki“.[353] Da bi bila privolitev informirana, morajo biti posamezniki seznanjeni tudi s tem, kakšne so posledice, če ne privolijo v obdelavo.

Zaradi pomena informirane privolitve se je ta pojem poskušalo pojasniti v SUVP in v Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108. V uvodnih izjavah SUVP je določeno, da informirana privolitev pomeni, da „bi posameznik, na katerega se nanašajo osebni podatki, […] moral poznati vsaj identiteto upravljavca in namene obdelave osebnih podatkov“, ki se obdelujejo.[354]

V izjemnem primeru privolitve, ki se uporablja kot odstopanje za zagotovitev zakonite podlage za mednarodni prenos osebnih podatkov, mora upravljavec

351 SUVP, člen 7(4).

352 Prav tam.

353 Delovna skupina za varstvo podatkov iz člena 29 (2007), Delovni dokument o obdelavi osebnih podatkov v zvezi z zdravjem v elektronskih zdravstvenih kartonih (EZK), WP 131, Bruselj, 15. februar 2007.

354 SUVP, uvodna izjava 42.

posameznika, na katerega se nanašajo osebni podatki, obvestiti o morebitnih tveganjih, ki jih zaradi nesprejetja sklepa o ustreznosti in ustreznih zaščitnih ukrepov takšni prenosi pomenijo zanj, da se navedena privolitev šteje za veljavno.[355]

V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je določeno, da je treba zagotoviti informacije o posledicah odločitve posameznika, na katerega se nanašajo osebni podatki, in sicer kaj pomeni privolitev in obseg, v katerem je ta dana.[356]

Pomembna je kakovost informacij. Kakovost informacij pomeni, da bi bilo treba jezik, v katerem se informacije navedejo, prilagoditi njihovim predvidljivim naslovnikom. Informacije je treba zagotoviti brez uporabe žargona ter v jasnem in preprostem jeziku, ki ga lahko običajen uporabnik razume.[357] Informacije morajo biti posamezniku, na katerega se nanašajo osebni podatki, tudi zlahka na voljo, in sicer se lahko zagotovijo ustno ali v pisni obliki. Dostopnost in vidnost informacij sta pomembna dejavnika: informacije morajo biti jasno vidne in na opaznem mestu. V spletnem okolju so lahko dobra rešitev večplastna informativna obvestila, saj ta posameznikom, na katere se nanašajo osebni podatki, omogočajo izbiro med dostopom do strnjene ali bolj izčrpne različice informacij.

Konkretna privolitev

Da je privolitev veljavna, mora biti povezana s konkretnim namenom obdelave, ki mora biti opisan jasno in nedvoumno. To je neločljivo povezano s kakovostjo informacij o namenu privolitve. Pri tem so pomembna razumna pričakovanja povprečnega posameznika, na katerega se nanašajo osebni podatki. Tega je treba znova vprašati za privolitev, če naj bi se dejanja obdelave dodala ali spremenila tako, da tega ob prvotni privolitvi ni bilo mogoče razumno predvideti, in bi tako privedla do spremembe namena. Kadar je obdelava večnamenska, bi bilo treba privolitev dati za vse namene obdelave.[358]

355 Prav tam, člen 49(1)(a).

356 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 42.

357 Delovna skupina za varstvo podatkov iz člena 29 (2011), *Mnenje št. 15/2011 o opredelitvi privolitve*, WP 187, Bruselj, 13. julij 2011, str. 20.

358 SUVP, uvodna izjava 32.

Primeri: SEU je v zadevi *Deutsche Telekom AG*[359] obravnavalo, ali ponudnik telekomunikacijskih storitev, ki je moral posredovati osebne podatke o naročnikih za njihovo objavo v imenikih, potrebuje novo privolitev posameznikov, na katere se nanašajo osebni podatki,[360] saj uporabniki ob privolitvi prvotno niso bili poimensko navedeni.

SEU je menilo, da na podlagi člena 12 Direktive o zasebnosti in elektronskih komunikacijah nova privolitev pred posredovanjem podatkov ni nujna, saj imajo posamezniki, na katere se nanašajo osebni podatki, možnost privoliti le v namen obdelave, tj. objavo njihovih podatkov, ne morejo pa izbirati med različnimi imeniki, v katerih bi se lahko ti podatki objavili.

Kot je poudarilo SEU, „iz kontekstualne in sistematične razlage člena 12 Direktive o zasebnosti in elektronskih komunikacijah izhaja, da se privolitev iz odstavka 2 tega člena nanaša na namen objave osebnih podatkov v javnem imeniku, ne pa posebej na identiteto ponudnika imenika“.[361] Poleg tega „bi naročniku utegnila škoditi sama objava osebnih podatkov v imeniku, katerega namen je poseben“,[362] ne pa identiteta izdajatelja imenika.

Zadeva *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV proti Autoriteit Consument en Markt (ACM)*[363] se je nanašala na zahtevo belgijske družbe, ki ponuja telefonske imeniške storitve in storitve zagotavljanja imenikov, naj ji podjetja, ki dodeljujejo telefonske številke na Nizozemskem, zagotovijo dostop do podatkov o svojih naročnikih. Belgijska družba se je sklicevala na obveznost iz Direktive o univerzalnih storitvah.[364] V skladu z njo morajo podjetja, ki dodeljujejo telefonske številke, te številke na zahtevo dati na voljo za vključitev v imenik, če so naročniki privolili v objavo svojih telefonskih

359 SEU, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, C-543/09, 5. maj 2011. Glej zlasti točki 53 in 54.

360 Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

361 SEU, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, C-543/09, 5. maj 2011, točka 61.

362 Prav tam, točka 62.

363 SEU, *Tele2 (Netherlands) BV in drugi proti Autoriteit Consument en Markt (ACM)*, C-536/15, 15. marec 2017.

364 Direktiva 2002/22/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami (Direktiva o univerzalnih storitvah) (UL L 108, 24.4.2002, str. 51), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 (Direktiva o univerzalnih storitvah) (UL L 337, 18.12.2009, str. 11).

številk. Nizozemska podjetja so posredovanje telefonskih številk zavrnila, pri čemer so trdila, da jim zadevnih podatkov ni treba zagotoviti podjetju, ustanovljenemu v drugi državi članici. Trdila so, da so uporabniki ob privolitvi v objavo svojih telefonskih številk mislili, da bodo objavljene v nizozemskem imeniku. SEU je ugotovilo, da so z Direktivo o univerzalnih storitvah zajete vse zahteve podjetij, ki zagotavljajo imeniške storitve, ne glede na to, v kateri državi članici so ustanovljena. Menilo je tudi, da s posredovanjem teh podatkov drugemu podjetju, ki namerava objaviti javni imenik, ne da bi zadevni naročniki še enkrat privolili v to, ne more biti kršeno samo bistvo pravice do varstva osebnih podatkov.[365] Zato podjetju, ki svojim naročnikom dodeljuje številke, prošnje za privolitev, ki jo naslovi na naročnike, ni treba oblikovati tako, da ti naročniki to privolitev dajo ločeno glede na državo članico, v katero se njihovi podatki lahko posredujejo.[366]

Nedvoumna privolitev

Vsaka privolitev mora biti nedvoumna.[367] To pomeni, da ne sme biti nikakršnega razumnega dvoma o tem, da je želel posameznik, na katerega se nanašajo osebni podatki, izraziti strinjanje z obdelavo svojih podatkov. Nedejavnost posameznika, na katerega se nanašajo osebni podatki, ne pomeni nedvoumne privolitve.

To bi veljalo v primeru, ko bi upravljavec privolitev pridobil z izjavami v svojih politikah o varovanju zasebnosti, kot je „z uporabo naše storitve soglašate z obdelavo svojih osebnih podatkov“. V tem primeru bi morda upravljavci morali zagotoviti, da uporabniki ročno in posamično soglašajo s takimi politikami.

Če je privolitev dana v obliki pisne izjave, ki je del pogodbe, mora biti privolitev v obdelavo osebnih podatkov prilagojena posamezniku, vsekakor pa „bi morali zaščitni ukrepi zagotoviti, da se posameznik, na katerega se nanašajo osebni podatki, zaveda dejstva, da daje privolitev in v kakšnem obsegu jo daje“.[368]

365 SEU, *Tele2 (Netherlands) BV in drugi proti Autoriteit Consument en Markt (ACM)*, C-536/15, 15. marec 2017, točka 36.

366 Prav tam, točki 40 in 41.

367 SUVP, člen 4(11).

368 Prav tam, uvodna izjava 42.

Zahteve glede privolitve za otroke

SUVP določa posebno varstvo za otroke v okviru zagotavljanja storitev informacijske družbe, saj „se morda manj zavedajo zadevnih tveganj, posledic in zaščitnih ukrepov in svojih pravic v zvezi z obdelavo osebnih podatkov".[369] Kadar v skladu s **pravom EU** ponudniki storitev informacijske družbe na podlagi privolitve obdelujejo osebne podatke otrok, mlajših od 16 let, je zato taka obdelava zakonita le, „če in kolikor takšno privolitev da ali odobri nosilec starševske odgovornosti za otroka".[370] Države članice lahko v nacionalnem pravu določijo nižjo starost, vendar ta ne sme biti nižja od 13 let.[371] Privolitev nosilca starševske odgovornosti ni potrebna „v okviru storitev preventive ali svetovanja, ki se nudijo neposredno otroku".[372] Informacije in komunikacija, pri katerih se obdelava nanaša na otroka, bi morale biti v jasnem in preprostem jeziku, ki ga lahko otrok zlahka razume.[373]

Pravica, da se privolitev kadar koli prekliče

SUVP vključuje splošno pravico, da se lahko privolitev kadar koli prekliče.[374] Posameznika, na katerega se nanašajo osebni podatki, je treba o taki pravici obvestiti pred privolitvijo, to pravico pa lahko uveljavlja po svoji presoji. Navedba razlogov za preklic se ne bi smela zahtevati, niti ne bi smelo biti nevarnosti za negativne posledice poleg prenehanja ugodnosti, ki so morda izhajale iz predhodne odobritve uporabe osebnih podatkov. Privolitev bi moralo biti enako enostavno preklicati kot dati.[375] Privolitev ne more biti prostovoljna, če je posameznik, na katerega se nanašajo osebni podatki, ne more preklicati brez škode ali če privolitve ni tako enostavno preklicati, kot jo je bilo dati.[376]

369 Prav tam, uvodna izjava 38.

370 Prav tam, člen 8(1), prvi pododstavek. Pojem storitev informacijske družbe je opredeljen v členu 4(25) SUVP.

371 SUVP, člen 8(1), drugi pododstavek.

372 Prav tam, uvodna izjava 38.

373 Prav tam, uvodna izjava 58. Glej tudi posodobljeno Konvencijo št. 108, člen 15(2)(e). Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točki 68 in 125.

374 SUVP, člen 7(3). Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 45.

375 SUVP, člen 7(3).

376 SUVP, uvodna izjava 42; Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 42.

Primer: stranka privoli v prejemanje reklamne pošte na naslov, ki ga navede upravljavcu osebnih podatkov. Če stranka privolitev prekliče, mora upravljavec nemudoma prenehati pošiljati reklamno pošto. Stranka ne sme biti kaznovana, na primer s pristojbino. Vendar se preklic uporablja za prihodnost in nima učinka za nazaj. Obdobje, v katerem so se osebni podatki stranke zaradi njene privolitve obdelovali zakonito, je bilo zakonito. Preklic preprečuje kakršno koli nadaljnjo obdelavo teh podatkov, razen če je taka obdelava v skladu s pravico do izbrisa.[377]

Potrebnost za izvajanje pogodbe

V okviru prava EU člen 6(1)(b) SUVP določa še eno podlago za zakonito obdelavo, in sicer če je obdelava „potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki". S to določbo so zajeta tudi predpogodbena razmerja, na primer kadar stranka namerava skleniti pogodbo, vendar tega še ni storila, morda zato, ker še niso bila dokončana nekatera preverjanja. Če mora ena od strank zato obdelati osebne podatke, je taka obdelava zakonita, če je „potrebna za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe".[378]

Pojem obdelave podatkov kot zakonite podlage, določene z zakonom, v členu 5(2) posodobljene Konvencije št. 108 zajema tudi obdelavo osebnih podatkov za izvajanje pogodbe (ali predpogodbenih ukrepov na zahtevo posameznika, na katerega se nanašajo osebni podatki), katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki.[379]

Zakonske obveznosti upravljavca

V **pravu EU** je opredeljen še en razlog za zakonito obdelavo osebnih podatkov, in sicer če „je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca" (člen 6(1)(c) SUVP). Ta določba se nanaša na upravljavce v zasebnem in javnem sektorju; pravne obveznosti upravljavcev osebnih podatkov v javnem sektorju lahko spadajo tudi na področje uporabe člena 6(1)(e) SUVP. Upravljavci v zasebnem

377 SUVP, člen 17(1)(b).

378 Prav tam, člen 6(1)(b).

379 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 46; Svet Evrope, Odbor ministrov (2010), Priporočilo CM/Rec(2010)13 državam članicam o varstvu posameznikov v zvezi z avtomatsko obdelavo osebnih podatkov pri oblikovanju profilov, 23. november 2010, člen 3(4)(b).

sektorju morajo v skladu z zakonodajo v številnih primerih obdelovati podatke o konkretnih posameznikih, na katere se nanašajo osebni podatki. Tako morajo na primer delodajalci podatke o svojih zaposlenih obdelovati zaradi socialne varnosti in obdavčenja, podjetja pa morajo podatke o svojih strankah obdelovati zaradi obdavčitve.

Pravna obveznost lahko izvira iz prava Unije ali prava države članice, ki je lahko podlaga za eno ali več dejanj obdelave. V pravu bi bilo treba opredeliti namen obdelave ter natančnejša pravila za določitev upravljavca, vrst osebnih podatkov, ki se obdelujejo, zadevnih posameznikov, na katere se nanašajo osebni podatki, subjektov, katerim se osebni podatki lahko razkrijejo, omejitve namena, roka hranjenja in drugih ukrepov za zagotovitev zakonite in poštene obdelave.[380] Vsako tako pravo, ki je podlaga za obdelavo osebnih podatkov, mora biti skladno s členoma 7 in 8 Listine ter členom 8 EKČP.

Pravne obveznosti upravljavca so tudi podlaga za zakonito obdelavo osebnih podatkov **po pravu Sveta Evrope**.[381] Kot je bilo že poudarjeno, so pravne obveznosti upravljavca v zasebnem sektorju le en primer zakonitih interesov drugih, kot so navedeni v členu 8(2) EKČP. Primer o delodajalcih, ki obdelujejo podatke o svojih zaposlenih, je zato upošteven tudi za pravo Sveta Evrope.

Življenjski interesi posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe

V okviru prava EU člen 6(1)(d) SUVP določa, da je obdelava osebnih podatkov zakonita, če „je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe". Na ta zakoniti razlog se je mogoče sklicevati za obdelavo osebnih podatkov na podlagi življenjskih interesov druge fizične osebe le, če take obdelave „ni mogoče očitno izvesti na drugi pravni podlagi".[382] Včasih lahko neka vrsta obdelave temelji na razlogih javnega interesa in življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge osebe. To na primer velja pri spremljanju epidemij in njihovega širjenja ali v izrednih humanitarnih razmerah.

380 SUVP, uvodna izjava 45.

381 Svet Evrope, Odbor ministrov (2010), Priporočilo Rec(2010)13 državam članicam o varstvu posameznikov v zvezi z avtomatsko obdelavo osebnih podatkov pri oblikovanju profilov, 23. november 2010, člen 3(4)(a).

382 SUVP, uvodna izjava 46.

V okviru prava Sveta Evrope življenjski interesi posameznika, na katerega se nanašajo osebni podatki, niso navedeni v členu 8 EKČP. Vendar se šteje, da so življenjski interesi posameznika, na katerega se nanašajo osebni podatki, zajeti v pojmu „zakonita podlaga" iz člena 5(2) posodobljene Konvencije št. 108, v katerem je obravnavana zakonitost obdelave osebnih podatkov.[383]

Javni interes in izvajanje javne oblasti

Ker so lahko javne zadeve urejene različno, člen 6(1)(e) SUVP določa, da se lahko osebni podatki zakonito obdelujejo, če je obdelava „potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu".[384]

Primer: v zadevi *Huber proti Bundesrepublik Deutschland*[385] je H. Huber, avstrijski državljan s stalnim prebivališčem v Nemčiji, zvezni urad za migracije in begunce zaprosil, naj izbriše njegove podatke iz centralnega registra tujcev (v nadaljnjem besedilu: AZR). Register, ki vsebuje osebne podatke o nenemških državljanih EU, ki prebivajo v Nemčiji več kot tri mesece, se uporablja za statistične namene, uporabljajo pa ga tudi organi pregona in pravosodni organi, kadar preiskujejo in preganjajo kazniva dejanja ali dejanja, ki ogrožajo javno varnost. Predložitveno sodišče je postavilo vprašanje, ali je obdelava osebnih podatkov v registru, kot je centralni register tujcev, do katerega imajo dostop tudi drugi javni organi, združljiva s pravom EU, ker za nemške državljane tak register ne obstaja.

SEU je menilo, da je lahko obdelava osebnih podatkov na podlagi člena 7(e) Direktive 95/46/ES[386] zakonita le, če je potrebna za izvajanje naloge, ki se opravlja v javnem interesu ali pri izvrševanju javne oblasti.

Po mnenju Sodišča „se vsebina pojma nujnosti – kot izhaja iz člena 7(e) Direktive 95/46/ES[387] [...] – ob upoštevanju cilja zagotovitve enakovredne ravni varstva v vseh državah članicah ne more spreminjati glede na posamezno

383 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 46.

384 Glej SUVP, uvodna izjava 45.

385 SEU, *Heinz Huber proti Bundesrepublik Deutschland* (veliki senat), C-524/06, 16. december 2008.

386 Prej direktiva o varstvu osebnih podatkov, člen 7(e), zdaj SUVP, člen 6(1)(e).

387 Prav tam.

državo članico. Gre torej za samostojen pojem prava Skupnosti, ki ga je treba razlagati tako, da popolnoma ustreza namenu te direktive, kot je opredeljen v njenem členu 1(1)".[388]

Sodišče je ugotovilo, da pravica do prebivanja državljana Unije na ozemlju države članice, v kateri ni državljan, ni brezpogojna, temveč je lahko odvisna od omejitev in pogojev, določenih s Pogodbo o ustanovitvi Evropske skupnosti in določbami, ki so bile sprejete za njeno uporabo. Država članica lahko torej načeloma uporablja register, kot je AZR, s katerim si pomagajo organi, pristojni za izvajanje zakonodaje v zvezi s pravico do prebivanja, vendar tak register ne sme vsebovati informacij, ki niso nujne za zadevni namen. Sodišče ugotavlja, da je tak sistem obdelave osebnih podatkov v skladu s pravom EU, če vsebuje samo podatke, ki so nujni za izvajanje navedene zakonodaje, in če njegova centraliziranost omogoča učinkovitejše izvajanje navedene zakonodaje. Nacionalno sodišče mora ugotoviti, ali so navedeni pogoji izpolnjeni v obravnavani zadevi. Če niso, potem nikakor ni mogoče šteti, da sta shranjevanje in obdelava osebnih podatkov za statistične namene v registru, kot je AZR, nujna v smislu člena 7(e)[389] Direktive 95/46/ES.[390]

SEU je v zvezi z vprašanjem uporabe podatkov iz registra za boj proti kriminalu menilo, da se ta cilj „nujno nanaša na pregon kaznivih in protizakonitih dejanj, ne glede na državljanstvo storilcev". Sporni register ne vsebuje osebnih podatkov o državljanih zadevne države članice, zato tako različno obravnavanje pomeni diskriminacijo, ki je prepovedana s členom 18 PDEU. SEU je zato ugotovilo, da ta določba „nasprotuje temu, da država članica zaradi boja proti kriminalu uvede sistem obdelave osebnih podatkov, ki velja le za državljane Unije, ki niso državljani te države članice".[391]

Če osebne podatke uporabljajo organi, ki delujejo v javni sferi, morajo upoštevati tudi člen 8 **EKČP**, pri čemer naj bi bila taka uporaba po potrebi zajeta s členom 5(2) posodobljene Konvencije št. 108.[392]

388 SEU, *Heinz Huber proti Bundesrepublik Deutschland* (veliki senat), C-524/06, 16. december 2008, točka 52.

389 Prej direktiva o varstvu osebnih podatkov, člen 7(e), zdaj SUVP, člen 6(1)(e).

390 SEU, *Heinz Huber proti Bundesrepublik Deutschland* (veliki senat), C-524/06, 16. december 2008, točke 54, 58, 59 in 66–68.

391 Prav tam, točki 78 in 81.

392 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točki 46 in 47.

Zakoniti interesi, za katere si prizadeva upravljavec ali tretja oseba

V skladu s **pravom EU** posameznik, na katerega se nanašajo osebni podatki, ni edina oseba z zakonitimi interesi. Člen 6(1)(f) SUVP določa, da se osebni podatki lahko zakonito obdelujejo, če je obdelava „potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba [razen javnih organov pri opravljanju njihovih nalog], razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov […]“.[393]

V vsakem posameznem primeru je treba skrbno oceniti, ali obstaja zakonit interes.[394] Če se opredelijo zakoniti interesi upravljavca, je treba izvesti uravnoteženje teh interesov in interesov ali temeljnih pravic posameznika, na katerega se nanašajo osebni podatki.[395] Pri tej presoji je treba upoštevati razumna pričakovanja posameznika, na katerega se nanašajo osebni podatki, da se ugotovi, ali interesi upravljavca prevladajo nad interesi ali temeljnimi pravicami zadevnega posameznika.[396] Če pravice posameznika, na katerega se nanašajo osebni podatki, prevladajo nad zakonitimi interesi upravljavca, lahko upravljavec sprejme ukrepe in izvaja zaščitne ukrepe, s katerimi zagotovi, da je vpliv na pravice zadevnega posameznika omejen (npr. s psevdonimizacijo osebnih podatkov), s čimer nagne tehtnico na svojo stran, šele potem pa se lahko upravičeno sklicuje na to zakonito podlago za obdelavo. Delovna skupina iz člena 29 je v svojem mnenju o pojmu zakonitih interesov upravljavca podatkov poudarila ključno vlogo odgovornosti in preglednosti ter pravic posameznika, na katerega se nanašajo osebni podatki, da ugovarja obdelavi svojih osebnih podatkov ali da do njih dostopa ter jih spreminja, izbriše ali pošlje, pri tehtanju zakonitih interesov upravljavca in interesov ali temeljnih pravic posameznika, na katerega se nanašajo osebni podatki.[397]

V uvodnih izjavah SUVP je navedenih nekaj primerov zakonitega interesa zadevnega upravljavca osebnih podatkov. Obdelava osebnih podatkov brez privolitve posameznika, na katerega se nanašajo osebni podatki, je na primer dovoljena, kadar se

393 V primerjavi z Direktivo 95/46 je v SUVP več primerov, za katere se šteje, da pomenijo zakonit interes.

394 SUVP, uvodna izjava 47.

395 Delovna skupina za varstvo podatkov iz člena 29 (2014), *Mnenje št. 6/2014 o pojmu zakonitih interesov upravljavca podatkov iz člena 7 Direktive 95/46/ES*, 4. april 2014.

396 Prav tam.

397 Prav tam.

opravlja za namene neposrednega trženja ali kadar je „nujno potrebna za preprečevanje zlorab“.[398]

SEU je v svoji sodni praksi podrobneje obravnavalo merila za opredelitev, kaj jezakonit interes.

Primer: zadeva *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] se je nanašala na poškodbo avtobusa prevoznika Rīgas satiksme, ki jo je povzročil potnik v taksiju s tem, ko je nenadoma odprl vrata taksija. Družba Rīgas satiksme je zoper njega hotela vložiti odškodninsko tožbo, vendar ji je policija posredovala le ime potnika, zavrnila pa je posredovanje številke njegovega identifikacijskega dokumenta in naslova, pri čemer je trdila, da bi bilo v skladu z nacionalno zakonodajo o varstvu osebnih podatkov razkritje teh podatkov nezakonito.

Latvijsko predložitveno sodišče je SEU v predhodno odločanje predložilo vprašanje, ali je treba v skladu z zakonodajo EU o varstvu osebnih podatkov razkriti vse osebne podatke, potrebne za vložitev civilnopravne tožbe proti osebi, ki je domnevno odgovorna za upravni prekršek.[400]

SEU je pojasnilo, da pravo EU o varstvu osebnih podatkov vključuje možnost – ne pa obveznosti –, da se tretji osebi posredujejo osebni podatki, potrebni za uresničitev zakonitega interesa, za katerega si ta prizadeva.[401] Navedlo je tri kumulativne pogoje, ki morajo biti izpolnjeni, da je obdelava osebnih podatkov zakonita na podlagi zakonitih interesov.[402] Prvič, tretja oseba, ki so ji osebni podatki posredovani, si mora prizadevati za zakonit interes. V obravnavanem primeru to pomeni, da zahteva po razkritju osebnih podatkov za vložitev tožbe zoper osebo, ki je povzročila materialno škodo, pomeni zakonit interes tretje osebe. Drugič, obdelava osebnih podatkov mora biti potrebna za uresničitev tega zakonitega interesa. V tem primeru je treba za identifikacijo zadevne osebe nujno pridobiti osebne podatke, kot sta naslov in/ali številka identifikacijskega dokumenta. Tretjič, temeljne pravice in svoboščine

398 SUVP, uvodna izjava 47.

399 SEU, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde proti Rīgas pašvaldības SIA „Rīgas satiksme“*, C-13/16, 4. maj 2017.

400 Prav tam, točka 23.

401 Prav tam, točka 26.

402 Prav tam, točke 28–34.

posameznika, na katerega se nanašajo osebni podatki, ne smejo prevladati nad zakonitimi interesi upravljavca ali tretje osebe. Uravnoteženje je treba izvesti za vsak primer posebej, pri čemer se upoštevajo elementi, kot so teža kršitve pravic posameznika, na katerega se nanašajo osebni podatki, v nekaterih okoliščinah pa celo njegova starost. Vendar v obravnavanem primeru SEU ni menilo, da je zavrnitev razkritja upravičena le zato, ker je bil posameznik, na katerega se nanašajo osebni podatki, mladoleten.

SEU je v sodbi v zadevi *ASNEF in FECEMD* izrecno razsodilo na podlagi zakonite obdelave osebnih podatkov, ki temelji na „zakonitih interesih", ki je bila takrat določena v členu 7(f) direktive o varstvu osebnih podatkov.[403]

Primer: SEU je v združenih zadevah *ASNEF in FECEMD*[404] pojasnilo, da z nacionalno zakonodajo ni dovoljeno določiti dodatnih pogojev, kot so za zakonito obdelavo osebnih podatkov navedeni v členu 7(f) navedene direktive.[405] To se je nanašalo na primer, v katerem je španska zakonodaja o varstvu osebnih podatkov vsebovala določbo, na podlagi katere so se lahko druge zasebne stranke na zakonit interes pri obdelavi osebnih podatkov sklicevale le, če so informacije že v javno dostopnih virih.

SEU je najprej navedlo, da je namen Direktive 95/46/ES[406], da v vseh državah članicah zagotovi enakovredno raven varstva pravic in svoboščin posameznikov pri obdelavi osebnih podatkov. Poleg tega približevanje nacionalnih zakonodaj, ki se uporabljajo na tem področju, ne sme povzročiti zmanjšanja varstva, ki ga zagotavljajo. Namesto tega mora imeti za cilj zagotovitev visoke ravni varstva v EU.[407] SEU je zato menilo, da „iz cilja zagotoviti enako raven varstva v vseh državah članicah izhaja, da je v členu 7 Direktive 95/46/ES[408] določen izčrpen in taksativen seznam primerov, v katerih je mogoče šteti,

403 Prej direktiva o varstvu osebnih podatkov, člen 7(f), zdaj SUVP, člen 6(1)(f).

404 SEU, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, združeni zadevi C-468/10 in C-469/10, 24. november 2011.

405 Prej direktiva o varstvu osebnih podatkov, člen 7(f), zdaj SUVP, člen 6(1)(f).

406 Prej direktiva o varstvu osebnih podatkov, zdaj SUVP.

407 SEU, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, združeni zadevi C-468/10 in C-469/10, 24. november 2011, točka 28. Glej direktivo o varstvu osebnih podatkov, uvodni izjavi 8 in 10.

408 Prej direktiva o varstvu osebnih podatkov, člen 7, zdaj SUVP, člen 6(1)(f).

da je obdelava osebnih podatkov dopustna". Poleg tega „države članice ne smejo niti dodati novih načel glede zakonitosti obdelave osebnih podatkov iz člena 7 Direktive 95/46/ES[409] niti določiti dodatnih zahtev, ki bi spreminjale obseg enega od šestih načel, določenih" v členu 7.[410] SEU je potrdilo, da je, kar zadeva uravnoteženje, ki je potrebno na podlagi člena 7(f) Direktive 95/46/ES, mogoče upoštevati, da je teža posega v temeljne pravice osebe, na katero se navedena obdelava nanaša, lahko različna glede na to, ali so ti podatki že v javno dostopnih virih ali ne.

Vendar člen 7(f) navedene direktive „nasprotuje temu, da država članica kategorično in na splošno izključi obdelavo nekaterih vrst osebnih podatkov, ne da bi dovolila tehtanje zadevnih nasprotujočih si pravic in interesov v posameznem primeru".

SEU je glede na navedeno ugotovilo, da je treba člen 7(f) Direktive 95/46/ES[411] razlagati tako, da „nasprotuje nacionalni ureditvi, ki – kadar ni privolitve zadevne osebe – za dovolitev obdelave njenih osebnih podatkov, ki je potrebna zaradi uresničitve zakonitega interesa upravljavca podatkov ali tretje osebe oziroma tretjih oseb, ki so jim ti podatki posredovani, poleg spoštovanja pravic in temeljnih svoboščin zadevne osebe zahteva, da so navedeni podatki iz javno dostopnih virov, pri čemer kategorično in na splošno izključuje vsako obdelavo podatkov, ki niso v takih virih".[412]

V skladu s členom 21(1) SUVP ima posameznik na podlagi razlogov, povezanih z njegovim posebnim položajem, pravico, da kadar koli ugovarja obdelavi osebnih podatkov, kadar se ti obdelujejo na podlagi zakonitih interesov. Upravljavec mora ustaviti obdelavo, razen če dokaže nujne zakonite razloge za njeno nadaljevanje.

V okviru **prava Sveta Evrope** je podobne formulacije mogoče najti v posodobljeni Konvenciji št. 108[413] in priporočilih Sveta Evrope. V Priporočilu o oblikovanju profilov se obdelava osebnih podatkov zaradi profiliranja priznava kot zakonita, če je nujna

409 Prej direktiva o varstvu osebnih podatkov, člen 7, zdaj SUVP, člen 6.

410 Prav tam.

411 Prej direktiva o varstvu osebnih podatkov, člen 7(f), zdaj SUVP, člen 6(1)(f).

412 SEU, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, združeni zadevi C-468/10 in C-469/10, 24. november 2011, točke 40, 44, 48 in 49.

413 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 46.

zaradi zakonitih interesov drugih, razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.[414] Poleg tega je v členu 8(2) EKČP navedeno, da je pravico do varstva osebnih podatkov mogoče zakonito omejiti med drugim za to, da se „zavarujejo pravice in svoboščine drugih ljudi".

Primer: v zadevi *Y proti Turčiji*[415] je bil pritožnik okužen z virusom HIV. Ker je bil ob prihodu v bolnišnico nezavesten, je reševalna ekipa bolnišnično osebje obvestila, da je okužen z virusom HIV. Pritožnik je v postopku pred ESČP trdil, da je bila z razkritjem te informacije kršena njegova pravica do zasebnega življenja. Vendar se je zaradi potrebe po zaščiti bolnišničnega osebja štelo, da izmenjava informacij ni pomenila kršitve njegovih pravic.

4.1.2 Obdelava posebnih vrst osebnih podatkov (občutljivih osebnih podatkov)

V skladu s **pravom Sveta Evrope** je določitev ustreznega varstva za uporabo občutljivih osebnih podatkov prepuščena nacionalnemu pravu, pod pogojem, da so izpolnjeni pogoji iz člena 6 posodobljene Konvencije št. 108, in sicer da so uzakonjeni ustrezni zaščitni ukrepi, ki dopolnjujejo druge določbe konvencije. V okviru **prava EU** je v členu 9 SUVP opredeljena podrobna ureditev za obdelavo posebnih vrst osebnih podatkov (ki se imenujejo tudi občutljivi osebni podatki). Ti osebni podatki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, med občutljive osebne podatke pa spadajo tudi genski in biometrični podatki, namenjeni edinstveni identifikaciji posameznika, ter podatki v zvezi z zdravjem, posameznikovim spolnim življenjem ali spolno usmerjenostjo. Obdelava občutljivih osebnih podatkov je načeloma prepovedana.[416]

Vendar člen 9(2) uredbe vsebuje izčrpen seznam izjem od te prepovedi, ki pomenijo zakonite razloge za obdelavo občutljivih osebnih podatkov. Te izjeme vključujejo primere, v katerih:

414 Svet Evrope, Odbor ministrov (2010), Priporočilo Rec(2010)13 in obrazložitveni memorandum državam članicam o varstvu posameznikov v zvezi z avtomatsko obdelavo osebnih podatkov pri oblikovanju profilov, 23. november 2010, člen 3(4)(b) (priporočilo o oblikovanju profilov).

415 ESČP, *Y proti Turčiji*, pritožba št. 648/10, 17. februar 2015.

416 Prej direktiva o varstvu osebnih podatkov, člen 7(f), zdaj SUVP, člen 9(1).

- je posameznik, na katerega se nanašajo osebni podatki, izrecno privolil v obdelavo osebnih podatkov;

- obdelavo v okviru svojih zakonitih dejavnosti izvaja nepridobitno telo s političnim, filozofskim, verskim ali sindikalnim ciljem in pod pogojem, da se obdelava nanaša samo na (nekdanje) člane telesa ali na osebe, ki so v take namene v rednem stiku z njim;

- je obdelava povezana z osebnimi podatki, ki jih posameznik, na katerega se nanašajo, sam objavi;

- je obdelava potrebna za:

    - izpolnjevanje obveznosti in izvajanje posebnih pravic upravljavca ali posameznika, na katerega se nanašajo osebni podatki, v okviru zaposlovanja, socialne varnosti in socialnega varstva;

    - zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe (kadar posameznik, na katerega se nanašajo osebni podatki, ne more dati privolitve);

    - uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali kadar koli sodišča izvajajo svojo sodno pristojnost;

    - namene preventivne medicine ali medicine dela: za „oceno delovne sposobnosti zaposlenega, zdravstveno diagnozo, zagotovitev zdravstvene ali socialne oskrbe ali zdravljenja ali upravljanje sistemov in storitev zdravstvenega ali socialnega varstva na podlagi prava Unije ali prava države članice ali v skladu s pogodbo z zdravstvenim delavcem“;

    - za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinsko-raziskovalne namene ali statistične namene;

    - iz razlogov javnega interesa na področju javnega zdravja ali

    - iz razlogov bistvenega javnega interesa.

V zvezi z obdelavo posebnih vrst osebnih podatkov se pogodbeno razmerje s posameznikom, na katerega se nanašajo osebni podatki, zato ne šteje za pravno podlago

za zakonito obdelavo občutljivih osebnih podatkov, izjema je pogodba z zdravstvenim delavcem, za katero velja obveznost varovanja poklicne skrivnosti.[417]

Izrecna privolitev posameznika, na katerega se nanašajo osebni podatki

V skladu s **pravom EU** je prva možna podlaga za zakonito obdelavo katerih koli osebnih podatkov, ne glede na to, ali so neobčutljivi ali občutljivi, privolitev posameznika, na katerega se nanašajo osebni podatki. Če so osebni podatki občutljivi, mora biti taka privolitev izrecna. Vendar se lahko v pravu Unije ali nacionalnem pravu določi, da zadevni posameznik ne more odstopiti od prepovedi obdelave posebnih vrst osebnih podatkov.[418] To bi lahko na primer veljalo, kadar obdelava vključuje neobičajna tveganja za posameznika, na katerega se nanašajo osebni podatki.

Delovno pravo ali pravo socialne varnosti in socialnega varstva

V skladu s **pravom EU** se prepoved iz člena 9(1) SUVP lahko odpravi, če je obdelava potrebna za izpolnjevanje obveznosti ali izvajanje pravic upravljavca ali posameznika, na katerega se nanašajo osebni podatki, na področju zaposlovanja ali socialne varnosti. Vendar mora biti obdelava dovoljena s pravom EU, nacionalnim pravom ali kolektivno pogodbo v skladu z nacionalnim pravom, ki zagotavlja ustrezne zaščitne ukrepe za temeljne pravice in interese posameznika, na katerega se nanašajo osebni podatki.[419] Evidence o zaposlitvi, ki jih hrani neka organizacija, lahko pod določenimi pogoji iz SUVP in ustreznega nacionalnega prava vključujejo občutljive osebne podatke. Občutljivi osebni podatki so lahko na primer podatki o članstvu v sindikatu ali podatki v zvezi z zdravjem.

Življenjski interesi posameznika, na katerega se nanašajo osebni podatki, ali druge osebe

V skladu s **pravom EU** se lahko občutljivi osebni podatki – tako kot neobčutljivi – obdelujejo zaradi življenjskih interesov posameznika, na katerega se nanašajo, ali druge fizične osebe.[420] Če obdelava temelji na življenjskih interesih druge osebe, se je na ta zakoniti razlog mogoče sklicevati le, kadar take obdelave „ni mogoče očitno

417 SUVP, člen 9(2)(h) in (i).

418 Prav tam, člen 9(2)(a).

419 SUVP, člen 9(2)(b).

420 Prav tam, člen 9(2)(c).

izvesti na drugi pravni podlagi".[421] V nekaterih primerih se lahko z obdelavo osebnih podatkov ščitijo tako interesi posameznika kot javni interesi, na primer kadar je obdelava potrebna v humanitarne namene.[422]

Da bi bila taka obdelava občutljivih osebnih podatkov zakonita, je nujno, da posameznika, na katerega se nanašajo osebni podatki, ni bilo mogoče vprašati za privolitev, na primer ker je bil nezavesten ali odsoten in z njim ni bilo mogoče navezati stika. Z drugimi besedami, oseba je bila fizično ali pravno nesposobna dati privolitev.

Dobrodelne organizacije ali nepridobitna telesa

Obdelava osebnih podatkov je dovoljena tudi v okviru zakonitih dejavnosti ustanov, združenj ali drugih nepridobitnih teles s političnim, filozofskim, verskim ali sindikalnim ciljem. Vendar se mora obdelava nanašati samo na člane ali nekdanje člane telesa ali na osebe, ki so v rednem stiku z njim.[423] Občutljivih osebnih podatkov se zunaj teh teles ne sme razkriti brez privolitve posameznika, na katerega se nanašajo.

Osebni podatki, ki jih posameznik, na katerega se nanašajo, sam objavi

Člen 9(2)(e) SUVP določa, da obdelava ni prepovedana, če je povezana z osebnimi podatki, ki jih posameznik, na katerega se nanašajo, sam objavi. Čeprav pomen stavka „ki jih posameznik, na katerega se nanašajo osebni podatki, sam objavi" v navedeni uredbi ni opredeljen, ga je treba, ker gre za izjemo od prepovedi obdelave občutljivih osebnih podatkov, razlagati ozko, in sicer kot zahtevo, da je posameznik, na katerega se nanašajo osebni podatki, namerno objavil svoje osebne podatke. Če se v okviru televizijskega programa predvaja posnetek z nadzorne kamere, ki med drugim prikazuje, kako se je gasilec poškodoval med tem, ko je poskušal evakuirati prebivalce zgradbe, ni mogoče šteti, da je gasilec sam objavil osebne podatke. Če pa se po drugi strani gasilec odloči opisati dogodek ter videoposnetek in fotografije objaviti na javni spletni strani, bi bilo to namerno pritrdilno dejanje, s katerim bi njegovi osebni podatki postali javni. Opozoriti je treba, da objava osebnih podatkov ne pomeni privolitve, temveč je oblika dovoljenja za obdelavo posebnih vrst osebnih podatkov.

421 Prav tam, uvodna izjava 46.

422 Prav tam.

423 Prav tam, člen 9(2)(d).

Dejstvo, da je posameznik, na katerega se nanašajo osebni podatki, objavil osebne podatke, ki se obdelujejo, upravljavcev ne izvzema iz njihovih obveznosti po pravu o varstvu osebnih podatkov. Načelo omejitve namena se na primer še naprej uporablja, tudi če so taki osebni podatki objavljeni.[424]

Pravni zahtevki

V skladu s SUVP je dovoljena tudi obdelava posebnih vrst osebnih podatkov, ki je „potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov" v sodnem postopku ali v upravnem ali izvensodnem postopku[425].[426] V tem primeru mora biti obdelava povezana s konkretnim pravnim zahtevkom in njegovo obrambo oziroma izvajanjem, zanjo pa lahko zaprosi katera koli stranka v sporu.

Kadar sodišča izvajajo svojo sodno pristojnost, lahko v okviru reševanja pravnega spora obdelujejo posebne vrste osebnih podatkov.[427] Te posebne vrste osebnih podatkov, ki se obdelujejo v tem okviru, bi lahko na primer vključevale genske podatke pri ugotavljanju očetovstva in materinstva ali podatke o zdravstvenem stanju, kadar se del dokazov nanaša na podrobnosti o poškodbi, ki jo je utrpela žrtev kaznivega dejanja.

Razlogi bistvenega javnega interesa

Države članice lahko v skladu s členom 9(2)(g) SUVP opredelijo dodatne okoliščine, v katerih je mogoče obdelovati občutljive osebne podatke, če je:

- obdelava osebnih podatkov potrebna iz razlogov bistvenega javnega interesa;
- to določeno v pravu Unije ali nacionalnem pravu;
- pravo Unije ali pravo države članice sorazmerno, spoštuje pravico do varstva osebnih podatkov ter zagotavlja ustrezne in posebne ukrepe za zaščito pravic in interesov posameznika, na katerega se nanašajo osebni podatki.[428]

424 Delovna skupina za varstvo podatkov iz člena 29 (2013), *Mnenje št. 3/13 o omejitvi namena*, WP 203, Bruselj, 2. april 2013, str. 14.

425 SUVP, uvodna izjava 52.

426 Prav tam, člen 9(2)(f).

427 Prav tam.

428 Prav tam, člen 9(2)(g).

Dober primer so sistemi elektronskih zdravstvenih kartotek. Taki sistemi omogočajo, da se zdravstveni podatki, ki jih izvajalci zdravstvene dejavnosti zberejo med zdravljenjem pacienta, v širšem obsegu (običajno na nacionalni ravni) dajo na voljo drugim izvajalcem zdravstvene dejavnosti, ki izvajajo storitve zdravljenja tega pacienta.

Delovna skupina iz člena 29 je ugotovila, da vzpostavitev takih sistemov ni mogoča na podlagi veljavnih pravil za obdelavo osebnih podatkov o pacientih.[429] Vendar lahko sistemi elektronskih zdravstvenih kartotek obstajajo, če temeljijo na „razlog[ih] bistvenega javnega interesa".[430] Za njihovo vzpostavitev bi bila potrebna izrecna pravna podlaga, ki bi vsebovala tudi potrebne zaščitne ukrepe za zagotavljanje varnega delovanja sistema.[431]

Drugi razlogi za obdelavo občutljivih osebnih podatkov

V SUVP je določeno, da se osebni podatki lahko obdelujejo, kadar je obdelava potrebna:[432]

- za namene preventivne medicine ali medicine dela, oceno delovne sposobnosti zaposlenega, zdravstveno diagnozo, zagotovitev zdravstvene ali socialne oskrbe ali zdravljenja ali upravljanje sistemov in storitev zdravstvenega ali socialnega varstva na podlagi prava EU ali prava države članice ali v skladu s pogodbo z zdravstvenim delavcem;

- iz razlogov javnega interesa na področju javnega zdravja, kot je zaščita pred resnimi čezmejnimi tveganji za zdravje ali zagotovitev visokih standardov kakovosti in varnosti zdravstvenega varstva ter zdravil ali medicinskih pripomočkov, na podlagi prava EU ali prava države članice. Pravo mora zagotavljati ustrezne in posebne ukrepe za zaščito pravic posameznika, na katerega se nanašajo osebni podatki;

429 Delovna skupina za varstvo podatkov iz člena 29 (2007), *Delovni dokument o obdelavi osebnih podatkov v zvezi z zdravjem v elektronskih zdravstvenih kartonih (EZK)*, WP 131, Bruselj, 15. februar 2007. Glej tudi SUVP, člen 9(3).

430 SUVP, člen 9(2)(g).

431 Delovna skupina za varstvo podatkov iz člena 29 (2007), *Delovni dokument o obdelavi osebnih podatkov v zvezi z zdravjem v elektronskih zdravstvenih kartonih (EZK)*, WP 131, Bruselj, 15. februar 2007.

432 SUVP, člen 9(2)(h), (i) in (j).

- za namene arhiviranja, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene na podlagi prava EU ali prava države članice. Pravo mora biti sorazmerno z zastavljenim ciljem, spoštovati bistvo pravice do varstva podatkov ter zagotavljati ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika, na katerega se nanašajo osebni podatki.

Dodatni pogoji na podlagi nacionalnega prava

Države članice lahko v skladu s SUVP uvedejo ali ohranijo tudi dodatne pogoje, vključno z omejitvami glede obdelave genskih in biometričnih podatkov ter podatkov v zvezi z zdravjem.[433]

4.2 Pravila o varnosti obdelave osebnih podatkov

Ključni poudarki

- V skladu s pravili o varnosti obdelave podatkov morata upravljavec in obdelovalec izvajati ustrezne tehnične in organizacijske ukrepe za preprečitev nepooblaščenega poseganja v dejanja obdelave osebnih podatkov.
- Potrebna raven varnosti osebnih podatkov je odvisna od:
  - varnostnih značilnosti, ki so na trgu na voljo za posamezno vrsto obdelave,
  - stroškov,
  - tveganj, ki jih obdelava osebnih podatkov pomeni za temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.
- Zagotavljanje zaupnosti osebnih podatkov je del splošnega načela, določenega v SUVP.

Upravljavci imajo v skladu s **pravom EU in Sveta Evrope** splošno obveznost, da pri obdelavi osebnih podatkov in zlasti v primeru kršitev varnosti osebnih podatkov, kadar se te zgodijo, ravnajo pregledno in odgovorno. Upravljavci morajo v primeru kršitev varnosti osebnih podatkov o tem obvestiti nadzorne organe, razen če je malo verjetno, da bi bile z zadevno kršitvijo ogrožene pravice in svoboščine

433 Prav tam, člen 9(2)(h) in (4).

posameznikov. O kršitvi varnosti osebnih podatkov bi bilo treba obvestiti tudi posameznike, na katere se nanašajo osebni podatki, kadar je verjetno, da bo povzročila veliko tveganje za pravice in svoboščine fizičnih oseb.

4.2.1 Elementi varnosti osebnih podatkov

Zadevne določbe **prava EU** se glasijo:

> *„Ob upoštevanju najnovejšega tehnološkega razvoja in stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, upravljavec in obdelovalec z izvajanjem ustreznih tehničnih in organizacijskih ukrepov zagotovita ustrezno raven varnosti glede na tveganje […].“*[434]

Ti ukrepi med drugim vključujejo:

- psevdonimizacijo in šifriranje osebnih podatkov;[435]
- zagotavljanje stalne zaupnosti, celovitosti, dostopnosti in odpornosti sistemov in storitev za obdelavo;[436]
- pravočasno povrnitev razpoložljivosti in dostopa do osebnih podatkov v primeru izgube podatkov;[437]
- postopek testiranja, ocenjevanja in vrednotenja učinkovitosti ukrepov za zagotavljanje varnostni obdelave.[438]

Podobno določbo vsebuje **pravo Sveta Evrope**:

> *Vsaka pogodbenica določi, da upravljavec in, kjer je primerno, obdelovalec sprejmeta ustrezne varnostne ukrepe v zvezi s tveganji, kot so nenameren*

434 Prav tam, člen 32(1).
435 Prav tam, člen 32(1)(a).
436 Prav tam, člen 32(1)(b).
437 Prav tam, člen 32(1)(c).
438 Prav tam, člen 32(1)(d).

ali nepooblaščen dostop do osebnih podatkov, njihovo uničenje, izguba, uporaba, sprememba ali razkritje.[439]

V skladu s **pravom EU in Sveta Evrope** mora upravljavec v primeru kršitve varnosti osebnih podatkov, ki bi lahko vplivala na pravice in svoboščine posameznikov, o njej uradno obvestiti nadzorni organ (glej razdelek 4.2.3).

Pogosto obstajajo tudi industrijski, nacionalni in mednarodni standardi za varno obdelavo osebnih podatkov. Evropski pečat zaupnosti (EuroPriSe) je na primer projekt eTEN (vseevropska telekomunikacijska omrežja) EU, s katerim se raziskujejo možnosti certificiranja izdelkov, zlasti programske opreme, kot izdelkov, ki omogočajo skladnost z evropskim pravom o varstvu osebnih podatkov. Evropska agencija za varnost omrežij in informacij (ENISA) je bila ustanovljena, da bi se povečala sposobnost EU, držav članic EU in poslovne skupnosti za preprečevanje težav v zvezi z varnostjo omrežij in informacij, njihovo obravnavanje in odzivanje nanje.[440] Agencija ENISA redno objavlja analize varnostnih groženj in svetuje, kako jih obravnavati.[441]

Varnosti osebnih podatkov ni mogoče doseči samo z namestitvijo ustrezne (strojne in programske) opreme. Potrebna so tudi primerna notranja organizacijska pravila. Najbolje bi bilo, če bi se s takimi notranjimi pravili obravnavala naslednja vprašanja:

- redno zagotavljanje informacij vsem zaposlenim o pravilih v zvezi z varnostjo osebnih podatkov in njihovih obveznostih na podlagi prava o varstvu osebnih podatkov, zlasti v zvezi z njihovimi obveznostmi glede zaupnosti;

- jasna razdelitev odgovornosti in jasno začrtane pristojnosti na področju obdelave osebnih podatkov, zlasti v zvezi z odločitvami za obdelavo osebnih podatkov in njihovo posredovanje tretjim osebam ali posameznikom, na katere se nanašajo osebni podatki;

- uporaba osebnih podatkov izključno v skladu z navodili pristojne osebe ali v skladu s splošno določenimi pravili;

439 Posodobljena konvencija št. 108, člen 7(1).

440 Uredba (EU) št. 526/2013 Evropskega parlamenta in Sveta z dne 21. maja 2013 o agenciji Evropske unije za varnost omrežij in informacij (ENISA) in razveljavitvi Uredbe (ES) št. 460/2004 (UL L 165, 18.6.2013, str. 41).

441 Na primer ENISA, Kibernetska varnost in odpornost pametnih avtomobilov. Dobre prakse in priporočila, 2016; ENISA, Varnost mobilnih plačil in digitalnih denarnic, 2016.

- omejevanje dostopa do prostorov ter strojne in programske opreme upravljavca ali obdelovalca, vključno s preverjanjem pooblastila za dostop;

- zagotavljanje, da so pooblastila za dostop do osebnih podatkov dodeljena pristojni osebi in da se zanje zahteva ustrezna dokumentacija;

- avtomatizirani protokoli za elektronski dostop do osebnih podatkov in redno preverjanje takih protokolov, ki ga izvaja notranja nadzorna služba (zato je treba vse dejavnosti obdelave osebnih podatkov evidentirati);

- natančno dokumentiranje drugih oblik razkritja poleg avtomatiziranega dostopa do osebnih podatkov, s čimer se lahko dokaže, da ni bilo nezakonitih prenosov podatkov.

Pomemben dejavnik učinkovitih varnostnih ukrepov je tudi, da se zaposlenim zagotovita ustrezno usposabljanje in izobraževanje o varnosti osebnih podatkov. Vzpostaviti je treba tudi postopke preverjanja za zagotovitev, da ustrezni ukrepi ne obstajajo samo na papirju, temveč se tudi izvajajo in delujejo v praksi (na primer notranje in zunanje revizije).

Ukrepi za izboljšanje stopnje varnosti upravljavca ali obdelovalca vključujejo mehanizme, kot so odgovorne osebe za varstvo osebnih podatkov, izobraževanje zaposlenih o varnosti, redne revizije, preskusi vdora in pečati kakovosti.

Primer: pritožnica v zadevi *I proti Finski*[442] ni mogla dokazati, da so do njene zdravstvene kartoteke nezakonito dostopali drugi zaposleni v bolnišnici, v kateri je bila zaposlena. Nacionalna sodišča so zato zavrnila njeno trditev, da je bila kršena njena pravica do varstva osebnih podatkov. ESČP je ugotovilo, da je bil kršen člen 8 EKČP, ker je bil evidenčni sistem zdravstvenih kartotek bolnišnice tak, da uporabe kartotek pacientov ni bilo mogoče pojasniti za nazaj, saj je razkrival samo zadnjih pet vpogledov, te informacije pa so se izbrisale, ko je bila kartoteka vrnjena v arhiv. Za sodišče je bilo odločilnega pomena, da evidenčni sistem, uveden v bolnišnici, očitno ni bil v skladu z zakonskimi zahtevami nacionalnega prava, temu dejstvu pa nacionalna sodišča niso pripisala ustreznega pomena.

442 ESČP, *I proti Finski*, pritožba št. 20511/03,17. julij 2008.

EU je sprejela direktivo o varnosti omrežij in informacijskih sistemov,[443] ki je prvi pravni instrument o kibernetski varnosti na ravni EU. Njen cilj je po eni strani izboljšati kibernetsko varnost na nacionalni ravni, po drugi strani pa povečati raven sodelovanja v EU. Poleg tega se z njo izvajalcem bistvenih storitev (vključno z izvajalci v sektorjih energetike, zdravstva, bančništva, prometa, digitalne infrastrukture itd.) in ponudnikom digitalnih storitev nalagajo obveznosti glede obvladovanja tveganj, zagotavljanja varnosti svojih omrežij in informacijskih sistemov ter poročanja o varnostnih incidentih.

Obeti

Evropska komisija je septembra 2017 predlagala osnutek uredbe o reformi mandata agencije ENISA, da bi se upoštevale nove pristojnosti in odgovornosti agencije v skladu z direktivo o varnosti omrežij in informacijskih sistemov. Cilj predlagane uredbe je razviti naloge agencije ENISA in okrepiti njeno vlogo „referenčne točke v ekosistemu EU za kibernetsko varnost".[444] Predlagana uredba, ki ne bi smela posegati v načela SUVP, naj bi s pojasnitvijo potrebnih elementov, ki sestavljajo evropske certifikacijske sheme za kibernetsko varnost, tudi okrepila varnost osebnih podatkov. Vzporedno s tem je Evropska komisija septembra 2017 predlagala osnutek izvedbene uredbe o specifikaciji elementov, ki jih morajo upoštevati ponudniki digitalnih storitev za zagotavljanje varnosti svojih omrežij in informacijskih sistemov v skladu s členom 16(8) direktive o varnosti omrežij in informacijskih sistemov. V času priprave tega priročnika so potekale razprave o teh dveh predlogih.

4.2.2 Zaupnost

V okviru prava EU je v SUVP zaupnost osebnih podatkov določena kot del splošnega načela.[445] Ponudniki javno dostopnih elektronskih komunikacijskih storitev morajo zagotavljati zaupnost. Poleg tega zanje velja obveznost zagotavljanja varnosti lastnih storitev.[446]

443 Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

444 Predlog uredbe Evropskega parlamenta in Sveta o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti) (COM(2017) 477 final z dne 13. septembra 2017), str. 6.

445 SUVP, člen 5(1)(f).

446 Direktiva o zasebnosti in elektronskih komunikacijah, člen 5(1).

Primer: uslužbenka zavarovalnice na delovnem mestu prejme telefonski klic osebe, ki trdi, da je stranka, in želi informacije o svoji zavarovalni pogodbi.

Uslužbenka mora v skladu z obveznostjo zagotavljanja zaupnosti podatkov strank pred razkritjem osebnih podatkov izvesti vsaj minimalne varnostne ukrepe. Tako bi lahko na primer predlagala, da vrne klic na telefonsko številko, navedeno v spisu stranke.

V skladu s členom 5(1)(f) SUVP se morajo osebni podatki obdelovati na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi (celovitost in zaupnost).

Upravljavec in obdelovalec morata na podlagi člena 32 zadevne uredbe izvajati tehnične in organizacijske ukrepe za zagotavljanje visoke ravni varnosti. Taki ukrepi med drugim vključujejo psevdonimizacijo in šifriranje osebnih podatkov, zmožnost zagotavljanja stalne zaupnosti, celovitosti, dostopnosti in odpornosti obdelave, vrednotenje in testiranje učinkovitosti ukrepov ter zmožnost ponovne vzpostavitve obdelave v primeru fizičnega ali tehničnega incidenta. Poleg tega se lahko kot element za dokazovanje skladnosti z načelom celovitosti in zaupnosti uporabi tudi zavezanost k odobrenemu kodeksu ravnanja ali izvajanje odobrenega mehanizma certificiranja. V skladu s členom 28 SUVP mora poleg tega pogodba, v kateri so določene obveznosti obdelovalca do upravljavca, določati, da obdelovalec zagotovi, da so osebe, ki so pooblaščene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon.

Obveznost zaupnosti se ne nanaša na primere, v katerih posameznik za osebne podatke izve zasebno kot fizična oseba in ne kot uslužbenec upravljavca ali obdelovalca. Člena 28 in 32 SUVP se v tem primeru ne uporabljata, saj je uporaba osebnih podatkov s strani fizičnih oseb v celoti izvzeta iz področja uporabe navedene uredbe, če taka uporaba spada v okvir t. i. izjeme obdelave za domače potrebe.[447] Izjema obdelave za domače potrebe je uporaba osebnih podatkov „s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti“.[448] To izjemo je treba od sprejetja odločbe SEU v zadevi *Bodil Lindqvist*[449] kljub vsemu razlagati ozko, zlasti v zvezi z razkritjem osebnih podatkov. Izjema obdelave za domače potrebe zlasti ne velja za

447 SUVP, člen 2(2)(c).

448 Prav tam.

449 SEU, *Kazenski postopek proti Bodil Lindqvist*, C-101/01, 6. november 2003.

objavo osebnih podatkov neomejenemu številu uporabnikov na spletu ali za obdelavo osebnih podatkov, ki ima poklicne ali komercialne vidike (za več podrobnosti o tej zadevi glej razdelke 2.1.2, 2.2.2 in 2.3.1).

Zaupnost sporočil je eden od vidikov zaupnosti, za katerega se uporablja načelo *lex specialis*. Države članice morajo v skladu s posebnimi pravili za zagotavljanje zaupnosti elektronskih komunikacij na podlagi Direktive o zasebnosti in elektronskih komunikacijah vsem osebam razen uporabnikom prepovedati, da brez privolitve zadevnih uporabnikov poslušajo, prisluškujejo, shranjujejo ali na druge načine prestrezajo ali nadzirajo komunikacije (sporočila) in z njimi povezane metapodatke.[450] V nacionalnem pravu se lahko izjeme od tega načela dovolijo le zaradi nacionalne varnosti, obrambe, preprečevanja ali odkrivanja kaznivih dejanj in le, če so taki ukrepi potrebni in sorazmerni za doseganje zastavljenih ciljev.[451] Enaka pravila se bodo uporabljala na podlagi prihodnje uredbe o zasebnosti in elektronskih komunikacijah, vendar bo področje uporabe tega pravnega akta o zasebnosti in elektronskih komunikacijah razširjeno, in sicer bo poleg javno dostopnih elektronskih komunikacijskih storitev zajemalo tudi komunikacije prek storitev OTT (kot so mobilne aplikacije).

V pravu Sveta Evrope je obveznost zaupnosti zajeta s pojmom varnosti osebnih podatkov v členu 7(1) posodobljene Konvencije št. 108, v katerem je obravnavana varnost osebnih podatkov.

Za obdelovalce zaupnost pomeni, da osebnih podatkov ne smejo razkriti tretjim osebam ali drugim uporabnikom brez dovoljenja. Za zaposlene pri upravljavcu ali obdelovalcu zaupnost pomeni, da lahko osebne podatke uporabljajo samo v skladu z navodili pristojnih nadrejenih.

Obveznost zaupnosti mora biti vključena v vsako pogodbo med upravljavci in njihovimi pogodbenimi obdelovalci. Poleg tega morajo upravljavci in obdelovalci sprejeti posebne ukrepe, s katerimi svojim zaposlenim naložijo pravno obveznost zaupnosti, kar običajno storijo tako, da v pogodbo o zaposlitvi vključijo določila o zaupnosti.

Kršitev poklicne dolžnosti varovanja zaupnosti se v številnih državah članicah EU in pogodbenicah Konvencije št. 108 kaznuje po kazenskem pravu.

450 Direktiva o zasebnosti in elektronskih komunikacijah, člen 5(1).

451 Prav tam, člen 15(1).

4.2.3 Obvestila o kršitvi varnosti osebnih podatkov

Kršitev varnosti osebnih podatkov se nanaša na kršitev varnosti, ki povzroči namerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do obdelanih osebnih podatkov.[452] Čeprav nove tehnologije, kot je šifriranje, zdaj ponujajo več možnosti za zagotavljanje varnosti obdelave, so kršitve varnosti osebnih podatkov še vedno pogost pojav. Vzroki teh kršitev so lahko različni, od nenamernih napak oseb, zaposlenih v neki organizaciji, do zunanjih groženj, kot so hekerji in združbe kibernetskega kriminala.

Kršitve varnosti osebnih podatkov so lahko zelo škodljive za pravici do zasebnosti in varstva osebnih podatkov posameznikov, ki zaradi kršitve izgubijo nadzor nad svojimi osebnimi podatki. Privedejo lahko do kraje ali zlorabe identitete, finančne izgube ali premoženjske škode, izgube zaupnosti osebnih podatkov, ki se varujejo kot poklicna skrivnost, in okrnitve ugleda posameznika, na katerega se nanašajo osebni podatki. Delovna skupina iz člena 29 je v Smernicah o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe 2016/679 pojasnila, da imajo lahko kršitve tri vrste vpliva na osebne podatke: razkritje, izgubo in/ali spremembo.[453] Poleg obveznosti sprejetja ukrepov za zagotavljanje varnosti obdelave, kot je pojasnjeno v razdelku 4.2, je treba zagotoviti še, da se upravljavci na kršitve, kadar do njih pride, odzovejo ustrezno in pravočasno.

Nadzorni organi in posamezniki se pogosto ne zavedajo, da je prišlo do kršitve varnosti osebnih podatkov, kar posameznikom preprečuje, da bi sprejeli ukrepe, s katerimi bi se zavarovali pred negativnimi posledicami. Da bi utrdila pravice posameznikov in omejila vpliv kršitev varnosti osebnih podatkov, **EU in Svet Evrope** upravljavcem v nekaterih okoliščinah nalagata obveznost obveščanja.

V skladu s posodobljeno Konvencijo **Sveta Evrope** št. 108 morajo pogodbenice od upravljavcev vsaj zahtevati, da pristojni nadzorni organ obvestijo o kršitvah varnosti osebnih podatkov, ki bi lahko resno posegle v pravice posameznikov, na katere se nanašajo osebni podatki. Tako obvestilo je treba predložiti brez odlašanja.[454]

452 SUVP, člen 4(12); glej tudi Delovna skupina za varstvo podatkov iz člena 29 (2017), *Smernice o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe 2016/679*, WP 250, 3. oktober 2017, str. 8.

453 Delovna skupina za varstvo podatkov iz člena 29 (2017), *Smernice o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe 2016/679*, WP 250, 3. oktober 2017, str. 7.

454 Posodobljena Konvencija št. 108, člen 7(2); Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točke 64–66.

V **pravu EU** je vzpostavljena podrobna ureditev časovnega okvira in vsebine obvestil.[455] V skladu z njo morajo upravljavci brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, nadzorne organe obvestiti o nekaterih kršitvah varnosti osebnih podatkov. Če obvestila ne predložijo v 72 urah, mu morajo priložiti pojasnilo z navedbo razlogov za zamudo. Upravljavci so zahteve po obvestilu oproščeni le, če lahko dokažejo, da ni verjetno, da bi bile s kršitvijo varnosti osebnih podatkov ogrožene pravice in svoboščine zadevnih posameznikov.

V uredbi so določene osnovne informacije, ki jih je treba vključiti v obvestilo, da se nadzornemu organu omogoči sprejetje potrebnih ukrepov.[456] Obvestilo mora vsebovati vsaj opis vrste kršitve varnosti osebnih podatkov ter kategorij in približnega števila zadevnih posameznikov, na katere se nanašajo osebni podatki, opis verjetnih posledic kršitve in opis ukrepov, ki jih je upravljavec izvedel za obravnavanje kršitve in ublažitev njenih posledic. Poleg tega bi bilo treba v njem navesti ime in kontaktne podatke pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, da lahko pristojni nadzorni organ po potrebi pridobi dodatne informacije.

Kadar je verjetno, da kršitev varnosti osebnih podatkov povzroči velika tveganja za pravice in svoboščine posameznikov, morajo upravljavci te posameznike (na katere se nanašajo osebni podatki) brez nepotrebnega odlašanja obvestiti o kršitvi.[457] Informacije, vključno z opisom kršitve varnosti osebnih podatkov, morajo biti posameznikom, na katere se nanašajo osebni podatki, predložene v jasnem in preprostem jeziku ter vključevati informacije, podobne tistim, ki jih je treba navesti v uradnih obvestilih nadzornim organom. Upravljavci so lahko v nekaterih okoliščinah izvzeti iz obveznosti, da posameznike, na katere se nanašajo osebni podatki, obvestijo o takih kršitvah. Izjeme se uporabljajo, če je upravljavec izvedel ustrezne tehnične in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za osebne podatke, v zvezi s katerimi je bila storjena kršitev varnosti, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih, kot na primer šifriranje. Upravljavec je poleg tega lahko izvzet iz obveznosti obveščanja posameznikov, na katere se nanašajo osebni podatki, če po kršitvi sprejme ukrepe za zagotovitev, da se grožnja za pravice posameznikov, na katere se nanašajo osebni podatki, ne bo več uresničila. Če bi bil za uradno obvestilo potreben nesorazmeren napor upravljavca, so lahko posamezniki, na katere se nanašajo osebni podatki,

455 SUVP, člena 33 in 34.

456 Prav tam, člen 33(3).

457 Prav tam, člen 34.

o kršitvi obveščeni z drugimi sredstvi, na primer z javnim sporočilom ali podobnimi ukrepi.[458]

Obveznost uradnega obveščanja nadzornih organov in posameznikov, na katere se nanašajo osebni podatki, o kršitvah varnosti osebnih podatkov velja za upravljavce. Vendar se lahko kršitve varnosti osebnih podatkov zgodijo ne glede na to, ali obdelavo izvaja upravljavec ali obdelovalec. Zato je treba zagotoviti, da morajo o kršitvah varnosti osebnih podatkov poročati tudi obdelovalci. V tem primeru morajo obdelovalci brez nepotrebnega odlašanja upravljavca obvestiti o kršitvah varnosti osebnih podatkov.[459] Upravljavec je nato odgovoren za obveščanje nadzornih organov in prizadetih posameznikov, na katere se nanašajo osebni podatki, in sicer ob upoštevanju zgoraj navedenih pravil in časovnega okvira.

4.3 Pravila o odgovornosti in spodbujanju skladnosti

Ključni poudarki

- Upravljavci in obdelovalci morajo za zagotavljanje odgovornosti pri obdelavi osebnih podatkov voditi evidence o dejavnostih obdelave, za katere so odgovorni, in jih na zahtevo predložiti nadzornim organom.
- V SUVP so navedeni številni instrumenti za spodbujanje skladnosti:
  - imenovanje pooblaščenih oseb za varstvo podatkov v nekaterih primerih;
  - izvedba ocene učinka pred začetkom dejavnosti obdelave, ki bi lahko povzročile velika tveganja za pravice in svoboščine posameznikov;
  - predhodno posvetovanje z ustreznim nadzornim organom, če ocena učinka pokaže, da obdelava pomeni tveganja, ki jih ni mogoče ublažiti;
  - kodeksi ravnanja za upravljavce in obdelovalce, v katerih je določena uporaba te uredbe v različnih sektorjih za obdelavo;
  - mehanizmi certificiranja, pečati in označbe.
- V okviru prava Sveta Evrope so predlagani podobni instrumenti za spodbujanje skladnosti, in sicer v posodobljeni Konvenciji št. 108.

458 Prav tam, člen 34(3)(c).

459 Prav tam, člen 33(2).

Načelo odgovornosti je zlasti pomembno za zagotavljanje izvajanja pravil o varstvu osebnih podatkov v Evropi. Upravljavec je odgovoren za skladnost s pravili o varstvu osebnih podatkov in mora biti to skladnost zmožen dokazati. Odgovornost ne sme postati pomembna šele, ko se zgodi kršitev. Ravno nasprotno, upravljavci imajo proaktivno obveznost, da v vseh fazah obdelave osebnih podatkov izvajajo ustrezne politike upravljanja osebnih podatkov. V skladu z evropskim pravom o varstvu osebnih podatkov morajo upravljavci izvajati tehnične in organizacijske ukrepe za zagotavljanje, da obdelava poteka v skladu s pravom, in morajo biti to skladnost tudi zmožni dokazati. Med temi ukrepi so imenovanje pooblaščenih oseb za varstvo podatkov, vodenje evidenc in dokumentacije v zvezi z obdelavo ter izvajanje ocen učinka na zasebnost.

4.3.1 Pooblaščene osebe za varstvo podatkov

Pooblaščene osebe za varstvo podatkov so osebe, ki v organizacijah, v katerih se izvaja obdelava osebnih podatkov, svetujejo o spoštovanju pravil o varstvu osebnih podatkov. So temelj odgovornosti, saj spodbujajo skladnost, ob tem pa delujejo tudi kot posredniki med nadzornimi organi, posamezniki, na katere se nanašajo osebni podatki, in organizacijo, ki jih je imenovala.

V okviru prava Sveta Evrope je v členu 10(1) posodobljene Konvencije št. 108 splošna obveznost glede odgovornosti naložena upravljavcem in obdelovalcem. V skladu z njo morajo upravljavci in obdelovalci sprejeti vse ustrezne ukrepe za izpolnjevanje pravil o varstvu osebnih podatkov, določenih v konvenciji, in dokazati, da je obdelava osebnih podatkov pod njihovim nadzorom v skladu z določbami konvencije. Čeprav v konvenciji niso določeni konkretni ukrepi, ki bi jih morali sprejeti upravljavci in obdelovalci, je v Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 navedeno, da je imenovanje pooblaščene osebe za varstvo podatkov eden od možnih ukrepov, ki pripomore k dokazovanju skladnosti. Pooblaščenim osebam za varstvo podatkov bi bilo treba zagotoviti vsa potrebna sredstva za izpolnjevanje njihovih pooblastil.[460]

V nasprotju s pravom Sveta Evrope imenovanje pooblaščene osebe za varstvo podatkov **v okviru prava EU** ni vedno prepuščeno presoji upravljavcev in obdelovalcev, temveč je v nekaterih okoliščinah obvezno. SUVP, v kateri je priznana ključna vloga, ki jo ima pooblaščena oseba za varstvo podatkov v novem sistemu upravljanja,

460 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 87.

vsebuje podrobne določbe o imenovanju pooblaščene osebe ter njenem položaju, dolžnostih in nalogah.[461]

V skladu s SUVP je imenovanje pooblaščene osebe za varstvo podatkov obvezno v treh primerih: kadar obdelavo opravlja javni organ ali telo, kadar temeljne dejavnosti upravljavca ali obdelovalca zajemajo dejanja obdelave, pri katerih je treba posameznike, na katere se nanašajo osebni podatki, redno in sistematično obsežno spremljati, ali kadar temeljne dejavnosti zajemajo obsežno obdelavo posebnih vrst podatkov in osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški.[462] Čeprav v zadevni uredbi niso opredeljeni izrazi, kot sta „sistematično obsežno spremljati" in „temeljne dejavnosti", je Delovna skupina iz člena 29 objavila smernice, kako bi jih bilo treba razlagati.[463]

Primer: družbe, ki upravljajo družbene medije in iskalnike, se verjetno štejejo za upravljavce, katerih dejanja obdelave vključujejo redno in sistematično spremljanje posameznikov, na katere se nanašajo osebni podatki. Poslovni model takih družb temelji na obdelavi velikih količin osebnih podatkov, pri čemer te družbe ustvarijo precejšnje prihodke z zagotavljanjem storitev ciljnega oglaševanja in omogočanjem podjetjem, da se oglašujejo na spletnih mestih. Ciljno oglaševanje je prikazovanje oglasov na podlagi demografskih podatkov in preteklih nakupov potrošnikov ali njihovega vedenja. Zato je zanj potrebno sistematično spremljanje spletnih navad in vedenja posameznikov, na katere se nanašajo osebni podatki.

Primer: bolnišnica in zdravstvena zavarovalnica sta značilna primera upravljavcev, katerih dejavnosti zajemajo obsežno obdelavo posebnih vrst osebnih podatkov. Podatki, ki razkrivajo informacije o zdravju posameznika, v skladu s pravom Sveta Evrope in pravom EU spadajo med posebne vrste osebnih podatkov, zato je v zvezi z njimi potrebno okrepljeno varstvo. V okviru prava EU se poleg tega med posebne vrste osebnih podatkov uvrščajo tudi genski in biometrični podatki. Če zdravstvene ustanove in zavarovalnice take podatke obdelujejo v velikem obsegu, morajo v skladu s SUVP imenovati pooblaščeno osebo za varstvo podatkov.

461 SUVP, členi 37–39.

462 Prav tam, člen 37(1).

463 Delovna skupina za varstvo podatkov iz člena 29 (2017), *Smernice o pooblaščenih osebah za varstvo podatkov*, WP 243 rev.01, nazadnje revidirane in sprejete 5. aprila 2017.

Poleg tega člen 37(4) SUVP določa, da v primerih, ki niso trije obvezni primeri iz člena 37(1), upravljavec ali obdelovalec ali združenja in druga telesa, ki predstavljajo vrste upravljavcev ali obdelovalcev, lahko imenujejo ali, kadar tako zahteva pravo Unije ali pravo države članice, morajo imenovati pooblaščeno osebo za varstvo podatkov.

Druge organizacije niso pravno zavezane imenovati pooblaščeno osebo za varstvo podatkov. Vendar je v SUVP določeno, da se lahko upravljavci in obdelovalci odločijo za prostovoljno imenovanje pooblaščene osebe za varstvo podatkov, hkrati pa je z njo državam članicam omogočeno, da določijo, da je tako imenovanje obvezno za več vrst organizacij, kot so tiste, predvidene v navedeni uredbi.[464]

Ko upravljavec imenuje pooblaščeno osebo za varstvo podatkov, mora zagotoviti, da je „ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov“ v organizaciji.[465] Pooblaščene osebe za varstvo podatkov bi morale na primer biti vključene v zagotavljanje nasvetov o izvajanju ocen učinka v zvezi z varstvom podatkov ter oblikovanje in vodenje evidence o dejavnostih obdelave v organizaciji. Da se jim omogoči učinkovito opravljanje nalog, jim morajo upravljavci in obdelovalci zagotoviti potrebne vire, vključno s finančnimi viri, infrastrukturo in opremo. Dodatne zahteve vključujejo zagotovitev zadostnega časa, v katerem lahko pooblaščene osebe za varstvo podatkov izpolnijo svoje dolžnosti, in stalno usposabljanje, da se pooblaščenim osebam za varstvo podatkov omogoči, da izpopolnjujejo svoje strokovno znanje in da so vedno seznanjene z razvojem dogodkom na področju prava o varstvu osebnih podatkov.[466]

V SUVP so določena nekatera osnovna jamstva za zagotavljanje, da pooblaščene osebe za varstvo podatkov delujejo neodvisno. Upravljavec in obdelovalec morata zagotoviti, da pooblaščene osebe za varstvo podatkov pri opravljanju nalog v zvezi z varstvom osebnih podatkov ne prejemajo nobenih navodil od podjetja, niti od oseb na najvišji upravni ravni. Poleg tega ne smejo biti razrešene ali kakor koli kaznovane zaradi opravljanja svojih nalog.[467] Na primer, pooblaščena oseba za varstvo podatkov upravljavcu ali obdelovalcu svetuje, naj izvede oceno učinka v zvezi z varstvom podatkov, saj meni, da bi obdelava verjetno povzročila veliko tveganje za

464 SUVP, člen 37(3) in (4).

465 Prav tam, člen 38(1).

466 Delovna skupina za varstvo podatkov iz člena 29 (2017), *Smernice o pooblaščenih osebah za varstvo podatkov*, WP 243 rev.01, nazadnje revidirane in sprejete 5. aprila 2017, točka 3.1.

467 SUVP, člen 38(2) in (3).

posameznike, na katere se nanašajo osebni podatki. Podjetje se ne strinja z nasvetom pooblaščene osebe za varstvo podatkov, saj meni, da ni dobro utemeljen, in se nato odloči, da ocene učinka ne bo izvedlo. Podjetju ni treba upoštevati nasveta, ne sme pa razrešiti pooblaščene osebe za varstvo podatkov ali je kaznovati, ker je dala tak nasvet.

V členu 39 SUVP so podrobno opredeljene naloge in dolžnosti pooblaščenih oseb za varstvo podatkov, ki vključujejo zahteve po obveščanju podjetij in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu z zakonodajo ter spremljanju skladnosti s pravili EU in nacionalnimi pravili o varstvu osebnih podatkov, in sicer z izvajanjem revizij in usposabljanjem osebja, vključenega v dejanja obdelave. Pooblaščene osebe za varstvo podatkov morajo poleg tega sodelovati z nadzornim organom in delovati kot kontaktna točka zanj pri zadevah v zvezi z obdelavo osebnih podatkov, kot je na primer kršitev varnosti osebnih podatkov.

Kar zadeva osebne podatke, ki jih obdelujejo institucije in organi EU, je v Uredbi (ES) št. 45/2001 določeno, da mora vsaka institucija in organ EU imenovati pooblaščeno osebo za varstvo podatkov. Ta oseba zagotavlja, da se v institucijah in organih EU pravilno uporabljajo določbe zadevne uredbe ter da so posamezniki, na katere se nanašajo osebni podatki, in upravljavci osebnih podatkov obveščeni o svojih pravicah in obveznostih.[468] Odgovorna je tudi za odgovarjanje na zahteve ENVP in sodelovanje z njim, kadar je to potrebno. Uredba (ES) št. 45/2001 podobno kot SUVP vsebuje določbe o neodvisnosti pooblaščenih oseb za varstvo podatkov pri opravljanju njihovih nalog in potrebi po tem, da se jim zagotovijo osebje in viri.[469] Pooblaščene osebe za varstvo podatkov je treba uradno obvestiti, preden institucija ali organ EU (ali službe teh organizacij) izvedejo katera koli dejanja obdelave. Pooblaščene osebe morajo voditi evidenco dejanj obdelave, o katerih so bile uradno obveščene.[470]

4.3.2 Evidenca dejavnosti obdelave

Da lahko podjetja dokažejo skladnost in odgovarjajo za svoja dejanja, so pogosto pravno zavezana k dokumentiranju in evidentiranju svojih dejavnosti. Pomemben primer sta davčna zakonodaja in revidiranje, v skladu s katerima se od vseh podjetij

468 Za popoln seznam nalog pooblaščenih oseb za varstvo podatkov glej člen 24(1) Uredbe (ES) št. 45/2001.

469 Uredba (ES) št. 45/2001, člen 24(6) in (7).

470 Prav tam, člena 25 in 26.

zahteva, da hranijo obsežno dokumentacijo in vodijo evidence. Pomembno je tudi, da se podobne zahteve opredelijo na drugih področjih prava, zlasti prava o varstvu osebnih podatkov, saj je vodenje evidenc pomembno za spodbujanje skladnosti s pravili o varstvu osebnih podatkov. V okviru **prava EU** je tako določeno, da morajo upravljavci ali njihovi predstavniki voditi evidenco dejavnosti obdelave, ki se opravljajo v okviru njihove odgovornosti.[471] Namen te obveznosti je zagotoviti, da imajo nadzorni organi po potrebi na voljo potrebno dokumentacijo, ki jim omogoča potrditev zakonitosti obdelave.

Informacije, ki jih je treba dokumentirati, vključujejo:

- naziv ali ime in kontaktne podatke upravljavca in, kadar obstajajo, skupnega upravljavca, predstavnika upravljavca in pooblaščene osebe za varstvo podatkov;
- namene obdelave;
- opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov, ki se obdelujejo;
- informacije o kategorijah uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki;
- informacije o tem, ali so bili opravljeni prenosi osebnih podatkov v tretjo državo ali mednarodno organizacijo oziroma ali bodo opravljeni;
- kadar je mogoče, predvidene roke za izbris različnih vrst podatkov in pregled tehničnih ukrepov, sprejetih za zagotavljanje varnosti obdelave.[472]

Obveznost vodenja evidenc o dejavnostih obdelave v skladu s SUVP ne velja le za upravljavce, temveč tudi za obdelovalce. To je pomembna sprememba, saj so bile pred sprejetjem navedene uredbe obveznosti obdelovalca določene predvsem v pogodbi, sklenjeni med upravljavcem in obdelovalcem. Njihova obveznost vodenja evidenc je zdaj določena neposredno z zakonodajo.

471 SUVP, člen 30.

472 Prav tam, člen 30(1).

SUVP določa izjemo od te obveznosti. Zahteva po vodenju evidenc se ne uporablja za podjetje ali organizacijo (upravljavca ali obdelovalca), ki zaposluje manj kot 250 oseb. Vendar je ta izjema pogojena s tem, da zadevna organizacija ne izvaja obdelave, za katero je verjetno, da pomeni tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, da je obdelava le občasna in da ne vključuje posebnih vrst podatkov iz člena 9(1) ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz člena 10 zadevne uredbe.

Vodenje evidenc o dejavnostih obdelave bi moralo upravljavcem in obdelovalcem omogočati dokazovanje skladnosti z zadevno uredbo. Poleg tega bi moralo nadzornim organom omogočati spremljanje zakonitosti obdelave. Če nadzorni organ zahteva dostop do teh evidenc, morajo upravljavci in obdelovalci sodelovati ter mu omogočiti dostop do njih.

4.3.3 Ocena učinka v zvezi z varstvom podatkov in predhodno posvetovanje

Z dejanji obdelave so neločljivo povezana nekatera tveganja za pravice posameznikov. Osebni podatki se lahko izgubijo, razkrijejo nepooblaščenim osebam ali nezakonito obdelujejo. Tveganja se seveda razlikujejo glede na naravo obdelave in njen obseg. Pri obsežnih dejanjih obdelave, ki vključujejo obdelavo občutljivih osebnih podatkov, je na primer stopnja tveganja za posameznike, na katere se nanašajo osebni podatki, precej višja v primerjavi s potencialnimi tveganji, kadar manjše podjetje obdeluje naslove in osebne telefonske številke svojih zaposlenih.

Ker se pojavljajo nove tehnologije in postaja obdelava vse bolj zapletena, morajo upravljavci pred začetkom dejanja obdelave obravnavati taka tveganja, tako da proučijo verjetni učinek predvidene obdelave. To organizacijam omogoča, da vnaprej ustrezno opredelijo, obravnavajo in ublažijo tveganja, kar znatno omeji verjetnost negativnega vpliva na posameznike, ki ga povzroči obdelava.

Ocene učinka v zvezi z varstvom podatkov so predvidene **v pravu Sveta Evrope in pravu EU**. V pravnem okviru Sveta Evrope morajo pogodbenice v skladu s členom 10(2) posodobljene Konvencije št. 108 zagotoviti, da upravljavci in obdelovalci proučijo verjetni učinek predvidene obdelave osebnih podatkov na pravice in temeljne svoboščine posameznikov, na katere se nanašajo osebni podatki, pred začetkom take obdelave, in da po oceni obdelavo prilagodijo tako, da se preprečijo ali zmanjšajo tveganja v zvezi z obdelavo.

S pravom EU je naložena podobna podrobnejša obveznost upravljavcem, ki spadajo na področje uporabe SUVP. Člen 35 določa, da je oceno učinka v zvezi z varstvom podatkov treba opraviti, kadar je možno, da bi lahko obdelava povzročila veliko tveganje za pravice in svoboščine posameznikov. V tej uredbi ni opredeljeno, kako je treba oceniti verjetnost tveganja, je pa v njej navedeno, katera bi lahko bila ta tveganja.[473] Uredba vsebuje seznam dejanj obdelave, ki se štejejo za zelo tvegana in v zvezi s katerimi je zlasti potrebna predhodna ocena učinka, in sicer v primerih, kadar:

- se osebni podatki obdelujejo za sprejemanje odločitev o posameznikih po vsakem sistematičnem in obsežnem vrednotenju osebnih vidikov v zvezi s posamezniki (oblikovanje profilov);

- se občutljivi podatki ali osebni podatki v zvezi s kazenskimi obsodbami in prekrški obdelujejo obsežno;

- obdelava vključuje obsežno sistematično spremljanje javno dostopnih območij.

Nadzorni organi morajo sprejeti in objaviti seznam vrst dejanj obdelave, za katere je treba opraviti oceno učinka. Določijo lahko tudi seznam dejanj obdelave, ki so izvzeta iz te obveznosti.[474]

Če je potrebna ocena učinka, morajo upravljavci oceniti potrebnost in sorazmernost obdelave ter možna tveganja za pravice posameznikov. Ocena učinka mora vsebovati tudi načrtovane varnostne ukrepe za obravnavo ugotovljenih tveganj. Da bi nadzorni organi držav članic oblikovali te sezname, morajo sodelovati med seboj in z Evropskim odborom za varstvo podatkov. Tako bo zagotovljen skladen pristop po vsej EU v zvezi z dejanji, za katera je potrebna ocena učinka, upravljavci pa bodo morali izpolnjevati podobne zahteve ne glede na to, kje so.

Če se po oceni učinka zdi, da bi obdelava povzročila veliko tveganje za pravice posameznikov, če ne bi bili sprejeti ukrepi za ublažitev tveganja, se mora upravljavec pred začetkom obdelave posvetovati z ustreznim nadzornim organom.[475]

473 SUVP, uvodna izjava 75.

474 Prav tam, člen 35(4) in (5).

475 Prav tam, člen 36(1); Delovna skupina za varstvo podatkov iz člena 29 (2017), *Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679*, WP 248 rev.01, Bruselj, 4. oktober 2017.

Delovna skupina iz člena 29 je objavila smernice o ocenah učinka v zvezi z varstvom podatkov in tem, kako opredeliti verjetnost, da bo obdelava povzročila veliko tveganje.[476] Oblikovala je devet meril za pomoč pri ugotavljanju, ali je v posameznem primeru potrebna ocena učinka v zvezi z varstvom podatkov:[477] (1) vrednotenje ali točkovanje, (2) avtomatizirano odločanje, ki ima pravne ali podobno pomembne učinke, (3) sistematično spremljanje, (4) občutljivi podatki, (5) podatki, ki se obdelujejo v velikem obsegu, (6) usklajeni ali združeni nabori podatkov, (7) podatki o ranljivih posameznikih, na katere se nanašajo osebni podatki, (8) inovativna uporaba ali uporaba novih tehnoloških ali organizacijskih rešitev, (9) kadar sama dejanja obdelave „posameznikom preprečujejo uresničevanje pravice ali uporabo storitve ali pogodbe". Delovna skupina iz člena 29 je uvedla okvirno pravilo, da dejanja obdelave, ki izpolnjujejo manj kot dve merili, pomenijo nižjo raven tveganja in da v zvezi z njimi ni potrebna ocena učinka v zvezi z varstvom podatkov, medtem ko je taka ocena potrebna za tista dejanja obdelave, ki izpolnjujejo dve merili ali več. Če ni jasno, ali je v posameznem primeru ocena učinka v zvezi z varstvom podatkov obvezna, Delovna skupina iz člena 29 priporoča izvedbo take ocene, saj je „uporabno orodje, ki je upravljavcem v pomoč pri zagotavljanju skladnosti z zakonodajo o varstvu podatkov".[478] Če se uvaja nova tehnologija za obdelavo podatkov, je pomembno, da se izvede ocena učinka v zvezi z varstvom podatkov.[479]

4.3.4 Kodeksi ravnanja

Namen kodeksov ravnanja, ki naj bi se uporabljali v različnih sektorjih, je opisati in opredeliti uporabo SUVP v posameznih sektorjih. V zvezi z upravljavci in obdelovalci osebnih podatkov bi lahko oblikovanje takih kodeksov znatno izboljšalo skladnost in okrepilo izvajanje pravil EU o varstvu osebnih podatkov. S strokovnim znanjem udeležencev sektorja se bo spodbudilo iskanje rešitev, ki so praktične in se bodo zato verjetno tudi uporabljale. V SUVP, v kateri je priznan pomen takih kodeksov za učinkovito izvajanje prava o varstvu osebnih podatkov, so države članice, nadzorni organi, Komisija in Evropski odbor za varstvo podatkov pozvani, naj spodbujajo pripravljanje kodeksov ravnanja, katerih namen je prispevati k pravilni uporabi navedene uredbe v vsej EU.[480] V kodeksih bi lahko bila opredeljena uporaba navedene

476 Delovna skupina za varstvo podatkov iz člena 29 (2017), *Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje", za namene Uredbe (EU) 2016/679*, WP 248 rev.01, Bruselj, 4. oktober 2017.

477 Prav tam, str. 10–12.

478 Prav tam, str. 9.

479 Prav tam.

480 SUVP, člen 40(1).

uredbe v posameznih sektorjih, vključno z zadevami, kot so zbiranje osebnih podatkov, informacije, ki jih je treba zagotoviti posameznikom, na katere se nanašajo osebni podatki, in javnosti, ter uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki.

Da se zagotovi skladnost teh kodeksov ravnanja s pravili, določenimi v SUVP, je treba kodekse pred njihovim sprejetjem predložiti pristojnemu nadzornemu organu. Nadzorni organ nato poda mnenje, ali predloženi osnutek kodeksa spodbuja skladnost z zadevno uredbo, in kodeks odobri, če ugotovi, da zagotavlja ustrezne zaščitne ukrepe.[481] Nadzorni organi morajo objaviti odobrene kodekse ravnanja in merila, na katerih je temeljila njihova potrditev. Kadar se osnutek kodeksa ravnanja nanaša na dejavnosti obdelave v več državah članicah, pristojni nadzorni organ pred odobritvijo osnutka kodeksa, spremembe ali razširitve kodeks predloži Evropskemu odboru za varstvo podatkov, ki poda mnenje o skladnosti kodeksa s SUVP. Komisija lahko z izvedbenimi akti sklene, da je odobren kodeks ravnanja, ki ji je bil predložen, v Uniji splošno veljaven.

Zavezanost h kodeksu ravnanja ima pomembne prednosti za posameznike, na katere se nanašajo osebni podatki, ter upravljavce in obdelovalce. Taki kodeksi zagotavljajo podrobne smernice, ki pravne zahteve prilagajajo posameznim sektorjem in spodbujajo preglednost dejavnosti obdelave. Upravljavci in obdelovalci lahko zavezanost h kodeksom uporabljajo kot dokaz, da ravnajo v skladu s pravom EU, in kot sredstvo za krepitev svoje javne podobe kot organizacij, ki pri svojih dejavnostih dajejo prednost varstvu osebnih podatkov in so mu zavezane. Odobreni kodeksi ravnanja se lahko skupaj z zavezujočimi in izvršljivimi zavezami uporabljajo kot ustrezni zaščitni ukrepi za prenos osebnih podatkov v tretje države. Za zagotavljanje, da organizacije, ki so zavezane h kodeksom ravnanja, dejansko ravnajo v skladu z njimi, se lahko imenuje posebno telo (ki ga akreditira ustrezni nadzorni organ) za spremljanje in zagotavljanje skladnosti. Da bi telo učinkovito izpolnjevalo svoje naloge, mora biti neodvisno, imeti dokazano strokovno znanje o zadevah, urejenih s kodeksom ravnanja, ter imeti pregledne postopke in strukture, ki mu omogočajo obravnavanje pritožb zaradi kršitev kodeksa.[482]

V okviru **prava Sveta Evrope** je v posodobljeni Konvenciji št. 108 določeno, da se lahko raven varstva osebnih podatkov, zagotovljena z nacionalnim pravom, koristno okrepi z ukrepi prostovoljne ureditve, kot so kodeksi dobre prakse ali kodeksi

481 Prav tam, člen 40(5).

482 Prav tam, člen 41(1) in (2).

strokovnega ravnanja. Vendar so to le prostovoljni ukrepi na podlagi posodobljene Konvencije št. 108: iz nje ni mogoče izpeljati pravne obveznosti glede sprejetja takih ukrepov, čeprav je to priporočljivo, poleg tega taki ukrepi sami po sebi ne zadoščajo za zagotavljanje skladnosti s konvencijo.[483]

4.3.5 Certificiranje

Poleg kodeksov ravnanja so mehanizmi certificiranja ter pečati in označbe za varstvo podatkov še en način, s katerim lahko upravljavci in obdelovalci dokažejo skladnost s SUVP. Zato je v navedeni uredbi določen sistem prostovoljnega certificiranja, v okviru katerega lahko nekatera telesa ali nadzorni organi izdajajo certifikate. Upravljavci in obdelovalci, ki se zavežejo k uporabi mehanizma certificiranja, lahko postanejo prepoznavnejši in verodostojnejši, saj lahko posamezniki, na katere se nanašajo osebni podatki, na podlagi certifikatov, pečatov in označb hitro ocenijo raven varstva pri obdelavi osebnih podatkov v neki organizaciji. Treba je poudariti, da dejstvo, da ima upravljavec ali obdelovalec tak certifikat, nikakor ne zmanjšuje njegovih dolžnosti in obveznosti glede izpolnjevanja vseh zahtev iz navedene uredbe.

4.4 Vgrajeno in privzeto varstvo osebnih podatkov

Vgrajeno varstvo osebnih podatkov

V skladu s **pravom EU** morajo upravljavci sprejeti ukrepe za učinkovito izvajanje načel varstva osebnih podatkov ter v obdelavo vključiti potrebne zaščitne ukrepe, da se izpolnijo zahteve zadevne uredbe in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki.[484] Te ukrepe bi bilo treba izvajati tako v času obdelave kot v času določanja sredstev obdelave. Upravljavec mora pri izvajanju teh ukrepov upoštevati najnovejši tehnološki razvoj, stroške izvajanja ter naravo, obseg in namene obdelave osebnih podatkov, pa tudi tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in resnost teh tveganj.[485]

483 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 33.

484 SUVP, člen 25(1).

485 Glej Delovna skupina za varstvo podatkov iz člena 29 (2017), *Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679*, WP 248 rev.01, 4. oktober 2017. Glej tudi ENISA (2015), Zasebnost in vgrajeno varstvo podatkov – od politike do inženirstva, 12. januar 2015.

V skladu s **pravom Sveta Evrope** morajo upravljavci in obdelovalci pred začetkom obdelave oceniti verjetni učinek, ki ga bo obdelava osebnih podatkov imela na pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Poleg tega morajo obdelavo osebnih podatkov zasnovati tako, da preprečijo ali čim bolj zmanjšajo tveganje poseganja v te pravice in svoboščine, ter izvajati tehnične in organizacijske ukrepe, pri katerih se upoštevajo posledice, ki jih ima pravica do varstva osebnih podatkov v vseh fazah obdelave osebnih podatkov.[486]

Privzeto varstvo osebnih podatkov

V skladu s **pravom EU** mora upravljavec izvesti ustrezne ukrepe, s katerimi zagotovi, da se privzeto obdelajo samo osebni podatki, ki so potrebni za zadevne namene obdelave. Ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost.[487] S takšnim ukrepom je treba na primer zagotoviti, da osebni podatki posameznikov niso samodejno dostopni vsem zaposlenim pri upravljavcu. ENVP je pripravil dodatne smernice v dokumentu o naboru orodij za presojo potrebnosti.[488]

Upravljavci in obdelovalci morajo v skladu s **pravom Sveta Evrope** izvesti tehnične in organizacijske ukrepe, da upoštevajo posledice, ki jih ima pravica do varstva osebnih podatkov, ter izvesti tehnične in organizacijske ukrepe, pri katerih se upoštevajo posledice, ki jih ima pravica do varstva osebnih podatkov v vseh fazah obdelave osebnih podatkov.[489]

Agencija ENISA je leta 2016 objavila poročilo o razpoložljivih orodjih in storitvah za zagotavljanje zasebnosti.[490] V tej oceni je med drugim na voljo seznam meril in parametrov, ki so kazalniki dobre ali slabe prakse v zvezi z zasebnostjo. Nekatera merila se nanašajo neposredno na določbe SUVP – na primer uporaba psevdonimizacije in odobrenih mehanizmov certificiranja –, druga merila pa vsebujejo inovativne pobude za zagotavljanje vgrajene in privzete zasebnosti. Tako bi lahko na primer merilo

486 Posodobljena Konvencija št. 108, člen 10(2) in (3), Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 89.

487 SUVP, člen 25(2).

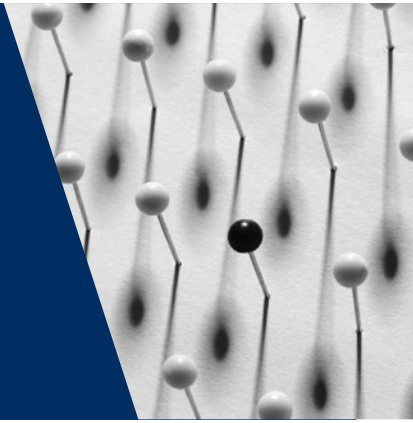
488 Evropski nadzornik za varstvo podatkov (ENVP) (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Bruselj, 11. april 2017.

489 Posodobljena Konvencija št. 108, člen 10(3), Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 89.

490 ENISA, Kontrolni seznam v zvezi s tehnologijo za boljše varovanje zasebnosti: sistematični pristop za ocenjevanje spletnih in mobilnih orodij za varstvo zasebnosti, 20. december 2016.

uporabnosti, ki sicer ni neposredno povezano z zasebnostjo, okrepilo zasebnost, saj lahko omogoči širše sprejetje orodja ali storitve za varstvo zasebnosti. Dejansko je lahko za orodja za varstvo zasebnosti, ki jih je v praksi težko izvajati, značilna zelo nizka stopnja sprejetja v širši javnosti, čeprav zagotavljajo zelo zanesljiva jamstva glede zasebnosti. Poleg tega je ključnega pomena merilo zrelosti in stabilnosti orodja za varstvo zasebnosti, tj. načina, kako se orodje sčasoma razvija in se odziva na obstoječe ali nove izzive v zvezi z zasebnostjo. Druge tehnologije z izboljšanim varovanjem zasebnosti v okviru varnih komunikacij vključujejo šifriranje od konca do konca (komunikacija, v okviru katere lahko preberejo sporočila le osebe, ki komunicirajo), šifriranje odjemalec-strežnik (šifriranje komunikacijskega kanala, vzpostavljenega med odjemalcem in strežnikom), avtentikacijo (preverjanje identitete strank, ki komunicirajo) in anonimno komuniciranje (nobena tretja oseba ne more identificirati strank, ki komunicirajo).

5 Neodvisen nadzor



EU	Obravnavane teme	Svet Evrope
Listina, člen 8(3) Pogodba o delovanju EU, člen 16(2) SUVP, členi 51–59 SEU, C-518/07, *Evropska komisija proti Zvezni republiki Nemčiji* (veliki senat), 2010 SEU, C-614/10, *Evropska komisija proti Republiki Avstriji* (veliki senat), 2012 SEU, C-288/12, *Evropska komisija proti Madžarski* (veliki senat), 2014 SEU, C-362/14, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), 2015	**Nadzorni organi**	Posodobljena Konvencija št. 108, člen 15
SUVP, členi 60–67	**Sodelovanje med nadzornimi organi**	Posodobljena Konvencija št. 108, členi 16–21
SUVP, členi 68–76	**Evropski odbor za varstvo podatkov**	

Ključni poudarki

- Neodvisen nadzor je bistven del evropskega prava varstva podatkov in je določen v členu 8(3) Listine.
- Za zagotovitev učinkovitega varstva osebnih podatkov morajo biti na podlagi nacionalne zakonodaje vzpostavljeni neodvisni nadzorni organi.
- Nadzorni organi morajo delovati popolnoma neodvisno, kar je treba zagotoviti z ustanovnim zakonom in kar mora biti izraženo v posebni organizacijski strukturi nadzornega organa.
- Nadzorni organi imajo posebna pooblastila in naloge, da med drugim:
  - spremljajo in spodbujajo varstvo osebnih podatkov na nacionalni ravni;
  - svetujejo posameznikom, na katere se nanašajo osebni podatki, upravljavcem ter vladi in širši javnosti;
  - obravnavajo pritožbe in posameznikom, na katere se nanašajo osebni podatki, pomagajo pri domnevnih kršitvah pravic do varstva osebnih podatkov;
  - nadzorujejo upravljavce in obdelovalce.
- Nadzorni organi imajo tudi pooblastila, da po potrebi ukrepajo z:
  - opozorilom, opominom ali celo denarno kaznijo upravljavcem in obdelovalcem,
  - odreditvijo popravka, blokiranja ali izbrisa osebnih podatkov,
  - odreditvijo prepovedi obdelave ali naložitvijo upravne globe,
  - predložitvijo zadeve sodišču.
- Ker obdelava osebnih podatkov pogosto vključuje upravljavce, obdelovalce in posameznike, na katere se nanašajo osebni podatki, ki so v različnih državah, morajo nadzorni organi medsebojno sodelovati pri čezmejnih vprašanjih, da bi zagotovili učinkovito varstvo posameznikov v Evropi.
- V EU je bil s SUVP vzpostavljen mehanizem vse na enem mestu za primere čezmejne obdelave osebnih podatkov. Nekatere družbe opravljajo dejavnosti čezmejne obdelave zaradi obdelave osebnih podatkov v okviru dejavnosti poslovnih enot v več kot eni državi članici ali v okviru ene same poslovne enote v Uniji, ki pa znatno vpliva na posameznike, na katere se nanašajo osebni podatki, v več kot eni državi članici. V okviru zadevnega mehanizma bodo take družbe v stiku le z enim nacionalnim nadzornim organom za varstvo podatkov.

- Mehanizem za sodelovanje in skladnost bo omogočal usklajen pristop vseh nadzornih organov, vključenih v zadevni primer. Vodilni nadzorni organ – sedeža ali edine poslovne enote – se posvetuje z drugimi zadevnimi nadzornimi organi in jim predloži osnutek odločitve.
- Podobno kot sedanja Delovna skupina iz člena 29 bodo nadzorni organi posameznih držav članic in Evropski nadzornik za varstvo podatkov (ENVP) člani Evropskega odbora za varstvo podatkov.
- Naloge Evropskega odbora za varstvo podatkov vključujejo na primer spremljanje pravilne uporabe SUVP, svetovanje Komisiji o zadevnih vprašanjih ter izdajanje mnenj, smernic in najboljše prakse v zvezi z najrazličnejšimi temami.
- Glavna razlika je, da Evropski odbor za varstvo podatkov (EOVP) ne bo izdajal le mnenj, kot je bilo urejeno v skladu z Direktivo 95/46/ES. Izdajal bo tudi zavezujoče odločitve v zvezi s primeri, kadar nadzorni organ da ustrezen in utemeljen ugovor v zadevah, obravnavanih v okviru mehanizma vse na enem mestu, kadar pride do nasprotujočih si stališč o tem, kateri od zadevnih nadzornih organov je vodilni, in, nenazadnje, kadar pristojni nadzorni organ ne zahteva ali ne upošteva mnenja EOVP. Cilj je zagotoviti dosledno uporabo te uredbe v vseh državah članicah.

Neodvisen nadzor je bistven del evropskega prava o varstvu osebnih podatkov. V pravu EU in Sveta Evrope se šteje, da je obstoj neodvisnih nadzornih organov nujen za učinkovito varstvo pravic in svoboščin posameznikov pri obdelavi njihovih osebnih podatkov. Ker je obdelava osebnih podatkov zdaj vseprisotna in jo posamezniki zaradi njene vse večje zapletenosti težko razumejo, so ti organi varuhi pravic v digitalni dobi. Obstoj neodvisnih nadzornih organov se v EU šteje za enega najpomembnejših elementov pravice do varstva osebnih podatkov, določene v primarni zakonodaji EU. V členu 8(3) Listine EU o temeljnih pravicah in členu 16(2) PDEU je varstvo osebnih podatkov priznano kot temeljna pravica, poleg tega je v njiju potrjeno, da mora skladnost s pravili o varstvu osebnih podatkov nadzorovati neodvisen organ.

Pomen neodvisnega nadzora za pravo o varstvu osebnih podatkov je priznan tudi v sodni praksi.

Primer: SEU je v zadevi *Schrems*[491] obravnavalo, ali je glede na razkritja Edwarda Snowdna o množičnem nadzoru, ki ga izvaja Agencija ZDA za nacionalno varnost, prenos osebnih podatkov v Združene države Amerike (ZDA) na podlagi prvega sporazuma med EU in ZDA o varnem pristanu v skladu s pravom EU o varstvu osebnih podatkov. Prenos osebnih podatkov v ZDA je

491 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015.

temeljil na odločbi Evropske komisije, sprejeti leta 2000, v skladu s katero so se lahko osebni podatki iz EU prenašali organizacijam ZDA, ki so se samocertificirale v okviru sheme varnega pristana, in sicer na podlagi tega, da shema zagotavlja ustrezno raven varstva osebnih podatkov. Ko je bil irski nadzorni organ zaprošen, naj prouči pritožnikovo pritožbo glede zakonitosti prenosov podatkov po Snowdnovih razkritjih, je pritožbo zavrgel z obrazložitvijo, da mu nadaljnjo proučitev pritožbe preprečuje odločba Komisije o ustreznosti ureditve ZDA za varstvo podatkov, izražene v načelih varnega pristana (v nadaljnjem besedilu: odločba o varnem pristanu).

Vendar je SEU menilo, da odločba Komisije, s katero je omogočen prenos podatkov v tretje države, ki zagotavljajo ustrezno raven varstva, ne more niti izničiti niti zmanjšati pooblastil nacionalnih nadzornih organov. Ugotovilo je, da pooblastila teh organov za nadzor in zagotavljanje skladnosti s pravili EU o varstvu osebnih podatkov izhajajo iz primarne zakonodaje EU, zlasti člena 8(3) Listine in člena 16(2) PDEU. „Ustanovitev neodvisnih nadzornih organov […] je torej […] bistveni element spoštovanja varstva oseb pri obdelavi osebnih podatkov.“[492]

SEU je zato odločilo, da mora nacionalni nadzorni organ, če je pri njem vložena pritožba, to pritožbo proučiti s potrebno skrbnostjo tudi v primeru, da prenos osebnih podatkov temelji na odločbi Komisije o primernosti. Nadzorni organ lahko pritožbo zavrne, če ugotovi, da je neutemeljena. SEU je poudarilo, da mora biti v takem primeru posameznikom na podlagi pravice do učinkovitega pravnega sredstva omogočeno, da tako odločbo izpodbijajo pred nacionalnimi sodišči, ki lahko zadevo predložijo SEU v predhodno odločanje o veljavnosti odločbe Komisije. Če nadzorni organ meni, da je pritožba utemeljena, mora imeti možnost sodelovati v sodnih postopkih in zadevo predložiti nacionalnim sodiščem. Nacionalna sodišča lahko zadevo predložijo SEU, saj je to edini organ, ki je pristojen za odločanje o veljavnosti odločbe Komisije o primernosti.[493]

SEU je nato proučilo veljavnost odločbe o varnem pristanu, da bi ugotovilo, ali je sistem prenosov skladen s pravili EU o varstvu osebnih podatkov. Ugotovilo je, da so s členom 3 odločbe o varnem pristanu omejena pooblastila

492 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015, točka 41.

493 Prav tam, točke 53–66.

nacionalnih nadzornih organov (dodeljena v skladu z direktivo o varstvu osebnih podatkov), da sprejmejo ukrepe za preprečevanje prenosa podatkov v primeru neustrezne ravni varstva osebnih podatkov v ZDA. Glede na pomen neodvisnih nadzornih organov pri zagotavljanju skladnosti z zakonodajo o varstvu osebnih podatkov je SEU menilo, da Komisija v skladu z direktivo o varstvu osebnih podatkov in v povezavi z Listino ni imela pristojnosti za tako omejitev pooblastil neodvisnih nadzornih organov. Omejitev pooblastil nadzornih organov je bil eden od razlogov, da je SEU odločbo o varnem pristanu razglasilo za neveljavno.

V skladu z evropskim pravom je torej potreben neodvisen nadzor, ki je pomemben mehanizem za zagotavljanje učinkovitega varstva osebnih podatkov. Neodvisni nadzorni organi so v primeru kršitev zasebnosti prve kontaktne točke za posameznike, na katere se nanašajo osebni podatki.[494] V okviru prava EU in Sveta Evrope je ustanovitev nadzornih organov obvezna. Naloge in pooblastila teh organov so v obeh pravnih okvirih opisani podobno kot naloge in pooblastila iz SUVP. Načeloma bi zato morali nadzorni organi delovati enako po pravu EU in pravu Sveta Evrope.[495]

5.1 Neodvisnost

V skladu s **pravom EU** in **pravom Sveta Evrope** mora vsak nadzorni organ pri opravljanju svojih nalog in izvajanju svojih pooblastil ravnati popolnoma neodvisno.[496] Neodvisnost nadzornega organa, njegovih članov in osebja od neposrednih ali posrednih zunanjih vplivov je temeljnega pomena za zagotavljanje popolne objektivnosti pri odločanju o zadevah v zvezi z varstvom osebnih podatkov. Zakon, ki je podlaga za ustanovitev nadzornega organa, mora vsebovati določbe, s katerimi se izrecno zagotavlja neodvisnost, in ta mora biti tudi izražena v organizacijski strukturi organa. SEU je leta 2010 prvič proučilo vprašanje obsega zahteve po neodvisnosti nadzornih organov za varstvo osebnih podatkov.[497] Izpostavljeni primeri ponazarjajo, kako je SEU opredelilo pomen izraza popolna neodvisnost.

494 SUVP, člen 13(2)(d).

495 Prav tam, člen 51; posodobljena Konvencija št. 108, člen 15.

496 SUVP, člen 52(1); posodobljena Konvencija št. 108, člen 15(5).

497 FRA (2010), *Fundamental rights: challenges and achievements in 2010* (Temeljne pravice: izzivi in dosežki v letu 2010), letno poročilo za leto 2010, str. 59; FRA (2010), *Data protection in the European Union: the role of National Data Protection Authorities* (Varstvo osebnih podatkov v Evropski uniji: vloga nacionalnih organov za varstvo osebnih podatkov), maj 2010.

Primer: Evropska komisija je v zadevi *Evropska komisija proti Zvezni republiki Nemčiji*[498] SEU predlagala, naj ugotovi, da je Nemčija nepravilno prenesla zahtevo po popolni samostojnosti nadzornih organov, odgovornih za zagotavljanje varstva osebnih podatkov, in tako ni izpolnila svojih obveznosti na podlagi člena 28(1) direktive o varstvu osebnih podatkov. Po mnenju Komisije je Nemčija s tem, ko je v različnih zveznih deželah (*Länder*) uvedla državni nadzor nad nadzornimi organi, pristojnimi za nadzorovanje obdelave osebnih podatkov, da bi zagotavljala skladnost z zakonodajo o varstvu osebnih podatkov, ravnala v nasprotju z zahtevo glede neodvisnosti.

SEU je poudarilo, da je treba izraz „popolnoma samostojno" razlagati na podlagi dejanskega besedila zadevne določbe ter ob upoštevanju ciljev in sistematike prava EU o varstvu osebnih podatkov.[499] Poudarilo je, da so nadzorni organi varuhi pravic v zvezi z obdelavo osebnih podatkov. Njihova ustanovitev v državah članicah se zato šteje za „bistven element varstva oseb pri obdelavi osebnih podatkov".[500] EU je ugotovilo, da „morajo nadzorni organi pri izvajanju nalog ravnati objektivno in nepristransko. Zaradi tega ne smejo podleči nobenemu zunanjemu vplivu – niti neposrednim ali posrednim vplivom [javnih organov] […]".[501]

SEU je poleg tega ugotovilo, da je treba pomen izraza „popolna samostojnost" razlagati ob upoštevanju neodvisnosti ENVP, kot je opredeljena v uredbi o varstvu osebnih podatkov v institucijah EU. ENVP v skladu s pojmom neodvisnosti iz te uredbe ne sme nikogar prositi za navodila niti jih od nikogar sprejemati.

SEU je v skladu s tem ugotovilo, da nadzorni organi v Nemčiji zaradi nadzora javnih organov niso popolnoma neodvisni v smislu zakonodaje EU o varstvu osebnih podatkov.

Primer: SEU je v zadevi *Evropska komisija proti Republiki Avstriji*[502] opozorilo na podobne težave v zvezi z neodvisnostjo nekaterih članov in osebja avstrijskega organa za varstvo osebnih podatkov (komisija za varstvo osebnih

498 SEU, *Evropska komisija proti Zvezni republiki Nemčiji* (veliki senat), C-518/07, 9. marec 2010, točka 27.

499 Prav tam, točki 17 in 29.

500 Prav tam, točka 23.

501 Prav tam, točka 25.

502 SEU, *Evropska komisija proti Republiki Avstriji* (veliki senat), C-614/10, 16. oktober 2012, točki 59 in 63.

podatkov). Ugotovilo je, da je dejstvo, da urad zveznega kanclerja nadzornemu organu zagotavlja osebje, v nasprotju z zahtevo glede neodvisnosti iz prava EU o varstvu osebnih podatkov. Poleg tega je menilo, da zahteva, v skladu s katero je treba urad kanclerja vedno obveščati o delu nadzornega organa, onemogoča popolno neodvisnost zadevnega organa.

Primer: v zadevi *Evropska komisija proti Madžarski*[503] so bile prepovedane podobne nacionalne prakse, ki so vplivale na neodvisnost osebja. SEU je poudarilo, da „zahteva [...], v skladu s katero je treba zagotoviti, da vsak nadzorni organ popolnoma samostojno opravlja naloge, ki so mu zaupane, vključuje obveznost zadevne države članice, da spoštuje trajanje mandata takega organa do njegovega prvotno predvidenega izteka". Menilo je tudi, da „Madžarska s tem, da je predčasno prekinila mandat nadzornega organa za varstvo osebnih podatkov, ni izpolnila svojih obveznosti na podlagi Direktive [...] 95/46/ES [...]."

Pojem „popolna neodvisnost" in z njo povezana merila so zdaj izrecno določeni v SUVP, ki vključuje načela, opredeljena na podlagi opisanih sodb SEU. V skladu z navedeno uredbo popolna neodvisnost pri opravljanju nalog in izvajanju pooblastil pomeni, da:[504]

- člani vsakega nadzornega organa ne smejo biti izpostavljeni niti neposrednemu niti posrednemu zunanjemu vplivu in ne smejo od nikogar sprejemati navodil;
- se morajo člani vsakega nadzornega organa vzdržati vsakršnega delovanja, ki je nezdružljivo z njihovimi dolžnostmi, da se prepreči nasprotje interesov;
- morajo države članice vsakemu nadzornemu organu dati na voljo človeške, tehnične in finančne vire ter infrastrukturo za učinkovito opravljanje njegovih nalog;
- morajo države članice zagotoviti, da vsak nadzorni organ izbere svoje osebje;
- finančni nadzor vsakega nadzornega organa, ki se izvaja v skladu z nacionalno zakonodajo, ne sme vplivati na njegovo neodvisnost. Nadzorni organi morajo imeti ločen in javen letni proračun, ki jim omogoča ustrezno delovanje.

503 SEU, *Evropska komisija proti Madžarski* (veliki senat), C-288/12, 8. april 2014, točki 50 in 67.

504 SUVP, člen 52.

Tudi v okviru prava Sveta Evrope se šteje, da je neodvisnost nadzornih organov bistvena zahteva. Nadzorni organi morajo v skladu s posodobljeno Konvencijo št. 108 pri opravljanju svojih nalog in izvajanju svojih pooblastil ravnati popolnoma neodvisno in nepristransko, pri čemer nikogar ne prosijo za navodila niti jih od nikogar ne sprejemajo.[505] V konvenciji je s tem potrjeno, da ti organi ne morejo učinkovito varovati pravic in svoboščin posameznikov, povezanih z obdelavo osebnih podatkov, če svojih nalog ne opravljajo popolnoma neodvisno. V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je opredeljenih več elementov, ki prispevajo k zagotavljanju te neodvisnosti. Med njimi so možnost nadzornih organov, da sami zaposlujejo osebje in sprejemajo odločitve, ne da bi bili izpostavljeni zunanjemu vmešavanju, ter dejavniki v zvezi s trajanjem opravljanja njihovih nalog in pogoji, pod katerimi lahko svoje naloge prenehajo opravljati.[506]

5.2 Pristojnosti in pooblastila

V okviru prava EU so v SUVP opisane pristojnosti in organizacijska struktura nadzornih organov, poleg tega ta uredba določa, da morajo biti ti organi pristojni in pooblaščeni za opravljanje nalog, ki se zahtevajo v skladu z navedeno uredbo.

Nadzorni organ je v nacionalnem pravu glavni organ, ki zagotavlja skladnost z zakonodajo EU o varstvu podatkov. Nadzorni organi imajo poleg spremljanja obsežno vrsto nalog in pooblastil, ki vključujejo proaktivne in preventivne nadzorne dejavnosti. Nadzorni organi morajo imeti za opravljanje teh nalog ustrezna preiskovalna, popravljalna in svetovalna pooblastila, ki so našteta v členih 57 in 58 SUVP, na primer da:[507]

- upravljavcem in posameznikom, na katere se nanašajo osebni podatki, svetujejo o vseh zadevah v zvezi z varstvom osebnih podatkov;
- odobrijo standardna pogodbena določila, zavezujoča poslovna pravila ali upravne dogovore;
- preiskujejo dejanja obdelave in ustrezno ukrepajo;

505 Posodobljena konvencija št. 108, člen 15(5).

506 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108.

507 SUVP, člen 58. Glej tudi Konvencijo št. 108, Dodatni protokol, člen 1.

- zahtevajo predložitev vseh informacij, ki so pomembne za nadzor dejavnosti upravljavca;
- izdajo opozorilo ali opomin upravljavcem in odredijo, da je treba posameznikom, na katere se nanašajo osebni podatki, poslati obvestila o kršitvi varnosti osebnih podatkov;
- odredijo popravek, blokiranje, izbris ali uničenje osebnih podatkov;
- uvedejo začasno ali dokončno prepoved obdelave ali naložijo upravne globe;
- predložijo zadevo sodišču.

Da bi lahko nadzorni organ opravljal svoje naloge, mora imeti dostop do vseh osebnih podatkov in informacij, ki so potrebni za preiskavo, ter dostop do vseh prostorov, v katerih upravljavec hrani zadevne informacije. SEU meni, da je treba pooblastila nadzornega organa razlagati široko, da se zagotovi polna učinkovitost varstva osebnih podatkov za posameznike, na katere se nanašajo osebni podatki, v EU.

Primer: SEU je v zadevi *Schrems* obravnavalo, ali je glede na razkritja Edwarda Snowdna prenos osebnih podatkov v ZDA na podlagi prvega sporazuma med EU in ZDA o varnem pristanu v skladu s pravom EU o varstvu osebnih podatkov. Menilo je, da lahko nacionalni nadzorni organi, ki delujejo kot neodvisni nadzorniki obdelave osebnih podatkov, ki jo izvajajo upravljavci, kljub odločbi o primernosti preprečijo prenos osebnih podatkov v tretjo državo, če so na voljo primerni dokazi, da v tretji državi ni več zagotovljena ustrezna zaščita.[508]

Vsak nadzorni organ je pristojen za izvajanje preiskovalnih pooblastil in pooblastil za ukrepanje na svojem ozemlju. Ker pa so dejavnosti upravljavcev in obdelovalcev pogosto čezmejne ter obdelava osebnih podatkov vpliva na posameznike, na katere se ti nanašajo, v več državah članicah, se pojavlja vprašanje glede delitve pristojnosti med različnimi nadzornimi organi. SEU je to vprašanje proučilo v zadevi *Weltimmo*.

508 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015, točke 26–36 ter 40 in 41.

Primer: SEU je v zadevi *Weltimmo*[509] proučilo pristojnost nacionalnih nadzornih organov za obravnavanje zadev, ki vključujejo organizacije, ki niso ustanovljene v njihovi jurisdikciji. Weltimmo je bila družba, registrirana na Slovaškem, ki je upravljala spletno mesto z oglasi za nepremičnine na Madžarskem. Oglaševalci so pri madžarskem nadzornem organu za varstvo podatkov vložili pritožbo zaradi kršitve madžarskega prava o varstvu osebnih podatkov, zadevni organ pa je družbi Weltimmo naložil globo. Družba je globo izpodbijala pred nacionalnimi sodišči, zadeva pa je bila predložena SEU, da bi to ugotovilo, ali je direktiva EU o varstvu osebnih podatkov nadzornim organom države članice omogočala, da nacionalno pravo o varstvu osebnih podatkov uporabljajo za družbo, registrirano v drugi državi članici.

SEU je člen 4(1)(a) direktive o varstvu osebnih podatkov razlagalo tako, da omogoča uporabo prava o varstvu osebnih podatkov države članice, ki ni država članica, v kateri je registriran upravljavec, „če ta upravljavec prek poslovne enote na ozemlju te države članice opravlja dejansko in resnično, čeprav majhno, dejavnost, v okviru katere se izvaja ta obdelava“. Na podlagi informacij, ki so mu bile predložene, je ugotovilo, da je družba Weltimmo na Madžarskem opravljala dejansko in resnično dejavnost, saj je v zadevni državi imela zastopnika, ki je bil naveden v slovaškem registru družb z naslovom na Madžarskem, ter madžarski bančni račun in poštni nabiralnik, poleg tega je na Madžarskem opravljala tudi dejavnosti v madžarskem jeziku. Iz teh informacij je bil razviden obstoj poslovne enote, zato naj bi za dejavnost družbe Weltimmo veljalo madžarsko pravo o varstvu osebnih podatkov, zanjo pa naj bi bil pristojen madžarski nadzorni organ. Vendar je SEU preverjanje informacij in sprejetje odločitve o tem, ali ima družba Weltimmo dejansko poslovno enoto na Madžarskem, prepustilo nacionalnemu sodišču.

Če bi predložitveno sodišče ugotovilo, da ima družba Weltimmo poslovno enoto na Madžarskem, bi bil madžarski nadzorni organ pooblaščen za naložitev globe. Če pa bi nacionalno sodišče odločilo drugače, tj. da družba Weltimmo na Madžarskem nima poslovne enote, bi se zato uporabljalo pravo države članice ali članic, v katerih je zadevna družba registrirana. Ker je treba v tem primeru pooblastila nadzornih organov izvajati v skladu z ozemeljsko suverenostjo drugih držav članic, madžarski organ ne bi mogel naložiti kazni. Ker pa je direktiva o varstvu osebnih podatkov vključevala obveznost

509 SEU, *Weltimmo s.r.o. proti Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14, 1. oktober 2015.

sodelovanja nadzornih organov, bi lahko madžarski organ od ustreznega slovaškega organa zahteval, naj prouči zadevo, ugotovi kršitev slovaškega prava in naloži kazni, določene s slovaško zakonodajo.

S sprejetjem SUVP so bila vzpostavljena podrobna pravila v zvezi s pristojnostjo nadzornih organov v čezmejnih zadevah. Navedena uredba, s katero je vzpostavljen mehanizem vse na enem mestu, vključuje določbe o obveznem sodelovanju med različnimi nadzornimi organi. Za učinkovito sodelovanje v čezmejnih zadevah je treba v skladu s SUVP določiti, da je vodilni nadzorni organ nadzorni organ sedeža ali edine poslovne enote upravljavca ali obdelovalca.[510] Vodilni nadzorni organ je pristojen za obravnavo čezmejnih zadev, je edini sogovornik upravljavca ali obdelovalca in usklajuje sodelovanje z drugimi nadzornimi organi za dosego soglasja. Sodelovanje vključuje izmenjavo informacij, medsebojno pomoč pri spremljanju in preiskovanju ter sprejemanje zavezujočih odločitev.[511]

V okviru prava Sveta Evrope so pristojnosti in pooblastila nadzornih organov določena v členu 15 posodobljene Konvencije št. 108. Ta pooblastila ustrezajo tistim, ki so nadzornim organom podeljena v skladu s pravom EU, vključno s pooblastili za preiskovanje in ukrepanje, pooblastili za izdajo odločitev in nalaganje upravnih sankcij zaradi kršitev določb konvencije ter pooblastili za sodelovanje v sodnih postopkih. Neodvisni nadzorni organi so pristojni tudi za obravnavanje zahtev in pritožb, ki jih vložijo posamezniki, na katere se nanašajo osebni podatki, ozaveščanje javnosti o pravu varstva osebnih podatkov ter svetovanje nacionalnim nosilcem odločanja v zvezi z vsemi zakonodajnimi ali upravnimi ukrepi, v katerih je predvidena obdelava osebnih podatkov.

5.3 Sodelovanje

V SUVP, s katero je vzpostavljen splošni okvir za sodelovanje med nadzornimi organi, so določena podrobnejša pravila o sodelovanju nadzornih organov pri čezmejnih dejavnostih obdelave osebnih podatkov.

Nadzorni organi v skladu s SUVP zagotavljajo medsebojno pomoč in si izmenjujejo zadevne informacije, da dosledno izvajajo in uporabljajo Uredbo.[512] To vključuje po-

510 SUVP, člen 56(1).

511 Prav tam, člen 60.

512 Prav tam, člen 61(1)–(3) in člen 62(1).

svetovanja, preglede in preiskave, ki jih opravi nadzorni organ, ki prejme zahtevo za pomoč. Nadzorni organi lahko skupaj ukrepajo, tudi z izvajanjem skupnih preiskav in skupnih izvršilnih ukrepov, pri katerih sodeluje osebje vseh nadzornih organov.[513]

Upravljavci in obdelovalci v EU vse bolj delujejo na nadnacionalni ravni. Zato je potrebno tesno sodelovanje med pristojnimi nadzornimi organi v državah članicah za zagotovitev, da je obdelava osebnih podatkov v skladu z zahtevami iz SUVP. V skladu z mehanizmom vse na enem mestu iz zadevne uredbe velja, da če ima upravljavec ali obdelovalec poslovne enote v več državah članicah ali če ima eno poslovno enoto, vendar dejanja obdelave vplivajo na posameznike, na katere se nanašajo osebni podatki, v več državah članicah, je nadzorni organ sedeža (ali edine poslovne enote) vodilni organ v zvezi s čezmejnimi dejavnostmi upravljavca ali obdelovalca. Vodilni organi so pooblaščeni za sprejemanje izvršilnih ukrepov zoper upravljavca ali obdelovalca. Cilj mehanizma vse na enem mestu je izboljšati usklajenost in enotno uporabo prava EU o varstvu osebnih podatkov v državah članicah. Mehanizem je koristen tudi za podjetja, saj se morajo ukvarjati le z vodilnim organom, ne pa z več nadzornimi organi. To krepi pravno varnost za podjetja, poleg tega pa naj bi v praksi pomenilo, da se odločitve sprejemajo hitreje in da podjetjem različni nadzorni organi ne nalagajo izpolnjevanja nasprotujočih si zahtev.

Opredelitev vodilnega organa vključuje določitev lokacije sedeža podjetja v EU. Pojem (glavnega) sedeža je opredeljen v SUVP. Poleg tega je Delovna skupina iz člena 29 izdala smernice za opredelitev vodilnega nadzornega organa upravljavca ali obdelovalca, ki vključujejo merila za opredelitev sedeža. [514]

Da bi se zagotovila visoka raven varstva osebnih podatkov po vsej EU, vodilni nadzorni organ ne deluje samostojno. Pri sprejemanju odločitev o obdelavi osebnih podatkov, ki jo izvajajo upravljavci in obdelovalci, mora sodelovati z drugimi zadevnimi nadzornimi organi, da bi se doseglo soglasje in zagotovila doslednost. Sodelovanje med ustreznimi nadzornimi organi vključuje izmenjavo informacij, medsebojno pomoč ter skupne preiskave in spremljanje.[515] Nadzorni organi morajo pri zagotavljanju medsebojne pomoči drug drugemu natančno obravnavati zahteve za informacije, ki jih predložijo drugi nadzorni organi, in izvajati nadzorne ukrepe, kot so zahteve za predhodna dovoljenja in posvetovanja z upravljavcem osebnih podatkov o njegovih

513 Prav tam, člen 62(1).

514 Delovna skupina za varstvo podatkov iz člena 29 (2016), *Smernice za opredelitev vodilnega nadzornega organa upravljavca ali obdelovalca*, WP 244, Bruselj, sprejete 13. decembra 2016 in revidirane 5. aprila 2017.

515 SUVP, člen 60(1)–(3).

dejavnostih obdelave, preglede ali preiskave. Medsebojno pomoč nadzornim organom v drugih državah članicah je treba na zahtevo zagotoviti brez nepotrebnega odlašanja in najpozneje en mesec po prejemu zahteve.[516]

Kadar ima upravljavec poslovne enote v več državah članicah, lahko nadzorni organi skupaj ukrepajo, vključno z izvajanjem preiskav in izvršilnih ukrepov, pri katerih sodelujejo člani osebja nadzornih organov drugih držav članic.[517]

Sodelovanje med različnimi nadzornimi organi je pomembna zahteva tudi v okviru prava Sveta Evrope. Posodobljena Konvencija št. 108 določa, da morajo nadzorni organi medsebojno sodelovati, če je to potrebno za opravljanje njihovih nalog.[518] Tako bi na primer morali drug drugemu zagotavljati vse ustrezne in koristne informacije, usklajevati preiskave in izvajati skupne ukrepe.[519]

5.4 Evropski odbor za varstvo podatkov

V tem poglavju so bili že opisani pomen neodvisnih nadzornih organov in glavne pristojnosti, ki jih ti imajo na podlagi evropskega prava o varstvu osebnih podatkov. Evropski odbor za varstvo podatkov (EOVP) je še en pomemben akter, ki zagotavlja, da se pravila o varstvu osebnih podatkov po vsej EU uporabljajo učinkovito in dosledno.

S SUVP je bil ustanovljen EOVP kot organ EU, ki je pravna oseba.[520] Je naslednik Delovne skupine iz člena 29,[521] ki je bila vzpostavljena z direktivo o varstvu osebnih podatkov, da bi Komisiji svetovala o vseh ukrepih EU, ki vplivajo na pravice posameznikov v zvezi z obdelavo osebnih podatkov in zasebnostjo, spodbujala enotno uporabo navedene direktive in Komisiji zagotavljala strokovno mnenje o zadevah, povezanih z varstvom osebnih podatkov. Delovno skupino iz člena 29 so poleg predstavnikov Komisije in ENVP sestavljali predstavniki nadzornih organov držav članic EU.

516 Prav tam, člen 61(1) in (2).

517 Prav tam, člen 62(1).

518 Posodobljena konvencija št. 108, člena 16 in 17.

519 Prav tam, člen 17.

520 SUVP, člen 68.

521 V skladu z Direktivo 95/46/ES je Delovna skupina iz člena 29 svetovala Komisiji o vseh ukrepih EU, ki vplivajo na pravice posameznikov v zvezi z obdelavo osebnih podatkov in zasebnostjo, spodbujala enotno uporabo direktive in Komisiji zagotavljala strokovno mnenje o zadevah, povezanih z varstvom osebnih podatkov. Delovno skupino iz člena 29 so skupaj s predstavnikoma Komisije in ENVP sestavljali predstavniki nadzornih organov držav članic EU.

Podobno, kot je veljalo za Delovno skupino iz člena 29, tudi EOVP sestavljajo vodje enega nadzornega organa iz vsake države članice in ENVP ali njihovi predstavniki.[522] ENVP ima enake glasovalne pravice, razen v zadevah, ki se nanašajo na reševanje sporov, pri katerih lahko glasuje samo o odločitvah v zvezi z načeli in pravili, ki se uporabljajo za institucije EU ter po vsebini ustrezajo načelom in pravilom iz SUVP. Komisija ima pravico, da sodeluje pri dejavnostih odbora EOVP in njegovih sestankih, vendar nima glasovalne pravice.[523] Odbor izmed svojih članov z navadno večino izvoli predsednika (ki je pooblaščen, da ga zastopa) in dva namestnika predsednika za petletni mandat. Poleg tega odboru EOVP pomaga tudi sekretariat, ki mu ga ENVP zagotovi za analitično, upravno in logistično podporo.[524]

Naloge EOVP, ki so podrobno opisane v členih 64, 65 in 70 SUVP, vključujejo celovite dolžnosti, ki jih je mogoče razdeliti v naslednje tri glavne dejavnosti.

- **Doslednost:** EOVP lahko izda pravno zavezujočo odločitev v treh primerih: kadar je nadzorni organ dal ustrezen in utemeljen ugovor v zadevah, obravnavanih v okviru mehanizma vse na enem mestu, kadar pride do nasprotujočih si stališč o tem, kateri od zadevnih nadzornih organov je vodilni, in kadar pristojni nadzorni organ ne zaprosi odbora EOVP za mnenje ali njegovega mnenja ne upošteva.[525] Glavna odgovornost odbora EOVP je zagotavljati, da se SUVP dosledno uporablja po vsej EU, njegova vloga je ključna za mehanizem za skladnost, kot je opisano v razdelku 5.5.
- **Svetovanje:** Naloge odbora EOVP vključujejo svetovanje Komisiji o vseh vprašanjih v zvezi z varstvom osebnih podatkov v Uniji, kot so spremembe SUVP, spremembe zakonodaje EU, ki vključujejo obdelavo osebnih podatkov in bi lahko bile v nasprotju s pravili EU o varstvu osebnih podatkov, ter izdaja sklepov Komisije o ustreznosti, ki omogočajo prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo.
- **Izdajanje smernic:** EOVP izdaja tudi smernice, priporočila in najboljše prakse za spodbujanje dosledne uporabe SUVP ter spodbuja sodelovanje in izmenjavo znanja med nadzornimi organi. Poleg tega mora združenja upravljavcev ali obdelovalcev spodbujati k pripravi kodeksov ravnanja ter vzpostavitvi mehanizmov certificiranja in pečatov za varstvo podatkov.

Odločitve odbora EOVP se lahko izpodbijajo pred SEU.

522 SUVP, člen 68(3).

523 Prav tam, člen 68(4) in (5).

524 Prav tam, člena 73 in 75.

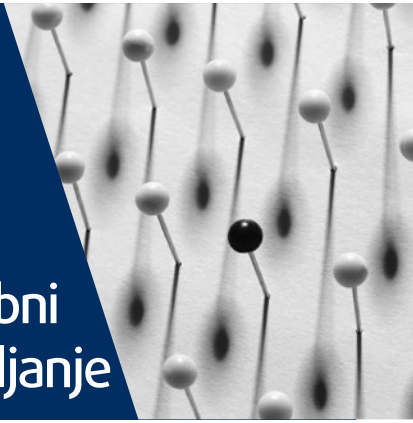
525 Prav tam, člen 65.

5.5 Mehanizem za skladnost iz SUVP

S SUVP je bil vzpostavljen mehanizem za skladnost, katerega cilj je zagotavljati dosledno uporabo te uredbe v vseh državah članicah, pri čemer nadzorni organi sodelujejo med seboj in po potrebi s Komisijo. Mehanizem za skladnost se uporablja v dveh primerih. Prvi se nanaša na mnenja odbora EOVP v primerih, ko pristojni nadzorni organ namerava sprejeti ukrepe, kot je seznam dejanj obdelave, za katera je potrebna ocena učinka v zvezi z varstvom podatkov, ali opredeliti standardna pogodbena določila. Drugi se nanaša na zavezujoče odločitve EOVP za nadzorne organe v zadevah, ki se obravnavajo v okviru mehanizma vse na enem mestu, in primere, ko nadzorni organ ne upošteva mnenja EOVP ali zanj ne zaprosi.

6

Pravice posameznikov, na katere se nanašajo osebni podatki, in njihovo uveljavljanje



EU	Obravnavane teme	Svet Evrope
Pravica do obveščenosti		
SUVP, člen 12 SEU, C-473/12, *Institut professionnel des agents immobiliers (IPI) proti Englebertu*, 2013 SEU, C-201/14, *Smaranda Bara in drugi proti Președintele Casei Naționale de Asigurări de Sănătate in drugim*, 2015	Preglednost informacij	Posodobljena Konvencija št. 108, člen 8
SUVP, člen 13(1) in (2) ter člen 14(1) in (2)	Vsebina informacij	Posodobljena Konvencija št. 108, člen 8(1)
SUVP, člen 13(1) in člen 14(3)	Čas zagotovitve informacij	Posodobljena Konvencija št. 108, člen 9(1)(b)
SUVP, člen 12(1), (5) in (7)	Način zagotovitve informacij	Posodobljena Konvencija št. 108, člen 9(1)(b)
SUVP, člen 13(2)(d), člen 14(2)(e) ter členi 77, 78 in 79	Pravica do vložitve pritožbe	Posodobljena Konvencija št. 108, člen 9(1)(f)
Pravica do dostopa		
SUVP, člen 15(1) SEU, C-553/07, *College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer*, 2009 SEU, združeni zadevi C-141/12 in C-372/12, *YS proti Minister voor Immigratie, Integratie en Asiel in Minister voor Immigratie, Integratie en Asiel proti M in S*, 2014 SEU, C-434/16, *Peter Nowak proti Data Protection Commissioner*, 2017	Pravica do dostopa do svojih osebnih podatkov	Posodobljena Konvencija št. 108, člen 9(1)(b) ESČP, *Leander proti Švedski*, pritožba št. 9248/81, 1987

EU	Obravnavane teme	Svet Evrope
Pravica do popravka		
SUVP, člen 16	**Popravek netočnih osebnih podatkov**	Posodobljena Konvencija št. 108, člen 9(1)(e) ESČP, *Cemalettin Canli proti Turčiji*, pritožba št. 22427/04, 2008 ESČP, *Ciubotaru proti Moldaviji*, pritožba št. 27138/04, 2010
Pravica do izbrisa		
SUVP, člen 17(1)	**Izbris osebnih podatkov**	Posodobljena Konvencija št. 108, člen 9(1)(e) ESČP, *Segerstedt-Wiberg in drugi proti Švedski*, pritožba št. 62332/00, 2006
SEU, C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), 2014 SEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju*, 2017	**Pravica do pozabe**	
Pravica do omejitve obdelave		
SUVP, člen 18(1)	**Pravica do omejitve uporabe osebnih podatkov**	
SUVP, člen 19	**Obveznost obveščanja**	
Pravica do prenosljivosti podatkov		
SUVP, člen 20	**Pravica do prenosljivosti podatkov**	
Pravica do ugovora		
SUVP, člen 21(1) SEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju*, 2017	**Pravica do ugovora zaradi posebnega položaja posameznika, na katerega se nanašajo osebni podatki**	Priporočilo o oblikovanju profilov, člen 5(3) Posodobljena Konvencija št. 108, člen 9(1)(d)

EU	Obravnavane teme	Svet Evrope
SUVP, člen 21(2)	Pravica do ugovora uporabi osebnih podatkov za namene trženja	Priporočilo o neposrednem trženju, člen 4(1)
SUVP, člen 21(5)	Pravica do ugovora z avtomatiziranimi sredstvi	
Pravice v zvezi z avtomatiziranim sprejemanjem odločitev in oblikovanjem profilov		
SUVP, člen 22	Pravice v zvezi z avtomatiziranim sprejemanjem odločitev in oblikovanjem profilov	Posodobljena Konvencija št. 108, člen 9(1)(a)
SUVP, člen 21	Pravice do ugovora avtomatiziranemu sprejemanju odločitev	
SUVP, člen 13(2)(f)	Pravice do smiselne razlage	Posodobljena Konvencija št. 108, člen 9(1)(c)
Pravna sredstva, odgovornost, sankcije in odškodnina		
Listina, člen 47 SEU, C-362/14, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), 2015 SUVP, členi 77–84	Zaradi kršitev nacionalnega prava o varstvu osebnih podatkov	EKČP, člen 13 (samo za države članice Sveta Evrope) Posodobljena Konvencija št. 108, člen 9(1)(f), člena 12 in 15 ter členi 16–21 ESČP, *K. U. proti Finski*, pritožba št. 2872/02, 2008 ESČP, *Biriuk proti Litvi*, pritožba št. 23373/03, 2008
Uredba o varstvu osebnih podatkov v institucijah EU, člena 34 in 49 SEU, C-28/08 P, *Evropska komisija proti The Bavarian Lager Co. Ltd.* (veliki senat), 2010	Zaradi kršitev prava EU, ki so jih storili institucije in organi EU	

Učinkovitost pravnih pravil je na splošno zelo odvisna od obstoja ustreznih mehanizmov za njihovo uveljavljanje, kar velja tudi za pravice posameznikov, na katere se nanašajo osebni podatki. V digitalni dobi je obdelava osebnih podatkov postala splošno razširjena in je posameznikom vse težje razumljiva. Da bi ublažili neravnovesje moči med posamezniki, na katere se nanašajo osebni podatki, in upravljavci,

so posamezniki dobili nekatere pravice za izvajanje večjega nadzora nad obdelavo svojih osebnih podatkov. Pravica dostopa do lastnih osebnih podatkov in pravica do njihovega popravka sta določeni v členu 8(2) Listine EU o temeljnih pravicah, ki je del primarne zakonodaje EU in je temeljnega pomena v pravnem redu EU. S sekundarno zakonodajo EU, zlasti SUVP, je bil vzpostavljen skladen pravni okvir, s katerim so posamezniki, na katere se nanašajo osebni podatki, opolnomočeni, in sicer so jim zagotovljene pravice v zvezi z upravljavci osebnih podatkov. Poleg pravic do dostopa in popravka je s SUVP priznana tudi vrsta drugih pravic, kot so pravica do izbrisa („pravica do pozabe"), pravica do ugovora obdelavi osebnih podatkov ali njene omejitve in pravice v zvezi z avtomatiziranim sprejemanjem odločitev in oblikovanjem profilov. Podobni zaščitni ukrepi, ki posameznikom, na katere se nanašajo osebni podatki, omogočajo izvajanje učinkovitega nadzora nad njihovimi osebnimi podatki, so vključeni tudi v posodobljeno Konvencijo št. 108. V členu 9 so navedene pravice, ki naj bi jih posamezniki lahko uveljavljali v zvezi z obdelavo svojih osebnih podatkov. Pogodbenice morajo zagotoviti, da so te pravice na voljo vsem posameznikom v njihovi pristojnosti, na katere se nanašajo osebni podatki, in sicer skupaj z učinkovitimi pravnimi in praktičnimi sredstvi, ki tem posameznikom omogočajo njihovo uveljavljanje.

Poleg zagotavljanja pravic posameznikom je treba vzpostaviti mehanizme, ki posameznikom, na katere se nanašajo osebni podatki, omogočajo, da se pritožijo zoper kršitve svojih pravic, uveljavljajo odgovornost upravljavcev za te kršitve in zahtevajo odškodnino. Pravica do učinkovitega pravnega sredstva, ki je zagotovljena na podlagi EKČP in Listine, pomeni, da morajo biti vsaki osebi na voljo pravna sredstva.

6.1 Pravice posameznikov, na katere se nanašajo osebni podatki

Ključni poudarki

- Vsak posameznik, na katerega se nanašajo osebni podatki, ima ob upoštevanju omejenih izjem pravico do informacij o vsakršni obdelavi svojih osebnih podatkov, ki jo izvaja upravljavec osebnih podatkov.
- Posamezniki, na katere se nanašajo osebni podatki, imajo pravico, da:
  - dostopajo do svojih podatkov in pridobijo nekatere informacije o obdelavi;

  - upravljavec, ki obdeluje njihove osebne podatke, te podatke popravi, če so netočni;
  - upravljavec po potrebi njihove osebne podatke izbriše, če jih obdeluje nezakonito;
  - začasno omejijo obdelavo;
  - se njihovi osebni podatki pod določenimi pogoji prenesejo na drugega upravljavca.
- Poleg tega imajo posamezniki, na katere se nanašajo osebni podatki, pravico, da ugovarjajo obdelavi:
  - na podlagi razlogov, povezanih s svojim posebnim položajem;
  - svojih osebnih podatkov za namene neposrednega trženja.
- Posamezniki, na katere se nanašajo osebni podatki, imajo pravico, da zanje ne veljajo odločitve, ki temeljijo zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, in ki imajo pravne učinke v zvezi z njimi ali nanje znatno vplivajo. Posamezniki, na katere se nanašajo osebni podatki, imajo tudi pravico:
  - do osebnega posredovanja upravljavca;
  - do izražanja lastnega stališča in izpodbijanja odločitve, ki temelji na avtomatizirani obdelavi.

6.1.1 Pravica do obveščenosti

Upravljavci dejanj obdelave morajo v skladu s **pravom Sveta Evrope** in **pravom EU** posameznika, na katerega se nanašajo osebni podatki, obvestiti o predvideni obdelavi osebnih podatkov v času njihovega zbiranja. Ta obveznost ni odvisna od zahteve posameznika, na katerega se nanašajo osebni podatki, temveč jo mora upravljavec izvajati proaktivno, ne glede na to, ali tak posameznik pokaže zanimanje za take informacije ali ne.

V okviru prava Sveta Evrope morajo pogodbenice v skladu s členom 8 posodobljene Konvencije št. 108 določiti, da upravljavci posameznike, na katere se nanašajo osebni podatki, obvestijo o svoji identiteti in običajnem prebivališču ali poslovni enoti, pravni podlagi in namenu obdelave, vrstah obdelanih osebnih podatkov, uporabnikih njihovih osebnih podatkov (če obstajajo) in tem, kako lahko uveljavljajo svoje pravice po členu 9, vključno s pravicami do dostopa, popravka in pravnega sredstva. Sporočiti bi jim morali tudi vse druge dodatne informacije, za katere menijo, da so potrebne za zagotovitev poštene in pregledne obdelave osebnih podatkov. V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je pojasnjeno, da bi morale biti

informacije, ki se predložijo posameznikom, na katere se nanašajo osebni podatki, zlahka dostopne, čitljive, razumljive in prilagojene zadevnim posameznikom, na katere se nanašajo osebni podatki.[526]

V okviru prava EU bi morala biti v skladu z načelom preglednosti vsaka obdelava osebnih podatkov na splošno pregledna za posameznike. Posamezniki imajo pravico vedeti, kako se zbirajo, uporabljajo ali kako drugače obdelujejo osebni podatki in kateri osebni podatki se zbirajo, uporabljajo ali kako drugače obdelujejo, pa tudi, da so seznanjeni s tveganji, zaščitnimi ukrepi in svojimi pravicami v zvezi z obdelavo.[527] S členom 12 SUVP je tako določena splošna celovita obveznost za upravljavce, da posameznikom, na katere se nanašajo osebni podatki, zagotovijo pregledne informacije in/ali jim sporočijo, kako lahko uveljavljajo svoje pravice.[528] Informacije morajo biti jedrnate, pregledne, razumljive in zlahka dostopne ter izražene v jasnem in preprostem jeziku. Predložiti jih je treba v pisni obliki, med drugim z elektronskimi sredstvi, kadar je to ustrezno, pri čemer se lahko na zahtevo posameznika, na katerega se nanašajo osebni podatki, predložijo tudi ustno, če se njegova identiteta nedvoumno dokaže. Informacije se zagotovijo brez večjih zamud ali stroškov.[529]

V členu 13 SUVP je obravnavana pravica posameznikov, na katere se nanašajo osebni podatki, do obveščenosti v primerih, ko so bili osebni podatki pridobljeni neposredno od njih, v členu 14 pa v primerih, ko osebni podatki niso bili pridobljeni od njih.

Obseg pravice do obveščenosti in njene omejitve v skladu s pravom EU so bili pojasnjeni v sodni praksi SEU.

Primer: SEU je bilo v zadevi *Institut professionnel des agents immobiliers (IPI) proti Englebertu*[530] zaprošeno za razlago člena 13(1) Direktive 95/46/ES. V skladu s tem členom so imele države članice možnost, da sprejmejo zakonodajne ukrepe za omejitev obsega pravice posameznika, na katerega se nanašajo osebni podatki, do obveščenosti, kadar je to potrebno za zaščito pravic in svoboščin drugih ter za preprečevanje in preiskovanje kaznivih dejanj ali kršitev etike za regulirane poklice. IPI je belgijsko strokovno združenje

526 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 68.

527 SUVP, uvodna izjava 39.

528 Prav tam, člena 13 in 14; posodobljena Konvencija št. 108, člen 8(1)(b).

529 SUVP, člen 12(5); posodobljena Konvencija št. 108, člen 9(1)(b).

530 SEU, *Institut professionnel des agents immobiliers (IPI) proti Geoffreyju Englebertu in drugim*, C-473/12, 7. november 2013.

nepremičninskih posrednikov, ki je odgovorno za nadzor ustreznega opravljanja poklica nepremičninskega posrednika. Nacionalnemu sodišču je predlagalo, naj ugotovi, da so tožene stranke kršile poklicna pravila, in jim naloži opustitev različnih nepremičninskih dejavnosti. Tožba je temeljila na dokazih, ki so jih zbrali zasebni detektivi, ki jih je najelo združenje IPI.

Nacionalno sodišče je dvomilo o vrednosti dokazov, ki so jih zbrali zasebni detektivi, ob upoštevanju možnosti, da so bili zbrani brez spoštovanja zahtev belgijske zakonodaje o varstvu osebnih podatkov, zlasti obveznosti, da se posameznike, na katere se nanašajo osebni podatki, obvesti o obdelavi njihovih osebnih podatkov, preden se ti podatki začnejo zbirati. SEU je opozorilo, da člen 13(1) Direktive 95/46/ES določa, da države članice lahko v svoji nacionalni zakonodaji določijo izjeme od obveznosti obvestitve posameznikov, na katere se nanašajo osebni podatki, o obdelavi njihovih osebnih podatkov, da pa k temu niso zavezane. Ker so v členu 13(1) med razlogi, na podlagi katerih lahko države članice omejijo pravico posameznikov, navedeni preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ali kršitev etike, bi dejavnost organa, kot je združenje IPI, in zasebnih detektivov, ki so delovali v njegovem imenu, lahko spadala na področje uporabe navedenega člena. Če pa država članica take izjeme ni določila, je posameznike, na katere se nanašajo osebni podatki, treba obvestiti.

Primer: SEU je v zadevi *Smaranda Bara in drugi proti Președintele Casei Naționale de Asigurări de Sănătate in drugim*[531] pojasnilo, ali pravo EU nacionalnemu javnemu upravnemu organu preprečuje prenos osebnih podatkov drugemu javnemu upravnemu organu v naknadno obdelavo, če posamezniki, na katere se nanašajo osebni podatki, o tem prenosu in obdelavi niso obveščeni. V navedeni zadevi nacionalna agencija davčne uprave pred prenosom ni obvestila tožečih strank, da je njihove osebne podatke posredovala nacionalnemu zavodu za zdravstveno zavarovanje.

SEU je menilo, da je zahteva, določena s pravom EU, po obvestitvi posameznika, na katerega se nanašajo osebni podatki, o obdelavi njegovih osebnih podatkov „še toliko pomembnejša, ker je ta zahteva pogoj za to, da lahko ti posamezniki izvajajo pravico dostopa do obdelanih podatkov in popravka teh podatkov […] in pravico ugovora zoper obdelavo navedenih podatkov“.

531 SEU, *Smaranda Bara in drugi proti Președintele Casei Naționale de Asigurări de Sănătate in drugim*, C-201/14, 1. oktober 2015.

V skladu z načelom poštene obdelave je treba posameznike, na katere se nanašajo osebni podatki, obvestiti o prenosu njihovih podatkov drugemu javnemu organu, ki jih nadalje obdeluje. Države članice lahko v skladu s členom 13(1) Direktive 95/46/ES omejijo pravico do obveščenosti, če se šteje, da je to potrebno za zaščito pomembnega gospodarskega interesa države, vključno z davčnimi zadevami. Vendar je treba take omejitve sprejeti z zakonodajnimi ukrepi. Ker opredelitev podatkov, ki naj bi se prenesli, ter podrobnosti glede izvedbe prenosa niso bile določene z zakonodajnim ukrepom, ampak le s protokolom, ki je bil sklenjen med zadevnima javnima organoma, pogoji za odstopanje po pravu EU niso bili izpolnjeni. Tožeče stranke bi morale biti vnaprej obveščene o prenosu njihovih osebnih podatkov nacionalnemu zavodu za zdravstveno zavarovanje in njihovi naknadni obdelavi, ki jo je izvedel ta organ.

Vsebina informacij

Upravljavec mora v skladu s členom 8(1) posodobljene Konvencije št. 108 posameznику, na katerega se nanašajo osebni podatki, predložiti vse informacije, ki zagotavljajo pošteno in pregledno obdelavo osebnih podatkov, vključno z:

- identiteto upravljavca in njegovim običajnim prebivališčem ali sedežem;
- pravno podlago in nameni predvidene obdelave;
- kategorijami osebnih podatkov, ki se obdelujejo;
- uporabniki ali kategorijami uporabnikov osebnih podatkov, če obstajajo;
- načini, kako lahko posamezniki, na katere se nanašajo osebni podatki, uveljavljajo svoje pravice.

Kadar se v skladu s SUVP od posameznika, na katerega se nanašajo osebni podatki, pridobijo njegovi osebni podatki, mora upravljavec zadevnemu posamezniku takrat, ko pridobi osebne podatke, zagotoviti naslednje informacije:[532]

- identiteto in kontaktne podatke upravljavca, vključno s podatki pooblaščene osebe za varstvo podatkov, kadar ta obstaja;

532 SUVP, člen 13(1).

- namen in pravno podlago za obdelavo, tj. pogodbo ali pravno obveznost;
- zakoniti interes upravljavca osebnih podatkov, kadar je ta podlaga za obdelavo;
- morebitne uporabnike ali kategorije uporabnikov osebnih podatkov;
- ali bodo osebni podatki preneseni v tretjo državo ali mednarodno organizacijo ter ali prenos temelji na sklepu o ustreznosti ali na ustreznih zaščitnih ukrepih;
- obdobje hrambe osebnih podatkov ali, če navedenega obdobja ni mogoče opredeliti, merila, ki se uporabijo za določitev obdobja hrambe osebnih podatkov;
- pravice posameznikov, na katere se nanašajo osebni podatki, v zvezi z obdelavo, kot so pravice do dostopa, popravka in izbrisa osebnih podatkov ter pravica do omejitve obdelave ali ugovora obdelavi;
- ali je zagotovitev osebnih podatkov določena z zakonom ali pogodbo, ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke ter kakšne so posledice, če se podatki ne zagotovijo;
- obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov;
- pravico do vložitve pritožbe pri nadzornem organu;
- obstoj pravice do preklica privolitve.

V primeru avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, morajo uporabniki, na katere se nanašajo osebni podatki, prejeti smiselne informacije o razlogih za oblikovanje profilov, njegovem pomenu in predvidenih posledicah, ki jih ima obdelava zanje.

V primerih, ko se osebni podatki ne pridobijo neposredno od posameznika, na katerega se nanašajo, mora upravljavec osebnih podatkov zadevnega posameznika uradno obvestiti o izvoru osebnih podatkov. Upravljavec mora v vsakem primeru med drugim posameznike, na katere se nanašajo osebni podatki, obvestiti o obstoju avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov.[533] Če upravljavec namerava obdelovati osebne podatke za namen, ki ni namen, ki je bil prvotno sporočen posamezniku, na katerega se nanašajo osebni podatki, mora v skladu z načeloma omejitve namena in preglednosti zadevnemu posamezniku zagotoviti

533 SUVP, člen 13(2) in člen 14(2)(g).

informacije o tem novem namenu. Upravljavci morajo pred vsako nadaljnjo obdelavo zagotoviti informacije o njej. Z drugimi besedami, če je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo osebnih podatkov, mora upravljavec od njega pridobiti novo privolitev, če se namen obdelave spremeni ali če se dodajo novi nameni.

Čas zagotovitve informacij

V SUVP se razlikuje med dvema položajema in dvema trenutkoma, v katerih mora upravljavec osebnih podatkov zagotoviti informacije posamezniku, na katerega se nanašajo osebni podatki.

- Kadar se osebni podatki pridobijo neposredno od posameznika, na katerega se nanašajo, mora upravljavec zadevnemu posamezniku takrat, ko pridobi njegove osebne podatke, zagotoviti vse ustrezne informacije in ga obvestiti o njegovih pravicah v skladu s SUVP.[534] Če namerava upravljavec nadalje obdelovati osebne podatke za drugačen namen, pred obdelavo posamezniku, na katerega se nanašajo, zagotovi vse ustrezne informacije.

- Če osebni podatki niso bili pridobljeni neposredno od posameznika, na katerega se nanašajo, mora upravljavec zadevnemu posamezniku informacije o obdelavi zagotoviti „v razumnem roku po prejemu osebnih podatkov, vendar najpozneje v enem mesecu“, ali preden se podatki razkrijejo tretji osebi.[535]

V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je določeno, da če posameznikov, na katere se nanašajo osebni podatki, ob začetku obdelave ni mogoče obvestiti, jih je o tem dopustno obvestiti pozneje, na primer ko upravljavec iz katerega koli razloga vzpostavi stik s posameznikom, na katerega se nanašajo osebni podatki.[536]

Različni načini zagotavljanja informacij

Informacije, ki jih mora upravljavec v skladu s pravom Sveta Evrope in pravom EU zagotoviti posameznikom, na katere se nanašajo osebni podatki, morajo biti jedrnate,

534 Prav tam, člen 13(1) in (2), uvodno besedilo, v katerem je navedeno, da je treba informacije zagotoviti „takrat, ko [upravljavec] pridobi osebne podatke“.

535 Prav tam, člen 13(3) in člen 14(3); glej tudi posodobljeno Konvencijo št. 108, člen 8(1)(b), v katerem je navedeno, da posameznik pridobi informacije v razumnih časovnih presledkih in brez večjih zamud.

536 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 70.

pregledne, razumljive in zlahka dostopne. Informacije morajo biti predložene v pisni obliki ali kako drugače, med drugim z elektronskimi sredstvi, ter izražene v jasnem, preprostem in zlahka razumljivem jeziku. Upravljavec lahko pri zagotavljanju informacij uporablja standardizirane ikone, da informacije predloži v jasno razvidni in razumljivi obliki.[537] Tako bi se na primer lahko z ikono ključavnice sporočalo, da se podatki varno zbirajo in/ali šifrirajo. Posamezniki, na katere se nanašajo osebni podatki, lahko zahtevajo, da se jim informacije predložijo ustno. Informacije morajo biti brezplačne, razen če so zahteve posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljene ali pretirane (tj. se ponavljajo).[538] Preprost dostop do zagotovljenih informacij je ključen, da lahko posameznik, na katerega se nanašajo osebni podatki, uveljavlja svoje pravice, ki jih ima v skladu s pravom EU o varstvu osebnih podatkov.

V skladu z načelom poštene obdelave morajo biti informacije zlahka razumljive posameznikom, na katere se nanašajo osebni podatki. Uporabiti je treba jezik, ki je primeren za naslovnike. Raven in vrsto jezika je treba prilagoditi glede na to, ali so ciljna javnost na primer odrasli ali otroci, splošna javnost ali akademski strokovnjaki. Kako uravnotežiti ta vidik razumljivosti informacij, je obravnavano v mnenju Delovne skupine iz člena 29 o bolj usklajenih določbah v zvezi z dajanjem informacij. Delovna skupina v njem zagovarja t. i. večdelna obvestila[539], ki posamezniku, na katerega se nanašajo osebni podatki, omogočajo, da sam izbere raven podrobnosti. Vendar ta način zagotavljanja informacij upravljavca ne odvezuje obveznosti, ki jih ima v skladu s členoma 13 in 14 SUVP. Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, še vedno zagotoviti vse informacije.

Eden od najučinkovitejših načinov za zagotavljanje informacij so ustrezna obvestila na domači strani upravljavca, na primer politika varstva zasebnosti na spletišču. Ker pa precejšen delež prebivalstva ne uporablja interneta, bi morala podjetja ali javni organi to upoštevati pri svoji politiki obveščanja.

537 Evropska komisija bo z delegiranimi akti podrobneje določila informacije, ki se navedejo v standardiziranih ikonah, in postopke za določitev standardiziranih ikon; glej SUVP, člen 12(8).

538 SUVP, člen 12(1), (5) in (7); posodobljena Konvencija št. 108, člen 9(1)(b).

539 Delovna skupina za varstvo podatkov iz člena 29 (2004), *Mnenje 10/2004 o bolj usklajenih določbah v zvezi z dajanjem informacij*, WP 100, Bruselj, 25. november 2004.

Primer izjave o varstvu osebnih podatkov pri njihovi obdelavi na spletni strani:

Kdo smo?

Upravljavec obdelave osebnih podatkov je gostišče C&U s sedežem v [naslov: xxx], tel. št.: xxx, št. telefaksa: xxx, e-naslov info@c&u.com, kontaktni podatki pooblaščene osebe za varstvo podatkov: [xxx].

Informativno obvestilo v zvezi z osebnimi podatki je del pogojev, ki urejajo zagotavljanje hotelskih storitev.

Katere osebne podatke pridobimo od vas?

Od vas pridobimo naslednje osebne podatke: vaše ime, poštni naslov, telefonsko številko, elektronski naslov, informacije o obisku, številko kreditne in debetne kartice ter IP-naslove ali domenska imena računalnikov, ki ste jih uporabili za povezavo na naše spletišče.

Zakaj zbiramo vaše osebne podatke?

Vaše osebne podatke obdelujemo na podlagi vaše privolitve, in sicer za izvedbo rezervacij, sklepanje in izpolnjevanje pogodb v zvezi s storitvami, ki vam jih ponujamo, ter izpolnjevanje zahtev, ki jih nalaga zakonodaja, na primer zakon o lokalnih pristojbinah, v skladu s katerim moramo zbirati osebne podatke za plačilo mestne turistične takse.

Kako obdelujemo vaše osebne podatke?

Vaši osebni podatki se hranijo tri mesece. V zvezi z njimi se ne uporabljajo postopki za avtomatizirano sprejemanje odločitev.

Gostišče C&U upošteva stroge varnostne postopke za zagotavljanje, da se vaši osebni podatki ne poškodujejo, uničijo ali razkrijejo tretji osebi brez vašega dovoljenja, in za preprečevanje nepooblaščenega dostopa. Računalniki, na katerih se hranijo informacije, so v varnem okolju z omejenim fizičnim dostopom. Uporabljamo varne požarne zidove in druge ukrepe za omejitev elektronskega dostopa. Če je treba osebne podatke prenesti tretji osebi, mora ta imeti vzpostavljene podobne ukrepe za varstvo vaših osebnih podatkov.

Vsi podatki, ki jih zbiramo ali evidentiramo, so omejeni na naše pisarne. Dostop do osebnih podatkov imajo le osebe, ki informacije potrebujejo za izpolnjevanje svojih dolžnosti po tej pogodbi. Ko bomo potrebovali informacije za vašo identifikacijo, vas bomo zanje izrecno prosili. Preden vam razkrijemo informacije, lahko od vas zahtevamo, da opravite naše varnostno preverjanje. Svoje osebne podatke, ki nam jih posredujete, lahko kadar koli posodobite tako, da se neposredno obrnete na nas.

Kakšne pravice imate?

Pravico imate, da dostopate do svojih osebnih podatkov, pridobite kopijo svojih osebnih podatkov, zahtevate njihov izbris ali popravek oziroma zahtevate prenos svojih osebnih podatkov k drugemu upravljavcu.

S svojimi zahtevami se lahko na nas obrnete na spletnem naslovu: info@c&u.com. Na vašo zahtevo moramo odgovoriti v enem mesecu, če pa je vaša zahteva preveč zapletena ali če prejmemo preveč drugih zahtev, vas bomo obvestili, da se lahko to obdobje podaljša za nadaljnja dva meseca.

Dostop do vaših osebnih podatkov

Pravico imate, da dostopate do svojih osebnih podatkov, da se na zahtevo seznanite z razlogi, na katerih temelji obdelava osebnih podatkov, da zahtevate njihov izbris ali popravek in da za vas ne velja odločitev, ki je bila sprejeta povsem avtomatizirano, ne da bi bila upoštevana vaša stališča. S svojimi zahtevami se lahko na nas obrnete na spletnem naslovu: info@c&u.com. Imate tudi pravico, da nasprotujete obdelavi, prekličete svojo privolitev in vložite pritožbo pri nacionalnem nadzornem organu, če menite, da je ta obdelava osebnih podatkov v nasprotju z zakonodajo, in zahtevate odškodnino za škodo, ki ste jo utrpeli zaradi nezakonite obdelave.

Pravica do vložitve pritožbe

Upravljavec mora v skladu s SUVP posameznike, na katere se nanašajo osebni podatki, obvestiti o mehanizmih uveljavljanja, ki so v skladu z nacionalnim pravom in pravom EU na voljo za primere kršitev varnosti osebnih podatkov. Upravljavec mora posameznike, na katere se nanašajo osebni podatki, obvestiti o njihovi pravici, da vložijo pritožbo o kršitvi varnosti osebnih podatkov pri nadzornem organu in po

potrebi pri nacionalnem sodišču.[540] V pravu Sveta Evrope je določena tudi pravica posameznikov, na katere se nanašajo osebni podatki, do obveščenosti o načinih uveljavljanja svojih pravic, vključno s pravico do pravnega sredstva, določeno v členu 9(1)(f).

Izjeme od obveznosti obveščanja

V SUVP je določena izjema od obveznosti obveščanja. V skladu s členom 13(4) in členom 14(5) SUVP se obveznost obveščanja posameznikov, na katere se nanašajo osebni podatki, ne uporablja, če posameznik, na katerega se nanašajo osebni podatki, že ima vse ustrezne informacije.[541] Poleg tega se, kadar osebni podatki niso bili pridobljeni od posameznika, obveznost obveščanja ne uporablja, če je zagotavljanje informacij nemogoče ali nesorazmerno, zlasti če se osebni podatki obdelujejo v namene arhiviranja v javnem interesu, v znanstveno- ali zgodovinskoraziskovalne namene oziroma v statistične namene.[542]

Države članice imajo poleg tega v skladu s SUVP diskrecijsko pravico, da omejijo obveznosti in pravice, ki so v skladu z navedeno uredbo zagotovljene posameznikom, če je to potreben in sorazmeren ukrep v demokratični družbi, na primer za zaščito državne in javne varnosti, obrambo, varstvo sodnih preiskav in postopkov ali zaščito gospodarskih in finančnih interesov ter zasebnih interesov, ki so pomembnejši od interesov varstva osebnih podatkov.[543]

Vse izjeme ali omejitve morajo biti nujne v demokratični družbi in sorazmerne z zastavljenim ciljem. V zares izjemnih primerih, na primer zaradi zdravstvenih indikacij, je lahko omejitev preglednosti potrebna za samo varstvo posameznika, na katerega se nanašajo osebni podatki; ta omejitev se nanaša zlasti na omejitev pravice dostopa vsakega posameznika, na katerega se nanašajo osebni podatki.[544] Za zagotavljanje minimalne ravni varstva pa je treba v nacionalnemu pravu spoštovati bistvo temeljnih pravic in svoboščin, varovanih s pravom EU.[545] Zato mora nacionalno pravo vse-

540 SUVP, člen 13(2)(d) in člen 14(2)(e); posodobljena Konvencija št. 108, člen 8(1)(f).

541 Prav tam, člen 13(4) in člen 14(5)(a).

542 Prav tam, člen 14(5)(b)–(e).

543 SUVP, člen 23(1).

544 SUVP, člen 15.

545 SUVP, člen 23(1).

bovati posebne določbe, s katerimi so pojasnjeni namen obdelave, vključene vrste osebnih podatkov, zaščitni ukrepi in druge postopkovne zahteve.[546]

Kadar se podatki zbirajo v znanstveno- ali zgodovinskoraziskovalne namene, statistične namene ali namene arhiviranja v javnem interesu, se lahko v pravu Unije ali pravu držav članic določijo odstopanja od obveznosti obveščanja, če je verjetno, da bi takšna obveznost onemogočila ali resno ovirala doseganje posebnih namenov.[547]

Podobne omejitve obstajajo v pravu Sveta Evrope, v skladu s katerim lahko za pravice, ki so posameznikom, na katere se nanašajo osebni podatki, dodeljene na podlagi člena 9 posodobljene Konvencije št. 108, pod strogimi pogoji veljajo morebitne omejitve v skladu s členom 11 posodobljene Konvencije št. 108. Poleg tega se v skladu s členom 8(2) posodobljene Konvencije št. 108 obveznost preglednosti obdelave, ki je naložena upravljavcem, ne uporablja, če posameznik, na katerega se nanašajo osebni podatki, informacije že ima.

Pravica do dostopa do lastnih osebnih podatkov

Po pravu Sveta Evrope je pravica do dostopa do lastnih osebnih podatkov izrecno priznana v členu 9 posodobljene Konvencije št. 108. Ta določa, da ima vsak posameznik pravico, da na zahtevo pridobi informacije o obdelavi osebnih podatkov, ki se nanašajo nanj, pri čemer se te informacije sporočijo na razumljiv način. Pravica dostopa je priznana ne le v določbah posodobljene Konvencije št. 108, temveč tudi v sodni praksi ESČP. ESČP je večkrat odločilo, da imajo posamezniki pravico, da dostopajo do informacij o svojih osebnih podatkih, in da ta pravica izhaja iz potrebe po spoštovanju zasebnega življenja.[548] Vendar je pravico do dostopa do osebnih podatkov, ki jih hranijo javne ali zasebne organizacije, v nekaterih okoliščinah mogoče omejiti.[549]

V pravu EU je pravica do dostopa do svojih osebnih podatkov izrecno priznana v členu 15 SUVP, poleg tega je kot element temeljne pravice do varstva osebnih

546 Prav tam, člen 23(2).

547 Prav tam, člen 89(2) in (3).

548 ESČP, *Gaskin proti Združenemu kraljestvu*, pritožba št. 10454/83, 7. julij 1989; ESČP, *Odièvre proti Franciji* (veliki senat), pritožba št. 42326/98, 13. februar 2003; ESČP, *K. H. in drugi proti Slovaški*, pritožba št. 32881/04, 28. april 2009, in ESČP, *Godelli proti Italiji*, pritožba št. 33783/09, 25. september 2012.

549 ESČP, *Leander proti Švedski*, pritožba št. 9248/81, 26. marec 1987.

podatkov določena tudi v členu 8(2) Listine EU o temeljnih pravicah.[550] Pravica posameznika do dostopa do svojih osebnih podatkov je ključni element evropskega prava o varstvu osebnih podatkov.[551]

V SUVP je določeno, da ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico do dostopa do svojih osebnih podatkov in nekaterih informacij o obdelavi, ki jih morajo zagotoviti upravljavci.[552] Zlasti ima zadevni posameznik pravico, da (od upravljavca) dobi potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in informacije vsaj o naslednjem:

- namenih obdelave;
- vrstah zadevnih osebnih podatkov;
- uporabnikih ali kategorijah uporabnikov, ki so jim razkriti osebni podatki;
- predvidenem obdobju hrambe osebnih podatkov ali, če to ni mogoče, o merilih, ki se uporabijo za določitev tega obdobja;
- obstoju pravice do popravka ali izbrisa osebnih podatkov ali do omejitve obdelave osebnih podatkov;
- pravici do vložitve pritožbe pri nadzornem organu;
- vse razpoložljive informacije v zvezi z virom osebnih podatkov, ki se obdelujejo, če osebni podatki niso zbrani pri posamezniku, na katerega se nanašajo;
- v primeru avtomatiziranih odločitev o razlogih za avtomatizirano obdelavo osebnih podatkov.

Upravljavec osebnih podatkov mora posamezniku, na katerega se nanašajo osebni podatki, zagotoviti kopijo osebnih podatkov, ki se obdelujejo. Vse informacije, ki se

550 Glej tudi SEU, *YS proti Minister voor Immigratie, Integratie en Asiel* in *Minister voor Immigratie, Integratie en Asiel proti M in S*, združeni zadevi C-141/12 in C-372/12, 17. julij 2014, in SEU, *ClientEarth, Pesticide Action Network Europe (PAN Europe) proti Evropski agenciji za varno hrano in Evropski komisiji*, C-615/13 P, 16 .julij 2015.

551 SEU, *YS proti Minister voor Immigratie, Integratie en Asiel* in *Minister voor Immigratie, Integratie en Asiel proti M in S*, združeni zadevi C-141/12 in C-372/12, 17. julij 2014.

552 SUVP, člen 15(1).

sporočijo posamezniku, na katerega se nanašajo osebni podatki, je treba predložiti v razumljivi obliki, kar pomeni, da mora upravljavec zagotoviti, da lahko zadevni posameznik razume informacije, ki so mu predložene. Tako na primer ni dovolj, da se v odgovor na zahtevo za dostop vključijo tehnične okrajšave, kodirani izrazi ali kratice, razen če je pojasnjen njihov pomen. Če se izvaja avtomatizirano sprejemanje odločitev, vključno z oblikovanjem profilov, je treba pojasniti splošne razloge za avtomatizirano sprejemanje odločitev, vključno z merili, ki se upoštevajo pri ocenjevanju posameznika, na katerega se nanašajo osebni podatki. Podobne zahteve obstajajo v okviru **prava Sveta Evrope**.[553]

Primer: posameznik, na katerega se nanašajo osebni podatki, lahko z dostopom do svojih osebnih podatkov ugotovi, ali so podatki točni ali ne. Zato je bistveno, da je posameznik, na katerega se nanašajo osebni podatki, na razumljiv način obveščen ne le o dejanskih osebnih podatkih, ki se obdelujejo, temveč tudi o kategorijah, v okviru katerih se ti osebni podatki obdelujejo, kot so ime, IP-naslov, geolokacijske koordinate, številka kreditne kartice itd.

V odgovoru na zahtevo za dostop je treba navesti informacije o viru podatkov, kadar se osebni podatki ne pridobijo od posameznika, na katerega se nanašajo, če so te informacije na voljo. To določbo je treba razumeti v okviru načel poštenosti, preglednosti in odgovornosti. Upravljavec ne sme uničiti informacij o viru podatkov, zato da mu jih ne bi bilo treba razkriti – razen če bi bile informacije izbrisane kljub prejeti zahtevi za dostop –, in mora še vedno izpolnjevati splošne zahteve glede odgovornosti.

Kot je določeno v sodni praksi SEU, za pravico do dostopa do osebnih podatkov ne smejo neupravičeno veljati časovne omejitve. Posameznikom, na katere se nanašajo osebni podatki, je poleg tega treba razumno omogočiti, da dobijo informacije o preteklih dejanjih obdelave osebnih podatkov.

Primer: SEU je bilo v zadevi *Rijkeboer*[554] zaprošeno, naj ugotovi, ali je lahko posameznikova pravica do dostopa do informacij o uporabnikih ali vrstah uporabnikov osebnih podatkov in o vsebini podatkov omejena na leto pred vložitvijo njegove zahteve za dostop.

553 Glej posodobljeno Konvencijo št. 108, člen 8(1)(c).

554 SEU, *College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer*, C-553/07, 7. maj 2009.

SEU je odločilo, da je treba za določitev, ali je v skladu z zakonodajo EU takšna časovna omejitev dovoljena, člen 12 razlagati glede na namene Direktive 95/46/ES. Najprej je navedlo, da je pravica do dostopa potrebna, da se posamezniku, na katerega se nanašajo osebni podatki, omogoči uveljavljanje pravice, da upravljavec podatke popravi, izbriše ali blokira, ali da tretje osebe, ki so jim bili osebni podatki posredovani, uradno obvesti o teh popravkih, izbrisu ali blokiranju. Učinkovita pravica do dostopa je poleg tega potrebna, da se posamezniku, na katerega se nanašajo osebni podatki, omogoči uveljavljanje njegove pravice, da ugovarja obdelavi svojih osebnih podatkov, ali pravice, da vloži pritožbo in zahteva odškodnino.[555]

Da bi se zagotovil polni učinek pravic, ki jih imajo posamezniki, na katere se nanašajo osebni podatki, je SEU ugotovilo, „da mora ta pravica nujno zadevati preteklost […]. V nasprotnem primeru zainteresirana oseba ne bi mogla učinkovito uveljavljati svoje pravice doseči popravo, izbris ali blokiranje podatkov, ki naj bi bili nezakoniti ali nepravilni, ter pravice vložiti pravno sredstvo pri sodišču in doseči povrnitev nastale škode."

6.1.2 Pravica do popravka

Posamezniki, na katere se nanašajo osebni podatki, imajo v skladu s **pravom EU** in **pravom Sveta Evrope** pravico do popravka svojih osebnih podatkov. Točnost osebnih podatkov je bistvena za zagotavljanje visoke ravni varstva osebnih podatkov za posameznike, na katere se nanašajo.[556]

Primer: v zadevi *Ciubotaru proti Moldaviji*[557] je bilo pritožniku onemogočeno, da bi vpis svojega etničnega porekla v uradnih evidencah spremenil iz moldavijskega v romunskega, domnevno zato, ker svoje zahteve ni utemeljil. Po mnenju ESČP je dopustno, da države ob vpisu posameznikove narodnostne identitete zahtevajo objektivne dokaze. Če taka zahteva temelji na popolnoma subjektivnih in neutemeljenih razlogih, jo lahko organi zavrnejo. Vendar pritožnikova zahteva ni temeljila samo na subjektivnem dojemanju lastne narodnosti; predložil je objektivno preverljive povezave z romunsko etnično skupino, kot so jezik, ime, empatija in druge. Kljub temu je moral v skladu

555 SUVP, člen 15(1)(c) in (f), člen 16, člen 17(2) in člen 21 ter poglavje VIII.

556 Prav tam, člen 16 in uvodna izjava 65; posodobljena Konvencija št. 108, člen 9(1)(e).

557 ESČP, *Ciubotaru proti Moldaviji*, pritožba št. 27138/04, 27. april 2010, točki 51 in 59.

z nacionalno zakonodajo predložiti dokaze, da so bili njegovi starši pripadniki romunske etnične skupine. Taka zahteva je glede na zgodovino Moldavije ustvarila nepremostljivo oviro za vpis druge narodnostne identitete, kot so jo v zvezi z njegovimi starši evidentirali sovjetski organi. S tem ko je država pritožniku preprečila, da bi se njegova zahteva proučila ob upoštevanju objektivno preverljivih dokazov, ni izpolnila svoje pozitivne obveznosti, da pritožniku zagotovi učinkovito spoštovanje zasebnega življenja. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Včasih zadostuje, da posameznik, na katerega se nanašajo osebni podatki, preprosto zahteva na primer popravek imena, spremembo naslova ali telefonske številke. V skladu s **pravom EU** in **pravom Sveta Evrope** je treba netočne osebne podatke popraviti brez nepotrebnega ali pretiranega odlašanja.[558] Če pa so taki zahtevki povezani s pravno pomembnimi zadevami, na primer pravnim statusom osebe, na katero se nanašajo osebni podatki, ali točnim naslovom prebivališča za vročanje pravnih dokumentov, zahteve za popravek morda niso dovolj in upravljavec ima lahko pravico zahtevati dokaz o domnevni netočnosti. S takimi zahtevami posamezniku, na katerega se nanašajo osebni podatki, ne sme biti naloženo nerazumno dokazno breme, da bi se mu tako onemogočil popravek osebnih podatkov. ESČP je ugotovilo kršitve člena 8 EKČP v več primerih, v katerih je bilo pritožniku onemogočeno izpodbijanje točnosti informacij, shranjenih v tajnih registrih.[559]

Primer: ESČP je v zadevi *Cemalettin Canli proti Turčiji*[560] ugotovilo kršitev člena 8 EKČP zaradi nepravilnega poročanja policije v kazenskem postopku.

Pritožnik je bil zaradi domnevnega članstva v nezakonitih organizacijah dvakrat udeležen v kazenskem postopku, vendar ni bil spoznan za krivega. Ko je bil znova aretiran in obdolžen še enega kaznivega dejanja, je policija kazenskemu sodišču predložila poročilo z naslovom *Informacije o dodatnih kaznivih dejanjih*, v katerem je bil pritožnik naveden kot član dveh nezakonitih organizacij. Pritožnikovi zahtevi, naj se poročilo in policijska kartoteka popravita, ni bilo ugodeno. ESČP je ugotovilo, da informacije iz policijskega poročila spadajo na področje uporabe člena 8 EKČP, saj lahko tudi javne

558 SUVP, člen 16; posodobljena Konvencija št. 108, člen 9(1).

559 ESČP, *Rotaru proti Romuniji* (veliki senat), pritožba št. 28341/95, 4. maj 2000.

560 ESČP, *Cemalettin Canli proti Turčiji*, pritožba št. 22427/04, 18. november 2008, točke 33, 42 in 43, in ESČP, *Dalea proti Franciji*, pritožba št. 964/07, 2. februar 2010.

informacije, ki se sistematično zbirajo in shranjujejo v datotekah organov, spadajo na področje zasebnega življenja. Poleg tega policijsko poročilo ni bilo pravilno pripravljeno, njegova predložitev kazenskemu sodišču pa ni bila v skladu z zakonom. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Posameznik, na katerega se nanašajo osebni podatki, lahko v civilnem sporu ali postopku pred javnim organom, ki mora odločiti, ali so podatki točni ali ne, zahteva, naj se glede teh osebnih podatkov doda vnos ali zaznamek o tem, da se izpodbija njihova točnost in da uradna odločitev še ni bila sprejeta.[561] Upravljavec v tem obdobju osebnih podatkov ne sme predstavljati kot točnih ali dokončnih, zlasti ne tretjim osebam.

6.1.3 Pravica do izbrisa („pravica do pozabe“)

Zagotavljanje, da imajo posamezniki, na katere se nanašajo osebni podatki, pravico do izbrisa svojih osebnih podatkov, je posebej pomembno za učinkovito uporabo načel varstva osebnih podatkov, zlasti načela najmanjšega obsega podatkov (osebni podatki morajo biti omejeni na tisto, kar je potrebno za namene, za katere se obdelujejo). Pravica do izbrisa je zato vključena v pravne instrumente Sveta Evrope in EU.[562]

Primer: v zadevi *Segerstedt-Wiberg in drugi proti Švedski*[563] so bili pritožniki pripadniki določenih liberalnih in komunističnih političnih strank. Sumili so, da so bile informacije o njih vnesene v tajne policijske kartoteke, in zahtevali njihov izbris. ESČP je menilo, da je imela hramba spornih podatkov pravno podlago in da se je z njo uresničeval legitimen cilj. Vendar je v zvezi z nekaterimi pritožniki ugotovilo, da trajna hramba osebnih podatkov pomeni nesorazmeren poseg v njihovo zasebno življenje. V primeru enega pritožnika so organi na primer hranili podatek, da se je leta 1969 domnevno zavzemal za nasilno upiranje policijskemu nadzoru med protesti. ESČP je ugotovilo, da te informacije ne morejo biti v nikakršnem pomembnem interesu nacionalne varnosti, zlasti ker se nanašajo na oddaljeno preteklost. Ugotovilo je, da je

561 SUVP, člen 18 in uvodna izjava 67.

562 Prav tam, člen 17.

563 ESČP, *Segerstedt-Wiberg in drugi proti Švedski*, pritožba št. 62332/00, 6. junij 2006, točki 89 in 90; glej na primer tudi ESČP, *M. K. proti Franciji*, pritožba št. 19522/09, 18. april 2013.

bil v zvezi s štirimi od petih pritožnikov kršen člen 8 EKČP, saj trajna hramba njihovih podatkov ni imela pomena, glede na to, da je od domnevnih dejanj pritožnikov preteklo veliko časa.

Primer: v zadevi *Brunet proti Franciji*[564] je pritožnik nasprotoval hrambi svojih osebnih podatkov v policijski podatkovni zbirki, ki je vsebovala informacije o obsojenih in obdolženih osebah ter žrtvah. Čeprav je bil kazenski postopek zoper pritožnika ustavljen, so se njegovi podatki pojavili v podatkovni zbirki. ESČP je menilo, da je bil kršen člen 8 EKČP. Sodišče je v zvezi s to ugotovitvijo menilo, da v praksi ni bilo nobene možnosti, da bi pritožnik dosegel izbris svojih osebnih podatkov iz podatkovne zbirke. ESČP je proučilo tudi naravo informacij, vključenih v podatkovno zbirko, in menilo, da informacije posegajo v zasebnost pritožnika, saj vsebujejo podrobne podatke o njegovi identiteti in osebnosti. Ugotovilo je tudi, da je 20-letno obdobje hrambe osebnih podatkov v podatkovni zbirki predolgo, predvsem zato, ker pritožnik ni bil nikoli obsojen na sodišču.

V posodobljeni Konvenciji št. 108 je izrecno določeno, da ima vsak posameznik pravico do izbrisa netočnih, napačnih ali nezakonito obdelanih podatkov.[565]

V okviru prava EU se na podlagi člena 17 SUVP uveljavljajo zahteve posameznikov, na katere se nanašajo osebni podatki, za izbris osebnih podatkov. Pravica do izbrisa osebnih podatkov brez nepotrebnega odlašanja velja, če:

- osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;
- posameznik, na katerega se nanašajo osebni podatki, prekliče privolitev, na podlagi katere poteka obdelava, in za obdelavo ne obstaja nobena druga pravna podlaga;
- posameznik, na katerega se nanašajo osebni podatki, obdelavi ugovarja, za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi;
- so bili osebni podatki obdelani nezakonito;

564 ESČP, *Brunet proti Franciji*, pritožba št. 21010/10, 18. september 2014.

565 Posodobljena konvencija št. 108, člen 9(1)(e).

- je treba osebne podatke izbrisati za izpolnitev pravne obveznosti v skladu s pravom Unije ali pravom države članice, ki velja za upravljavca;

- so bili osebni podatki zbrani v zvezi s ponudbo storitev informacijske družbe otrokom v skladu s členom 8 SUVP.[566]

Dokazno breme, da je obdelava podatkov zakonita, nosijo upravljavci podatkov, saj so odgovorni za zakonitost obdelave.[567] Upravljavec mora biti v skladu z načelom odgovornosti kadar koli zmožen dokazati, da ima trdno pravno podlago za obdelavo osebnih podatkov, sicer je treba obdelavo prekiniti.[568] V SUVP so določene izjeme od pravice do pozabe, med drugim če je obdelava potrebna:

- za uresničevanje pravice do svobode izražanja in obveščanja;

- za izpolnjevanje pravne obveznosti obdelave na podlagi prava Unije ali prava države članice, ki velja za upravljavca, ali za izvajanje naloge v javnem interesu ali pri izvajanju javne oblasti, ki je bila dodeljena upravljavcu;

- iz razlogov javnega interesa na področju javnega zdravja;

- za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene;

- za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.[569]

SEU je potrdilo pomen, ki ga ima pravica do izbrisa za zagotavljanje visoke ravni varstva osebnih podatkov.

Primer: SEU je v zadevi *Google Spain*[570] obravnavalo, ali bi morala družba Google zastarele informacije o finančnih težavah pritožnika izbrisati s seznama zadetkov iskanja. Družba Google je med drugim oporekala temu, da bi bila odgovorna, pri čemer je trdila, da zagotavlja le hiperpovezavo na spletno stran izdajatelja, na kateri so objavljene zadevne informacije, v tem primeru

566 SUVP, člen 17(1).

567 Prav tam.

568 Prav tam, člen 5(2).

569 Prav tam, člen 17(3).

570 SEU, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), C-131/12, 13. maj 2014, točke 55–58.

na časopisna članka, v katerih se je poročalo o pritožnikovi plačilni nesposobnosti.[571] Trdila je, da bi bilo treba zahtevo za izbris zastarelih informacij s spletne strani nasloviti na gostitelja te spletne strani, ne pa nanjo, saj da le zagotavlja povezavo na izvirno stran. SEU je ugotovilo, da družba Google s tem, ko po spletu išče informacije in spletne strani ter indeksira vsebine, da bi zagotovila zadetke iskanja, postane upravljavec podatkov, za katerega veljajo odgovornosti in obveznosti po pravu EU.

SEU je pojasnilo, da je z internetnimi iskalniki in zadetki iskanja, ki zagotavljajo osebne podatke, mogoče sestaviti podroben profil osebe.[572] Zaradi iskalnikov so informacije, vsebovane na takem seznamu zadetkov, vseprisotne. Poseganje zaradi svoje potencialne teže ne more biti upravičeno zgolj na podlagi gospodarskega interesa, ki ga ima upravljavec takega iskalnika pri navedeni obdelavi. Najti je treba pravično ravnotežje zlasti med zakonitim interesom internetnih uporabnikov za dostop do informacij in temeljnimi pravicami posameznika, na katerega se nanašajo osebni podatki, v skladu s členom 7 in 8 Listine EU o temeljnih pravicah. V vse bolj digitalizirani družbi je zahteva po točnosti osebnih podatkov in tem, da ne presegajo tega, kar je potrebno (tj. obveščanje javnosti), bistvenega pomena za zagotavljanje visoke ravni varstva osebnih podatkov za posameznike. „[U]pravljavec tega iskalnika, ki je odgovoren za to obdelavo, [mora] v okviru svoje odgovornosti, pristojnosti in zmožnosti zagotoviti, da ta obdelava izpolnjuje zahteve" prava EU, da imajo lahko vzpostavljena pravna jamstva polni učinek.[573] To pomeni, da pravica do izbrisa svojih osebnih podatkov, kadar je obdelava zastarela ali ni več potrebna, zajema tudi upravljavce osebnih podatkov, ki zadevne informacije reproducirajo.[574]

---

571 Družba Google je izpodbijala tudi uporabo pravil EU o varstvu osebnih podatkov, ker je družba Google Inc. ustanovljena v ZDA in se je obdelava spornih osebnih podatkov iz obravnavane zadeve izvajala tudi v ZDA. Drugi argument za neuporabo prava EU o varstvu osebnih podatkov se je nanašal na trditev, da iskalnikov ni mogoče šteti za „upravljavce" v zvezi s podatki, prikazanimi v zadetkih iskanja, saj družbe, ki upravljajo iskalnike, zadevnih podatkov ne poznajo in jih ne nadzorujejo. SEU je oba argumenta zavrnilo, saj je menilo, da se Direktiva 95/46/ES uporablja v navedeni zadevi, in nato proučilo obseg pravic, zagotovljenih z navedeno direktivo, zlasti pravice do izbrisa osebnih podatkov.

572 Prav tam, točke 36, 38, 80, 81 in 97.

573 Prav tam, točke 81–83.

574 SEU, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), C-131/12, 13. maj 2014, točka 88. Glej tudi Delovna skupina za varstvo podatkov iz člena 29, *Smernice za izvajanje sodbe Sodišča EU v zadevi Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu, C-131/12*, WP 225, Bruselj, 2014, in Priporočilo CM/Rec 2012(3) Odbora ministrov državam članicam o varstvu človekovih pravic v zvezi z iskalniki, 2012.

V zvezi s tem, ali bi morala družba Google odstraniti povezave, ki se nanašajo na pritožnika, je SEU menilo, da imajo posamezniki pod določenimi pogoji pravico, da zahtevajo izbris osebnih podatkov. Ta pravica se lahko uveljavlja, kadar so podatki v zvezi s posameznikom netočni, neprimerni, neustrezni ali pretirani glede na namene obdelave osebnih podatkov. SEU je navedlo, da ta pravica ni absolutna, temveč da jo je treba uravnotežiti z drugimi pravicami in interesi, zlasti interesom širše javnosti, da ima dostop do nekaterih informacij. Vsak zahtevek za izbris je treba oceniti za vsak primer posebej, da se vzpostavi ravnotežje med temeljnima pravicama do varstva osebnih podatkov in spoštovanja zasebnega življenja posameznika, na katerega se nanašajo, na eni strani ter zakonitimi interesi vseh internetnih uporabnikov, vključno z izdajatelji, na drugi strani. SEU je zagotovilo smernice o dejavnikih, ki jih je treba upoštevati pri izvedbi tega uravnoteženja. Zlasti pomemben dejavnik je narava zadevnih informacij. Če se informacije nanašajo na zasebno življenje posameznika in če ni javnega interesa za njihovo razpoložljivost, bi pravici do varstva osebnih podatkov in zasebnosti prevladali nad pravico širše javnosti do dostopa do informacij. Če se nasprotno zdi, da je posameznik, na katerega se nanašajo osebni podatki, javna osebnost ali da je narava zadevnih informacij taka, da je zaradi nje upravičena njihova razpoložljivost širši javnosti, bi lahko prevladujoči interes navedene javnosti za dostop do zadevnih informacij upravičeval poseg v temeljni pravici posameznika, na katerega se nanašajo osebni podatki, do varstva osebnih podatkov in zasebnosti.

Delovna skupina iz člena 29 je na podlagi te sodbe SEU sprejela smernice za njeno izvajanje.[575] Te smernice vključujejo seznam skupnih meril, ki jih morajo nadzorni organi uporabljati pri obravnavi pritožb v zvezi z zahtevki posameznikov za izbris, pri čemer je pojasnjeno, kaj pomeni pravica do izbrisa, v njih pa so na voljo tudi napotki za uravnoteženje pravic. V smernicah je poudarjeno, da je treba presojo izvesti za vsak primer posebej. Ker pravica do pozabe ni absolutna, se lahko izid zahtevka razlikuje glede na zadevni primer. To je razvidno tudi iz sodne prakse SEU po sodbi v zadevi Google.

575 Delovna skupina za varstvo podatkov iz člena 29, *Smernice za izvajanje sodbe Sodišča EU v zadevi Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu, C-131/12*, WP 225, Bruselj, 2014.

Primer: SEU je moralo v zadevi *Camera di Commercio di Lecce proti Manniju*[576] proučiti, ali ima posameznik pravico, da doseže izbris svojih osebnih podatkov iz javnega registra družb, ko njegova družba preneha obstajati. S. Manni je zahteval, naj gospodarska zbornica v Lecceju izbriše njegove osebne podatke iz navedenega registra, saj je ugotovil, da lahko potencialne stranke ob vpogledu v register vidijo, da je bil upravitelj družbe, zoper katero je bil pred več kot desetimi leti uveden stečajni postopek. Menil je, da te informacije na potencialne stranke delujejo odvračilno.

SEU je uravnotežilo pravico S. Mannija do varstva njegovih osebnih podatkov in interes širše javnosti za dostop do informacij, pri čemer je najprej proučilo namen javnega registra. Opozorilo je na dejstvo, da je objava določena z zakonom, zlasti z direktivo EU, katere cilj je zagotavljati lažji dostop tretjih oseb do informacij o družbah. Tretje osebe bi zato morale imeti dostop in možnost vpogleda v osnovne dokumente družbe ter druge informacije o družbi, „zlasti [...] podatk[e] o osebah, ki so pooblaščene za zastopanje in sprejemanje obveznosti v imenu družbe". Namen objave je bil tudi zagotoviti pravno varnost zaradi okrepljenih poslovnih tokov med državami članicami, in sicer z zagotavljanjem dostopa tretjih oseb do vseh bistvenih informacij o družbah po vsej EU.

SEU je poleg tega ugotovilo, da se pravice in pravne obveznosti, povezane z družbo, pogosto ohranijo tudi po preteku daljšega časovnega obdobja in tudi po prenehanju družbe. Spori v zvezi s prenehanjem družbe so lahko dolgotrajni, vprašanja v zvezi z družbo, njenimi direktorji in upravitelji pa se lahko pojavljajo še dolga leta po njenem prenehanju. SEU je menilo, da je glede na številne možne scenarije in razlike v zastaralnih rokih, ki so določeni v posameznih državah članicah, „razvidno, da je trenutno nemogoče ugotoviti enoten rok, ki bi tekel od prenehanja družbe, ob poteku katerega vpis navedenih podatkov v register in njihova objava ne bi bila več potrebna". Zaradi zakonitega cilja objave in težav pri določitvi obdobja, po izteku katerega bi se lahko osebni podatki izbrisali iz registra, ne da bi bili s tem oškodovani interesi tretjih oseb, je SEU ugotovilo, da pravila EU o varstvu osebnih podatkov ne zagotavljajo pravice do izbrisa osebnih podatkov za osebe v položaju S. Mannija.

576 SEU, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju*, C-398/15, 9. marec 2017.

Če je upravljavec objavil osebne podatke ter mora zadevne informacije izbrisati, mora sprejeti razumne ukrepe, da druge upravljavce, ki obdelujejo iste osebne podatke, obvesti o zahtevi posameznika, na katerega se nanašajo osebni podatki, za izbris. Upravljavec mora pri svojih dejavnostih upoštevati razpoložljivo tehnologijo in stroške izvajanja.[577]

6.1.4 Pravica do omejitve obdelave

V skladu s členom 18 SUVP imajo posamezniki, na katere se nanašajo osebni podatki, pravico doseči, da upravljavec začasno omeji obdelavo njihovih osebnih podatkov. Od upravljavca lahko zahtevajo, da omeji obdelavo, če:

- oporekajo točnosti osebnih podatkov;
- je obdelava nezakonita in posameznik, na katerega se nanašajo osebni podatki, namesto izbrisa osebnih podatkov zahteva omejitev njihove uporabe;
- je treba osebne podatke hraniti za uveljavljanje ali obrambo pravnih zahtevkov;
- še ni sprejeta odločitev, ali zakoniti interesi upravljavca osebnih podatkov prevladajo nad interesi posameznika, na katerega se nanašajo osebni podatki.[578]

Metode, po katerih lahko upravljavec omeji obdelavo osebnih podatkov, lahko na primer zajemajo začasni prenos izbranih podatkov v drug sistem za obdelavo, preprečitev dostopnosti osebnih podatkov uporabnikom ali začasno odstranitev osebnih podatkov.[579] Upravljavec mora pred preklicem omejitve obdelave o tem obvestiti posameznika, na katerega se nanašajo osebni podatki.[580]

Obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave

Upravljavec mora vsakemu uporabniku, ki so mu bili razkriti osebni podatki, sporočiti vse popravke ali izbrise osebnih podatkov ali omejitve obdelave, razen če je to

577 SUVP, člen 17(2) in uvodna izjava 66.

578 Prav tam, člen 18(1).

579 Prav tam, uvodna izjava 67.

580 Prav tam, člen 18(3).

nemogoče ali nesorazmerno.[581] Če posameznik, na katerega se nanašajo osebni podatki, zahteva informacije o teh uporabnikih, mu jih mora upravljavec predložiti.[582]

6.1.5 Pravica do prenosljivosti podatkov

V skladu s SUVP imajo posamezniki, na katere se nanašajo osebni podatki, pravico do prenosljivosti podatkov v primerih, kadar se obdelava osebnih podatkov, ki so jih zagotovili upravljavcu, izvaja z avtomatiziranimi sredstvi na podlagi privolitve, ali kadar je obdelava osebnih podatkov potrebna za izvajanje pogodbe in se izvaja z avtomatiziranimi sredstvi. To pomeni, da pravica do prenosljivosti podatkov ne velja v primerih, kadar obdelava osebnih podatkov temelji na pravni podlagi, ki ni privolitev ali pogodba.[583]

Če pravica do prenosljivosti podatkov velja, imajo posamezniki, na katere se nanašajo osebni podatki, pravico, da se njihovi osebni podatki neposredno prenesejo od enega upravljavca k drugemu, če je to tehnično izvedljivo.[584] Da bi to olajšali, bi morali upravljavci razviti interoperabilne oblike, ki omogočajo prenosljivost podatkov za posameznike, na katere se nanašajo osebni podatki.[585] V SUVP je določeno, da morajo biti te oblike strukturirane, splošno uporabljane in strojno berljive, da se olajša interoperabilnost.[586] V širšem smislu bi lahko interoperabilnost opredelili kot zmožnost informacijskih sistemov, da si izmenjujejo podatke in omogočajo souporabo informacij.[587] Čeprav je namen uporabljenih oblik doseči interoperabilnost, SUVP ne vsebuje posebnih priporočil glede konkretne oblike osebnih podatkov, ki jo je treba zagotoviti: oblike se lahko razlikujejo glede na sektor.[588]

V skladu s smernicami Delovne skupine iz člena 29 pravica do prenosljivosti podatkov „podpira izbiro uporabnika, nadzor uporabnika in opolnomočenje uporabnika“, njen cilj pa je posameznikom, na katere se nanašajo osebni podatki, dati nadzor nad

581 Prav tam, člen 19.

582 Prav tam.

583 Prav tam, uvodna izjava 68 in člen 20(1).

584 Prav tam, člen 20(2).

585 Prav tam, uvodna izjava 68 in člen 20(1).

586 Prav tam, uvodna izjava 68.

587 Evropska komisija, Sporočilo o trdnejših in pametnejših informacijskih sistemih za meje in varnost, COM(2016) 205 final, 2. april 2016.

588 Delovna skupina za varstvo podatkov iz člena 29 (2016), *Smernice o pravici do prenosljivosti podatkov*, WP 242, sprejete 13. decembra 2016 in revidirane 5. aprila 2017, str. 13.

njihovimi osebnimi podatki.[589] V smernicah so pojasnjeni glavni elementi prenosljivosti podatkov, ki vključujejo:

- pravico posameznikov, na katere se nanašajo osebni podatki, da svoje osebne podatke, ki jih obdeluje upravljavec, prejmejo v strukturirani, splošno uporabljani, strojno berljivi in interoperabilni obliki;
- pravico do neoviranega prenosa osebnih podatkov od enega upravljavca osebnih podatkov k drugemu, če je to tehnično izvedljivo;
- ureditev upravljanja – kadar upravljavec podatkov odgovori na zahtevo za prenosljivost podatkov, deluje v skladu z navodili posameznika, na katerega se nanašajo osebni podatki, kar pomeni, da ni odgovoren za skladnost uporabnika s pravom o varstvu osebnih podatkov, saj je posameznik, na katerega se nanašajo osebni podatki, tisti, ki določi, komu naj se prenesejo osebni podatki;
- uveljavljanje pravice do prenosljivosti podatkov ne posega v nobeno drugo pravico, kot velja za vse druge pravice iz SUVP.

6.1.6 Pravica do ugovora

Posamezniki, na katere se nanašajo osebni podatki, se lahko na podlagi razlogov, povezanih z njihovim posebnim položajem, sklicujejo na pravico do ugovora obdelavi osebnih podatkov in obdelavi osebnih podatkov za namene neposrednega trženja. Pravica do ugovora se lahko uveljavlja z avtomatiziranimi sredstvi.

Pravica do ugovora na podlagi razlogov, povezanih s posebnim položajem posameznikov, na katere se nanašajo osebni podatki

Posamezniki, na katere se nanašajo osebni podatki, nimajo splošne pravice do ugovora zoper obdelavo svojih osebnih podatkov.[590] Posameznik, na katerega se nanašajo osebni podatki, ima v skladu s členom 21(1) SUVP pravico vložiti ugovor na podlagi razlogov, povezanih z njegovim posebnim položajem, kadar je pravna podlaga za obdelavo izvajanje naloge v javnem interesu, dodeljene upravljavcu, ali kadar

589 Prav tam.

590 Glej tudi ESČP, *M. S. proti Švedski*, pritožba št. 20837/92, 27. avgust 1997 (v kateri so bili zdravstveni podatki sporočeni brez privolitve ali možnosti ugovora); ESČP, *Leander proti Švedski*, pritožba št. 9248/81, 26. marec 1987, in ESČP, *Mosley proti Združenemu kraljestvu*, pritožba št. 48009/08, 10. maj 2011.

obdelava temelji na zakonitih interesih upravljavca.[591] Pravica do ugovora se uporablja za dejavnosti oblikovanja profilov. Podobna pravica je priznana v posodobljeni Konvenciji št. 108.[592]

Namen pravice do ugovora na podlagi razlogov, povezanih s posebnim položajem posameznika, na katerega se nanašajo osebni podatki, je vzpostaviti ustrezno ravnovesje med njegovimi pravicami do varstva osebnih podatkov in zakonitimi interesi drugih pri obdelavi njegovih osebnih podatkov. Vendar je SEU pojasnilo, da pravice posameznika, na katerega se nanašajo osebni podatki, „na splošno" prevladajo nad interesi upravljavca podatkov, odvisno od „narave zadevne informacije, od tega, kako občutljiva je za zasebnost zadevne osebe, in od interesa javnosti, da razpolaga s to informacijo".[593] V skladu s SUVP nosijo dokazno breme upravljavci, ki morajo dokazati nujne razloge za nadaljevanje obdelave.[594] Podobno je v Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 pojasnjeno, da je treba zakonite razloge za obdelavo osebnih podatkov (ki lahko prevladajo nad pravico posameznikov, na katere se nanašajo osebni podatki, do ugovora) dokazati za vsak primer posebej.[595]

Primer: SEU je v zadevi *Manni*[596] menilo, da zaradi zakonitega namena razkritja osebnih podatkov v registru družb, zlasti potrebe po zaščiti interesov tretjih oseb in zagotovitvi pravne varnosti, S. Manni načeloma nima pravice, da doseže izbris svojih osebnih podatkov iz registra družb. Vendar je potrdilo obstoj pravice do ugovora obdelavi, in sicer je navedlo, da „ni mogoče izključiti, da lahko pride do posebnih položajev, v katerih je iz zakonitih in nujnih razlogov, povezanih s konkretnim primerom zadevne osebe, izjemoma upravičeno, da je dostop do osebnih podatkov, ki se nanašajo nanjo in so vpisani v register, ko preteče dovolj časa [...], omejen na tretje osebe, ki izkažejo poseben interes za vpogled v te podatke".

591 SUVP, uvodna izjava 69; člen 6(1)(e) in (f).

592 Posodobljena konvencija št. 108, člen 9(1)(d); Priporočilo o oblikovanju profilov, člen 5(3).

593 SEU, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu* (veliki senat), C-131/12, 13. maj 2014, točka 81.

594 Glej tudi posodobljeno Konvencijo št. 108, člen 98(1)(d), ki določa, da lahko posameznik, na katerega se nanašajo osebni podatki, ugovarja obdelavi svojih osebnih podatkov, razen če upravljavec dokaže, da ima zakonito podlago za obdelavo, ki prevlada nad njegovimi interesi ali pravicami in temeljnimi svoboščinami.

595 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 78.

596 SEU, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju*, C-398/15, 9. marec 2017, točki 47 in 60.

SEU je menilo, da so nacionalna sodišča odgovorna, da vsak primer presodijo ob upoštevanju vseh ustreznih okoliščin posameznika in tega, ali obstajajo zakoniti in nujni razlogi, ki bi lahko izjemoma upravičevali omejitev dostopa tretjih oseb do osebnih podatkov v registrih družb. Vendar je pojasnilo, da v primeru S. Mannija zgolj dejstva, da razkritje njegovih osebnih podatkov v registru domnevno vpliva na njegove stranke, ni mogoče šteti za tak zakonit in nujen razlog. Njegove potencialne stranke imajo zakonit interes za dostop do informacij o stečaju njegovega nekdanjega podjetja.

Posledica uspešnega ugovora je, da upravljavec zadevnih osebnih podatkov ne sme več obdelovati. Vendar dejanja obdelave osebnih podatkov posameznika, na katerega se nanašajo, izvedena pred vložitvijo ugovora, ostanejo še naprej zakonita.

Pravica do ugovora obdelavi osebnih podatkov za namene neposrednega trženja

Člen 21(2) SUVP določa posebno pravico do ugovora zoper uporabo osebnih podatkov za namene neposrednega trženja, s čimer je dodatno pojasnjen člen 13 Direktive o zasebnosti in elektronskih komunikacijah. Taka pravica je določena tudi v posodobljeni Konvenciji št. 108 in Priporočilu Sveta Evrope o neposrednem trženju.[597] V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je pojasnjeno, da bi moral ugovor obdelavi osebnih podatkov za namene neposrednega trženja privesti do brezpogojnega izbrisa ali odstranitve zadevnih osebnih podatkov.[598]

Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da kadar koli in brezplačno ugovarja uporabi svojih osebnih podatkov za namene neposrednega trženja. Posameznike, na katere se nanašajo osebni podatki, je treba o tej pravici obvestiti jasno in ločeno od vseh drugih informacij.

Pravica do ugovora z avtomatiziranimi sredstvi

Kadar se osebni podatki uporabljajo in obdelujejo za storitve informacijske družbe, lahko posameznik, na katerega se nanašajo osebni podatki, pravico do ugovora obdelavi svojih osebnih podatkov uveljavlja z avtomatiziranimi sredstvi.

597 Svet Evrope, Odbor ministrov (1985), Priporočilo Rec(85)20 državam članicam o varstvu osebnih podatkov, ki se uporabljajo za neposredno trženje, 25. oktober 1985, člen 4(1).

598 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 79.

Storitve informacijske družbe so opredeljene kot katere koli storitve, ki se običajno zagotavljajo za plačilo, na daljavo, z elektronskimi sredstvi in na osebno zahtevo prejemnika storitev.[599]

Upravljavci osebnih podatkov, ki ponujajo storitve informacijske družbe, morajo vzpostaviti ustrezno tehnično ureditev in postopke, da zagotovijo učinkovito uveljavljanje pravice do ugovora z avtomatiziranimi sredstvi.[600] To lahko na primer vključuje blokiranje piškotkov na spletnih straneh ali izklop sledenja brskanju po spletu.

Pravica do ugovora obdelavi osebnih podatkov v znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene

V skladu s pravom EU bi bilo treba izraz znanstvene raziskave razlagati široko, tako da vključuje tudi na primer tehnološki razvoj, predstavitvene dejavnosti, temeljne raziskave, uporabne raziskave in zasebno financirane raziskave.[601] Zgodovinske raziskave vključujejo tudi raziskave v genealoške namene, pri čemer bi bilo treba upoštevati, da se SUVP ne bi smela uporabljati za umrle osebe.[602] Statistični nameni pomenijo vsako dejanje zbiranja in obdelave osebnih podatkov, potrebno za statistične raziskave ali pripravo statističnih rezultatov.[603] Poseben položaj posameznika, na katerega se nanašajo osebni podatki, je pravna podlaga tudi v zvezi s pravico do ugovora obdelavi osebnih podatkov v raziskovalne namene.[604] Edina izjema je potreba po obdelavi za opravljanje naloge, ki se izvaja iz razlogov javnega interesa. Vendar pravica do izbrisa ne velja, kadar je obdelava nujna (iz razlogov javnega interesa ali ne) za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene.[605]

V členu 89 SUVP so zahteve glede znanstvenih, statističnih ali zgodovinskih raziskav in pravice posameznikov, na katere se nanašajo podatki, uravnotežene s posebnimi zaščitnimi ukrepi in odstopanji. V pravu Unije ali pravu držav članic je tako mogoče določiti odstopanja od pravice do ugovora, če je verjetno, da bi taka pravica onemogočila ali resno ovirala doseganje raziskovalnih namenov, in če so taka odstopanja nujna za uresničitev teh namenov.

599 Direktiva 98/34/ES o določitvi postopka za zbiranje informacij na področju tehničnih standardov in tehničnih predpisov, kakor je bila spremenjena z Direktivo 98/48/ES, člen 1(2).

600 SUVP, člen 21(5).

601 Prav tam, uvodna izjava 159.

602 Prav tam, uvodna izjava 160.

603 Prav tam, uvodna izjava 162.

604 Prav tam, člen 21(6).

605 Prav tam, člen 17(3)(d).

V okviru **prava Sveta Evrope** člen 11(2) posodobljene Konvencije št. 108 določa, da se lahko z zakonom določijo omejitve pravic posameznikov, na katere se nanašajo osebni podatki, vključno s pravico do ugovora, v zvezi z obdelavo osebnih podatkov za namene arhiviranja v javnem interesu, znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene, kadar ni prepoznano tveganje kršitve pravic in temeljnih svoboščin posameznikov, na katere se nanašajo osebni podatki.

Vendar je v Pojasnjevalnem poročilu (točka 43) navedeno tudi, da bi morali imeti posamezniki, na katere se nanašajo osebni podatki, možnost, da privolijo le v nekatera področja raziskav ali dele raziskovalnih projektov v obsegu, ki ga dovoljuje predvideni namen, in da ugovarjajo, če menijo, da obdelava brez zakonitega razloga čezmerno posega v njihove pravice in svoboščine.

Z drugimi besedami, taka obdelava bi se zato vnaprej štela za združljivo, če obstajajo drugi zaščitni ukrepi in če dejanja načeloma izključujejo vsakršno uporabo pridobljenih informacij za odločitve ali ukrepe v zvezi z določenim posameznikom.

6.1.7 Avtomatizirano sprejemanje posameznih odločitev, vključno z oblikovanjem profilov

Avtomatizirane odločitve so odločitve, sprejete na podlagi osebnih podatkov, obdelanih izključno z avtomatskimi sredstvi brez človekovega posredovanja. V skladu s **pravom EU** za posameznike, na katere se nanašajo osebni podatki, ne smejo veljati avtomatizirane odločitve, ki imajo pravne učinke ali nanje podobno pomembno vplivajo. Če bi take odločitve verjetno znatno vplivale na življenje posameznikov, ker se nanašajo na primer na kreditno sposobnost, e-zaposlovanje, delovno uspešnost ali analizo ravnanja ali zanesljivosti, je potrebno posebno varstvo, da se preprečijo škodljive posledice. Avtomatizirano sprejemanje odločitev vključuje oblikovanje profilov v kakršni koli obliki avtomatiziranega ocenjevanja „osebni[h] vidik[ov] v zvezi s posameznikom, na katerega se nanašajo osebni podatki, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa ali interesov, zanesljivosti ali vedenja, lokacije ali gibanja“.[606]

Primer: da bi agencije za poročanje o boniteti potrošnikov na hitro ocenile kreditno sposobnost prihodnje stranke, zbirajo nekatere podatke, kot so podatki o tem, kako je stranka vzdrževala svoj kreditni račun in transakcijski račun

606 Prav tam, uvodna izjava 71, člen 4(4) in člen 22.

za plačevanje gospodinjskih/stanovanjskih stroškov, podrobnosti o prejšnjih naslovih stranke ter informacije iz javnih virov, kot so volilni imenik, javne evidence (vključno s sodbami sodišč) ali podatki o stečaju in plačilni nesposobnosti. Ti osebni podatki se nato vnesejo v točkovalni algoritem, s katerim se izračuna skupna vrednost, ki predstavlja kreditno sposobnost potencialne stranke.

Po navedbah Delovne skupine iz člena 29 pravica posameznika, na katerega se nanašajo osebni podatki, da zanj ne veljajo odločitve, ki temeljijo zgolj na avtomatizirani obdelavi in bi lahko imele pravne učinke v zvezi z njim ali nanj znatno vplivale, pomeni splošno prepoved, zato posamezniku, na katerega se nanašajo osebni podatki, ni treba proaktivno vložiti ugovora zoper tako odločitev.[607]

Vseeno je lahko v skladu s SUVP avtomatizirano sprejemanje odločitev s pravnimi učinki ali znatnim vplivom na posameznike sprejemljivo, če je potrebno za sklenitev ali izvajanje pogodbe med upravljavcem osebnih podatkov in posameznikom, na katerega se nanašajo osebni podatki, ali če je ta posameznik vanj izrecno privolil. Avtomatizirano sprejemanje odločitev je poleg tega sprejemljivo, če je dovoljeno v pravu ter če so ustrezno zaščitene pravice, svoboščine in zakoniti interesi posameznika, na katerega se nanašajo osebni podatki.[608]

V SUVP je tudi določeno, da je ena od obveznosti upravljavca v zvezi z informacijami, ki jih je treba zagotoviti pri zbiranju osebnih podatkov, ta, da je treba posameznike, na katere se nanašajo osebni podatki, seznaniti z obstojem avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov.[609] To ne vpliva na pravico do dostopa do osebnih podatkov, ki jih obdeluje upravljavec.[610] Ni dovolj, da se predložijo le informacije o tem, da bo potekalo oblikovanje profilov, temveč bi bilo treba zagotoviti tudi smiselne informacije o razlogih zanj in predvidenih posledicah zadevne obdelave za posameznike.[611] Na primer, zdravstvena zavarovalnica, ki uporablja avtomatizirano sprejemanje odločitev v zvezi z vlogami, bi morala posameznikom, na katere se nanašajo osebni podatki, zagotoviti splošne informacije o tem, kako algoritem deluje in na podlagi katerih dejavnikov izračuna njihove zavarovalne premije.

607 Delovna skupina za varstvo podatkov iz člena 29, *Smernice o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679*, WP 251, 3. oktober 2017, str. 15.

608 SUVP, člen 22(2).

609 Prav tam, člen 12.

610 Prav tam, člen 15.

611 Prav tam, člen 13(2)(f).

Podobno lahko posamezniki, na katere se nanašajo osebni podatki, pri uveljavljanju pravice do dostopa od upravljavca zahtevajo informacije o obstoju avtomatiziranega sprejemanja odločitev in smiselne informacije o razlogih zanj.[612]

Informacije, ki se zagotovijo posameznikom, na katere se nanašajo osebni podatki, naj bi zagotavljale preglednost in tem posameznikom omogočile, da dajo informirano privolitev, če je to primerno, ali pridobijo osebno posredovanje. Upravljavec osebnih podatkov mora izvajati ustrezne ukrepe za zaščito pravic, svoboščin in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki. To vključuje vsaj pravico do osebnega posredovanja upravljavca ter možnost, da posameznik, na katerega se nanašajo osebni podatki, izrazi svoje stališče in izpodbija odločitev, ki temelji na avtomatizirani obdelavi njegovih osebnih podatkov.[613]

Delovna skupina iz člena 29 je zagotovila dodatne smernice o uporabi avtomatiziranega sprejemanja odločitev v skladu s SUVP.[614]

V skladu s pravom Sveta Evrope imajo posamezniki pravico, da zanje ne velja odločitev, ki bo nanje znatno vplivala in temelji zgolj na avtomatizirani obdelavi, ne da bi se upoštevala njihova stališča.[615] Zahteva po upoštevanju stališč posameznika, na katerega se nanašajo osebni podatki, kadar odločitve temeljijo zgolj na avtomatizirani obdelavi, pomeni, da imajo ti posamezniki pravico, da take odločitve izpodbijajo, ter da bi jim bilo treba omogočiti, da opozorijo na vse netočne osebne podatke, ki jih uporablja upravljavec, in izpodbijajo relevantnost katerega koli profila, ki se uporablja zanje.[616] Vendar posameznik te pravice ne more uveljavljati, če je avtomatizirana odločitev dovoljena z zakonom, ki velja za upravljavca in v katerem so določeni tudi ustrezni ukrepi za zaščito pravic, svoboščin in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki. Poleg tega imajo ti posamezniki pravico, da se na zahtevo seznanijo z razlogi za izvedeno obdelavo osebnih podatkov.[617] V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je naveden primer kreditnega točkovanja. Posamezniki bi morali imeti pravico, da se seznanijo ne le s pozitivno ali negativno odločitvijo v zvezi s točkovanjem, temveč tudi z *razlogi*, na katerih temelji

612 Prav tam, člen 15(1)(h).

613 Prav tam, člen 22(3).

614 Delovna skupina za varstvo podatkov iz člena 29 (2017), *Smernice o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679*, WP 251, 3. oktober 2017.

615 Posodobljena Konvencija št. 108, člen 9(1)(a).

616 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 75.

617 Posodobljena Konvencija št. 108, člen 9(1)(c).

obdelava njihovih osebnih podatkov, ki je privedla do sprejetja take odločitve. Razumevanje teh elementov prispeva k učinkovitemu uresničevanju drugih bistvenih zaščitnih ukrepov, kot sta pravica do ugovora in pravica do vložitve pritožbe pri pristojnem organu.[618]

V Priporočilu o oblikovanju profilov, ki sicer ni pravno zavezujoče, so določeni pogoji za zbiranje in obdelavo osebnih podatkov pri profiliranju.[619] Priporočilo vključuje določbe o potrebi po zagotovitvi, da je obdelava pri oblikovanju profilov poštena, zakonita, sorazmerna ter da se izvaja za določene in zakonite namene. Vključuje tudi določbe o informacijah, ki bi jih morali upravljavci zagotoviti posameznikom, na katere se nanašajo osebni podatki. V priporočilu je poleg tega upoštevano načelo kakovosti podatkov, v skladu s katerim morajo upravljavci sprejeti ukrepe za odpravo dejavnikov netočnosti podatkov, omejiti tveganja ali napake, ki jih lahko povzroči oblikovanje profilov, ter redno ocenjevati kakovost uporabljenih podatkov in algoritmov.

6.2 Pravna sredstva, odgovornost, kazni in odškodnina

Ključni poudarki

- V skladu s posodobljeno Konvencijo št. 108 je treba v nacionalnem pravu pogodbenic določiti ustrezna pravna sredstva in sankcije zoper kršitve pravice do varstva osebnih podatkov.
- V EU so v SUVP določena pravna sredstva, ki so na voljo posameznikom, na katere se nanašajo osebni podatki, v primeru kršitev njihovih pravic, in sankcije zoper upravljavce in obdelovalce, ki ne izpolnjujejo določb navedene uredbe. Poleg tega sta v njej predvideni tudi pravica do odškodnine in odgovornost.
  - Posamezniki, na katere se nanašajo osebni podatki, imajo pravico, da pri nadzornem organu vložijo pritožbo zaradi domnevnih kršitev uredbe, ter pravico do učinkovitega pravnega sredstva in odškodnine.
  - Posameznike lahko pri uveljavljanju pravice do učinkovitega pravnega sredstva zastopajo nepridobitne organizacije, dejavne na področju varstva osebnih podatkov.

618 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 77.

619 Svet Evrope, Priporočilo Rec(2010)13 Odbora ministrov državam članicam o varstvu posameznikov v zvezi z avtomatsko obdelavo osebnih podatkov pri oblikovanju profilov, člen 5(5).

  - Upravljavec ali obdelovalec je odgovoren za vsakršno premoženjsko in nepremoženjsko škodo, ki nastane zaradi kršitve.
  - Nadzorni organi so pooblaščeni za nalaganje upravnih glob za kršitve zadevne uredbe v znesku do 20 000 000 EUR ali v primeru družbe v znesku do 4 % njenega skupnega svetovnega letnega prometa, odvisno od tega, kateri znesek je višji.
- Posamezniki, na katere se nanašajo osebni podatki, lahko kot zadnje sredstvo pod določenimi pogoji pri ESČP vložijo pritožbo zaradi kršitev prava o varstvu osebnih podatkov.
- Vsaka fizična ali pravna oseba ima pravico, da pri SEU vloži pritožbo zoper katero koli odločitev Evropskega odbora za varstvo podatkov pod pogoji, določenimi v Pogodbah.

Sprejetje pravnih instrumentov ne zadostuje za zagotavljanje varstva osebnih podatkov v Evropi. Da bi bila evropska pravila o varstvu osebnih podatkov učinkovita, je treba vzpostaviti mehanizme, ki posameznikom omogočajo, da se odzovejo na kršitve svojih pravic in zahtevajo odškodnino za škodo, ki so jo utrpeli. Pomembno je tudi, da so nadzorni organi pooblaščeni za nalaganje sankcij, ki so učinkovite, odvračilne in sorazmerne z zadevno kršitvijo.

Pravice na podlagi prava o varstvu osebnih podatkov lahko uveljavlja samo oseba, katere pravice so ogrožene, torej posameznik, na katerega se nanašajo osebni podatki. Vendar lahko posameznike, na katere se nanašajo osebni podatki, pri uveljavljanju njihovih pravic zastopajo tudi druge osebe, ki izpolnjujejo potrebne zahteve v skladu z nacionalnim pravom. V več nacionalnih zakonodajah je določeno, da morajo otroke in osebe z motnjami v duševnem razvoju zastopati njihovi skrbniki.[620] V skladu s pravom EU o varstvu osebnih podatkov lahko posameznike, na katere se nanašajo osebni podatki, pred nadzornim organom ali sodiščem zastopajo tudi združenja, katerih zakoniti cilj je spodbujati pravice do varstva osebnih podatkov.[621]

620 FRA (2015), Priročnik o evropskem pravu v zvezi z otrokovimi pravicami, Urad za publikacije Evropske unije, Luxembourg; FRA (2013), Pravna in poslovna sposobnost oseb z motnjami v duševnem razvoju in oseb s težavami z duševnim zdravjem, Urad za publikacije Evropske unije, Luxembourg.

621 SUVP, člen 80.

6.2.1 Pravica do vložitve pritožbe pri nadzornem organu

V skladu s **pravom Sveta Evrope** in **pravom EU** imajo posamezniki pravico, da pri pristojnem nadzornem organu vložijo zahtevke in pritožbe, če menijo, da se obdelava njihovih osebnih podatkov ne izvaja v skladu s pravom.

S posodobljeno Konvencijo št. 108 je priznana pravica posameznikov, na katere se nanašajo osebni podatki, da so pri uveljavljanju svojih pravic po konvenciji deležni pomoči nadzornega organa, in sicer ne glede na njihovo državljanstvo ali prebivališče.[622] Zahteva za pomoč se lahko zavrne le v izjemnih okoliščinah, pri čemer posamezniki, na katere se nanašajo osebni podatki, ne bi smeli kriti stroškov in pristojbin zvezi s pomočjo.[623]

Podobne določbe je mogoče najti v pravnem sistemu EU. V skladu s SUVP morajo nadzorni organi sprejeti ukrepe za olajšanje postopka vložitve pritožb, kot je oblikovanje elektronskega obrazca za vložitev pritožbe.[624] Posameznik, na katerega se nanašajo osebni podatki, lahko vloži pritožbo pri nadzornem organu v državi članici, v kateri ima običajno prebivališče, v kateri je njegov kraj dela ali v kateri je domnevno prišlo do kršitve.[625] Pritožbe je treba preiskati, nadzorni organ pa mora zadevno osebo obvestiti o izidu postopka obravnave zahtevka.[626]

O morebitnih kršitvah, ki jih storijo institucije ali organi EU, je mogoče vložiti pritožbo pri Evropskem nadzorniku za varstvo podatkov.[627] Če ENVP ne odgovori v šestih mesecih, se pritožba šteje za zavrnjeno. Zoper sklepe ENVP je mogoče vložiti pritožbo pri SEU, in sicer na podlagi Uredbe (ES) št. 45/2001, s katero je institucijam in organom EU naložena obveznost spoštovanja pravil o varstvu osebnih podatkov.

Dovoljeno mora biti, da se pri sodiščih vloži pritožba zoper odločbe nacionalnega sodnega organa. To velja za posameznike, na katere se nanašajo osebni podatki, ter upravljavce in obdelovalce, ki so stranka v postopku pred nadzornim organom.

622 Posodobljena Konvencija št. 108, člen 18.

623 Prav tam, člena 16 in 17.

624 SUVP, člen 57(2).

625 Prav tam, člen 77(1).

626 Prav tam, člen 77(2).

627 Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

Primer: španski organ za varstvo podatkov je septembra 2017 družbi Facebook naložil globo zaradi kršitve več predpisov o varstvu osebnih podatkov. Nadzorni organ je obsodil družbeno omrežje zaradi zbiranja, hrambe in obdelave osebnih podatkov, vključno s posebnimi vrstami osebnih podatkov, za namene oglaševanja in brez pridobitve privolitve posameznika, na katerega se nanašajo osebni podatki. Odločitev je temeljila na preiskavi, ki jo je nadzorni organ opravil na lastno pobudo.

6.2.2 Pravica do učinkovitega pravnega sredstva

Poleg pravice do vložitve pritožbe pri nadzornem organu morajo imeti posamezniki tudi pravico do učinkovitega pravnega sredstva in vložitve tožbe pred sodiščem. Pravica do pravnega sredstva je v evropski pravni tradiciji dobro uveljavljena ter je kot temeljna pravica priznana v členu 47 Listine EU o temeljnih pravicah in členu 13 EKČP.[628]

V skladu s pravom EU je treba posameznikom, na katere se nanašajo osebni podatki, zagotoviti učinkovita pravna sredstva v primeru kršitve njihovih pravic, in sicer je to jasno razvidno iz določb SUVP, v kateri je določena pravica do učinkovitega pravnega sredstva zoper nadzorne organe, upravljavce in obdelovalce, in iz sodne prakse SEU.

Primer: SEU je v zadevi *Schrems*[629] razglasilo neveljavnost odločbe o primernosti varnega pristana. S to odločbo je bil omogočen mednarodni prenos osebnih podatkov iz EU organizacijam v ZDA, ki so se samocertificirale v okviru sheme varnega pristana. SEU je menilo, da ima shema varnega pristana več pomanjkljivosti, ki ogrožajo temeljne pravice državljanov EU do varstva zasebnosti, varstva osebnih podatkov in učinkovitega pravnega sredstva.

V zvezi s kršitvijo pravic do zasebnosti in varstva osebnih podatkov je SEU poudarilo, da zakonodaja ZDA nekaterim javnim organom omogoča, da dostopajo do osebnih podatkov, prenesenih iz držav članic v ZDA, ter jih obdelujejo na način, ki ni združljiv s prvotnimi nameni njihovega prenosa, in obširneje, kot bi bilo nujno potrebno in sorazmerno za zaščito nacionalne varnosti. Kar zadeva pravico do učinkovitega pravnega sredstva, je ugotovilo,

628 Glej na primer ESČP, *Karabeyoğlu proti Turčiji*, pritožba št. 30083/10, 7. junij 2016, in ESČP, *Mustafa Sezgin Tanrıkulu proti Turčiji*, pritožba št. 27473/06, 18. julij 2017.

629 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015.

da posamezniki, na katere se nanašajo osebni podatki, nimajo dostopa do upravnega in sodnega varstva, ki bi omogočalo, da pridobijo dostop do osebnih podatkov, ki se nanje nanašajo, in, če bi bilo to potrebno, da dosežejo njihovo popravo ali njihov izbris. SEU je ugotovilo, da ureditev, ki ne določa nobene možnosti uporabe pravnih sredstev za pridobitev dostopa do osebnih podatkov ali njihov popravek ali izbris, „posega v bistvo temeljne pravice do učinkovitega sodnega varstva, določene v členu 47 Listine“. Poudarilo je, da je obstoj pravnega sredstva, ki zagotavlja spoštovanje pravnih pravil, neločljivo povezan z obstojem pravne države.

Posamezniki, upravljavci ali obdelovalci, ki želijo izpodbijati pravno zavezujočo odločitev nadzornega organa, lahko sprožijo postopek pri sodišču.[630] Izraz odločitev bi bilo treba razlagati široko, pri čemer bi moral zajemati izvajanje pooblastil nadzornih organov za preiskovanje in sankcioniranje ter pooblastila v zvezi z dovoljenji, pa tudi odločitve o tem, da se pritožbe zavržejo ali zavrnejo. Vendar ukrepi, ki niso pravno zavezujoči, na primer mnenja, ki jih izdajo nadzorni organi, ali njihovi nasveti, ne morejo biti predmet postopka pred sodiščem.[631] Za postopke zoper zadevni nadzorni organ so pristojna sodišča države članice, v kateri je nadzorni organ ustanovljen.[632]

V primerih, ko upravljavec ali obdelovalec krši pravice posameznikov, na katere se nanašajo osebni podatki, lahko ti posamezniki vložijo tožbo pri sodišču.[633] V zvezi s postopkom, ki se začne zoper upravljavca ali obdelovalca, je zlasti pomembno, da lahko posamezniki izbirajo, kje bodo ta postopek začeli. To lahko storijo v državi članici, v kateri ima upravljavec ali obdelovalec poslovno enoto, ali v državi članici, v kateri imajo zadevni posamezniki, na katere se nanašajo osebni podatki, svoje običajno prebivališče.[634] Druga možnost posameznikom močno olajša uveljavljanje njihovih pravic, saj jim omogoča, da postopek začnejo v državi, v kateri prebivajo, in v okviru znane jurisdikcije. Če bi kraj, v katerem se lahko začne postopek zoper upravljavce in obdelovalce, omejili na državo članico, v kateri imajo ti poslovno enoto, bi to lahko posameznike, na katere se nanašajo osebni podatki in ki prebivajo v drugih državah članicah, odvrnilo od tega, da začnejo sodni postopek, saj bi to pomenilo potne in dodatne stroške, postopek pa bi lahko potekal v tujem jeziku in v okviru tuje jurisdikcije. Edina izjema se nanaša na primere, v katerih je upravljavec ali obdelovalec

630 SUVP, člen 78.

631 Prav tam, uvodna izjava 143.

632 Prav tam, člen 78(3).

633 Prav tam, člen 79.

634 Prav tam, člen 79(2).

javni organ in se obdelava opravlja v okviru izvajanja njegovih javnih pooblastil. V tem primeru so za obravnavo tožbe pristojna le sodišča države zadevnega javnega organa.[635]

Čeprav se v večini primerov o zadevah v zvezi s pravili o varstvu osebnih podatkov odloča na sodiščih držav članic, se lahko nekatere zadeve predložijo SEU. To se lahko zgodi, kadar posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec ali nadzorni organ vloži tožbo za razveljavitev odločitve Evropskega odbora za varstvo podatkov. Vendar za tožbo veljajo pogoji iz člena 263 PDEU, kar pomeni, da je dopustna le, če lahko ti posamezniki in subjekti dokažejo, da se odločitev Odbora nanje nanaša neposredno in posamično.

Druga možnost se nanaša na primere, v katerih institucije ali organi EU nezakonito obdelujejo osebne podatke. Posamezniki, na katere se nanašajo osebni podatki, lahko v primerih, ko institucije EU kršijo pravo o varstvu osebnih podatkov, tožbo vložijo neposredno pri Splošnem sodišču EU (Splošno sodišče je del SEU). Splošno sodišče je odgovorno za obravnavo tožb zaradi kršitev prava EU, ki jih storijo institucije EU, na prvi stopnji. Zato se lahko tožbe zoper Evropskega nadzornika za varstvo podatkov kot institucijo EU vložijo tudi pred Splošnim sodiščem.[636]

Primer: v zadevi *Bavarian Lager*[637] je zadevna družba Evropsko komisijo zaprosila za dostop do celotnega zapisnika sestanka Komisije, ki naj bi se domnevno nanašal na pravna vprašanja, pomembna za družbo. Komisija je prošnjo družbe za dostop zavrnila na podlagi prevladujočih interesov varstva osebnih podatkov.[638] Družba Bavarian Lager je na podlagi člena 32 uredbe o varstvu osebnih podatkov v institucijah EU zoper to odločitev vložila pritožbo pri Sodišču prve stopnje (predhodniku Splošnega sodišča). Sodišče prve stopnje je z odločitvijo (v zadevi T-194/04, *The Bavarian Lager Co. Ltd proti Komisiji Evropskih skupnosti*) odločbo Komisije, s katero je bila zavrnjena prošnja za dostop, razglasilo za nično. Evropska komisija se je zoper to odločitev pritožila pri SEU.

635 Prav tam.

636 Uredba (ES) št. 45/2001, člen 32(3).

637 SEU, *Evropska komisija proti The Bavarian Lager Co. Ltd.* (veliki senat), C-28/08 P, 2010.

638 Za analizo utemeljitve glej ENVP (2011), *Dostop javnosti do dokumentov, ki vsebujejo osebne podatke, po odločitvi Sodišča v zadevi Bavarian Lager*, Bruselj.

SEU (veliki senat) je razveljavilo sodbo Sodišča prve stopnje in potrdilo odločitev Evropske komisije, in sicer da zavrne prošnjo za dostop do celotnega zapisnika sestanka, da bi zaščitila osebne podatke oseb na sestanku. SEU je menilo, da je Komisija ravnala pravilno, ko je zavrnila razkritje teh informacij, saj udeleženci sestanka niso privolili v razkritje svojih osebnih podatkov. Poleg tega družba Bavarian Lager ni dokazala potrebe po dostopu do teh informacij.

Posamezniki, na katere se nanašajo osebni podatki, upravljavci ali obdelovalci lahko nacionalno sodišče v postopku pred njim zaprosijo, naj od SEU zahteva pojasnilo glede razlage in veljavnosti aktov institucij, organov, uradov ali agencij EU. Taka pojasnila se imenujejo predhodne odločbe. Za pritožnika to ni neposredno pravno sredstvo, vendar nacionalnim sodiščem omogoča, da zagotovijo, da uporabijo pravilno razlago prava EU. Prav na podlagi tega mehanizma predhodnega odločanja so bile SEU predložene ključne zadeve, kot na primer *Digital Rights Ireland* in *Kärntner Landesregierung in drugi*[639] ter *Schrems*[640], ki so močno vplivale na razvoj prava EU o varstvu osebnih podatkov.

Primer: *Digital Rights Ireland* in *Kärntner Landesregierung in drugi*[641] sta bili združeni zadevi, ki sta ju predložili irsko višje sodišče in avstrijsko ustavno sodišče v zvezi s skladnostjo Direktive 2006/24/ES (direktiva o hrambi podatkov) s pravom EU o varstvu osebnih podatkov. Avstrijsko ustavno sodišče je SEU predložilo vprašanja v zvezi z veljavnostjo členov 3 do 9 Direktive 2006/24/ES z vidika členov 7, 9 in 11 Listine EU o temeljnih pravicah. Eno od predloženih vprašanj je bilo, ali so nekatere določbe avstrijskega zveznega zakona o telekomunikacijah, s katerim je bila prenesena direktiva o hrambi podatkov, nezdružljive z vidiki prejšnje direktive o varstvu osebnih podatkov in uredbe o varstvu osebnih podatkov v institucijah EU.

V zadevi *Kärntner Landesregierung in drugi* je M. Seitlinger, eden od pritožnikov v postopku pred ustavnim sodiščem, trdil, da telefon, internet in e-pošto uporablja na delovnem mestu in v zasebnem življenju. Informacije, ki jih je pošiljal in prejemal, so se zato prenašale prek javnih telekomunikacijskih

639 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim in Kärntner Landesregierung in drugi* (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014.

640 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015.

641 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim in Kärntner Landesregierung in drugi* (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014.

omrežij. Njegov ponudnik telekomunikacijskih storitev je moral na podlagi avstrijskega zakona o telekomunikacijah iz leta 2003 po zakonu zbirati in shranjevati podatke o njegovi uporabi omrežja. M. Seitlinger je menil, da zbiranje in shranjevanje njegovih osebnih podatkov nista nujna za tehnični vidik pošiljanja in prejemanja informacij v omrežju. Poleg tega zbiranje in shranjevanje navedenih podatkov nista bila potrebna za obračunavanje. M. Seitlinger je trdil, da ni privolil v to uporabo osebnih podatkov, ki so se zbirali in shranjevali samo zaradi avstrijskega zakona o telekomunikacijah iz leta 2003.

M. Seitlinger je zato pri avstrijskem ustavnem sodišču vložil tožbo, v kateri je trdil, da se z zakonskimi obveznostmi njegovega ponudnika telekomunikacijskih storitev kršijo njegove temeljne pravice na podlagi člena 8 Listine EU o temeljnih pravicah. Ker se je z avstrijsko zakonodajo izvajalo pravo EU (tedanja direktiva o hrambi podatkov), je avstrijsko ustavno sodišče zadevo predložilo Sodišču EU, da bi odločilo o skladnosti direktive s pravicama do zasebnosti in varstva osebnih podatkov, določenima v Listini EU o temeljnih pravicah.

Veliki senat SEU je odločil o zadevi, kar je imelo za posledico razglasitev neveljavnosti direktive EU o hrambi podatkov. SEU je ugotovilo, da zadevna direktiva pomeni posebej resno poseganje v temeljni pravici do zasebnosti in varstva osebnih podatkov, pri čemer navedeno poseganje ni omejeno na to, kar je nujno potrebno. Direktiva je uresničevala zakonit cilj, saj je nacionalnim organom omogočala dodatne možnosti za preiskovanje in pregon hudih kaznivih dejanj, zato je bila dragoceno orodje za kazenske preiskave. Vendar je SEU ugotovilo, da bi se morale omejitve temeljnih pravic uporabljati le, če so nujno potrebne, pri čemer bi bilo treba skupaj z njimi določiti jasna in natančna pravila glede njihovega obsega ter zaščitne ukrepe za posameznike.

SEU je menilo, da ta direktiva ni prestala tega preizkusa nujnosti. Prvič, v njej niso bila določena jasna in natančna pravila za omejitev obsega poseganja. Namesto da bi se z zadevno direktivo zahtevala povezava med hranjenimi podatki in hudim kaznivim dejanjem, se je ta uporabljala za vse metapodatke vseh uporabnikov vseh elektronskih komunikacijskih sredstev. Zato je pomenila poseganje v pravici do zasebnosti in varstva osebnih podatkov tako rekoč celotnega prebivalstva EU, kar bi se lahko štelo za nesorazmerno. Direktiva ni vsebovala pogojev za omejitev števila oseb, pooblaščenih za dostop do osebnih podatkov, poleg tega se za tak dostop niso uporabljali vsebinski in

postopkovni pogoji, kot je zahteva, da se pred dostopom pridobi odobritev upravnega organa ali sodišča. V njej niso bili določeni jasni zaščitni ukrepi za varstvo hranjenih podatkov. Direktiva zato ni zagotavljala učinkovitega varstva teh podatkov pred tveganji zlorabe ter vsakršnim nezakonitim dostopom do teh podatkov in njihovo nezakonito uporabo.[642]

SEU mora načeloma odgovoriti na vprašanja, ki so mu predložena, in sprejetja predhodne odločbe ne more zavrniti z obrazložitvijo, da bi bil tak odgovor za prvotno zadevo brezpredmeten in prepozen. Lahko pa to zavrne, če vprašanje ne spada pod njegovo pristojnost.[643] SEU odloča samo o sestavnih elementih predloga za sprejetje predhodne odločbe, ki mu je predložen, za odločanje o prvotni zadevi pa je še naprej pristojno nacionalno sodišče.[644]

V skladu s **pravom Sveta Evrope** morajo pogodbenice določiti ustrezna sodna in izvensodna pravna sredstva za kršitve določb posodobljene Konvencije št. 108.[645] Očitki o kršitvah pravic do varstva osebnih podatkov, ki pomenijo kršitev člena 8 EKČP, zoper pogodbenico se po uporabi vseh razpoložljivih nacionalnih pravnih sredstev obravnavajo tudi pred ESČP. Za sklicevanje na kršitev člena 8 EKČP pred ESČP morajo biti izpolnjena tudi druga merila dopustnosti (člena 34 in 35 EKČP).[646]

Čeprav je mogoče pri ESČP vložiti samo pritožbe zoper pogodbenice, se lahko z njimi posredno obravnavajo tudi dejanja ali opustitve zasebnih strank, če pogodbenica ni izpolnila pozitivnih obveznosti, ki jih ima na podlagi EKČP, in v nacionalnem pravu ni zagotovila zadostnega varstva pred kršitvami pravic do varstva osebnih podatkov.

Primer: v zadevi *K. U. proti Finski*[647] je pritožnik, mladoletna oseba, zatrjeval, da je bil na spletni strani za zmenke o njem objavljen oglas spolne narave. Ponudnik storitve zaradi obveznosti glede zaupnosti po finski zakonodaji ni

642 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim* in Kärntner Landesregierung in drugi (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014, točka 66.

643 SEU, *Pasquale Foglia proti Marielli Novello (št. 2)*, C-244/80, 16. december 1981, in SEU, *Kazenski postopek proti Gaspariniju in drugim*, C-467/04, 28. september 2006.

644 SEU, *International Transport Workers' Federation in Finnish Seamen's Union proti Viking Line ABP in OÜ Viking Line Eesti* (veliki senat), C-438/05, 11. december 2007, točka 85.

645 Posodobljena Konvencija št. 108, člen 12.

646 EKČP, členi 34–37.

647 ESČP, *K. U. proti Finski*, pritožba št. 2872/02, 2. december 2008.

razkril identitete osebe, ki je objavila informacije. Pritožnik je trdil, da finska zakonodaja ne zagotavlja zadostnega varstva pred takimi dejanji fizične osebe, ki je na spletu objavila obremenilne podatke o pritožniku. ESČP je odločilo, da se morajo države ne samo vzdržati samovoljnega poseganja v zasebno življenje posameznikov, ampak lahko zanje poleg tega veljajo pozitivne obveznosti, ki vključujejo sprejetje ukrepov za zagotovitev spoštovanja zasebnega življenja tudi v okviru medosebnih odnosov med posamezniki. V pritožnikovem primeru je bilo treba zaradi njegovega dejanskega in učinkovitega varstva sprejeti učinkovite ukrepe za ugotovitev identitete storilca in njegov pregon. Vendar država takega varstva ni zagotovila, zato je Sodišče ugotovilo, da je bil kršen člen 8 EKČP.

Primer: v zadevi *Köpke proti Nemčiji*[648] je bila pritožnica osumljena tatvine na delovnem mestu, zato je bila podvržena tajnemu videonadzoru. ESČP je ugotovilo, da ni mogoče sklepati, da nacionalnim organom v okviru pravice do proste presoje ni uspelo doseči pravičnega ravnotežja med pritožničino pravico do spoštovanja zasebnega življenja na podlagi člena 8 ter interesom njenega delodajalca za varstvo lastninskih pravic in javnim interesom za pravilno izvrševanje javne oblasti. Pritožba je bila zato razglašena za nedopustno.

Če ESČP ugotovi, da je pogodbenica kršila katero od pravic, ki so zavarovane z EKČP, mora navedena pogodbenica izvršiti sodbo ESČP (člen 46 EKČP). Z izvršilnimi ukrepi je treba najprej ustaviti kršitev in čim bolj odpraviti njene negativne posledice za pritožnika. Pri izvrševanju sodb so lahko potrebni tudi splošni ukrepi za preprečitev podobnih kršitev, kot jih je ugotovilo Sodišče, bodisi s spremembami zakonodaje in sodne prakse bodisi z drugimi ukrepi.

Če ESČP ugotovi kršitev EKČP, člen 41 EKČP določa, da lahko pritožniku nakloni pravično zadoščenje na stroške pogodbenice.

Pravica do pooblastitve nepridobitnega telesa, organizacije ali združenja

V skladu s SUVP lahko posamezniki, ki vložijo pritožbo pri nadzornem organu ali tožbo pri sodišču, pooblastijo nepridobitno telo, organizacijo ali združenje, da jih

648 ESČP, *Köpke proti Nemčiji*, pritožba št. 420/07, sklep z dne 5. oktobra 2010.

zastopa.[649] Ti nepridobitni subjekti morajo imeti s pravnimi akti določene cilje v javnem interesu in biti dejavni na področju varstva osebnih podatkov. V imenu posameznikov, na katere se nanašajo osebni podatki, lahko vložijo pritožbo ali uveljavljajo pravico do pravnega sredstva. V skladu z navedeno uredbo lahko države članice v skladu z nacionalnim pravom določijo, ali ima tako telo neodvisno od pooblastila posameznikov, na katere se nanašajo osebni podatki, pravico, da vlaga pritožbe v njihovem imenu.

Ta pravica do zastopanosti posameznikom omogoča, da izkoristijo strokovno znanje ter organizacijsko in finančno sposobnost takih nepridobitnih subjektov, s čimer se posameznikom močno olajša uveljavljanje njihovih pravic. V skladu s SUVP lahko ti subjekti vlagajo kolektivne tožbe v imenu več posameznikov, na katere se nanašajo osebni podatki. To koristi tudi delovanju in učinkovitosti pravosodnega sistema, saj se sorodne tožbe združijo in obravnavajo skupaj.

6.2.3 Odgovornost in pravica do odškodnine

Pravica do učinkovitega pravnega sredstva mora posameznikom omogočati, da zahtevajo odškodnino za škodo, ki nastane zaradi obdelave njihovih osebnih podatkov na način, ki je v nasprotju z veljavno zakonodajo. V SUVP je izrecno določena odgovornost upravljavcev in obdelovalcev za nezakonito obdelavo.[650] V skladu z navedeno uredbo imajo posamezniki pravico, da od upravljavca ali obdelovalca dobijo odškodnino za nastalo premoženjsko in nepremoženjsko škodo, pri čemer je v njenih uvodnih izjavah navedeno, da bi bilo treba „[p]ojem škode […] razlagati široko ob upoštevanju sodne prakse Sodišča na način, ki v celoti odraža cilje te uredbe“.[651] Upravljavci so odgovorni in nanje se lahko naslovijo odškodninski zahtevki, če ne izpolnjujejo svojih obveznosti po navedeni uredbi. Obdelovalec osebnih podatkov je odgovoren za škodo, ki jo povzroči obdelava, le, kadar ne izpolnjuje obveznosti iz navedene uredbe, ki so posebej namenjene obdelovalcem, ali kadar je prekoračil zakonita navodila upravljavca ali ravnal v nasprotju z njimi. Kadar je upravljavec ali obdelovalec plačal celotno odškodnino, lahko v skladu s SUVP od drugih upravljavcev ali obdelovalcev, vključenih v isto obdelavo, zahteva povračilo tistega dela odškodnine, ki ustreza njihovemu delu odgovornosti za škodo.[652] Hkrati so izjeme od

649 SUVP, člen 80.

650 Prav tam, člen 82.

651 Prav tam, uvodna izjava 146.

652 Prav tam, člen 82(2) in (5).

odgovornosti zelo stroge, pri čemer je za njihovo uporabo treba dokazati, da upravljavec ali obdelovalec ni nikakor odgovoren za dogodek, ki je povzročil škodo.

Odškodnina mora biti celotna in učinkovita v zvezi z nastalo škodo. Kadar škoda nastane zaradi obdelave, v katero je vključenih več upravljavcev in obdelovalcev, mora biti vsak upravljavec ali obdelovalec odgovoren za celotno škodo. Cilj tega pravila je zagotoviti učinkovito odškodnino za posameznika, na katerega se nanašajo osebni podatki, ter usklajen pristop upravljavcev in obdelovalcev, vključenih v dejavnosti obdelave, k skladnosti.

Primer: posameznikom, na katere se nanašajo osebni podatki, ni treba sprožiti postopka in zahtevati odškodnino od vseh subjektov, ki so odgovorni za škodo, saj bi to lahko pomenilo drag in dolgotrajen postopek. Zadostuje, če se začne postopek zoper enega od skupnih upravljavcev, ki ga je nato mogoče šteti za odgovornega za celotno škodo. V takih primerih ima upravljavec ali obdelovalec, ki plača odškodnino, pravico, da plačani znesek pozneje izterja od drugih subjektov, ki so bili vključeni v obdelavo in so odgovorni za kršitev, in sicer za njihov del odgovornosti za škodo. Ta postopek med različnimi skupnimi upravljavci in obdelovalci poteka po tem, ko posameznik, na katerega se nanašajo osebni podatki, prejme odškodnino, pri čemer ta posameznik v postopku ne sodeluje.

V pravnem okviru Sveta Evrope morajo pogodbenice v skladu s členom 12 posodobljene Konvencije št. 108 vzpostaviti ustrezna pravna sredstva za kršitve nacionalnega prava, s katerim se izvajajo zahteve konvencije. V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je navedeno, da morajo pravna sredstva vključevati možnost sodnega izpodbijanja odločitve ali prakse, pri čemer morajo biti na voljo tudi izvensodna pravna sredstva.[653] Podrobnosti in različna pravila v zvezi z dostopom do teh pravnih sredstev so skupaj s postopkom, ki ga je treba upoštevati, prepuščena presoji vsake pogodbenice. Pogodbenice in nacionalna sodišča bi morali razmisliti tudi o določbah o finančni odškodnini za premoženjsko in nepremoženjsko škodo, ki jo povzroči obdelava, ter možnosti, da se omogočijo kolektivne tožbe.[654]

653 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 100.

654 Prav tam.

6.2.4 Sankcije

V okviru prava Sveta Evrope člen 12 posodobljene Konvencije št. 108 določa, da mora vsaka pogodbenica določiti ustrezne sankcije in pravna sredstva za kršitve določb nacionalne zakonodaje, s katerimi se uresničujejo temeljna načela varstva osebnih podatkov, določena v Konvenciji št. 108. Z njo ni določen ali naložen poseben sklop sankcij. Nasprotno, v njej je jasno navedeno, da ima vsaka pogodbenica diskrecijsko pravico, da določi vrsto sodnih ali izvensodnih sankcij, ki so lahko kazenske, upravne ali civilnopravne. V Pojasnjevalnem poročilu k posodobljeni Konvenciji št. 108 je določeno, da morajo biti sankcije učinkovite, sorazmerne in odvračilne.[655] Pogodbenice morajo to načelo spoštovati, kadar določajo vrsto in težo sankcij, ki so na voljo v njihovem nacionalnem pravnem redu.

V okviru prava EU so nadzorni organi držav članic na podlagi člena 83 SUVP pooblaščeni za nalaganje upravnih glob v zvezi s kršitvami navedene uredbe. V tem členu so določene tudi višina glob in okoliščine, ki jih nacionalni organi upoštevajo pri odločanju o tem, ali naj se naloži upravna globa, pa tudi skupne zgornje meje te globe. Sistem sankcij je zato usklajen po vsej EU.

V SUVP se uporablja stopenjski pristop h globam. Nadzorni organi so pooblaščeni za nalaganje upravnih glob za kršitve zadevne uredbe v znesku do 20 000 000 EUR ali v primeru družbe v znesku do 4 % njenega skupnega svetovnega letnega prometa, odvisno od tega, kateri znesek je višji. Kršitve, ki lahko privedejo do naložitve globe te stopnje, vključujejo kršitve osnovnih načel obdelave in pogojev za privolitev ter kršitve pravic posameznikov, na katere se nanašajo osebni podatki, in določb navedene uredbe, ki urejajo prenos osebnih podatkov uporabnikom v tretjih državah. Nadzorni organi lahko za druge kršitve naložijo upravne globe v znesku do 10 000 000 EUR ali v primeru družbe v znesku do 2 % njenega skupnega svetovnega letnega prometa, odvisno od tega, kateri znesek je višji.

Nadzorni organi morajo pri določanju vrste in višine globe, ki jo bodo naložili, upoštevati več dejavnikov.[656] Ustrezno morajo upoštevati na primer naravo, težo in trajanje kršitve, vrste osebnih podatkov, ki jih zadeva kršitev, in to, ali je bila kršitev naklepna ali posledica malomarnosti. Če je upravljavec ali obdelovalec sprejel ukrepe za ublažitev škode, ki so jo utrpeli posamezniki, na katere se nanašajo osebni podatki, bi bilo treba upoštevati tudi ta dejavnik. Pomembna sta tudi druga dejavnika, na katera se nadzorni organi opirajo pri odločanju, in sicer stopnja sodelovanja z nadzornim

655 Prav tam.

656 SUVP, člen 83(2).

organom po kršitvi in način, kako se je nadzorni organ seznanil s kršitvijo (na primer, ali ga je obvestil subjekt, odgovoren za obdelavo, ali posameznik, na katerega se nanašajo osebni podatki in katerega pravice so bile kršene).[657]

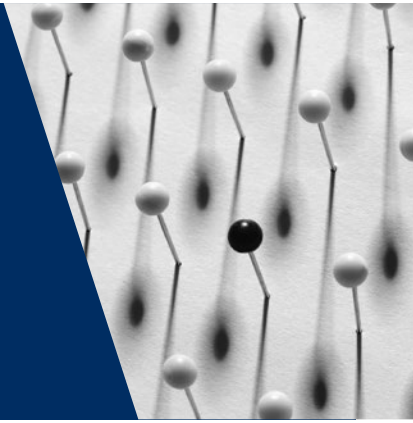
Nadzorni organi imajo poleg pristojnosti za nalaganje upravnih glob na voljo najrazličnejša druga t. i. popravljalna pooblastila. Določena so v členu 58 SUVP, segajo pa od izdajanja odredb, opozoril in opominov upravljavcem in obdelovalcem do uvedbe začasne ali celo dokončne prepovedi dejavnosti obdelave.

Kar zadeva sankcije za kršitve prava EU, ki jih storijo institucije ali organi EU, so te zaradi posebne vloge uredbe o varstvu osebnih podatkov v institucijah EU lahko predvidene samo kot disciplinski ukrepi. V skladu s členom 49 navedene uredbe je „[z]a vsako neizpolnjevanje obveznosti v skladu s to uredbo, bodisi namerno ali iz malomarnosti, […] uradnik ali drugi uslužbenec Evropskih skupnosti disciplinsko odgovoren […]".

657 Delovna skupina za varstvo podatkov iz člena 29 (2017), *Smernice o uporabi in določanju upravnih glob za namene Uredbe 2016/679*, WP 253, 3. oktober 2017.

7

Mednarodni prenosi osebnih podatkov



EU	Obravnavane teme	Svet Evrope
Prenosi osebnih podatkov		
SUVP, člen 44	Koncept	Posodobljena Konvencija št. 108, člen 14(1) in (2)
Prosti pretok osebnih podatkov		
SUVP, člen 1(3) in uvodna izjava 170	Med državami članicami EU	
	Med pogodbenicami Konvencije št. 108	Posodobljena Konvencija št. 108, člen 14(1)
Prenosi osebnih podatkov v tretje države ali mednarodne organizacije		
SUVP, člen 45 SEU, C-362/14, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), 2015	Sklep o ustreznosti/tretje države ali mednarodne organizacije z ustrezno ravnjo varstva	Posodobljena Konvencija št. 108, člen 14(2)
SUVP, člen 46(1) in (2)	Ustrezni zaščitni ukrepi, vključno z izvršljivimi pravicami in pravnimi sredstvi za posameznike, na katere se nanašajo osebni podatki, ki se zagotavljajo s standardnimi pogodbenimi določili, zavezujočimi poslovnimi pravili, kodeksi ravnanja in mehanizmi certificiranja	Posodobljena Konvencija št. 108, člen 14(2), (3), (5) in (6)
SUVP, člen 46(3)	Z dovoljenjem pristojnega nadzornega organa: pogodbena določila in določbe, vključene v upravne dogovore med javnimi organi	

EU	Obravnavane teme	Svet Evrope
SUVP, člen 46(5)	Obstoječa dovoljenja na podlagi Direktive 95/46/ES	
SUVP, člen 47	Zavezujoča poslovna pravila	
SUVP, člen 49	Odstopanja v posebnih primerih	Posodobljena Konvencija št. 108, člen 14(4)
Primeri: Sporazum med EU in ZDA o evidenci imen letalskih potnikov (PNR) Sporazum med EU in ZDA o dostopu do finančnih podatkov (SWIFT)	Mednarodni sporazumi	Posodobljena Konvencija št. 108, člen 14(3)(a)

V okviru prava EU je v SUVP določen prosti pretok podatkov v Evropski uniji. Vendar ta uredba vsebuje posebne zahteve glede prenosov osebnih podatkov v tretje države zunaj EU in mednarodne organizacije. V njej je priznan pomen takih prenosov, zlasti zaradi mednarodne trgovine in sodelovanja, priznano pa je tudi povečano tveganje za osebne podatke. Njen cilj je zato zagotoviti enako raven varstva osebnih podatkov, ki se prenašajo v tretje države, kot je v zvezi z njimi zagotovljena v EU.[658] Tudi v pravu Sveta Evrope je priznan pomen izvedbenih pravil za čezmejni prenos osebnih podatkov, ki temelji na prostem pretoku med pogodbenicami in posebnih zahtevah za prenos osebnih podatkov nepogodbenicam.

7.1 Narava prenosov osebnih podatkov

Ključna poudarka

- Pravo EU in pravo Sveta Evrope vsebujeta pravila o prenosih osebnih podatkov uporabnikom v tretjih državah ali mednarodnim organizacijam.
- Zagotavljanje varstva pravic posameznikov, na katere se nanašajo osebni podatki, pri prenosu osebnih podatkov zunaj EU omogoča, da se varstvo, zagotovljeno s pravom EU, še naprej uporablja za osebne podatke, ki izvirajo iz EU.

V okviru **prava Sveta Evrope** je čezmejni prenos osebnih podatkov opisan kot prenos osebnih podatkov uporabnikom, ki so pod tujo jurisdikcijo.[659] Čezmejni prenos

658 SUVP, uvodni izjavi 101 in 116.

659 Pojasnjevalno poročilo k posodobljeni Konvenciji št. 108, točka 102.

osebnih podatkov uporabniku, ki ni pod jurisdikcijo pogodbenice, je dovoljen le, če je zagotovljena ustrezna raven varstva.[660]

S **pravom EU** so urejeni prenosi „osebnih podatkov, ki se obdelujejo ali so namenjeni obdelavi po prenosu v tretjo državo ali mednarodno organizacijo […]".[661] Taki prenosi osebnih podatkov so dovoljeni le, če so v skladu s pravili iz poglavja V SUVP.

Dovoljeni so čezmejni prenosi osebnih podatkov uporabniku, ki je v skladu s pravom Sveta Evrope oziroma pravom EU pod jurisdikcijo pogodbenice ali države članice. V okviru obeh pravnih sistemov je dovoljen tudi prenos osebnih podatkov v državo, ki ni pogodbenica ali država članica, če so izpolnjeni določeni pogoji.

7.2 Prosti pretok osebnih podatkov med državami članicami ali pogodbenicami

Ključni poudarek

- Prenos osebnih podatkov v EU in med pogodbenicami posodobljene Konvencije št. 108 ne sme biti omejen. Ker pa vse pogodbenice posodobljene Konvencije št. 108 niso države članice EU, so prenosi iz države članice EU v tretjo državo, ki pa je pogodbenica posodobljene Konvencije št. 108, mogoči le, če so izpolnjeni pogoji iz SUVP.

V skladu s pravom Sveta Evrope je treba med pogodbenicami posodobljene Konvencije št. 108 zagotoviti prosti pretok osebnih podatkov. Vendar je prenos mogoče prepovedati, če obstaja resno in dejansko tveganje, da bi prenos osebnih podatkov drugi pogodbenici privedel do izogibanja določbam konvencije ali če je pogodbenica to zavezana storiti na podlagi usklajenih pravil o varstvu, ki so skupna državam, ki pripadajo regionalni mednarodni organizaciji.[662]

Po pravu EU so prepovedane omejitve ali prepovedi prostega pretoka osebnih podatkov med državami članicami EU iz razlogov, povezanih z varstvom posameznikov pri obdelavi osebnih podatkov.[663] Območje prostega pretoka osebnih podatkov je

660 Posodobljena konvencija št. 108, člen 14(2).

661 SUVP, člen 44.

662 Posodobljena konvencija št. 108, člen 14(1).

663 SUVP, člen 1(3).

bilo razširjeno s Sporazumom o Evropskem gospodarskem prostoru (EGP)[664], s katerim so se na notranji trg vključili Islandija, Lihtenštajn in Norveška.

Primer: če odvisna družba mednarodne skupine družb, ki ima poslovne enote v več državah članicah EU, med drugim v Sloveniji in Franciji, iz Slovenije v Francijo prenese osebne podatke, tak prenos podatkov ne sme biti omejen ali prepovedan s slovensko nacionalno zakonodajo iz razlogov, povezanih z varstvom osebnih podatkov.

Če pa želi ista slovenska odvisna družba iste osebne podatke prenesti matični družbi v Maleziji, mora slovenski izvoznik osebnih podatkov upoštevati pravila iz poglavja V SUVP. Namen teh določb je varovati osebne podatke posameznikov, na katere se nanašajo in ki so pod jurisdikcijo EU.

V skladu s pravom EU se za prenose osebnih podatkov v države članice EGP za namene, povezane s preprečevanjem, preiskovanjem, odkrivanjem ali pregonom kaznivih dejanj ali izvrševanjem kazenskih sankcij, uporablja Direktiva (EU) 2016/680.[665] Z njo se tudi zagotavlja, da izmenjava osebnih podatkov med pristojnimi organi v Uniji ni omejena ali prepovedana zaradi varstva osebnih podatkov. V skladu s pravom Sveta Evrope je na področje uporabe Konvencije št. 108 vključena obdelava vseh osebnih podatkov (vključno z njihovim čezmejnim prenosom v druge pogodbenice Konvencije št. 108), in sicer brez izjem na podlagi namena ali področja ukrepanja, čeprav lahko pogodbenice določijo izjeme. Vse države članice EGP so tudi pogodbenice Konvencije št. 108.

664 Sklep Sveta in Komisije z dne 13. decembra 1993 o sklenitvi Sporazuma o Evropskem gospodarskem prostoru med Evropskimi skupnostmi in njihovimi državami članicami na eni strani in Republiko Avstrijo, Republiko Finsko, Republiko Islandijo, Kneževino Lihtenštajn, Kraljevino Norveško, Kraljevino Švedsko in Švicarsko konfederacijo na drugi strani (UL L 1, 3.1.1994, str. 1).

665 Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

7.3 Prenosi osebnih podatkov v tretje države/nepogodbenice ali mednarodne organizacije

Ključna poudarka

- **Svet Evrope** in **EU** dovoljujeta prenose osebnih podatkov v tretje države ali mednarodne organizacije, če so izpolnjeni določeni pogoji za varstvo osebnih podatkov.
  - **V skladu s pravom Sveta Evrope** je ustrezno raven varstva mogoče zagotoviti s pravom države ali mednarodne organizacije ali z vzpostavitvijo ustreznih standardov.
  - **V skladu s pravom EU** se prenosi lahko izvajajo, če tretja država zagotavlja ustrezno raven varstva ali če upravljavec ali obdelovalec osebnih podatkov zagotovi ustrezne zaščitne ukrepe, vključno z izvršljivimi pravicami posameznikov, na katere se nanašajo osebni podatki, in pravnimi sredstvi, na primer s standardnimi določili o varstvu osebnih podatkov ali zavezujočimi poslovnimi pravili.
- **V pravu Sveta Evrope in pravu EU** so določena odstopanja, ki omogočajo prenos osebnih podatkov v posebnih okoliščinah, tudi če niso vzpostavljeni niti ustrezna raven varstva niti ustrezni zaščitni ukrepi.

Čeprav so s pravom Sveta Evrope in pravom EU omogočeni prenosi osebnih podatkov v tretje države ali mednarodne organizacije, pa so z njima določeni različni pogoji. V obojih pogojih so upoštevani različna struktura in nameni zadevne organizacije.

V skladu s **pravom EU** načeloma obstajata dva načina, kako omogočiti prenos osebnih podatkov v tretje države ali mednarodne organizacije. Prenos osebnih podatkov lahko poteka na podlagi sklepa o ustreznosti, ki ga sprejme Evropska komisija,[666] ali, če tak sklep o ustreznosti ni sprejet, kadar upravljavec ali obdelovalec zagotovi ustrezne zaščitne ukrepe, vključno z izvršljivimi pravicami in pravnimi sredstvi za posameznika, na katerega se nanašajo osebni podatki.[667] Če sklep o ustreznosti ni sprejet ali pa niso sprejeti ustrezni zaščitni ukrepi, je na voljo več odstopanj.

V skladu s **pravom Sveta Evrope** pa so prosti prenosi osebnih podatkov nepogodbenicam konvencije dovoljeni le na podlagi:

666 SUVP, člen 45.

667 Prav tam, člen 46.

- prava zadevne države ali mednarodne organizacije, vključno z veljavnimi mednarodnimi pogodbami ali sporazumi, ki zagotavljajo ustrezne zaščitne ukrepe;

- *ad hoc* ali odobrenih standardiziranih zaščitnih ukrepov, ki se zagotavljajo s pravno zavezujočimi in izvršljivimi instrumenti, ki jih sprejmejo in izvajajo osebe, vključene v prenos in nadaljnjo obdelavo.[668]

Kadar ustrezna raven varstva osebnih podatkov ni zagotovljena, je podobno kot v okviru prava EU na voljo več odstopanj.

7.3.1 Prenosi na podlagi sklepa o ustreznosti

V okviru prava EU je prosti pretok osebnih podatkov v tretje države z ustrezno ravnjo varstva osebnih podatkov določen v členu 45 SUVP. SEU je pojasnilo, da mora tretja država v skladu z izrazom ustrezna raven varstva zagotavljati raven varstva temeljnih pravic in svoboščin, ki je v bistvenem enaka[669] jamstvom, ki se zagotavljajo s pravom v EU. Hkrati, čeprav so sredstva, ki jih tretja država uporabi za zagotovitev take ravni varstva, lahko drugačna od sredstev, ki se uporabljajo v EU, standard ustreznosti ne zahteva dobesednega prepisa pravil EU.[670]

Evropska komisija ocenjuje raven varstva osebnih podatkov v tujih državah s proučitvijo njihovega nacionalnega prava in veljavnih mednarodnih obveznosti. Upoštevati je treba tudi sodelovanje države v večstranskih ali regionalnih sistemih, zlasti v zvezi z varstvom osebnih podatkov. Če Evropska komisija ugotovi, da tretja država ali mednarodna organizacija zagotavlja ustrezno raven varstva, lahko izda sklep o ustreznosti, ki ima zavezujoč učinek.[671] SEU je kljub temu navedlo, da so nacionalni nadzorni organi še vedno pristojni za proučitev zahteve posameznika v zvezi z varstvom njegovih osebnih podatkov, ki so bili preneseni v tretjo državo, za katero Komisija meni, da zagotavlja ustrezno raven varstva, kadar ta posameznik zatrjuje,

668 Posodobljena Konvencija št. 108, člen 14(3)(a) in (b).

669 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015, točka 96.

670 Prav tam, točka 74. Glej tudi Evropska komisija (2017), Sporočilo Komisije Evropskemu parlamentu in Svetu, Izmenjava in varstvo osebnih podatkov v globaliziranem svetu, COM(2017) 7 final z dne 10. januarja 2017, str. 6.

671 Za nenehno posodobljen seznam držav, v zvezi s katerimi je bila sprejeta ugotovitev o ustreznosti, glej stran Evropske komisije.

da veljavno pravo in praksa v zadevni tretji državi ne zagotavljata ustrezne ravni varstva.[672]

Evropska komisija lahko tudi oceni ustreznost ozemlja v tretji državi ali pa se omeji na posamezne sektorje, kot je na primer naredila v zvezi z zakonodajo Kanade za zasebne gospodarske organizacije.[673] Ugotovitve o ustreznosti se sprejemajo tudi za prenose na podlagi sporazumov med EU in tretjimi državami. Te odločitve se nanašajo izključno na eno vrsto prenosa osebnih podatkov, na primer prenos evidenc podatkov o potnikih od letalskih družb tujim organom za nadzor meje, če letalska družba leti iz EU v nekatere čezmorske destinacije (glej razdelek 7.3.4).

Sklepi o ustreznosti se stalno spremljajo. Evropska komisija jih redno pregleduje, da spremlja razvoj dogodkov, ki bi lahko vplival na njihovo stanje. Če torej Evropska komisija ugotovi, da tretja država ali mednarodna organizacija ne izpolnjuje več pogojev, ki upravičujejo sklep o ustreznosti, lahko sklep spremeni, začasno prekine njegovo izvajanje ali ga razveljavi. Komisija lahko začne pogajanja z zadevno tretjo državo ali mednarodno organizacijo, da bi odpravila pomanjkljivosti, zaradi katerih je sprejela takšno odločitev.

Sklepi o ustreznosti, ki jih je Evropska komisija sprejela na podlagi Direktive 95/46/ES, ostanejo veljavni, dokler jih Komisija ne spremeni, nadomesti ali razveljavi s sklepom, sprejetim v skladu s pravili iz člena 45 SUVP.

Evropska komisija je doslej potrdila, da ustrezno varstvo zagotavljajo Andora, Argentina, Ferski otoki, Guernsey, Izrael, Jersey, Kanada (gospodarske organizacije, ki spadajo na področje uporabe zakona o varstvu osebnih podatkov in elektronskih dokumentih – PIPEDA), Nova Zelandija, Otok Man, Švica in Urugvaj. Kar zadeva prenose v ZDA, je Evropska komisija leta 2000 sprejela odločbo o ustreznosti, s katero so bili dovoljeni prenosi družbam, ki so samocertificirale varstvo osebnih podatkov, prenesenih iz EU, in skladnost s tako imenovanimi načeli varnega pristana.[674] SEU je

672 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015, točke 63, 65 in 66.

673 Evropska komisija, Odločba 2002/2/ES z dne 20. decembra 2001 na podlagi Direktive 95/46/ES Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja kanadski Zakon o varstvu osebnih podatkov in elektronskih dokumentih (UL L 2, 4.1.2002, str. 13).

674 Odločba Komisije 2000/520/ES z dne 26. julija 2000 po Direktivi Evropskega parlamenta in Sveta 95/46/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA (UL L 215, 25.8.2000, str. 7). SEU jo je v zadevi *Maximilian Schrems proti Data Protection Commissioner* (veliki senat) (C-362/14) razglasilo za neveljavno.

to odločbo razveljavilo leta 2015, nov sklep o ustreznosti pa je bil sprejet julija 2016. Družbe se mu lahko pridružijo od 1. avgusta 2016.

Primer: v zadevi *Schrems*[675] je bil avstrijski državljan Maximilian Schrems več let uporabnik Facebooka. Nekateri ali vsi podatki, ki jih je M. Schrems zagotovil Facebooku, so bili iz Facebookove hčerinske družbe na Irskem preneseni na strežnike v ZDA, kjer so se obdelovali. M. Schrems je vložil pritožbo pri irskem organu za varstvo podatkov, saj je menil, da glede na razkritja ameriškega žvižgača Edwarda Snowdna v zvezi z dejavnostmi nadzora, ki jih izvajajo ameriške obveščevalne službe, pravo in praksa ZDA ne zagotavljata zadostnega varstva osebnih podatkov, ki se prenašajo v navedeno državo. Irski organ je zavrnil pritožbo z utemeljitvijo, da je Komisija v svoji odločbi z dne 26. julija 2000 menila, da ZDA v okviru sheme varnega pristana zagotavljajo ustrezno raven varstva prenesenih osebnih podatkov. Zadeva je bila predložena irskemu višjemu sodišču, ki jo je predložilo SEU v predhodno odločanje.

SEU je odločilo, da je odločba Komisije o ustreznosti okvira varnega pristana neveljavna. Najprej je ugotovilo, da je v skladu s to odločbo mogoče omejiti uporabo načel varstva osebnih podatkov iz sheme varnega pristana, in sicer zaradi nacionalne varnosti, javnega interesa ali kazenskega pregona ali na podlagi nacionalne zakonodaje ZDA. Odločba je torej omogočala poseganje v temeljne pravice tistih oseb, katerih osebni podatki so bili ali bi lahko bili preneseni v ZDA.[676] Poleg tega je opozorilo, da odločba ne vsebuje ugotovitev niti glede obstoja pravil v ZDA za omejitev takih posegov niti glede obstoja učinkovitega pravnega varstva pred takimi posegi.[677] SEU je poudarilo, da je treba zaradi ravni varstva temeljnih pravic in svoboščin, ki se zagotavlja v EU, v zakonodaji, ki posega v člena 7 in 8 Listine, določiti jasna in natančna pravila, ki opredeljujejo obseg in uporabo ukrepa ter določajo minimalne zaščitne ukrepe, odstopanja in omejitve glede varstva osebnih podatkov.[678] Ker v odločbi Komisije ni bilo ugotovljeno, da ZDA dejansko zagotavljajo ustrezno raven varstva zaradi svoje nacionalne zakonodaje ali

675 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015.

676 Prav tam, točka 84.

677 Prav tam, točki 88 in 89.

678 Prav tam, točki 91 in 92.

mednarodnih obveznosti, je SEU sklenilo, da zadevna odločba ne izpolnjuje zahtev ustrezne določbe o prenosu iz direktive o varstvu osebnih podatkov in je zato neveljavna.[679]

Raven varstva v ZDA zato ni bila v bistvenem enaka ravni varstva temeljnih svoboščin in pravic, zagotovljeni v EU.[680] SEU je menilo, da je bilo kršenih več členov Listine EU o temeljnih pravicah. Prvič, ameriška ureditev, „ki [je] javnim organom omogoča[la] splošen dostop do vsebine elektronskih komunikacij“, je pomenila poseg v bistvo člena 7 Listine. Drugič, kršeno je bilo tudi bistvo člena 47 Listine, saj z zakonodajo posameznikom niso bila zagotovljena pravna sredstva v zvezi z dostopom do osebnih podatkov ali popravkom oziroma izbrisom osebnih podatkov. Ker sta bila z ureditvijo varnega pristana kršena navedena člena, se osebni podatki niso več zakonito obdelovali, kar je pomenilo kršitev člena 8 Listine.

Po tem, ko je SEU ureditev varnega pristana razglasilo za neveljavno, sta se Komisija in ZDA dogovorili o novem okviru, imenovanem zasebnostni ščit EU-ZDA. Komisija je 12. julija 2016 sprejela sklep, da ZDA zagotavljajo ustrezno raven varstva osebnih podatkov, ki se v okviru zasebnostnega ščita prenašajo iz Unije v ZDA.[681]

Cilj okvira zasebnostnega ščita EU-ZDA je podobno kot pri ureditvi varnega pristana varovati osebne podatke, ki se prenašajo iz EU v ZDA v komercialne namene.[682] Ameriške družbe lahko prostovoljno samocertificirajo zavezanost k izpolnjevanju standardov tega okvira za varstvo osebnih podatkov in se s tem uvrstijo na seznam zasebnostnega ščita. Pristojni ameriški organi spremljajo in preverjajo skladnost certificiranih družb s temi standardi.

679 Prav tam, točki 96 in 97.

680 Prav tam, točke 73, 74 in 96.

681 Izvedbeni sklep Komisije (EU) 2016/1250 z dne 12. julija 2016 na podlagi Direktive Evropskega parlamenta in Sveta 95/46/ES o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA (UL L 207, 1.8.2016, str. 1). Delovna skupina iz člena 29 je pozdravila izboljšave, ki jih je v primerjavi z odločbo o varnem pristanu prinesel mehanizem zasebnostnega ščita, ter pohvalila Komisijo in ameriške organe, da so v končni različici dokumentov v zvezi z zasebnostnim ščitom upoštevali pomisleke, ki jih je izrazila v mnenju WP 238 o osnutku sklepa o ustreznosti zasebnostnega ščita EU-ZDA. Vseeno je poudarila več nerešenih vprašanj. Za več podrobnosti glej Delovna skupina za varstvo podatkov iz člena 29, *Mnenje 1/2016 o osnutku sklepa o ustreznosti zasebnostnega ščita EU-ZDA*, sprejeto 13. aprila 2016, 16/SL WP 238.

682 Za več informacij glej informativni pregled o zasebnostnem ščitu EU-ZDA.

Okvir zasebnostnega ščita zlasti določa:

- obveznosti glede varstva osebnih podatkov za družbe, ki prejemajo osebne podatke iz EU;
- varstvo in pravna sredstva za posameznike, zlasti vzpostavitev mehanizma varuha človekovih pravic, ki je neodvisen od obveščevalnih služb ZDA in obravnava pritožbe posameznikov, ki menijo, da so organi ZDA na področju javne varnosti nezakonito uporabili njihove osebne podatke;
- letni skupni pregled za spremljanje izvajanja okvira;[683] prvi pregled je potekal septembra 2017.[684]

Vlada ZDA je predložila pisne zaveze in zagotovila, ki spremljajo sklep o zasebnostnem ščitu. Z njimi so določene omejitve in zaščitni ukrepi glede dostopa ameriške vlade do osebnih podatkov za namene kazenskega pregona in nacionalne varnosti.

7.3.2 Prenosi, za katere se uporabljajo ustrezni zaščitni ukrepi

V **pravu EU** in **pravu Sveta Evrope** je določeno, da so lahko ustrezni zaščitni ukrepi, vzpostavljeni med upravljavcem, ki iznaša osebne podatke, in uporabnikom v tretji državi ali mednarodno organizacijo, način za zagotavljanje zadostne ravni varstva osebnih podatkov za uporabnika.

V skladu s **pravom EU** so prenosi osebnih podatkov v tretjo državo ali mednarodno organizacijo dovoljeni, če upravljavec ali obdelovalec predvidi ustrezne zaščitne ukrepe in izvršljive pravice ter če so posameznikom, na katere se nanašajo osebni podatki, na voljo učinkovita pravna sredstva.[685] Seznam sprejemljivih ustreznih zaščitnih ukrepov je na voljo le v pravu EU o varstvu osebnih podatkov. Ustrezni zaščitni ukrepi se lahko vzpostavijo s:

- pravno zavezujočim in izvršljivim instrumentom, ki ga sprejmejo javni organi ali telesa;

683 Za več informacij glej spletno stran Evropske komisije o zasebnostnem ščitu EU-ZDA.

684 Evropska komisija, Poročilo Komisije Evropskemu parlamentu in Svetu o prvem letnem pregledu delovanja zasebnostnega ščita EU-ZDA, COM(2017) 611 final, 18. oktober 2017. Glej tudi Delovna skupina za varstvo podatkov iz člena 29, *EU – U.S. Privacy Shield – First annual Joint Review* (Zasebnostni ščit EU-ZDA – Prvi letni skupni pregled), sprejet 28. novembra 2017, 17/EN WP 255.

685 SUVP, člen 46.

- zavezujočimi poslovnimi pravili;
- standardnimi določili o varstvu osebnih podatkov, ki jih sprejme Evropska komisija ali nadzorni organ;
- kodeksi ravnanja;
- mehanizmi certificiranja.[686]

Ustrezni zaščitni ukrepi se lahko zagotovijo tudi s prilagojenimi pogodbenimi določili med upravljavcem ali obdelovalcem v EU in uporabnikom osebnih podatkov v tretji državi. Vendar mora taka pogodbena določila odobriti pristojni nadzorni organ, preden jih je mogoče uporabiti kot orodje za prenos osebnih podatkov. Podobno lahko javni organi določbe o varstvu osebnih podatkov, vključene v upravne dogovore, uporabljajo le, če jih je odobril nadzorni organ.[687]

V skladu s **pravom Sveta Evrope** je prenos osebnih podatkov v državo ali mednarodno organizacijo, ki ni pogodbenica posodobljene Konvencije št. 108, dovoljen, če je zagotovljena ustrezna raven varstva. To je mogoče doseči s:

- pravom države ali mednarodne organizacije ali
- *ad hoc* ali standardiziranimi zaščitnimi ukrepi, vključenimi v pravno zavezujoč dokument.[688]

Prenosi, za katere se uporabljajo pogodbena določila

V **pravu Sveta Evrope** in **pravu EU** je navedeno, da so pogodbena določila (klavzule) med upravljavcem, ki iznaša osebne podatke, in uporabnikom v tretji državi, lahko način za zagotavljanje zadostne ravni varstva osebnih podatkov za uporabnika.[689]

686 SUVP, člen 46(1)(c) in (d), člen 46(2)(a), (b), (e) in (f) ter člen 47.

687 Prav tam, člen 46(3).

688 Posodobljena Konvencija št. 108, člen 14(3)(b).

689 SUVP, člen 46(3); posodobljena Konvencija št. 108, člen 14(3)(b).

Na **ravni EU** je Evropska komisija ob pomoči Delovne skupine za varstvo podatkov iz člena 29 razvila standardne klavzule o varstvu osebnih podatkov, ki so bile z odločbo Komisije uradno potrjene kot dokaz o ustrezni ravni varstva osebnih podatkov.[690] Ker so sklepi Komisije v državah članicah zavezujoči v celoti, morajo nacionalni organi, ki nadzirajo prenose osebnih podatkov, te standardne pogodbene klavzule upoštevati v svojih postopkih.[691] Če se torej upravljavec, ki iznaša osebne podatke, in uporabnik v tretji državi dogovorita o teh določilih in jih podpišeta, mora biti to za nadzorni organ zadosten dokaz, da so uvedeni ustrezni zaščitni ukrepi. Vendar je SEU v zadevi *Schrems* menilo, da Evropska komisija ni pristojna za omejitev pooblastil nacionalnih nadzornih organov za nadzor nad prenosom osebnih podatkov v tretjo državo, v zvezi s katero je bil sprejet sklep Komisije o ustreznosti.[692] Zato nacionalnim nadzornim organom ni onemogočeno izvajanje njihovih pooblastil, vključno s pooblastilom za začasno prekinitev ali prepoved prenosa osebnih podatkov, kadar se prenos izvaja v nasprotju s pravom EU ali nacionalnim pravom o varstvu osebnih podatkov, na primer kadar uvoznik osebnih podatkov ne spoštuje standardnih pogodbenih določil.[693]

Obstoj standardnih pogodbenih klavzul v pravnem okviru EU pa ne pomeni, da upravljavci ne smejo izoblikovati drugih *ad hoc* individualnih pogodbenih določil, če jih odobri nadzorni organ.[694] Vendar bi bilo z njimi treba zagotoviti enako raven varstva, kot je zagotovljena s standardnimi pogodbenimi klavzulami o varstvu podatkov. Nadzorni organi morajo pri odobritvi *ad hoc* določil uporabljati mehanizem za skladnost, da bi se zagotovil dosleden regulativni pristop v vsej EU.[695] To pomeni, da mora pristojni nadzorni organ osnutek svoje odločitve o določilih posredovati Evropskemu odboru za varstvo podatkov. Ta izda mnenje o vsebini, nadzorni organ pa mora to mnenje čim bolj upoštevati pri nadaljnjem sprejemanju svoje odločitve. Če nadzorni organ mnenja zadevnega odbora ne namerava upoštevati, se bo sprožil

690 Prav tam, člen 46(2)(b) in člen 46(5).

691 Prav tam, člen 46(2)(c); Pogodba o delovanju Evropske unije, člen 288.

692 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015, točke 96–98 in 102–105.

693 Da bi Komisija upoštevala stališče SEU v zadevi *Schrems*, je spremenila svojo odločbo o standardnih pogodbenih klavzulah. Izvedbeni sklep Komisije (EU) 2016/2297 z dne 16. decembra 2016 o spremembi Odločbe 2001/497/ES in Sklepa 2010/87/EU o standardnih pogodbenih klavzulah za prenos osebnih podatkov v tretje države in obdelovalcem s sedežem v navedenih državah v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES (UL L 344, 17.12.2016, str. 100).

694 SUVP, člen 46(3)(a).

695 Prav tam, člen 63 in člen 64(1)(e).

mehanizem za reševanje sporov v okviru zadevnega odbora, Odbor pa bo sprejel zavezujočo odločitev.[696]

Najpomembnejše značilnosti standardnih pogodbenih klavzul so:

- določilo v korist tretjega, ki posameznikom, na katere se nanašajo osebni podatki, omogoča uveljavljanje pogodbenih pravic, tudi če niso pogodbena stranka;

- uporabnik ali uvoznik osebnih podatkov se strinja, da se zanj ob sporu uporabi postopek nadzornega organa in/ali sodišč upravljavca, ki iznaša osebne podatke.

Upravljavec, ki iznaša osebne podatke, lahko zdaj izbira med dvema sklopoma standardnih klavzul, ki sta na voljo za prenose med upravljavci.[697] Za prenose med upravljavcem in obdelovalcem obstaja samo en sklop standardnih pogodbenih klavzul.[698] Vendar so te standardne pogodbene klavzule trenutno predmet sodnega postopka.

Primer: po tem, ko je SEU odločbo o varnem pristanu razglasilo za neveljavno,[699] prenosi osebnih podatkov v ZDA niso več mogli temeljiti na tej odločbi o ustreznosti. Med pogajanji z ameriškimi organi in do sprejetja novega sklepa o ustreznosti (ki je bil sprejet 12. julija 2016)[700] so se prenosi lahko izvajali le na drugih pravnih podlagah, kot so standardna pogodbena določila ali zavezujoča poslovna pravila. Več družb, med drugim Facebook Ireland (na katero se je nanašal postopek v zadevi, ki je privedel do razveljavitve odločbe o varnem pristanu), je začelo uporabljati standardna pogodbena določila, da so lahko nadaljevale s prenosi osebnih podatkov med EU in ZDA.

696 Prav tam, člena 64 in 65.

697 Sklop I je vključen v Prilogo k Odločbi Komisije 2001/497/ES z dne 15. junija 2001 o standardnih pogodbenih klavzulah za prenos osebnih podatkov v tretje države v skladu z Direktivo 95/46/ES (UL L 181, 4.7.2001, str. 19); sklop II je vključen v Prilogo k Odločbi Komisije 2004/915/ES z dne 27. decembra 2004 o spremembi Odločbe 2001/497/ES glede uvedbe alternativnega sklopa standardnih pogodbenih klavzul za prenos osebnih podatkov v tretje države (UL L 385, 29.12.2004, str. 74).

698 Evropska komisija (2010), Sklep Komisije 2010/87/EU z dne 5. februarja 2010 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES (UL L 39, 12.2.2010, str. 5). V času priprave tega priročnika je bila uporaba standardnih pogodbenih klavzul kot podlage za prenose osebnih podatkov v ZDA predmet sodnega postopka pred irskim višjim sodiščem.

699 SEU, *Maximillian Schrems proti Data Protection Commissioner* (veliki senat), C-362/14, 6. oktober 2015.

700 Izvedbeni sklep Komisije (EU) 2016/1250 z dne 12. julija 2016 na podlagi Direktive Evropskega parlamenta in Sveta 95/46/ES o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA (UL L 207, 1.8.2016, str. 1).

M. Schrems je vložil pritožbo pri irskem nadzornem organu, s katero je od njega zahteval, naj začasno ustavi prenose osebnih podatkov v ZDA na podlagi standardnih pogodbenih klavzul. V bistvu je trdil, da ni zagotovljeno, da so njegovi osebni podatki varovani, ko se prenašajo od irske hčerinske družbe Facebooka na strežnike družbe Facebook Inc. v ZDA. Družbo Facebook Inc. zavezuje ameriška zakonodaja, v skladu s katero bi se ji lahko naložilo razkritje osebnih podatkov ameriškim organom kazenskega pregona, pri čemer evropski posamezniki nimajo na voljo pravnega sredstva za izpodbijanje te prakse.[701] SEU je zato sklenilo, da je odločba o varnem pristanu neveljavna, in čeprav je bila njegova sodba omejena na proučitev navedene odločbe, je pritožnik menil, da so obravnavana vprašanja enako pomembna tudi, kadar prenos temelji na pogodbenih klavzulah. V času pisanja je zadevo obravnavalo irsko višje sodišče. Pritožnik menda namerava zadevo pripeljati do SEU, pred katerim naj bi izpodbijal veljavnost odločbe Evropske komisije o standardnih pogodbenih klavzulah. Kot je navedeno v poglavju 5, je le SEU pristojno za razglasitev neveljavnosti instrumenta EU.

Prenosi, za katere se uporabljajo zavezujoča poslovna pravila

Pravo EU omogoča tudi prenose osebnih podatkov, ki temeljijo na zavezujočih poslovnih pravilih za mednarodne prenose znotraj iste povezane družbe ali skupin podjetij, ki skupaj opravljajo gospodarsko dejavnost.[702] Preden se lahko zavezujoča poslovna pravila uporabijo kot orodje za prenos osebnih podatkov, jih mora v skladu z mehanizmom za skladnost odobriti pristojni nadzorni organ.

Da se zavezujoča poslovna pravila odobrijo, morajo biti pravno zavezujoča in zajemati vsa bistvena načela varstva osebnih podatkov, uporabljati pa se morajo za vse člane skupine, ki jih tudi izvajajo. Posameznikom, na katere se nanašajo osebni podatki, morajo izrecno podeljevati izvršljive pravice, vključevati morajo vsa bistvena načela varstva osebnih podatkov in izpolnjevati nekatere formalne zahteve, v njih mora na primer biti opredeljena struktura podjetij ter opisani prenosi in uporaba načel varstva osebnih podatkov. To vključuje zagotavljanje takih informacij posameznikom, na katere se nanašajo osebni podatki. Zavezujoča poslovna pravila morajo med drugim določati pravice posameznikov, na katere se nanašajo osebni podatki, in

701 Več informacij je na voljo v revidirani pritožbi zoper družbo Facebook Ireland Ltd, ki jo je Maximilian Schrems 1. decembra 2015 predložil irskemu pooblaščencu za varstvo podatkov.

702 SUVP, člen 47.

vključevati določbe o odgovornosti za morebitno kršitev pravil.[703] Pri odobritvi zavezujočih poslovnih pravil se sproži mehanizem za skladnost za sodelovanje nadzornih organov (opisan v poglavju 5).

V okviru mehanizma za skladnost vodilni nadzorni organ pregleda predlagana zavezujoča poslovna pravila, sprejme osnutek odločitve in ga posreduje Evropskemu odboru za varstvo podatkov. Odbor izda mnenje o zadevi, vodilni nadzorni organ pa lahko formalno odobri zavezujoča poslovna pravila, pri čemer „čim bolj upošteva" mnenje odbora. Če tega mnenja, ki sicer ni pravno zavezujoče, nadzorni organ ne namerava upoštevati, se sproži mehanizem za reševanje sporov, odbor pa bo moral sprejeti pravno zavezujočo odločitev z dvotretjinsko večino svojih članov.[704]

V skladu s **pravom Sveta Evrope** *ad hoc* ali standardizirani zaščitni ukrepi, ki so vključeni v pravno zavezujoč dokument,[705] vključujejo tudi zavezujoča poslovna pravila.

7.3.3 Odstopanja v posebnih primerih

V skladu s **pravom EU** so prenosi osebnih podatkov v tretjo državo lahko upravičeni, tudi če sklep o ustreznosti ni sprejet ali če niso sprejeti zaščitni ukrepi, kot so standardna pogodbena določila ali zavezujoča poslovna pravila, in sicer v kateri koli od naslednjih okoliščin:

- posameznik, na katerega se nanašajo osebni podatki, je izrecno privolil v prenos osebnih podatkov;
- posameznik, na katerega se nanašajo osebni podatki, sklene ali namerava skleniti pogodbeno razmerje, v okviru katerega je potreben prenos osebnih podatkov v tujino;
- prenos je potreben za sklenitev pogodbe med upravljavcem osebnih podatkov in tretjo osebo, ki je v interesu posameznika, na katerega se nanašajo osebni podatki;
- prenos je potreben zaradi pomembnih razlogov javnega interesa;

703 Za podrobnejši opis glej SUVP, člen 47.

704 Prav tam, člen 57(1)(s), člen 58(1)(j), člen 64(1)(f) ter člen 65(1) in (2).

705 Posodobljena Konvencija št. 108, člen 14(3)(b).

- prenos je potreben za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;
- prenos je potreben za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki;
- prenos se opravi iz javnih registrov (to je primer prevladujočih interesov širše javnosti, da lahko dostopa do informacij, ki se hranijo v javnih registrih).[706]

Kadar ne velja nobeden od teh pogojev in kadar prenosi ne morejo temeljiti na sklepu o ustreznosti ali ustreznih zaščitnih ukrepih, se lahko prenos izvede le, če ni ponovljiv, zadeva le omejeno število posameznikov, na katere se nanašajo osebni podatki, in je potreben zaradi nujnih zakonitih interesov upravljavca osebnih podatkov, če nad njimi ne prevladajo pravice posameznika, na katerega se nanašajo osebni podatki.[707] V teh primerih mora upravljavec oceniti okoliščine v zvezi s prenosom in predvideti zaščitne ukrepe. Poleg tega mora o prenosu in zakonitih interesih, ki ga upravičujejo, obvestiti nadzorni organ in posameznike, na katere se nanašajo osebni podatki in na katere prenos vpliva.

Dejstvo, da so odstopanja zadnja možnost za zakonite prenose[708] (ki se lahko uporabi le, če ni sprejet sklep o ustreznosti ali če niso uvedeni drugi zaščitni ukrepi), poudarja njihovo izjemnost, ki je dodatno poudarjena v uvodnih izjavah SUVP[709]. Odstopanja so tako sprejeta kot možnost za „prenos[e] v določenih okoliščinah“ na podlagi privolitve in kadar je „prenos občasen in potreben“[710] zaradi pogodbe ali pravnega zahtevka.

Poleg tega je treba v skladu s smernicami Delovne skupine iz člena 29 odstopanja v posebnih primerih uporabljati izjemoma in na podlagi posameznih primerov, ni pa jih mogoče uporabiti za množične ali ponavljajoče se prenose.[711] Evropski nadzornik za varstvo podatkov je poudaril tudi izjemnost odstopanj, ki se uporabljajo kot pravna podlaga za prenose v skladu z Uredbo (ES) št. 45/2001, pri čemer je opozoril, da bi bilo treba to rešitev uporabljati „v omejenih primerih“ in „za občasne prenose“.[712]

706 SUVP, člen 49.

707 Prav tam.

708 Prav tam, člen 49(1).

709 Glej SUVP, člen 49(1)(a), (b) in (e) ter uvodno izjavo 113.

710 Prav tam, uvodna izjava 111.

711 Delovna skupina za varstvo podatkov iz člena 29 (2005), Delovni dokument o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995, WP 114, Bruselj, 25. november 2005.

712 Evropski nadzornik za varstvo podatkov, *Prenos osebnih podatkov tretjim državam in mednarodnim organizacijam s strani institucij in organov EU*, dokument o stališču, Bruselj, 14. julij 2014, str. 15.

Primer: družba za storitve globalnega distribucijskega sistema s sedežem v ZDA zagotavlja spletni sistem rezervacij za več letalskih prevoznikov, hotelov in družb za organizacijo križarjenj po vsem svetu ter obdeluje osebne podatke več deset milijonov ljudi v EU. Za prvotni prenos podatkov na svoje strežnike v ZDA se zadevna družba kot zakonito podlago za prenose sklicuje na odstopanje, in sicer potrebnost za sklenitev pogodbe. Ne navaja nobenih drugih zaščitnih ukrepov za osebne podatke, ki izvirajo iz Evrope, se prenašajo v ZDA in so nato prerazporejeni v hotele po vsem svetu (kar pomeni, da se zaščitni ukrepi ne uporabljajo niti za nadaljnje prenose). Zadevna družba ne izpolnjuje zahtev iz SUVP o zakonitih mednarodnih prenosih podatkov, saj se opira na odstopanje kot zakonito podlago za množične prenose osebnih podatkov.

Če sklep o ustreznosti ni bil sprejet, so EU ali njene države članice pooblaščene, da zaradi pomembnih razlogov javnega interesa določijo omejitve prenosa posebnih vrst osebnih podatkov v tretjo državo, čeprav so izpolnjeni drugi pogoji za take prenose. Te omejitve bi bilo treba razumeti kot izredne, države članice pa morajo o zadevnih določbah uradno obvestiti Komisijo.[713]

Pravo Sveta Evrope omogoča prenose osebnih podatkov na ozemlja, ki nimajo ustrezne ravni varstva osebnih podatkov, če:

- je posameznik, na katerega se osebni podatki nanašajo, vanje privolil;
- je tak prenos potreben zaradi interesov posameznika, na katerega se nanašajo osebni podatki;
- obstajajo prevladujoči zakoniti interesi, zlasti pomembni javni interesi, določeni s pravom;
- je prenos potreben in sorazmeren ukrep v demokratični družbi.[714]

713 Glej SUVP, člen 49(5).

714 Posodobljena Konvencija št. 108, člen 14(4).

7.3.4 Prenosi na podlagi mednarodnih sporazumov

EU lahko sklene mednarodne sporazume s tretjimi državami, s katerimi je urejen prenos osebnih podatkov za posebne namene. Ti sporazumi morajo vključevati ustrezne zaščitne ukrepe za zagotavljanje varstva osebnih podatkov zadevnih posameznikov. SUVP ne posega v te mednarodne sporazume.[715]

Države članice lahko poleg tega sklenejo mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki zagotavljajo ustrezno raven varstva temeljnih pravic in svoboščin posameznikov, če ti sporazumi ne vplivajo na uporabo SUVP.

Podobno pravilo je določeno v členu 12(3)(a) posodobljene Konvencije št. 108.

Primer mednarodnih sporazumov, ki vključujejo prenos osebnih podatkov, so sporazumi o evidencah podatkov o potnikih (PNR).

Evidence podatkov o potnikih

Podatki iz evidenc podatkov o potnikih (PNR), ki jih letalski prevozniki zbirajo med postopkom rezervacije leta, med drugim vključujejo imena, naslove, podatke o kreditni kartici in številke sedežev letalskih potnikov. Letalski prevozniki te informacije zbirajo tudi v lastne komercialne namene. EU je sklenila sporazume z nekaterimi tretjimi državami (Avstralijo, Kanado in ZDA) v zvezi s prenosom podatkov PNR za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj. Poleg tega je Unija leta 2016 sprejela Direktivo (EU) 2016/861, (direktiva EU o PNR)[716]. Ta direktiva državam članicam EU zagotavlja pravni okvir za prenos podatkov PNR pristojnim organom v drugih tretjih državah, in sicer da bi podobno preprečevali, odkrivali, preiskovali ali preganjali teroristična in huda kazniva dejanja. Prenosi podatkov PNR organom tretjih držav se izvajajo za vsak primer posebej, pri čemer se za vsakega od njih opravi ocena o tem, ali je prenos potreben za namene, določene v zadevni direktivi, in pod pogojem, da se spoštujejo temeljne pravice.

715 SUVP, uvodna izjava 102.

716 Direktiva (EU) 2016/681 Evropskega parlamenta in Sveta dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (UL L 119, 4.5.2016, str. 132).

Kar zadeva sporazume o PNR, sklenjene med EU in tretjimi državami, se je izpodbijala njihova skladnost s temeljnima pravicama do zasebnosti in varstva osebnih podatkov iz Listine EU o temeljnih pravicah. Ko je EU leta 2014 po pogajanjih s Kanado podpisala sporazum o prenosu in obdelavi podatkov PNR, se je Evropski parlament odločil, da zadevo predloži SEU v presojo združljivosti sporazuma s pravom EU, zlasti s členoma 7 in 8 Listine.

Primer: SEU je v svojem mnenju o zakonitosti sporazuma o PNR med Kanado in EU[717] ugotovilo, da predvideni sporazum v takratni obliki ni bil združljiv s temeljnimi pravicami, priznanimi z Listino, in da ga zato ni bilo mogoče skleniti. Ker je vključeval obdelavo osebnih podatkov, je to pomenilo poseganje v pravico do varstva osebnih podatkov, zaščiteno s členom 8 Listine. Hkrati je pomenil tudi omejitev pravice do spoštovanja zasebnega življenja iz člena 7, saj se lahko podatki PNR, obravnavani skupaj, združijo in analizirajo na način, ki razkriva potovalne navade, razmerja med posamezniki, informacije o njihovem finančnem položaju, njihove prehranske navade in njihovo zdravstveno stanje, s čimer se posega v njihovo zasebno življenje.

S poseganjem v temeljne pravice, ki ga je vključeval predvideni sporazum, se je uresničeval cilj v splošnem interesu, in sicer javna varnost ter boj proti terorizmu in hudim mednarodnim kaznivim dejanjem. Vendar je SEU opozorilo, da mora biti poseg, da bi bil upravičen, omejen na to, kar je nujno potrebno za uresničevanje zastavljenega cilja. Po proučitvi določb predvidenega sporazuma je ugotovilo, da ta ne izpolnjuje merila nujne potrebnosti. SEU je to ugotovilo na podlagi naslednjih dejavnikov.

- Predvideni sporazum je vključeval prenos občutljivih podatkov. Podatki PNR, ki bi se zbirali v skladu s predvidenim sporazumom, bi lahko vključevali občutljive podatke, kot so informacije, ki razkrivajo rasno ali etnično poreklo, verska prepričanja ali zdravstveno stanje potnika. Prenos občutljivih podatkov kanadskim organom in njihova obdelava, ki bi jo ti organi izvajali, bi lahko pomenila tveganje za načelo nediskriminacije, zato je v zvezi z njima potrebna natančna in trdna utemeljitev z razlogi, ki niso le zaščita javne varnosti in boj proti hudim kaznivim dejanjem. V predvidenem sporazumu taka utemeljitev ni bila zagotovljena.[718]

717 SEU, *Mnenje Sodišča 1/15* (veliki senat), 26. julij 2017.

718 Prav tam, točka 165.

- Poleg tega je menilo, da nadaljnja petletna hramba podatkov PNR za vse letalske potnike, tudi po njihovem odhodu iz Kanade, presega omejitve glede nujne potrebnosti. SEU je menilo, da bi bilo dopustno, če bi kanadski organi podatke o potnikih, za katere so na voljo objektivni dokazi, da bi lahko pomenili grožnjo javni varnosti, hranili tudi po njihovem odhodu iz Kanade. Nasprotno pa ni upravičena hramba osebnih podatkov *vseh* potnikov, za katere ne obstajajo niti posredni dokazi, da pomenijo tveganje za javno varnost.[719]

Posvetovalni odbor po Konvenciji št. 108 je predložil mnenje o posledicah, ki jih imajo sporazumi o PNR za varstvo osebnih podatkov na podlagi prava Sveta Evrope.[720]

Podatki o sporočilih glede plačil

Od Združenja za svetovne finančne telekomunikacije med bankami (SWIFT) s sedežem v Belgiji, ki je obdelovalec za večino svetovnega prenosa denarja iz evropskih bank in je imel enega od računalniških centrov v Združenih državah, se je zahtevalo, naj v skladu s programom za sledenje financiranja terorističnih dejavnosti ameriškemu ministrstvu za finance razkrije podatke zaradi preiskovanja terorizma.[721]

Z vidika EU ni bilo zadostne pravne podlage za razkritje teh podatkov, ki so se nanašali predvsem na državljane EU, samo zato, ker je imel eden od centrov združenja SWIFT za obdelavo storitev sedež v Združenih državah.

719 Prav tam, točke 204–207.

720 Svet Evrope, *Mnenje o posledicah, ki jih ima obdelava evidenc podatkov o potnikih za varstvo podatkov*, T-PD(2016)18rev, 19. avgust 2016.

721 V zvezi s tem glej Delovna skupina za varstvo podatkov iz člena 29 (2011), *Mnenje 14/2011 o varstvu podatkov v zvezi s preprečevanjem pranja denarja in bojem proti financiranju terorizma*, WP 186, Bruselj, 13. junij 2011; Delovna skupina za varstvo podatkov iz člena 29 (2006), *Mnenje 10/2006 o obdelavi osebnih podatkov Družbe za svetovne medbančne finančne telekomunikacije (SWIFT)*, WP 128, Bruselj, 22. november 2006; belgijska komisija za varstvo zasebnosti (*Commission de la protection de la vie privée*) (2008), *Control and recommendation procedure initiated with respect to the company SWIFT scrl* (Postopek nadzora in priporočil, sprožen v zvezi z družbo SWIFT scrl), sklep, 9. december 2008.

Leta 2010 je bil sklenjen poseben sporazum med EU in ZDA, imenovan sporazum SWIFT, da bi se zagotovili potrebna pravna podlaga in ustrezni standardi varstva osebnih podatkov.[722]

Na podlagi tega sporazuma se finančni podatki, ki jih shranjuje SWIFT, ameriškemu ministrstvu za finance posredujejo zaradi preprečevanja, preiskovanja, odkrivanja ali pregona terorizma ali njegovega financiranja. Ameriško ministrstvo za finance lahko združenje SWIFT zaprosi za finančne podatke, če v zvezi z zaprosilom velja naslednje:

- v njem so čim bolj jasno opredeljeni finančni podatki;
- v njem je jasno utemeljeno, zakaj so podatki potrebni;
- zasnovano je čim ožje, da se zahtevani podatki omejijo na najmanjši možni obseg;
- v njem se ne zahtevajo podatki v zvezi z enotnim območjem plačil v eurih (SEPA).[723]

Europol mora prejeti kopijo vsakega zaprosila ameriškega ministrstva za finance in preveriti, ali se upoštevajo načela iz sporazuma SWIFT ali ne.[724] Če potrdi, da se načela upoštevajo, mora združenje SWIFT finančne podatke posredovati neposredno ameriškemu ministrstvu za finance. Ministrstvo mora finančne podatke hraniti v varnem fizičnem okolju, tako da imajo dostop do podatkov samo analitiki, ki preiskujejo terorizem ali njegovo financiranje, finančni podatki pa ne smejo biti povezani z nobeno drugo podatkovno zbirko. Na splošno je treba finančne podatke, ki jih pošlje združenje SWIFT, izbrisati najpozneje pet let po prejemu. Finančni podatki, ki so relevantni za posamezne preiskave ali pregon, se lahko hranijo, dokler so potrebni za te preiskave ali pregon.

722 Sklep Sveta 2010/412/EU z dne 13. julija 2010 o sklenitvi Sporazuma med Evropsko unijo in Združenimi državami Amerike o obdelavi in posredovanju podatkov o sporočilih glede finančnih plačil iz Evropske unije Združenim državam Amerike za namene programa za sledenje financiranja terorističnih dejavnosti (UL L 195, 27.7.2010, str. 3). Temu sklepu je priloženo besedilo zadevnega sporazuma (UL L 195, 27.7.2010, str. 5).

723 Prav tam, člen 4(2).

724 Skupni nadzorni organ Europola je izvedel revizije dejavnosti Europola na tem področju.

Ameriško ministrstvo za finance lahko informacije iz podatkov, ki jih prejme od združenja SWIFT, posreduje določenim organom pregona in organom za javno varnost ali boj proti terorizmu v ZDA ali zunaj njih izključno za preiskovanje, odkrivanje, preprečevanje ali pregon terorizma in njegovega financiranja. Če nadaljnji prenos finančnih podatkov vključuje državljana ali prebivalca države članice EU, morajo v vsako izmenjavo osebnih podatkov z organi tretje države predhodno privoliti pristojni organi zadevne države članice. Izjeme so dovoljene, če je izmenjava podatkov nujna za preprečitev neposredne in resne grožnje za javno varnost.

Skladnost z načeli sporazuma SWIFT spremljajo neodvisni nadzorniki, vključno z osebo, ki jo imenuje Evropska komisija. Ti imajo možnost, da v realnem času in za nazaj pregledajo vsa iskanja po predloženih podatkih, zahtevajo dodatne informacije, ki upravičujejo povezavo teh iskanj s terorizmom, poleg tega pa lahko blokirajo posamezna ali vsa iskanja, v zvezi s katerimi se zdi, da so v nasprotju z zaščitnimi ukrepi iz zadevnega sporazuma.

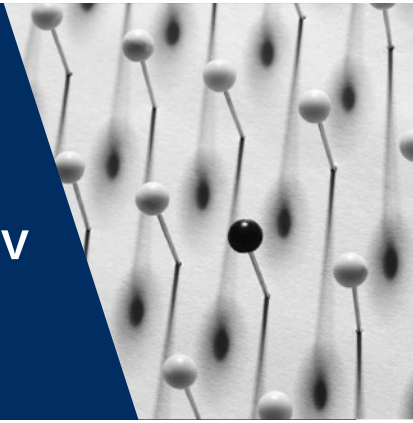
Posamezniki, na katere se nanašajo osebni podatki, imajo pravico od pristojnega organa EU za varstvo osebnih podatkov dobiti potrditev, da so bile spoštovane njihove pravice do varstva osebnih podatkov. Poleg tega imajo pravico do popravka, izbrisa ali blokiranja svojih osebnih podatkov, ki jih ameriško ministrstvo za finance zbira in shranjuje na podlagi sporazuma SWIFT. Vendar lahko za pravice do dostopa posameznikov, na katere se nanašajo osebni podatki, veljajo nekatere pravne omejitve. Če se dostop zavrne, je treba posameznika, na katerega se nanašajo osebni podatki, pisno obvestiti o zavrnitvi ter o njegovi pravici do upravnega in sodnega varstva v ZDA.

Sporazum SWIFT velja pet let, pri čemer je njegovo prvo obdobje veljavnosti trajalo do avgusta 2015. Nato se samodejno podaljšuje za nadaljnja enoletna obdobja, razen če ena od pogodbenic drugo vsaj šest mesecev vnaprej ne obvesti, da ga ne namerava podaljšati. Samodejno podaljšanje, ki je bilo uporabljeno avgusta 2015, 2016 in 2017, zagotavlja veljavnost sporazuma SWIFT vsaj do avgusta 2018.[725]

725 Prav tam, člen 23(2).

8

Varstvo osebnih podatkov v okviru policije in kazenskega pravosodja



EU	Obravnavane teme	Svet Evrope
Direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja	**Splošno**	Posodobljena Konvencija št. 108
	Policija	Priporočilo o uporabi osebnih podatkov v policijskem sektorju Praktični vodnik za uporabo osebnih podatkov v policijskem sektorju
	Nadzor	ESČP, *B. B. proti Franciji*, pritožba št. 5335/06, 2009 ESČP, združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 2008 ESČP, *Allan proti Združenemu kraljestvu*, pritožba št. 48539/99, 2002 ESČP, *Malone proti Združenemu kraljestvu*, pritožba št. 8691/79, 1984 ESČP, *Klass in drugi proti Nemčiji*, pritožba št. 5029/71, 1978 ESČP, *Szabó in Vissy proti Madžarski*, pritožba št. 37138/14, 2016 ESČP, *Vetter proti Franciji*, pritožba št. 59842/00, 2005

EU	Obravnavane teme	Svet Evrope
	Kibernetska kriminaliteta	Konvencija o kibernetski kriminaliteti
Drugi posebni pravni instrumenti		
Prümski sklep	**Za posebne osebne podatke: prstne odtise, DNK, huliganstvo, informacije o letalskih potnikih, telekomunikacijske podatke itd.**	Posodobljena Konvencija št. 108, člen 6 Priporočilo o uporabi osebnih podatkov v policijskem sektorju, Praktični vodnik za uporabo osebnih podatkov v policijskem sektorju
Švedska pobuda (Okvirni sklep Sveta 2006/960/PNZ)	**Poenostavitev izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona**	ESČP, združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 2008
Direktiva (EU) 2016/681 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj SEU, združeni zadevi C-293/12 in C-594/12, *Digital Rights Ireland* in Kärntner Landesregierung in drugi (veliki senat), 2014 SEU, združeni zadevi C-203/15 in C-698/15, *Tele2 Sverige in Home Department proti Tomu Watsonu in drugim* (veliki senat), 2016	**Hramba osebnih podatkov**	ESČP, *B. B. proti Franciji*, pritožba št. 5335/06, 2009
Uredba o Europolu Sklep o Eurojustu	**V posebnih agencijah**	Priporočilo o uporabi osebnih podatkov v policijskem sektorju
Sklep Schengen II Uredba VIS Uredba Eurodac Sklep CIS	**V posebnih skupnih informacijskih sistemih**	Priporočilo o uporabi osebnih podatkov v policijskem sektorju ESČP, *Dalea proti Franciji*, pritožba št. 964/07, 2010

Da bi Svet Evrope in EU za boj proti kriminalu in zagotavljanje nacionalne in javne varnosti uravnotežila posameznikove interese za varstvo osebnih podatkov ter interese družbe za zbiranje teh podatkov, sta uzakonila posebne pravne instrumente. V tem razdelku je na voljo pregled prava Sveta Evrope (razdelek 8.1) in prava EU

(razdelek 8.2) v zvezi z varstvom osebnih podatkov pri policijskih zadevah in zadevah s področja kazenskega pravosodja.

8.1 Pravo Sveta Evrope o varstvu osebnih podatkov in nacionalni varnosti, policijskih zadevah in zadevah s področja kazenskega pravosodja

Ključna poudarka

- Posodobljena Konvencija št. 108 in Priporočilo Sveta Evrope o uporabi osebnih podatkov v policijskem sektorju se uporabljata za varstvo osebnih podatkov na vseh področjih policijskega dela.
- Konvencija o kibernetski kriminaliteti (Budimpeška konvencija) je zavezujoči mednarodni pravni instrument, v katerem so obravnavana kazniva dejanja, storjena zoper elektronska omrežja in z njimi. Pomembna je tudi za preiskavo nekibernetskih kaznivih dejanj, ki vključujejo elektronske dokaze.

Ena od pomembnih razlik med pravom Sveta Evrope in pravom EU je, da se **pravo Sveta Evrope** v nasprotju s pravom EU uporablja tudi za področje nacionalne varnosti. To pomeni, da pogodbenice ne smejo prekoračiti pristojnosti iz člena 8 EKČP niti pri dejavnostih, povezanih z nacionalno varnostjo. Več sodb ESČP se nanaša na državne dejavnosti na občutljivih področjih prava in prakse v zvezi z nacionalno varnostjo.[726]

Kar zadeva policijo in kazensko pravosodje, posodobljena Konvencija št. 108 na evropski ravni zajema vsa področja obdelave osebnih podatkov, z njenimi določbami pa naj bi bila urejena obdelava osebnih podatkov na splošno. Zato se uporablja za varstvo osebnih podatkov na področju policije in kazenskega pravosodja. Obdelava genskih podatkov, osebnih podatkov v zvezi s prekrški, kazenskimi postopki in obsodbami ter vsemi povezanimi varnostnimi ukrepi, biometričnih podatkov, ki omogočajo edinstveno identifikacijo posameznika, ter vseh občutljivih osebnih podatkov, je dovoljena le, če obstajajo ustrezni zaščitni ukrepi proti tveganjem, ki bi jih lahko obdelava takih osebnih podatkov pomenila za interese, pravice in temeljne

726 Glej na primer ESČP, *Klass in drugi proti Nemčiji*, pritožba št. 5029/71, 6. september 1978; ESČP, *Rotaru proti Romuniji* (veliki senat), pritožba št. 28341/95, 4. maj 2000, in ESČP, *Szabó in Vissy proti Madžarski*, pritožba št. 37138/14, 12. januar 2016.

svoboščine posameznika, na katerega se nanašajo osebni podatki, zlasti pred tveganjem diskriminacije.[727]

Pri zakonskih nalogah policijskih in kazenskih pravosodnih organov je pogosto potrebna obdelava osebnih podatkov, ki ima lahko resne posledice za zadevne posameznike. Priporočilo o uporabi osebnih podatkov v policijskem sektorju, ki ga je Svet Evrope sprejel leta 1987, pogodbenicam zagotavlja smernice, kako naj načela iz posodobljene Konvencije št. 108 uveljavljajo v okviru obdelave osebnih podatkov, ki jo izvajajo policijski organi.[728] Priporočilo je bilo dopolnjeno s praktičnim vodnikom za uporabo osebnih podatkov v policijskem sektorju, ki ga je sprejel posvetovalni odbor po Konvenciji št. 108.[729]

Primer: v zadevi *D. L. proti Bolgariji*[730] so socialne službe pritožnico na podlagi sodne odločbe namestile v vzgojni zavod zaprtega tipa. Zavod je izvajal vsesplošen in neselektiven nadzor nad vso pisno korespondenco in telefonskimi pogovori. ESČP je menilo, da je bil kršen člen 8 EKČP, saj takšen ukrep v demokratični družbi ni potreben. Sodišče je navedlo, da je treba storiti vse, da se mladoletnikom, ki so nameščeni v zavod, omogočijo zadostni stiki z zunanjim svetom, saj je to del njihove pravice do dostojanstvene obravnave in je nujno potrebno, da se jih pripravi na ponovno vključitev v družbo. To velja tako za obiske kot za pisno korespondenco ali telefonske pogovore. Poleg tega se v okviru nadzora ni razlikovalo med komunikacijo z družinskimi člani ter komunikacijo z nevladnimi organizacijami za varstvo otrokovih pravic ali odvetniki. Poleg tega odločitev o prestrezanju komunikacije ni temeljila na individualni analizi tveganj v vsakem primeru posebej.

Primer: v zadevi *Dragojević proti Hrvaški*[731] je bil pritožnik osumljen, da se ukvarja z nedovoljenim prometom s prepovedanimi drogami. Za krivega je bil spoznan po tem, ko je preiskovalni sodnik odobril uporabo ukrepov tajnega nadzora za prestrezanje pritožnikovih telefonskih klicev. ESČP je menilo, da je zadevni ukrep, zoper katerega je bila vložena pritožba, pomenil poseganje

727 Posodobljena Konvencija št. 108, člen 6.

728 Svet Evrope, Odbor ministrov (1987), Priporočilo Rec(87)15 državam članicam, ki ureja uporabo osebnih podatkov v policijskem sektorju, 17. september 1987.

729 Svet Evrope (2018), Posvetovalni odbor po Konvenciji št. 108, Praktični vodnik za uporabo osebnih podatkov v policijskem sektorju, T-PD(2018)1.

730 ESČP, *D. L. proti Bolgariji*, pritožba št. 7472/14, 19. maj 2016.

731 ESČP, *Dragojević proti Hrvaški*, pritožba št. 68955/11, 15. januar 2015.

v pravico do spoštovanja zasebnega življenja in dopisovanja. Dovoljenje, ki ga je izdal preiskovalni sodnik, je temeljilo zgolj na izjavi organa pregona, da „preiskave ni mogoče izvesti drugače". ESČP je tudi ugotovilo, da so kazenska sodišča omejila svojo oceno uporabe nadzornih ukrepov in da vlada ni zagotovila informacij o pravnih sredstvih, ki so na voljo. Člen 8 EKČP je bil zato kršen.

8.1.1 Priporočilo o uporabi osebnih podatkov v policijskem sektorju

ESČP dosledno razsoja, da če policija ali organi za nacionalno varnost shranjujejo in hranijo osebne podatke, to pomeni poseganje v člen 8(1) EKČP. Utemeljitev takega poseganja je obravnavana v številnih sodbah ESČP.[732]

Primer: v zadevi *B. B. proti Franciji*[733] je bil pritožnik obstojen zaradi kršitev spolne nedotakljivosti z zlorabo položaja, ki jih je storil zoper mladoletne osebe, stare 15 let. Zaporno kazen je odslužil leta 2000. Leto pozneje je zahteval, da se omemba te obsodbe izbriše iz njegove kazenske evidence, vendar je bila njegova zahteva zavrnjena. Leta 2004 je bila na podlagi francoske zakonodaje vzpostavljena nacionalna sodna podatkovna zbirka o storilcih kaznivih dejanj zoper spolno nedotakljivost in pritožnik je bil obveščen, da je vanjo vključen. ESČP je menilo, da vključitev obsojenega storilca kaznivega dejanja zoper spolno nedotakljivost v nacionalno sodno zbirko osebnih podatkov spada na področje uporabe člena 8 EKČP. Ker pa so bili uvedeni zadostni zaščitni ukrepi za varstvo osebnih podatkov, na primer pravica posameznika, na katerega se nanašajo osebni podatki, da zahteva izbris podatkov, omejen čas hrambe podatkov in omejen dostop do takih podatkov, je bilo doseženo pravično ravnotežje med nasprotujočimi si zasebnimi in javnimi interesi. Sodišče je ugotovilo, da člen 8 EKČP ni bil kršen.

732 Glej na primer ESČP, *Leander proti Švedski*, pritožba št. 9248/81, 26. marec 1987; ESČP, *M. M. proti Združenemu kraljestvu*, pritožba št. 24029/07, 13. november 2012; ESČP, *M. K. proti Franciji*, pritožba št. 19522/09, 18. april 2013, in ESČP, *Aycaguer proti Franciji*, pritožba št. 8806/12, 22. junij 2017.

733 ESČP, *B. B. proti Franciji*, pritožba št. 5335/06, 17. december 2009.

Primer: v združenih zadevah *S. in Marper proti Združenemu kraljestvu*[734] sta bila oba pritožnika obdolžena kaznivih dejanj, vendar nista bila spoznana za kriva. Policija je kljub temu imela in hranila njune prstne odtise, celične vzorce in profil DNK. Neomejena hramba biometričnih osebnih podatkov je bila dovoljena z zakonom, če je bila oseba osumljena kaznivega dejanja, tudi če je bil osumljeni pozneje oproščen ali je bila obtožba zoper njega umaknjena. ESČP je razsodilo, da vsesplošna in neselektivna hramba osebnih podatkov, ki ni časovno omejena in pri kateri imajo oproščeni posamezniki samo omejene možnosti zahtevati izbris, pomeni nesorazmerno poseganje v pravico pritožnika do spoštovanja zasebnega življenja. Ugotovilo je, da je bil kršen člen 8 EKČP.

Ključno vprašanje v okviru elektronskih komunikacij je poseganje javnih organov v pravici do zasebnosti in varstva osebnih podatkov. Sredstvo nadzora ali prestrezanje komunikacij, kot so naprave za prisluškovanje, je dovoljeno le, če je to določeno z zakonom in če pomeni nujen ukrep v demokratični družbi, ki je v interesu:

- zaščite nacionalne varnosti,
- javne varnosti,
- denarnih interesov države,
- zatiranja kriminala ali
- varstva posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih.

V številnih drugih sodbah ESČP je obravnavana utemeljenost poseganja v pravico do zasebnosti z izvajanjem nadzora.

Primer: v zadevi *Allan proti Združenemu kraljestvu*[735] so organi na skrivaj snemali zasebne pogovore zapornika s prijateljico v zaporniškem prostoru za obiske in s soobtoženim v zaporniški celici. ESČP je razsodilo, da uporaba

734 ESČP, združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 4. december 2008, točki 119 in 125.

735 ESČP, *Allan proti Združenemu kraljestvu*, pritožba št. 48539/99, 5. november 2002.

naprav za zvočno in slikovno snemanje v pritožnikovi celici, v zaporniškem prostoru za obiske in pri sojetniku pomeni poseganje v pritožnikovo pravico do zasebnega življenja. Ker v času dejanskega stanja ni bilo zakonske ureditve, ki bi urejala policijsko uporabo naprav za skrivno snemanje, to poseganje ni bilo v skladu z zakonom. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Primer: v zadevi *Roman Zakharov proti Rusiji*[736] je pritožnik vložil tožbo zoper tri operaterje mobilnih omrežij. Trdil je, da je bila kršena njegova pravica do zasebnosti telefonskih komunikacij, saj so zadevni operaterji brez predhodne sodne odobritve namestili opremo, ki je zvezni službi nacionalne varnosti omogočala prestrezanje njegovih telefonskih komunikacij. ESČP je menilo, da nacionalne pravne določbe, s katerimi je urejeno prestrezanje komunikacij, ne zagotavljajo ustreznih in učinkovitih jamstev pred samovoljnostjo in tveganjem zlorabe. Zlasti se z nacionalno zakonodajo ni zahteval izbris shranjenih podatkov po tem, ko je bil dosežen namen hrambe. Poleg tega je bil sodni nadzor omejen, čeprav je bila potrebna sodna odobritev.

Primer: v zadevi *Szabó in Vissy proti Madžarski*[737] sta pritožnika trdila, da madžarska zakonodaja krši člen 8 EKČP, saj ni dovolj podrobna ali natančna. Poleg tega sta zatrjevala, da z njo niso zagotovljena zadostna jamstva pred zlorabo in samovoljnostjo. ESČP je ugotovilo, da se z madžarsko zakonodajo ne zahteva, da je za nadzor potrebna odobritev sodišča. Vseeno je opozorilo, da je nadzor, čeprav je pogojen z odobritvijo ministra za pravosodje, zelo političen in se z njim ne more zagotoviti, da se izvede zahtevana ocena „nujne potrebnosti". Poleg tega v nacionalni zakonodaji ni bil določen sodni nadzor, saj se zadevnim posameznikom ni poslalo nobeno obvestilo. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Ker ima obdelava osebnih podatkov, ki jo izvajajo policijski organi, lahko precejšnje posledice za zadevne osebe, so podrobna pravila o varstvu osebnih podatkov za obdelavo osebnih podatkov na tem področju še posebej nujna. To vprašanje je obravnavano v Priporočilu Sveta Evrope o uporabi osebnih podatkov v policijskem sektorju, ki vsebuje smernice o tem, kako je treba zbirati osebne podatke za policijsko delo, kako je treba hraniti zbirke osebnih podatkov na tem področju, kdo ima lahko dostop do teh zbirk, vključno s pogoji za prenos osebnih podatkov tujim policijskim organom, kako je treba posameznikom, na katere se nanašajo osebni podatki, omogočiti

736 ESČP, *Roman Zakharov proti Rusiji* (veliki senat), pritožba št. 47143/06, 4. december 2015.

737 ESČP, *Szabó in Vissy proti Madžarski*, pritožba št. 37138/14,12. januar 2016.

uveljavljanje pravic do varstva osebnih podatkov in kako je treba izvajati nadzor, ki ga zagotavljajo neodvisni organi. Obravnavana je tudi obveznost zagotavljanja ustrezne varnosti osebnih podatkov.

Priporočilo ne predvideva možnosti, da policijski organi osebne podatke zbirajo časovno neomejeno in neselektivno. Njihovo zbiranje osebnih podatkov je omejeno na to, kar je nujno za preprečevanje resne nevarnosti ali pregona nekega kaznivega dejanja. Vsako dodatno zbiranje osebnih podatkov bi moralo temeljiti na posebni nacionalni zakonodaji. Obdelava občutljivih osebnih podatkov bi morala biti omejena na to, kar je v okviru določene preiskave nujno potrebno.

Če se osebni podatki zbirajo brez vednosti posameznika, na katerega se nanašajo, ga je treba o zbiranju osebnih podatkov obvestiti takoj, ko tako razkritje več ne ogroža preiskave. Zbiranje osebnih podatkov s tehničnim nadzorom ali drugimi avtomatiziranimi sredstvi mora imeti posebno pravno podlago.

Primer: v zadevi *Versini-Campinchi in Crasnianski proti Franciji*[738] se je pritožnica, odvetnica, po telefonu pogovarjala s stranko, katere telefonski liniji se je na zahtevo preiskovalnega sodnika prisluškovalo. Iz zapisa pogovora je bilo razvidno, da je pritožnica razkrila informacije, ki jih varuje odvetniška zaupnost. Tožilec je te informacije poslal odvetniški zbornici, ki je pritožnici naložila kazen. ESČP je menilo, da je prišlo do poseganja v pravico do spoštovanja zasebnega življenja in dopisovanja ne le osebe, katere telefonskim pogovorom se je prisluškovalo, temveč tudi pritožnice, katere komunikacija je bila prestrežena in zapisana. Poseganje je bilo v skladu z zakonom in z njim se je uresničeval zakonit cilj preprečevanja nereda. Pritožnica je v okviru disciplinskega postopka, ki je bil sprožen zoper njo, dosegla ponovni preizkus zakonitosti predložitve zapisa posnetkov telefonskih prisluhov. Čeprav ni mogla vložiti predloga za ugotovitev ničnosti zapisa telefonskega pogovora, je ESČP menilo, da se je izvajal učinkovit nadzor, s katerim je bil očitani poseg omejen na tisto, kar je potrebno v demokratični družbi. ESČP je odločilo, da trditev, da bi možnost kazenskega postopka zoper odvetnika na podlagi zapisa lahko odvračilno vplivala na svobodo komunikacije med odvetnikom in njegovo stranko ter s tem na pravice stranke do obrambe, ni verodostojna, saj bi se lahko na podlagi informacij, ki jih je razkrila sama odvetnica, štelo, da je ravnala nezakonito. Zato ni bila ugotovljena kršitev člena 8 EKČP.

738 ESČP, *Versini-Campinchi in Crasnianski proti Franciji*, pritožba št. 49176/11, 16. junij 2016.

V Priporočilu Sveta Evrope o uporabi osebnih podatkov v policijskem sektorju je navedeno, da je treba pri shranjevanju osebnih podatkov jasno razlikovati med: upravnimi in policijskimi podatki, med osebnimi podatki različnih vrst posameznikov, na katere se ti podatki nanašajo, kot so osumljenci, obsojenci, žrtve in priče, ter med podatki, ki se štejejo za zanesljiva dejstva, in tistimi, ki temeljijo na sumih in domnevah.

Namen, za katerega se lahko uporabijo policijski podatki, mora biti strogo omejen. To vpliva na razkritje policijskih podatkov tretjim osebam: prenos ali razkritje takih podatkov v policijskem sektorju bi morala biti urejena glede na to, ali obstaja zakonit interes za izmenjavo informacij. Prenos ali razkritje takih podatkov zunaj policijskega sektorja bi morala biti dovoljena samo, če obstaja jasna pravna obveznost ali odobritev.

Primer: v zadevi *Karabeyoğlu proti Turčiji*[739] se je v okviru kazenske preiskave nezakonite organizacije prisluškovalo pritožnikovim telefonskim linijam, saj je obstajal sum, da je pritožnik, sodnik, član te organizacije oziroma da ji zagotavlja pomoč in podporo. Po tem, ko je bila sprejeta odločitev, da se pregon ne izvede, je državni tožilec, ki je vodil kazensko preiskavo, uničil zadevne posnetke. Vendar so sodni preiskovalci obdržali kopijo posnetkov in so jih nato uporabili v okviru disciplinskega postopka zoper pritožnika. ESČP je menilo, da je bila kršena zadevna zakonodaja, saj so bile informacije uporabljene za namene, ki niso tisti, za katere so bile informacije zbrane, in niso bile uničene v zakonsko določenem roku. Kar zadeva disciplinski postopek zoper pritožnika, poseganje v njegovo pravico do spoštovanja zasebnega življenja ni bilo v skladu z zakonom.

Mednarodni prenos ali razkritje bi morala biti omejena na tuje policijske organe in temeljiti na posebnih pravnih določbah, po možnosti mednarodnih sporazumih, razen če je to nujno za preprečevanje resne in neposredne nevarnosti.

Obdelava osebnih podatkov, ki jo izvaja policija, mora biti pod neodvisnim nadzorom, da se zagotovi upoštevanje nacionalne zakonodaje o varstvu osebnih podatkov. Posamezniki, na katere se nanašajo osebni podatki, morajo imeti vse pravice do dostopa, ki jih vsebuje posodobljena Konvencija št. 108. Če so pravice posameznikov, na katere se nanašajo osebni podatki, do dostopa v skladu s členom 11 navedene konvencije omejene v interesu učinkovitih policijskih preiskav in izvrševanja kazenskih sankcij, mora imeti tak posameznik na podlagi nacionalnega prava pravico, da se

739 ESČP, *Karabeyoğlu proti Turčiji*, pritožba št. 30083/10, 7. junij 2016.

pritoži pri nacionalnem nadzornem organu za varstvo osebnih podatkov ali drugem neodvisnem organu.

8.1.2 Budimpeška konvencija o kibernetski kriminaliteti

Ker pri kriminalnih dejavnostih narašča uporaba elektronskih sistemov za obdelavo osebnih podatkov in te dejavnosti vse bolj vplivajo nanje, so za spopadanje s tem izzivom potrebne nove kazenskopravne določbe. Svet Evrope je zato sprejel mednarodni pravni instrument, Konvencijo o kibernetski kriminaliteti, znano tudi kot Budimpeška konvencija, da bi obravnaval vprašanje kaznivih dejanj, storjenih zoper elektronska omrežja in z njimi.[740] K tej konvenciji lahko pristopijo tudi države, ki niso članice Sveta Evrope. Na začetku leta 2018 je bilo med njenimi pogodbenicami 14 držav nečlanic,[741] še sedem drugih pa je bilo povabljenih, da pristopijo k njej.

Konvencija o kibernetski kriminaliteti ostaja najvplivnejša mednarodna pogodba, v kateri se obravnavajo kršitve zakona prek interneta ali drugih informacijskih omrežij. Pogodbenicam nalaga, naj posodobijo in uskladijo svojo kazenskopravno zakonodajo proti vdorom v računalniške sisteme in drugim varnostnim kršitvam, vključno s kršitvami avtorske pravice, računalniškimi goljufijami, otroško pornografijo in drugimi nezakonitimi kibernetskimi dejavnostmi. Konvencija določa tudi procesna pooblastila za preiskovanje računalniških omrežij in prestrezanje komunikacij v okviru boja proti kibernetski kriminaliteti. Ne nazadnje omogoča tudi učinkovito mednarodno sodelovanje. V Dodatnem protokolu h Konvenciji je obravnavana kriminalizacija rasistične in ksenofobične propagande v računalniških omrežjih.

Čeprav Konvencija ni instrument za spodbujanje varstva osebnih podatkov, so z njo kriminalizirane dejavnosti, s katerimi bi se verjetno kršila pravica posameznika do varstva osebnih podatkov. Poleg tega morajo pogodbenice v skladu z njo sprejeti zakonodajne ukrepe, s katerimi nacionalnim organom omogočijo prestrezanje podatkov o prometu in vsebini.[742] Konvencija tudi določa, da morajo pogodbenice pri njenem izvajanju predvideti ustrezno varstvo človekovih pravic in svoboščin,

740 Svet Evrope, Odbor ministrov (2001), Konvencija o kibernetski kriminaliteti z dne 23. novembra 2001, ki je začela veljati 1. julija 2004, Budimpešta, CETS št. 185.

741 Avstralija, Čile, Dominikanska republika, Izrael, Japonska, Kanada, Kolumbija, Panama, Republika Mauritius, Senegal, Šrilanka, Tonga, Tunizija in Združene države Amerike. Glej preglednico podpisov in ratifikacij Pogodbe št. 185, stanje julija 2017.

742 Svet Evrope, Odbor ministrov (2001), Konvencija o kibernetski kriminaliteti z dne 23. novembra 2001, Budimpešta, CETS št. 185, člena 20 in 21.

vključno s pravicami, zagotovljenimi z EKČP, na primer pravico do varstva osebnih podatkov.[743] Od pogodbenic se ne zahteva, da pristopijo tudi h Konvenciji št. 108, da bi lahko pristopile k Budimpeški konvenciji o kibernetski kriminaliteti.

8.2 Pravo EU o varstvu osebnih podatkov pri policijskih zadevah in zadevah s področja kazenskega pravosodja

Ključni poudarki

- V EU je varstvo osebnih podatkov v policijskem sektorju in sektorju kazenskega pravosodja urejeno v okviru nacionalne in čezmejne obdelave, ki jo izvajajo policija in organi kazenskega pravosodja držav članic ter akterji EU.
- Na ravni držav članic je treba direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, prenesti v nacionalno pravo.
- Varstvo osebnih podatkov v okviru čezmejnega sodelovanja policijskih organov in organov kazenskega pregona, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu, je urejeno s posebnimi pravnimi instrumenti.
- Za Evropski policijski urad (Europol), Urad za evropsko pravosodno sodelovanje (Eurojust) in novo ustanovljeno Evropsko javno tožilstvo, ki so organi EU za pomoč in spodbujanje čezmejnega sodelovanja organov odkrivanja in pregona, se uporabljajo posebna pravila o varstvu osebnih podatkov.
- Posebna pravila o varstvu osebnih podatkov obstajajo tudi za skupne informacijske sisteme, ki so na ravni EU vzpostavljeni za čezmejne izmenjave informacij med pristojnimi policijskimi in pravosodnimi organi. Pomembni so zlasti schengenski informacijski sistem druge generacije (SIS II), vizumski informacijski sistem (VIS) in Eurodac, centraliziran sistem, ki vsebuje podatke o prstnih odtisih državljanov tretjih držav in oseb brez državljanstva, ki zaprosijo za azil v eni od držav članic EU.
- EU trenutno posodablja zgoraj navedene določbe o varstvu osebnih podatkov, da bi bile v skladu z določbami direktive o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja.

743 Prav tam, člen 15(1).

8.2.1 Direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja

Cilj Direktive (EU) 2016/680 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov (direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja),[744] je varstvo osebnih podatkov, ki se zbirajo in obdelujejo za namene kazenskega pravosodja, in sicer:

- za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;
- za izvršitev kazenske sankcije in
- v primerih, ko policija in drugi organi pregona ukrepajo, da bi zagotovili spoštovanje prava ter varovali pred grožnjami javni varnosti in temeljnim pravicam družbe, ki bi lahko pomenile kaznivo dejanje, in take grožnje preprečevali.

Z direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, se varujejo osebni podatki različnih kategorij posameznikov, vključenih v kazenski postopek, kot so priče, informatorji, žrtve, osumljenci in sostorilci. Kadar policija in organi kazenskega pravosodja obdelujejo take osebne podatke za namene kazenskega pregona, morajo ravnati v skladu z določbami direktive, kar velja tako za osebno kot stvarno področje uporabe direktive.[745]

Vendar je pod določenimi pogoji dovoljena tudi uporaba osebnih podatkov za druge namene. Obdelava osebnih podatkov za namen kazenskega pregona, ki ni namen, za katerega so bili osebni podatki zbrani, je dovoljena le, če je zakonita, potrebna in

744 Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89) (direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja).

745 Direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, člen 2(1).

sorazmerna v skladu z nacionalnim pravom ali pravom EU.[746] V zvezi z drugimi nameni se uporabljajo pravila SUVP. Vodenje dnevnikov o izmenjavi osebnih podatkov in njeno dokumentiranje sta dve od posebnih nalog pristojnih organov, ki pomagata pri pojasnjevanju odgovornosti v primeru pritožb.

Pristojni organi, ki delujejo na področju policije in kazenskega pravosodja, so javni organi ali organi, ki so pooblaščeni v skladu z nacionalnim pravom in imajo javna pooblastila za opravljanje nalog javnega organa,[747] na primer zasebni zapori.[748] Direktiva se uporablja za obdelavo osebnih podatkov na nacionalni ravni, čezmejno obdelavo med policijskimi in pravosodnimi organi držav članic ter mednarodne prenose v tretje države in mednarodne institucije, ki jih opravijo pristojni organi.[749] Z njo ni zajeta nacionalna varnost ali obdelava osebnih podatkov v institucijah, organih, uradih in agencijah EU.[750]

Direktiva večinoma temelji na načelih in opredelitvah iz SUVP, pri čemer je v njej upoštevana posebna narava področij policije in kazenskega pravosodja. Nadzor lahko izvajajo isti organi držav članic, ki ga izvajajo v skladu s SUVP. V zadevno direktivo sta bila kot novi obveznosti za policijo in organe kazenskega pravosodja vključena imenovanje pooblaščenih uradnikov za varstvo podatkov in izvajanje ocen učinka v zvezi z varstvom podatkov.[751] Čeprav ta pojma temeljita na SUVP, je v navedeni direktivi obravnavana posebna narava policije in organov kazenskega pravosodja. V primerjavi z obdelavo osebnih podatkov za komercialne namene, ki je urejena z navedeno uredbo, je lahko pri obdelavi, povezani z varnostjo, potrebna določena raven prožnosti. Če bi se na primer posameznikom, na katere se nanašajo osebni podatki, zagotovila enaka raven varstva v smislu pravic do obveščenosti, dostopa do njihovih osebnih podatkov ali njihovega izbrisa, kot v skladu s SUVP, bi to lahko pomenilo, da bi vsaka dejavnost nadzora, ki se izvaja za namene kazenskega pregona, v okviru kazenskega pregona postala neučinkovita. Direktiva zato ne vsebuje načela

746 Prav tam, člen 4(2).

747 Prav tam, člen 3(7).

748 Evropska komisija (2016), Sporočilo Komisije Evropskemu parlamentu v skladu s členom 294(6) Pogodbe o delovanju Evropske unije v zvezi s stališčem Sveta o sprejetju Direktive Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ, COM(2016) 213 final, Bruselj, 11. april 2016.

749 Direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, poglavje V.

750 Prav tam, člen 2(3).

751 Prav tam, v členu 32 oziroma členu 27.

preglednosti. Podobno je treba pri obdelavi, povezani z varnostjo, prožno uporabljati tudi načeli najmanjšega obsega podatkov in omejitve namena, v skladu s katerima je treba osebne podatke omejiti le na tiste, ki so potrebni za namene, za katere se obdelujejo, ter jih obdelovati za določene in izrecne namene. Informacije, ki jih pristojni organi zberejo in shranijo v zvezi s konkretnim primerom, so lahko izjemno koristne pri reševanju prihodnjih primerov.

Načela v zvezi z obdelavo

V direktivi o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, so določeni nekateri ključni zaščitni ukrepi v zvezi z uporabo osebnih podatkov. V njej so pojasnjena tudi načela, na katerih temelji obdelava teh podatkov. Države članice morajo v zvezi z osebnimi podatki zagotoviti, da:

- se obdelujejo zakonito in pošteno;
- so zbrani za določene, izrecne in zakonite namene ter da se ne obdelujejo na način, ki je nezdružljiv s temi nameni;
- so ustrezni, relevantni in ne prekomerni glede na namene, za katere se obdelujejo;
- so točni in se po potrebi posodabljajo; sprejeti je treba vse razumne ukrepe za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo, ob upoštevanju namenov, za katere se obdelujejo;
- se hranijo v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, in le toliko časa, kolikor je potrebno za namene, za katere se obdelujejo;
- se obdelujejo na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo, in sicer z ustreznimi tehničnimi ali organizacijskimi ukrepi.[752]

V skladu s to direktivo je obdelava zakonita le, če se izvaja v obsegu, ki je potreben za opravljanje ustrezne naloge. Poleg tega bi jo moral izvajati pristojni organ za

752 Prav tam, člen 4(1).

doseganje ciljev, opredeljenih v tej direktivi, temeljiti pa bi morala na pravu EU ali nacionalnem pravu.[753] Osebne podatke, ki se hranijo le toliko časa, kolikor je potrebno, je treba v določenih rokih izbrisati ali jih redno pregledovati. Uporabljati jih mora le pristojni organ, in sicer le za namene, za katere so bili zbrani, posredovani ali dani na voljo.

Pravice posameznika, na katerega se nanašajo osebni podatki

V zadevni direktivi so določene tudi naslednje pravice posameznika, na katerega se nanašajo osebni podatki.

- Pravica do informacij: države članice morajo upravljavcu osebnih podatkov naložiti obveznost, da posameznику, na katerega se nanašajo osebni podatki, da na voljo 1) informacije o identiteti in kontaktne podatke upravljavca, 2) kontaktne podatke pooblaščene osebe za varstvo podatkov, 3) informacije o namenih predvidene obdelave, 4) informacije o pravici do vložitve pritožbe pri nadzornem organu in njegove kontaktne podatke ter 5) informacije o pravici do dostopa do osebnih podatkov, njihovega popravka ali izbrisa ter do omejitve obdelave osebnih podatkov.[754] Direktiva poleg teh splošnih zahtev po informacijah določa, da morajo upravljavci v posebnih primerih posameznikom, na katere se nanašajo osebni podatki, dati na voljo informacije o pravni podlagi za obdelavo in obdobju hrambe osebnih podatkov, s čimer jim omogočijo uveljavljanje njihovih pravic. Če se bodo osebni podatki posredovali drugim uporabnikom, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah, je treba posameznike, na katere se nanašajo osebni podatki, obvestiti o kategorijah takih uporabnikov. Upravljavci morajo po potrebi zagotoviti dodatne informacije, pri čemer se upoštevajo posebne okoliščine, v katerih se obdelujejo osebni podatki, na primer kadar so bili osebni podatki zbrani med tajnim nadzorom, tj. brez vednosti posameznika, na katerega se nanašajo osebni podatki. S tem se zagotovi, da je obdelava poštena do posameznika, na katerega se nanašajo osebni podatki.[755]

- Pravica do dostopa do osebnih podatkov: države članice morajo zagotoviti, da ima posameznik, na katerega se nanašajo osebni podatki, pravico vedeti, ali se njegovi osebni podatki obdelujejo. Če se, bi moral imeti dostop do nekaterih

753 Prav tam, člen 8.

754 Prav tam, člen 13(1).

755 Prav tam, člen 13(2).

informacij, na primer vrst osebnih podatkov, ki se obdelujejo.[756] Vendar se ta pravica lahko omeji, na primer da se prepreči oviranje preiskave ali vplivanje na pregon kaznivega dejanja ali da se zaščitijo javna varnost ter pravice in svoboščine drugih.[757]

- Pravica do popravka osebnih podatkov: države članice morajo zagotoviti, da lahko posameznik, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja doseže popravek netočnih osebnih podatkov. Poleg tega ima tudi pravico do dopolnitve nepopolnih osebnih podatkov.[758]

- Pravica do izbrisa osebnih podatkov in omejitve obdelave: upravljavec mora v nekaterih primerih izbrisati osebne podatke. Poleg tega lahko posameznik, na katerega se nanašajo osebni podatki, doseže izbris svojih osebnih podatkov, vendar le v primeru njihove nezakonite obdelave.[759] V nekaterih primerih se lahko namesto izbrisa osebnih podatkov omeji njihova obdelava. To se lahko zgodi v primerih, kadar 1) se izpodbija točnost osebnih podatkov, vendar te ni mogoče preveriti, ali 2) kadar so osebni podatki potrebni za namene dokazovanja.[760]

Kadar upravljavec zavrne popravek ali izbris osebnih podatkov ali omejitev njihove obdelave, je treba posameznika, na katerega se nanašajo osebni podatki, o tem pisno obvestiti. Države članice lahko to pravico do obveščenosti omejijo, da med drugim zaščitijo javno varnost ali pravice in svoboščine drugih, in sicer iz istih razlogov kot pri omejitvi pravice do dostopa.[761]

Posameznik, na katerega se nanašajo osebni podatki, ima običajno pravico do informacij o obdelavi svojih osebnih podatkov, poleg tega ima tudi pravico do dostopa, popravka ali izbrisa osebnih podatkov ali omejitve obdelave, ki jo lahko uveljavlja neposredno pri upravljavcu. Kot nadomestna možnost je v skladu z direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, mogoče tudi posredno uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, veljati pa začne, ko upravljavec omeji pravico navedenega

756 Prav tam, člen 14.
757 Prav tam, člen 15.
758 Prav tam, člen 16(1).
759 Prav tam, člen 16(2).
760 Prav tam, člen 16(3).
761 Prav tam, člen 16(4).

posameznika.[762] Države članice morajo v skladu s členom 17 zadevne direktive sprejeti ukrepe, s katerimi se zagotovi, da lahko posamezniki, na katere se nanašajo osebni podatki, svoje pravice uveljavljajo tudi prek pristojnega nadzornega organa. Upravljavec mora zato posameznika, na katerega se nanašajo osebni podatki, obvestiti o možnosti posrednega dostopa.

Obveznosti upravljavca in obdelovalca

V okviru direktive o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, so upravljavci podatkov pristojni javni organi ali drugi organi z ustreznimi javnimi pooblastili in pristojnostmi, ki določijo namene in načine obdelave osebnih podatkov. Direktiva določa več obveznosti upravljavcev osebnih podatkov za zagotavljanje visoke ravni varstva osebnih podatkov, ki se obdelujejo za namene kazenskega pregona.

Pristojni organi morajo voditi dnevnike o dejanjih obdelave, ki jih izvajajo v avtomatiziranih sistemih obdelave. Dnevnike je treba voditi vsaj za zbiranje osebnih podatkov, njihovo predelavo in vpogled vanje ter njihovo razkritje, vključno s prenosi, kombiniranje in izbris.[763] Direktiva določa, da morajo dnevniki vpogleda in razkritja omogočati opredelitev datuma in časa dejanj, njihovo utemeljitev ter, če je to mogoče, identifikacijo osebe, ki je vpogledala v sistem ali razkrila osebne podatke, ter identiteto uporabnikov zadevnih osebnih podatkov. Dnevniki se lahko uporabljajo zgolj za preverjanje zakonitosti obdelave, notranje spremljanje, zagotavljanje neoporečnosti in varnosti osebnih podatkov ter v kazenskih postopkih.[764] Upravljavec in obdelovalec morata nadzornemu organu na zahtevo omogočiti dostop do dnevnikov.

Za upravljavce obstaja zlasti splošna obveznost, da izvajajo ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovijo, da obdelava poteka v skladu z zadevno direktivo, in da so zmožni dokazati zakonitost take obdelave.[765] Pri oblikovanju teh ukrepov morajo upoštevati naravo, obseg, okoliščine obdelave in, kar je posebej pomembno, morebitna tveganja za pravice in svoboščine posameznikov. Upravljavci bi morali sprejeti notranje politike in izvajati ukrepe, ki spodbujajo skladnost z načeli varstva osebnih podatkov, zlasti načelom vgrajenega in privzetega varstva osebnih

762 Prav tam, člen 17.

763 Prav tam, člen 25(1).

764 Prav tam, člen 25(2).

765 Prav tam, člen 19.

podatkov.[766] Kadar je verjetno, da bi lahko obdelava povzročila veliko tveganje za pravice posameznikov, na primer zaradi uporabe novih tehnologij, morajo upravljavci pred začetkom obdelave opraviti oceno učinka v zvezi z varstvom osebnih podatkov.[767] V tej direktivi so navedeni tudi ukrepi, ki jih morajo izvajati upravljavci za zagotavljanje varnosti obdelave. Med njimi so ukrepi za preprečevanje nepooblaščenega dostopa do osebnih podatkov, ki jih obdelujejo, ter ukrepi za zagotavljanje, da imajo pooblaščene osebe dostop samo do osebnih podatkov, ki jih zajema njihovo pooblastilo za dostop, da funkcije sistema za obdelavo ustrezno delujejo in da shranjeni osebni podatki ne morejo postati okvarjeni zaradi okvare sistema.[768] Če pride do kršitve varnosti osebnih podatkov, morajo upravljavci v treh dneh obvestiti nadzorni organ, pri čemer v obvestilu opišejo vrsto kršitve, njene verjetne posledice, vrste zadevnih osebnih podatkov in približno število zadevnih prizadetih posameznikov, na katere se nanašajo osebni podatki. Kršitev varnosti osebnih podatkov je poleg tega treba brez nepotrebnega odlašanja sporočiti posamezniku, na katerega se nanašajo osebni podatki, če je verjetno, da bi kršitev lahko povzročila veliko tveganje za njegove pravice in svoboščine.[769]

Z zadevno direktivo, v kateri je določeno načelo odgovornosti, je upravljavcem naložena dolžnost, da izvajajo ukrepe za zagotavljanje skladnosti z navedenim načelom. Upravljavci morajo voditi evidence vseh vrst dejavnosti obdelave, za katere so odgovorni. Podrobna vsebina takih evidenc je določena v členu 24 navedene direktive. Nadzornemu organu je treba na zahtevo omogočiti dostop do evidenc, da lahko spremlja dejanja obdelave, ki jih izvaja upravljavec. Še en pomemben ukrep za okrepitev odgovornosti je imenovanje pooblaščene osebe za varstvo podatkov. Upravljavci morajo imenovati pooblaščeno osebo za varstvo podatkov, čeprav lahko države članice v skladu z navedeno direktivo iz te obveznosti izvzamejo sodišča in druge neodvisne pravosodne organe.[770] Naloge pooblaščene osebe za varstvo podatkov po navedeni direktivi so podobne njenim nalogam iz SUVP. Ta oseba spremlja skladnost z navedeno direktivo, zagotavlja informacije in svetuje zaposlenim, ki izvajajo obdelavo osebnih podatkov, o njihovih obveznostih v skladu z zakonodajo o varstvu osebnih podatkov. Pooblaščena oseba za varstvo podatkov poleg tega svetuje glede potrebe po izvedbi ocene učinka v zvezi z varstvom podatkov in deluje kot kontaktna točka za nadzorni organ.

766 Prav tam, člen 20.

767 Prav tam, člen 27.

768 Prav tam, člen 29.

769 Prav tam, člena 30 in 31.

770 Prav tam, člen 32.

Prenosi v tretje države ali mednarodne organizacije

Podobno kot v SUVP so tudi v navedeni direktivi določeni pogoji za prenos osebnih podatkov v tretje države ali mednarodne organizacije. Če bi se osebni podatki prosto prenašali zunaj jurisdikcije EU, bi lahko bili ogroženi zaščitni ukrepi in visoka raven varstva, ki se zagotavljajo na podlagi prava EU. Vendar se sami pogoji precej razlikujejo od pogojev iz SUVP. Prenos osebnih podatkov v tretje države ali mednarodne organizacije je dovoljen, če:[771]

- je prenos potreben za cilje navedene direktive;
- se osebni podatki prenesejo pristojnemu organu – v smislu navedene direktive – tretje države ali mednarodne organizacije, čeprav se v posameznih in posebnih primerih uporablja odstopanje od tega pravila;[772]
- je za prenos osebnih podatkov, prejetih v okviru čezmejnega sodelovanja, potrebno dovoljenje države članice, iz katere izvirajo osebni podatki, v tretje države ali mednarodne organizacije, čeprav v nujnih primerih obstajajo izjeme;
- je Evropska komisija sprejela sklep o ustreznosti ali so bili sprejeti ustrezni zaščitni ukrepi ali se uporablja odstopanje za prenos v posebnih primerih;
- je za nadaljnje prenose osebnih podatkov v drugo tretjo državo ali mednarodno organizacijo potrebno predhodno dovoljenje pristojnega organa, ki je izvedel prvotni prenos, pri čemer ta organ med drugim upošteva resnost kaznivega dejanja in raven varstva osebnih podatkov v ciljni državi drugega mednarodnega prenosa.[773]

V skladu z zadevno direktivo se prenosi osebnih podatkov lahko izvedejo, če je izpolnjen eden od treh pogojev. Prvi pogoj je, da je Evropska komisija izdala sklep o ustreznosti v skladu z navedeno direktivo. Ta se lahko uporablja za celotno ozemlje tretje države, za posamezne sektorje tretje države ali za mednarodno organizacijo. Vendar je ta sklep mogoče sprejeti le, če je zagotovljena ustrezna raven varstva in so izpolnjeni pogoji iz navedene direktive.[774] V takih primerih za prenos osebnih podatkov

771 Prav tam, člen 35.

772 Prav tam, člen 39.

773 Prav tam, člen 35(1).

774 Prav tam, člen 36.

ni potrebno dovoljenje države članice.[775] Evropska komisija mora spremljati razvoj dogodkov, ki bi lahko vplivali na izvajanje sklepov o ustreznosti. Poleg tega mora sklep vključevati mehanizem za redni pregled. Komisija lahko tudi razveljavi, spremeni ali začasno odloži izvajanje sklepa, če je iz razpoložljivih informacij razvidno, da tretja država ali mednarodna organizacija ne zagotavlja več ustrezne ravni varstva. V tem primeru mora Komisija začeti posvetovanja s to tretjo državo ali mednarodno organizacijo, da bi izboljšala stanje.

Če sklep o ustreznosti ni bil sprejet, lahko prenosi temeljijo na ustreznih zaščitnih ukrepih. Ti so lahko določeni v pravno zavezujočem instrumentu ali pa upravljavec opravi lastno oceno okoliščin v zvezi s prenosom osebnih podatkov in ugotovi, da obstajajo ustrezni zaščitni ukrepi. Pri tej oceni bi bilo treba upoštevati morebitne sporazume o sodelovanju, sklenjene med Europolom ali Eurojustom in tretjo državo ali mednarodno organizacijo, obstoj obveznosti glede zaupnosti in načela omejitve namena ter dana zagotovila, da se osebni podatki ne bodo uporabljali za kakršno koli obliko krutega in nečloveškega ravnanja, vključno s smrtno kaznijo.[776] V tem zadnjem primeru mora upravljavec pristojni nadzorni organ obvestiti o kategorijah prenosov, izvedenih na podlagi takšne ocene.[777]

Če sklep o ustreznosti ni bil sprejet in niso bili vzpostavljeni ustrezni zaščitni ukrepi, je prenose še vedno mogoče dovoliti v posebnih primerih, ki so navedeni v zadevni direktivi. Ti med drugim vključujejo zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge osebe ter preprečitev neposredne in resne grožnje javni varnosti v državi članici ali tretji državi.[778]

V posameznih in posebnih primerih lahko pristojni organi prenesejo osebne podatke uporabnikom, ustanovljenim v tretjih državah, ki niso pristojni organi, če so poleg enega od treh zgoraj opisnih pogojev izpolnjeni tudi dodatni pogoji iz člena 39 zadevne direktive. Zlasti mora biti prenos nujno potreben za izvajanje naloge pristojnega organa, ki osebne podatke prenese, ki je odgovoren tudi za ugotovitev, da nobena temeljna pravica ali svoboščina posameznikov ne prevlada nad javnim interesom, ki utemeljuje prenos. Take prenose je treba dokumentirati, pristojni organ, ki osebne podatke prenese, pa mora obvestiti pristojni nadzorni organ.[779]

775 Prav tam, člen 36(1).

776 Prav tam, uvodna izjava 71.

777 Prav tam, člen 37(1).

778 Prav tam, člen 38(1).

779 Prav tam, člen 37(3).

V zvezi s tretjimi državami in mednarodnimi organizacijami je v skladu z direktivo treba oblikovati tudi mehanizme mednarodnega sodelovanja za spodbujanje učinkovitega izvrševanja zakonodaje, s čimer zadevna direktiva nadzornim organom za varstvo podatkov lajša sodelovanje s tujimi nadzornimi organi za varstvo podatkov.[780]

Neodvisen nadzor in pravna sredstva za posameznike, na katere se nanašajo osebni podatki

Vsaka država članica mora zagotoviti, da je eden ali več neodvisnih nacionalnih nadzornih organov pristojnih za svetovanje in spremljanje uporabe določb, sprejetih v skladu z zadevno direktivo.[781] Nadzorni organ, ustanovljen za namene te direktive, je lahko isti kot nadzorni organ, ustanovljen v skladu s SUVP, vendar lahko države članice imenujejo drug organ, če ta izpolnjuje merila neodvisnosti. Nadzorni organi poleg tega obravnavajo zahtevke, ki jih vloži katera koli oseba glede varstva svojih pravic in svoboščin v zvezi z obdelavo osebnih podatkov, ki jo izvajajo pristojni organi.

Če se uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, zavrne na podlagi tehtnih razlogov, mora imeti zadevni posameznik pravico vložiti pritožbo pri pristojnem nacionalnem nadzornem organu in/ali sodišču. Če oseba utrpi škodo zaradi kršitve nacionalnega prava, s katerim se izvaja zadevna direktiva, ima pravico, da od upravljavca ali drugega organa, pristojnega v skladu s pravom države članice, dobi odškodnino.[782] Na splošno morajo imeti posamezniki, na katere se nanašajo osebni podatki, dostop do pravnega sredstva za vsako kršitev svojih pravic, zagotovljenih z nacionalnim pravom, s katerim se izvaja navedena direktiva.[783]

8.3 Drugi posebni pravni instrumenti o varstvu osebnih podatkov v zadevah kazenskega pregona

Izmenjava informacij, ki jih imajo države članice na določenih področjih, je poleg z direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega

780 Prav tam, člen 40.

781 Prav tam, člen 41.

782 Prav tam, člen 56.

783 Prav tam, člen 54.

pravosodja, urejena tudi z več pravnimi instrumenti, kot so Okvirni sklep Sveta 2009/315/PNZ o organizaciji in vsebini izmenjave informacij iz kazenske evidence med državami članicami, Sklep Sveta 2000/642/PNZ o dogovoru glede sodelovanja med enotami za finančni nadzor (FIU-ji) držav članic pri izmenjavi informacij in Okvirni sklep Sveta 2006/960/PNZ o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona držav članic Evropske unije.[784]

Pomembno je, da čezmejno sodelovanje[785] med pristojnimi organi vse bolj vključuje izmenjavo podatkov o priseljevanju. To pravno področje ne spada med policijske in kazenskopravne zadeve, vendar je kljub temu v številnih vidikih pomembno za delo policije in pravosodnih organov. Enako velja za podatke o blagu, ki se uvaža v EU in izvaža iz nje. Z odpravo kontrol na notranjih mejah schengenskega območja se je povečalo tveganje goljufij, zato morajo države članice poglobiti sodelovanje, zlasti s krepitvijo čezmejne izmenjave informacij, da bi učinkoviteje odkrivale in preganjale kršitve nacionalne in evropske carinske zakonodaje. Ker se je poleg tega v zadnjih letih v svetu povečalo število primerov hudih kaznivih dejanj in organiziranega kriminala ter terorizma, ki lahko vključujejo mednarodna potovanja, se je v številnih primerih pokazala potreba po okrepljenem čezmejnem policijskem sodelovanju in sodelovanju organov kazenskega pregona.[786]

Prümski sklep

Pomemben primer institucionaliziranega čezmejnega sodelovanja z izmenjavo osebnih podatkov, shranjenih na nacionalni ravni, je Sklep Sveta 2008/615/PNZ skupaj s svojimi izvedbenimi določbami o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu (Prümski sklep), s katerim je

784 Svet Evropske unije (2009), Okvirni sklep Sveta 2009/315/PNZ z dne 26. februarja 2009 o organizaciji in vsebini izmenjave informacij iz kazenske evidence med državami članicami (UL L 93, 7.4.2009, str. 23); Svet Evropske unije (2000), Sklep Sveta 2000/642/PNZ z dne 17. oktobra 2000 o dogovoru glede sodelovanja med enotami za finančni nadzor (FIU-ji) držav članic pri izmenjavi informacij (UL L 271, 24.10.2000, str. 4); Svet Evropske unije, Okvirni sklep Sveta 2006/960/PNZ z dne 18. decembra 2006 o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona držav članic Evropske unije (UL L 386, 29.12.2006, str. 89).

785 Evropska komisija (2012), Sporočilo Komisije Evropskemu parlamentu in Svetu,Krepitev sodelovanja na področju kazenskega pregona v EU: evropski model za izmenjavo informacij (EIXM), COM(2012) 735 final, Bruselj, 7. december 2012.

786 Evropska komisija (2011), Predlog direktive Evropskega parlamenta in Sveta o uporabi podatkov iz evidence podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj, COM(2011) 32 final, Bruselj, 2. februar 2011, str. 1.

bila Prümska pogodba leta 2008 vključena v pravo EU.[787] Prümska pogodba je bila mednarodni sporazum o policijskem sodelovanju, ki so ga leta 2005 podpisali Avstrija, Belgija, Francija, Luksemburg, Nemčija, Nizozemska in Španija.[788]

Prümski sklep naj bi državam članicam podpisnicam pomagal izboljšati izmenjavo informacij za preprečevanje kriminala in boj proti njemu na treh področjih: terorizem, čezmejni kriminal in nezakonite migracije. Sklep zato vsebuje določbe v zvezi z:

- avtomatiziranim dostopom do profilov DNK, podatkov o prstnih odtisih ter nekaterih nacionalnih podatkov iz registrov vozil;
- zagotavljanjem podatkov o pomembnih dogodkih, ki imajo čezmejno razsežnost;
- zagotavljanjem podatkov za preprečevanje terorističnih dejanj;
- drugimi ukrepi za poglobitev čezmejnega policijskega sodelovanja.

Podatkovne zbirke, ki se dajo na voljo na podlagi Prümskega sklepa, so v celoti urejene z nacionalnim pravom, izmenjava osebnih podatkov pa je dodatno urejena s tem sklepom, katerega skladnost z direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, bo treba oceniti. Organi, pristojni za nadzor nad prenosom takih osebnih podatkov, so nacionalni nadzorni organi za varstvo osebnih podatkov.

Okvirni sklep 2006/960/PNZ – švedska pobuda

Okvirni sklep 2006/960/PNZ (švedska pobuda)[789] je še en primer čezmejnega sodelovanja v zvezi z izmenjavo osebnih podatkov, ki jih na nacionalni ravni hranijo organi kazenskega pregona. Člen 8 švedske pobude, ki je izrecno osredotočena na

787 Svet Evropske unije (2008), Sklep Sveta 2008/615/PNZ z dne 23. junija 2008 o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu (UL L 210, 6.8.2008, str. 1).

788 Konvencija med Kraljevino Belgijo, Zvezno republiko Nemčijo, Kraljevino Španijo, Francosko republiko, Velikim vojvodstvom Luksemburg, Kraljevino Nizozemsko in Republiko Avstrijo o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu ter nezakonitemu priseljevanju.

789 Svet Evropske unije (2006), Okvirni sklep Sveta 2006/960/PNZ z dne 18. decembra 2006 o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona držav članic Evropske unije (UL L 386, 29.12.2006, str. 89).

izmenjavo obveščevalnih podatkov in informacij, določa posebna pravila o varstvu osebnih podatkov.

V skladu s tem instrumentom mora biti uporaba izmenjanih informacij in obveščevalnih podatkov urejena z nacionalnimi določbami o varstvu osebnih podatkov države članice, ki prejme informacije, in sicer v skladu z enakimi pravili, kot če bi se zbrali v navedeni državi članici. V členu 8 je poleg tega navedeno, da lahko pristojni organ kazenskega pregona pri zagotavljanju informacij in obveščevalnih podatkov v skladu z nacionalnim pravom določi pogoje njihove uporabe, ki jih mora izpolnjevati pristojni organ kazenskega pregona, ki prejme informacije. Ti pogoji se lahko uporabljajo tudi za poročanje o izsledkih preiskave kaznivega dejanja ali operacije zbiranja obveščevalnih podatkov o kaznivih dejanjih, v okviru katerih je bila potrebna izmenjava informacij in obveščevalnih podatkov. Kadar pa so v nacionalnem pravu določene izjeme od omejitev glede uporabe (npr. za pravosodne organe, zakonodajna telesa itd.), se lahko informacije in obveščevalni podatki uporabljajo šele po predhodnem posvetovanju z državo članico, ki sporoča informacije in obveščevalne podatke.

Informacije in obveščevalni podatki se lahko uporabijo:

- za namene, za katere so bili posredovani, ali
- za preprečevanje neposredne in resne grožnje javni varnosti.

Obdelava v druge namene se lahko dovoli, vendar le s predhodno odobritvijo države članice, ki sporoča informacije in obveščevalne podatke.

V švedski pobudi je poleg tega navedeno, da je treba osebne podatke, ki se obdelujejo, varovati v skladu z mednarodnimi instrumenti, kot so:

- Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov;[790]
- dodatni protokol k navedeni konvenciji z dne 8. novembra 2001 v zvezi z nadzornimi organi in čezmejnim prenosom podatkov;[791]

790 Svet Evrope (1981), Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, CETS št. 108.

791 Svet Evrope (2001), Dodatni protokol h Konvenciji o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov v zvezi z nadzornimi organi in čezmejnim prenosom podatkov, CETS št. 181.

- Priporočilo R(87)15 Sveta Evrope državam članicam, ki ureja uporabo osebnih podatkov v policijskem sektorju.[792]

Direktiva EU o evidenci podatkov o potnikih

Podatki iz evidence podatkov o potnikih (PNR) se nanašajo na informacije o letalskih potnikih, ki se zberejo in hranijo v sistemih rezervacij in sistemih za nadzor odhodov pri letalskih prevoznikih. Ti podatki zajemajo več raznovrstnih informacij, na primer datume potovanja, načrt potovanja, informacije o vozovnici, kontaktne podatke, navedbo potovalne agencije, prek katere je bil let rezerviran, uporabljene načine plačila, številko sedeža in podatke o prtljagi.[793] Obdelava podatkov PNR je lahko organom kazenskega pregona v pomoč pri identifikaciji znanih ali potencialnih osumljencev in izvajanju ocen, ki temeljijo na vzorcih potovanja in drugih kazalnikih, ki so običajno povezani s kaznivimi dejavnostmi. Analiza podatkov PNR omogoča tudi naknadno spremljanje prepotovanih poti in stikov oseb, za katere se sumi, da so sodelovale v kaznivih dejavnostih, kar lahko organom kazenskega pregona omogoči odkrivanje kriminalnih mrež.[794] Kot je pojasnjeno v razdelku 7, je EU sklenila nekatere sporazume s tretjimi državami za izmenjavo podatkov PNR. Poleg tega je z Direktivo (EU) 2016/681 o uporabi podatkov PNR za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (direktiva EU o PNR) uvedla obdelavo podatkov PNR v EU.[795] V tej direktivi so določene obveznosti za letalske prevoznike, da podatke PNR posredujejo pristojnim organom in vzpostavijo stroge zaščitne ukrepe za varstvo osebnih podatkov pri obdelavi in zbiranju takih podatkov. Direktiva EU o PNR se uporablja za mednarodne lete v EU in iz nje ter za lete znotraj EU, če se država članica tako odloči.[796]

Zbrani podatki PNR smejo vsebovati le informacije, ki se lahko zbirajo v skladu z direktivo EU o PNR. Hraniti jih je treba v eni sami enoti za informacije na varni lokaciji

792 Svet Evrope, Odbor ministrov (1987), Priporočilo R(87)15 državam članicam, ki ureja uporabo osebnih podatkov v policijskem sektorju (to priporočilo je Odbor ministrov sprejel 17. septembra 1987 na 410. seji namestnikov ministrov).

793 Evropska komisija (2011), Predlog direktive Evropskega parlamenta in Sveta o uporabi podatkov iz evidence podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj, COM(2011) 32 final, Bruselj, 2. februar 2011, str. 1.

794 Evropska komisija (2015), Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives (Boj proti terorizmu na ravni EU, pregled dejavnosti, ukrepov in pobud Komisije), informativni pregled, Bruselj, 11. januar 2015.

795 Direktiva (EU) 2016/681 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (UL L 119, 4.5.2016, str. 132).

796 Direktiva o PNR (UL L 119, 4.5.2016, str. 132), člen 1(1) in člen 2(1).

v vsaki državi članici. Podatke PNR je treba depersonalizirati šest mesecev po tem, ko jih je letalski prevoznik posredoval, hranijo pa se lahko največ pet let.[797] Podatki PNR se izmenjujejo med državami članicami, med državami članicami in Europolom ter s tretjimi državami, vendar le za vsak primer posebej.

Prenos in obdelava podatkov PNR ter pravice, zagotovljene posameznikom, na katere se nanašajo osebni podatki, morajo biti v skladu z direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, ter zagotavljati visoko raven varstva zasebnosti in osebnih podatkov, kot se zahteva z Listino, posodobljeno Konvencijo št. 108 in EKČP.

Neodvisni nacionalni nadzorni organi, pristojni v skladu z direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, so odgovorni tudi za svetovanje glede uporabe predpisov, ki jih države članice sprejmejo v skladu z direktivo EU o PNR, in za spremljanje take uporabe.

Hramba telekomunikacijskih podatkov

Ponudniki komunikacijskih storitev so morali v skladu z direktivo o hrambi podatkov[798] – ki je bila 8. aprila 2014 razglašena za neveljavno v sodbi v zadevi *Digital Rights Ireland* – hraniti metapodatke za poseben namen boja proti hudim kaznivim dejanjem, in sicer vsaj za šest- in največ štiriindvajsetmesečno obdobje, ne glede na to, ali je ponudnik te podatke še potreboval za obračunavanje ali tehnično zagotavljanje storitve ali ne.

Hramba telekomunikacijskih podatkov očitno posega v pravico do varstva osebnih podatkov.[799] Ali je tako poseganje upravičeno ali ne, je bilo izpodbijano v več sodnih postopkih v državah članicah EU.[800]

797 Prav tam, člen 12(1) in (2).

798 Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13.4.2006, str. 54).

799 ENVP (2011), *Mnenje z dne 31. maja 2011 o ocenjevalnem poročilu Komisije Svetu in Evropskemu parlamentu o direktivi o hrambi podatkov (Direktiva 2006/24/ES)*.

800 Nemčija, zvezno ustavno sodišče (*Bundesverfassungsgericht*), 1 BvR 256/08, 2. marec 2010; Romunija, ustavno sodišče (*Curtea Constituțională a României*), št. 1258, 8. oktober 2009; Češka, ustavno sodišče (Ústavní soud České republiky), št. 94/2011 Coll., 22. marec 2011.

Primer: v združenih zadevah *Digital Rights Ireland* in *Kärntner Landesregierung in drugi*[801] sta organizacija Digital Rights in M. Seitlinger vložila tožbo pri višjem sodišču na Irskem oziroma ustavnem sodišču v Avstriji, s katero sta izpodbijala zakonitost nacionalnih ukrepov, ki omogočajo hrambo elektronskih telekomunikacijskih podatkov. Organizacija Digital Rights je irskemu sodišču predlagala, naj ugotovi neveljavnost Direktive 2006/24/ES in dela nacionalnega zakona o kazenskem pravu v zvezi s terorističnimi kaznivimi dejanji. Podobno je M. Seitlinger z več kot 11 000 drugimi tožečimi strankami izpodbijal določbo avstrijskega zakona o telekomunikacijah, s katerim je bila prenesena Direktiva 2006/24/ES, in predlagal, naj se razglasi njena ničnost.

SEU je pri obravnavi teh predlogov za sprejetje predhodne odločbe razglasilo, da je direktiva o hrambi podatkov neveljavna. Menilo je, da je mogoče na podlagi vseh podatkov, ki se lahko hranijo, pridobiti natančne informacije o posameznikih. Poleg tega je proučilo težo poseganja v temeljni pravici do spoštovanja zasebnega življenja in varstva osebnih podatkov. Ugotovilo je, da hramba izpolnjuje cilj v javnem interesu, in sicer prispeva k boju proti hudim kaznivim dejanjem in s tem k javni varnosti. SEU je kljub temu navedlo, da je zakonodajalec EU s sprejetjem zadevne direktive ravnal v nasprotju z načelom sorazmernosti. Čeprav je ta direktiva morda primerna za doseganje zahtevanega cilja, pa pomeni občutno in posebej hudo poseganje v temeljni pravici do spoštovanja zasebnosti in varstva osebnih podatkov, ne da bi bilo to poseganje natančno določeno v predpisih, s katerimi bi bilo zagotovljeno, da je dejansko omejeno na to, kar je nujno potrebno.

Če ne obstaja posebna zakonodaja o hrambi podatkov, je hramba teh podatkov dovoljena, in sicer kot izjema od zaupnosti telekomunikacijskih podatkov v skladu z Direktivo 2002/58/ES (Direktiva o zasebnosti in elektronskih komunikacijah)[802] kot preventivni ukrep, vendar le za namene boja proti hudim kaznivim dejanjem. Taka hramba mora biti omejena na to, kar je nujno potrebno glede na vrste podatkov, ki se hranijo, komunikacijska sredstva, ki se uporabljajo, zadevne osebe in izbrano obdobje hrambe. Nacionalni organi imajo lahko pod strogimi pogoji, vključno

801 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim in Kärntner Landesregierung in drugi* (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014, točka 65.

802 Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

s predhodnim pregledom, ki ga opravi neodvisni organ, dostop do shranjenih podatkov. Podatke je treba hraniti v EU.

Primer: po sodbi v zadevi *Digital Rights Ireland* in *Kärntner Landesregierung in drugi*[803] sta bili SEU predloženi še dve zadevi v zvezi s splošno obveznostjo hrambe telekomunikacijskih podatkov, ki je na Švedskem in v Združenem kraljestvu naložena ponudnikom elektronskih komunikacijskih storitev, kot se je zahtevalo z razveljavljeno direktivo o hrambi podatkov. SEU je v združenih zadevah *Tele2 Sverige* in *Home Department proti Tomu Watsonu in drugim*[804] odločilo, da nacionalna zakonodaja, ki določa splošno in neselektivno hrambo podatkov, ne da bi se zahtevala kakršna koli povezava med podatki, za katere se določa hramba, in grožnjo za javno varnost ter ne da bi bili določeni kakršni koli pogoji – npr. obdobje hrambe, geografsko območje, krog oseb, ki so lahko vpletene v hudo kaznivo dejanje –, presega meje nujno potrebnega in je ni mogoče šteti za upravičeno v demokratični družbi, kot se zahteva z Direktivo 2002/58/ES v povezavi z Listino EU o temeljnih pravicah.

Obeti

Evropska komisija je januarja 2017 objavila predlog uredbe o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij, s katero naj bi se razveljavila in nadomestila Direktiva 2002/58/ES.[805] Predlog ne vsebuje nikakršnih posebnih določb o hrambi osebnih podatkov. Vendar je v njem določeno, da lahko države članice z zakonom omejijo nekatere obveznosti in pravice iz zadevne uredbe, če je taka omejitev potreben in sorazmeren ukrep za zaščito posebnih javnih interesov, med drugim za nacionalno varnost, obrambo, javno varnost ter preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij.[806] Države članice bi zato lahko ohranile ali oblikovale nacionalne okvire za hrambo podatkov, ki zagotavljajo usmerjene ukrepe za hrambo, če so taki okviri v skladu s pravom Unije ob upoštevanju sodne prakse SEU glede razlage Direktive

803 SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim* in Kärntner Landesregierung in drugi (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014.

804 SEU, *Tele2 Sverige AB proti Post- och telestyrelsen* in *Secretary of State for the Home Department proti Tomu Watsonu in drugim* (veliki senat), združeni zadevi C-203/15 in C-698/15, 21. december 2016.

805 Evropska komisija (2017), Predlog uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah), COM(2017) 10 final, Bruselj, 10. januar 2017.

806 Prav tam, uvodna izjava 26.

o zasebnosti in elektronskih komunikacijah ter Listine EU o temeljnih pravicah.[807] V času pisanja tega priročnika so potekale razprave o sprejetju zadevne uredbe.

Krovni sporazum med EU in ZDA o varstvu osebnih podatkov, ki se izmenjujejo za namene kazenskega pregona

Krovni sporazum med EU in ZDA o obdelavi osebnih podatkov v zvezi s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj je začel veljati 1. februarja 2017.[808] Njegov cilj je zagotavljati visoko raven varstva osebnih podatkov za državljane EU, obenem pa krepiti sodelovanje med organi kazenskega pregona EU in ZDA. Zadevni sporazum dopolnjuje obstoječe sporazume med EU in ZDA ter sporazume med posameznimi državami članicami in ZDA, hkrati pa prispeva k oblikovanju jasnih in usklajenih pravil o varstvu osebnih podatkov za prihodnje sporazume na tem področju. V zvezi s tem je njegov cilj vzpostaviti trajen pravni okvir za lažjo izmenjavo informacij.

Sporazum kot tak sicer ne zagotavlja ustrezne pravne podlage za izmenjavo osebnih podatkov, vendar pa zadevnim posameznikom ponuja ustrezne zaščitne ukrepe za varstvo osebnih podatkov. Z njim so zajete vse vrste obdelave osebnih podatkov, potrebne za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj, vključno s terorizmom.[809]

V sporazumu je določenih več zaščitnih ukrepov za zagotovitev, da se osebni podatki uporabljajo le za namene, ki so določeni v njem. Državljanom EU zagotavlja zlasti naslednje varstvo:

- omejitve uporabe osebnih podatkov: osebni podatki se lahko uporabljajo le za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj;

807 Glej obrazložitveni memorandum k predlogu uredbe o zasebnosti in elektronskih komunikacijah, COM(2017) 10 final, točka 1.3.

808 Glej Svet EU (2016), *„Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign 'Umbrella agreement'"* (Izboljšane pravice do varstva podatkov za državljane EU pri sodelovanju na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj: EU in ZDA so podpisale „krovni sporazum"), sporočilo za javnost 305/16, 2. junij 2016.

809 Sporazum med Združenimi državami Amerike in Evropsko unijo o varstvu osebnih podatkov pri preprečevanju, preiskovanju, odkrivanju in pregonu kaznivih dejanj, dokument Sveta 8557/16 z dne 18. maja 2016, člen 3(1). Glej tudi obvestilo Komisije z dne 26. maja 2010 o pogajanjih med EU in ZDA o sporazumu o varstvu osebnih podatkov, MEMO/10/216, in Sporočilo za javnost Komisije EU (2010) z dne 26. maja 2010 o visokih standardih glede zasebnosti v sporazumu o varstvu podatkov med EU in ZDA, IP/10/609.

- varstvo pred samovoljno in neupravičeno diskriminacijo;
- nadaljnji prenosi: vsi nadaljnji prenosi v države, ki niso ZDA ali države članice EU, ali v mednarodno organizacijo se lahko izvedejo le s predhodnim soglasjem pristojnega organa države, ki je osebne podatke prvotno prenesel;
- kakovost osebnih podatkov: osebne podatke je treba hraniti ob upoštevanju njihove točnosti, ustreznosti, posodobljenosti in popolnosti;
- varnost obdelave, vključno s priglasitvijo kršitev varnosti osebnih podatkov;
- obdelava občutljivih osebnih podatkov se lahko izvaja le na podlagi ustreznih zaščitnih ukrepov in v skladu z zakonom;
- obdobje hrambe: osebni podatki se ne smejo hraniti dlje, kot je potrebno ali primerno;
- pravici do dostopa in popravka: vsak posameznik ima pravico, da pod določenimi pogoji dostopa do svojih osebnih podatkov, in pravico, da zahteva popravek osebnih podatkov, če so ti netočni;
- v zvezi z avtomatiziranimi odločitvami so potrebni ustrezni zaščitni ukrepi, vključno z možnostjo človeškega posredovanja;
- učinkovit nadzor, vključno s sodelovanjem med nadzornimi organi EU in ZDA, ter
- sodno varstvo in izvršljivost: državljani EU imajo pravico[810] do sodnega varstva pred sodišči ZDA v primerih, ko jim ameriški organi zavrnejo dostop do osebnih podatkov ali njihov popravek oziroma ko njihove osebne podatke nezakonito razkrijejo.

V okviru krovnega sporazuma je bil vzpostavljen tudi sistem za obveščanje pristojnega organa v državi članici prizadetih posameznikov o vseh kršitvah varstva

810 Predsednik Obama je 24. februarja 2016 razglasil ameriški zakon o sodnem varstvu.

osebnih podatkov, kadar je to potrebno. Pravna jamstva, določena s sporazumom, v primeru kršitve zasebnosti zagotavljajo enako obravnavo državljanov EU v ZDA.[811]

8.3.1 Varstvo osebnih podatkov v pravosodnih organih in organih kazenskega pregona EU

Europol

Europol, agencija EU za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ima sedež v Haagu, nacionalne enote Europola pa so v vsaki državi članici. Ustanovljen je bil leta 1998, njegov sedanji pravni status agencije EU pa temelji na uredbi o Agenciji Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (uredba o Europolu).[812] Cilj Europola je pomagati pri preprečevanju in preiskovanju organiziranega kriminala, terorizma in drugih oblik hudih kaznivih dejanj, navedenih v Prilogi I k uredbi o Europolu, ki prizadenejo dve ali več držav članic. To počne tako, da izmenjuje informacije in deluje kot informacijsko vozlišče, pri čemer zagotavlja obveščevalne analize in ocene ogroženosti.

Da bi Europol dosegel svoje cilje, je vzpostavil Europolov informacijski sistem, ki državam članicam zagotavlja podatkovno zbirko za izmenjavo obveščevalnih podatkov in informacij o kaznivih dejanjih prek nacionalnih enot. Europolov informacijski sistem se lahko uporablja za zagotavljanje osebnih podatkov, ki se nanašajo na: osebe, ki so osumljene ali obsojene zaradi kaznivega dejanja, ki je v pristojnosti Europola, ali osebe, v zvezi s katerimi obstajajo konkretni indici, da bodo taka dejanja storile. Europol in njegove nacionalne enote lahko osebne podatke vnašajo neposredno v Europolov informacijski sistem in jih tam tudi poiščejo. Podatke lahko spreminja,

811 Evropski nadzornik za varstvo podatkov je izdal mnenje o sporazumu med EU in ZDA, v katerem je med drugim priporočil naslednji prilagoditvi: 1) vključitev besedila „za poseben namen, za katerega so bili preneseni" v člen, v katerem je navedeno, da se osebni podatki ne hranijo dlje, kot je nujno in primerno, ter 2) izključitev množičnega prenosa občutljivih podatkov, ki bi se lahko izvajal. Glej Evropski nadzornik za varstvo podatkov, Mnenje 1/2016, *Preliminary Opinion on the agreement between the United State of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences* (Predhodno mnenje o sporazumu med Združenimi državami Amerike in Evropsko unijo o varstvu osebnih podatkov v zvezi s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj), odstavek 35.

812 Uredba (EU) 2016/794 Evropskega parlamenta in Sveta z dne 11. maja 2016 o Agenciji Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol) ter nadomestitvi in razveljavitvi sklepov Sveta 2009/371/PNZ, 2009/934/PNZ, 2009/935/PNZ, 2009/936/PNZ in 2009/968/PNZ (UL L 135, 24.5.2016, str. 53).

popravlja ali izbriše samo oseba, ki jih je vnesla v sistem. Informacije Europolu lahko zagotavljajo tudi organi EU, tretje države in mednarodne organizacije.

Europol lahko informacije, vključno z osebnimi podatki, pridobi tudi iz javno dostopnih virov, kot je internet. Prenosi osebnih podatkov organom EU so dovoljeni le, če so potrebni za opravljanje nalog Europola ali organa EU, ki osebne podatke prejema. Prenosi osebnih podatkov v tretje države ali mednarodne organizacije so dovoljeni le, če Evropska komisija odloči, da zadevna tretja država ali mednarodna organizacija zagotavlja ustrezno raven varstva osebnih podatkov („sklep o ustreznosti"), ali če je bil sklenjen mednarodni sporazum ali sporazum o sodelovanju. Europol lahko prejema in obdeluje osebne podatke, pridobljene od zasebnih strank in posameznikov, pod strogimi pogoji, in sicer jih mora prejeti od nacionalne enote v skladu z nacionalnim pravom, kontaktne točke tretje države ali mednarodne organizacije, s katero ima vzpostavljeno sodelovanje na podlagi sporazuma o sodelovanju, ali organa tretje države ali mednarodne organizacije, za katero velja sklep o ustreznosti ali s katero je EU sklenila mednarodni sporazum. Vse izmenjave informacij se opravijo z mrežno aplikacijo za varno izmenjavo informacij (SIENA).

V odziv na razvoj dogodkov so bili v okviru Europola ustanovljeni specializirani centri. Leta 2013 je bil pri Europolu ustanovljen Evropski center za boj proti kibernetski kriminaliteti.[813] Center deluje kot informacijsko vozlišče EU o kibernetski kriminaliteti, saj prispeva k hitrejšemu odzivanju na spletni kriminal, razvija in uvaja digitalne forenzične zmogljivosti ter zagotavlja najboljšo prakso pri preiskovanju kibernetske kriminalitete. Center se osredotoča na kibernetska kazniva dejanja, ki:

- so jih zagrešile organizirane kriminalne združbe, da bi ustvarile velike nezakonite dobičke, kot na primer spletne goljufije;
- žrtvi povzročijo resno škodo, kot je spolno izkoriščanje otrok na spletu;
- vplivajo na ključno infrastrukturo ali informacijske sisteme v EU.

Januarja 2016 je bil ustanovljen Evropski center za boj proti terorizmu (ECTC), da bi državam članicam zagotavljal operativno podporo pri preiskavah v zvezi

813 Glej tudi ENVP (2012), *Opinion of the Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre* (Mnenje Evropskega nadzornika za varstvo podatkov o sporočilu Evropske komisije Svetu in Evropskemu parlamentu o ustanovitvi Evropskega centra za boj proti kibernetski kriminaliteti), Bruselj, 29. junij 2012.

s terorističnimi kaznivimi dejanji. Operativne podatke v realnem času navzkrižno preverja s podatki, ki jih že ima Europol, s čimer hitro odkrije finančne sledi, in analizira vse razpoložljive podatke iz preiskav ter tako prispeva k oblikovanju strukturiranega opisa teroristične mreže.[814]

Evropski center za boj proti tihotapljenju migrantov (EMSC) je bil ustanovljen februarja 2016 po seji Sveta, ki je potekala novembra 2015, da bi države članice podpiral pri preiskovanju in razbijanju kriminalnih mrež, ki se ukvarjajo s tihotapljenjem migrantov. Deluje kot informacijsko vozlišče, ki podpira regionalni skupini EU za posredovanje v Catanii (Italija) in Pireju (Grčija), ki nacionalnim organom pomagata na več področjih, vključno z izmenjavo obveščevalnih podatkov, preiskavami kaznivih dejanj in pregonom kriminalnih mrež za tihotapljenje ljudi.[815]

Sistem varstva osebnih podatkov, s katerim so urejene dejavnosti Europola, je okrepljen in temelji na načelih iz uredbe o varstvu osebnih podatkov v institucijah EU[816], skladen pa je tudi z direktivo o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, posodobljeno Konvencijo št. 108 in Priporočilom o uporabi osebnih podatkov v policijskem sektorju.

Obdelava osebnih podatkov žrtev kaznivega dejanja, prič ali drugih oseb, ki lahko zagotovijo informacije o kaznivih dejanjih, ter oseb, mlajših od 18 let, se dovoli, če je nujno potrebna in sorazmerna za preprečevanje kaznivih dejanj, ki spadajo med cilje Europola, ali boj proti njim.[817] Obdelava občutljivih osebnih podatkov je prepovedana, razen če je nujno potrebna in sorazmerna za preprečevanje kaznivih dejanj, ki spadajo med cilje Europola, in boj proti njim in če ti podatki dopolnjujejo druge osebne podatke, ki jih Europol obdeluje.[818] V obeh primerih ima dostop do ustreznih podatkov le Europol.[819]

814 Glej Europolovo spletno stran o centru ECTC.

815 Glej Europolovo spletno stran o centru EMSC.

816 Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

817 Uredba o Europolu, člen 30(1).

818 Prav tam, člen 30(2).

819 Prav tam, člen 30(3).

Hramba osebnih podatkov je dovoljena le za nujno potrebno in sorazmerno obdobje, njeno nadaljevanje pa je pogojeno s pregledom, ki se opravi vsaka tri leta. Če se pregled ne opravi, se navedeni podatki po treh letih samodejno izbrišejo.[820]

Europol lahko pod določenimi pogoji osebne podatke neposredno prenaša organu Unije ali organu tretje države ali mednarodni organizaciji.[821] Če je verjetno, da bodo kršitve varnosti osebnih podatkov resno in negativno vplivale na pravice in svoboščine zadevnih posameznikov, na katere se nanašajo osebni podatki, je treba te posameznike o njih nemudoma obvestiti.[822] Vsaka država članica bo določila nacionalni nadzorni organ, ki bo spremljal obdelavo osebnih podatkov v Europolu.[823]

ENVP je odgovoren za spremljanje in zagotavljanje varstva temeljnih pravic in svoboščin posameznikov, kar zadeva obdelavo osebnih podatkov, ki jo izvaja Europol, ter svetovanje Europolu in posameznikom, na katere se nanašajo osebni podatki, o vseh zadevah, povezanih z obdelavo osebnih podatkov. V ta namen deluje kot preiskovalni organ in organ za pritožbe, in sicer v tesnem sodelovanju z nacionalnimi nadzornimi organi.[824] ENVP in nacionalni nadzorni organi se sestanejo vsaj dvakrat letno v okviru odbora za sodelovanje, ki ima svetovalno funkcijo.[825] Države članice morajo v skladu s pravom vzpostaviti nacionalni nadzorni organ, ki je pristojen za spremljanje dopustnosti prenosa osebnih podatkov Europolu z državne ravni ter priklica in vsakega sporočanja osebnih podatkov Europolu s strani zadevne države članice.[826] Države članice morajo poleg tega zagotoviti, da lahko nacionalni nadzorni organi pri opravljanju svojih nalog in dolžnosti v skladu z uredbo o Europolu delujejo popolnoma neodvisno.[827] Zaradi preverjanja zakonitosti obdelave osebnih podatkov, notranjega spremljanja svojih dejavnosti ter zagotavljanja ustrezne celovitosti in varnosti osebnih podatkov Europol hrani zapise (dnevnike) ali dokumentacijo o svojih dejavnostih obdelave osebnih podatkov. Ti zapisi vsebujejo informacije o postopkih obdelave v sistemih za avtomatizirano obdelavo, ki so povezani z zbiranjem,

820 Prav tam, člen 31.

821 Prav tam, člen 24 oziroma 25.

822 Prav tam, člen 35.

823 Uredba o Europolu, člen 42.

824 Prav tam, člena 43 in 44.

825 Prav tam, člen 45.

826 Prav tam, člen 42(1).

827 Prav tam, člen 42(1).

spreminjanjem, razkritjem, združevanjem in izbrisom osebnih podatkov ter vpogledom vanje.[828]

Pritožba zoper odločitev ENVP se lahko vloži pri SEU.[829] Vsak posameznik, ki je utrpel škodo zaradi nezakonite obdelave podatkov, ima pravico do odškodnine, bodisi od Europola bodisi od odgovorne države članice, in sicer mora v prvem primeru vložiti tožbo pri SEU, v drugem primeru pa pri pristojnem nacionalnem sodišču.[830] Poleg tega lahko nadzor dejavnosti Europola izvaja specializirana skupina za skupni parlamentarni nadzor, ki jo ustanovijo nacionalni parlamenti in Evropski parlament.[831] Vsak posameznik ima pravico do dostopa do vseh osebnih podatkov, ki jih Europol morda hrani v zvezi z njim, pri čemer ima tudi pravico zahtevati, da se ti osebni podatki preverijo, popravijo ali izbrišejo. Za ti pravici se lahko uporabljajo izjeme in omejitve.

Eurojust

Eurojust, ustanovljen leta 2002, je organ EU s sedežem v Haagu, ki spodbuja pravosodno sodelovanje pri preiskavah in pregonu hudih kaznivih dejanj, ki zadevajo vsaj dve državi članici.[832] Pristojen je za:

- spodbujanje in izboljševanje usklajevanja preiskav in pregona med pristojnimi organi različnih držav članic;

- lajšanje izvrševanja zaprosil za pravosodno sodelovanje in odločitev o njem.

Naloge Eurojusta izvajajo nacionalni člani. Vsaka država članica v Eurojust imenuje po enega sodnika ali tožilca, čigar status je urejen z nacionalno zakonodajo in ki ima potrebna pooblastila za izvajanje nalog, potrebnih za spodbujanje in izboljšanje

828 Prav tam, člen 40.

829 Prav tam, člen 48.

830 Prav tam, člen 50.

831 Prav tam, člen 51.

832 Svet Evropske unije (2002), Sklep Sveta 2002/187/PNZ z dne 28. februarja 2002 o ustanovitvi Eurojusta za okrepitev boja proti težjim oblikam kriminala (UL L 63, 6.3.2002, str. 1); Svet Evropske unije (2003), Sklep Sveta 2003/659/PNZ z dne 18. junija 2003 o spremembi Sklepa 2002/187/PNZ o ustanovitvi Eurojusta za okrepitev boja proti težjim oblikam kriminala (UL L 245, 29.9.2003, str. 44); Svet Evropske unije (2009), Sklep Sveta 2009/426/PNZ z dne 16. decembra 2008 o okrepitvi Eurojusta in spremembi Sklepa 2002/187/PNZ o ustanovitvi Eurojusta za okrepitev boja proti težjim oblikam kriminala (UL L 138, 4.6.2009, str. 14) (sklepi o Eurojustu).

pravosodnega sodelovanja. Poleg tega nacionalni člani delujejo skupaj kot kolegij, ki izvaja posebne naloge Eurojusta.

Eurojust lahko obdeluje osebne podatke, če je to nujno za izpolnitev njegovih ciljev. Vendar je to omejeno na točno določene informacije o osebah, ki so osumljene storitve ali sodelovanja pri storitvi kaznivega dejanja, za obravnavo katerega je pristojen Eurojust, ali ki so bile zaradi takega kaznivega dejanja pravnomočno obsojene. Eurojust lahko obdeluje tudi nekatere informacije v zvezi s pričami ali žrtvami kaznivih dejanj, za obravnavo katerih je pristojen.[833] V izjemnih okoliščinah lahko za določen čas obdeluje tudi obsežnejše osebne podatke, ki se nanašajo na okoliščine kaznivega dejanja, če so taki podatki neposredno pomembni za preiskavo v teku. Eurojust lahko v okviru svojih pristojnosti združi moči z drugimi institucijami, organi in agencijami EU ter si z njimi izmenjuje osebne podatke. Sodeluje lahko tudi s tretjimi državami in organizacijami ter si z njimi izmenjuje osebne podatke.

Eurojust mora v zvezi z varstvom osebnih podatkov zagotavljati raven varstva, ki je vsaj enakovredna načelom iz posodobljene Konvencije št. 108 in njenih poznejših sprememb. Ob izmenjavi osebnih podatkov je treba upoštevati posebna pravila in omejitve, ki so uvedene bodisi s sporazumom o sodelovanju bodisi z delovnim dogovorom v skladu s sklepi Sveta o Eurojustu in Eurojustovimi pravili o varstvu osebnih podatkov.[834]

Pri Eurojustu je bil ustanovljen neodvisni skupni nadzorni organ, katerega naloga je nadzorovati obdelavo osebnih podatkov, ki jo izvaja Eurojust. Posamezniki lahko pri skupnem nadzornem organu vložijo pritožbo, če niso zadovoljni z Eurojustovo odločitvijo glede zahtevka za dostop do osebnih podatkov ali za njihov popravek, blokiranje ali izbris. Če Eurojust osebne podatke obdeluje nezakonito, je v skladu z nacionalno zakonodajo države članice, v kateri ima sedež, tj. Nizozemske, odgovoren za vso škodo, ki jo povzroči posamezniku, na katerega se nanašajo osebni podatki.

Obeti

Evropska komisija je julija 2013 predstavila predlog uredbe o reformi Eurojusta. Temu predlogu je bil priložen predlog za ustanovitev Evropskega javnega tožilstva (glej spodaj). Namen te uredbe je racionalizirati funkcije in strukturo, da bi se uskladile

833 Prečiščena različica Sklepa Sveta 2002/187/PNZ, kakor je bil spremenjen s Sklepom Sveta 2003/659/PNZ in Sklepom Sveta 2009/426/PNZ, člen 15(2).

834 Določbe notranjega poslovnika Eurojusta o obdelavi in varstvu osebnih podatkov (UL C 68, 19.3.2005, str. 1).

z Lizbonsko pogodbo. Poleg tega je cilj reforme vzpostaviti jasno razmejitev med operativnimi nalogami Eurojusta, ki jih opravlja kolegij Eurojusta, in njegovimi upravnimi nalogami. To bo državam članicam tudi omogočilo, da se bodo bolj osredotočile na operativne naloge. Ustanovljen bo nov izvršni odbor, ki bo pomagal kolegiju pri opravljanju upravnih nalog.[835]

Evropsko javno tožilstvo

Države članice imajo izključno pristojnost za pregon kaznivih dejanj goljufije in nepravilne uporabe proračuna EU, ki imajo lahko tudi čezmejne posledice. Pomen preiskovanja, pregona in obtožbe storilcev takih kaznivih dejanj se je povečal zlasti zaradi dolgotrajne gospodarske krize.[836] Evropska komisija je predlagala uredbo o ustanovitvi neodvisnega Evropskega javnega tožilstva (EJT)[837], katerega cilj je boj proti kaznivim dejanjem, ki škodijo finančnim interesom EU. Evropsko javno tožilstvo bo vzpostavljeno s postopkom okrepljenega sodelovanja, ki najmanj devetim državam članicam omogoča, da vzpostavijo napredno sodelovanje na nekem področju v okviru struktur EU, in sicer brez sodelovanja drugih držav EU.[838] K okrepljenemu sodelovanju so pristopili Belgija, Bolgarija, Ciper, Češka, Estonija, Finska, Francija, Grčija, Hrvaška, Latvija, Litva, Luksemburg, Nemčija, Portugalska, Romunija, Slovenija, Slovaška in Španija; namero, da se pridružita, sta izrazili Avstrija in Italija.[839]

Evropsko javno tožilstvo bo pristojno za preiskovanje in pregon goljufij v škodo EU in drugih kaznivih dejanj, ki škodijo finančnim interesom EU, pri čemer bosta njegova cilja učinkovito usklajevanje preiskav in pregona v okviru različnih nacionalnih pravnih redov ter izboljšanje uporabe virov in izmenjave informacij na evropski ravni.[840]

Evropsko javno tožilstvo bo vodil evropski javni tožilec, pri čemer bo v vsaki državi članici vsaj en evropski delegirani tožilec, ki bo odgovoren za opravljanje preiskav in pregona v tej državi članici.

---

835 Glej spletno stran Evropske komisije o Eurojustu.

836 Glej Evropska komisija (2013), Predlog uredbe Sveta o ustanovitvi Evropskega javnega tožilstva, COM(2013) 534 final, Bruselj, 17. julij 2013, str. 1, in spletno stran Komisije o EJT.

837 Evropska komisija (2013), Predlog uredbe Sveta o ustanovitvi Evropskega javnega tožilstva, COM(2013) 534 final, Bruselj, 17. julij 2013.

838 Pogodba o delovanju EU, člen 86(1) in člen 329(1).

839 Glej Svet Evropske unije (2017), *20 držav članic doseglo dogovor o ustanovitvi Evropskega javnega tožilstva*, sporočilo za javnost, 8. junij 2017.

840 Evropska komisija (2013), Predlog uredbe Sveta o ustanovitvi Evropskega javnega tožilstva, COM(2013) 534 final, Bruselj, 17. julij 2013, str. 1 in 51–51. Glej tudi spletno stran Komisije o EJT.

V predlogu so določeni strogi zaščitni ukrepi za zagotavljanje pravic oseb, vključenih v preiskave Evropskega javnega tožilstva, kot so določene v nacionalnem pravu, pravu EU in Listini EU o temeljnih pravicah. Preiskovalne ukrepe, ki se nanašajo predvsem na temeljne pravice, bo moralo predhodno odobriti nacionalno sodišče.[841] Preiskave, ki jih bo opravljalo Evropsko javno tožilstvo, bodo predmet sodnega nadzora, ki ga bodo izvajala nacionalna sodišča.[842]

Za obdelavo upravnih osebnih podatkov, ki jo bo izvajalo Evropsko javno tožilstvo, se bo uporabljala uredba o varstvu osebnih podatkov v institucijah EU[843]. V zvezi z obdelavo osebnih podatkov, povezanih z operativnimi zadevami, bo Evropsko javno tožilstvo imelo samostojen sistem varstva osebnih podatkov, podobnega sistemu, s katerim so urejene dejavnosti Europola in Eurojusta, saj bo opravljanje nalog Evropskega javnega tožilstva vključevalo obdelavo osebnih podatkov z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter organi pregona na ravni držav članic. Pravila Evropskega javnega tožilstva o varstvu osebnih podatkov so zato skoraj enaka zadevnim pravilom iz direktive o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja. V skladu s predlogom za ustanovitev Evropskega javnega tožilstva mora biti obdelava osebnih podatkov skladna z načeli zakonitosti in poštenosti, omejitve namena, najmanjšega obsega podatkov, točnosti, celovitosti in zaupnosti. Evropsko javno tožilstvo mora čim bolj jasno razlikovati med osebnimi podatki različnih vrst posameznikov, na katere se ti nanašajo, kot so osebe, obsojene za kaznivo dejanje, osebe, ki so zgolj osumljenci, žrtve in priče. Poleg tega mora preveriti kakovost osebnih podatkov, ki se obdelujejo, ter čim bolj razlikovati med osebnimi podatki, ki temeljijo na dejstvih, in osebnimi podatki, ki temeljijo na osebnih ocenah.

Predlog vključuje določbe o pravicah posameznikov, na katere se nanašajo osebni podatki, zlasti pravicah do obveščenosti, dostopa do osebnih podatkov, popravka, izbrisa in omejitve obdelave, ter določa, da se lahko take pravice uveljavljajo tudi posredno prek Evropskega nadzornika za varstvo podatkov. Vključuje tudi načela varnosti obdelave in odgovornosti, v skladu s katerima mora Evropsko javno tožilstvo izvajati ustrezne tehnične in organizacijske ukrepe, da zagotovi ustrezno raven varnosti glede na tveganja, ki jih pomeni obdelava, vodi evidenco vseh dejavnosti

841 Evropska komisija (2013), Predlog uredbe Sveta o ustanovitvi Evropskega javnega tožilstva, COM(2013) 534 final, Bruselj, 17. julij 2013, člen 26(4).

842 Prav tam, člen 36.

843 Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

obdelave in pred obdelavo izvede oceno učinka v zvezi z varstvom podatkov, če je verjetno, da bo vrsta obdelave (na primer obdelava, ki vključuje uporabo novih tehnologij) povzročila veliko tveganje za pravice posameznikov. V predlogu je poleg tega določeno, da kolegij imenuje pooblaščeno osebo za varstvo podatkov, ki mora biti ustrezno vključena v vse zadeve v zvezi z varstvom osebnih podatkov in zagotavljati, da Evropsko javno tožilstvo ravna v skladu z veljavno zakonodajo o varstvu osebnih podatkov.

8.3.2 Varstvo osebnih podatkov v skupnih informacijskih sistemih na ravni EU

Poleg izmenjave osebnih podatkov med državami članicami in ustanovitve posebnih organov EU za boj proti čezmejnemu kriminalu, kot so Europol, Eurojust in EJT, je bilo na ravni EU vzpostavljenih več skupnih informacijskih sistemov, ki omogočajo in spodbujajo sodelovanje in izmenjavo osebnih podatkov med pristojnimi nacionalnimi organi in organi EU za določene namene na področjih varovanja meja, priseljevanja ter azila in carine. Ker je bilo schengensko območje prvotno vzpostavljeno na podlagi mednarodnega sporazuma, ki je veljal neodvisno od prava EU, se je schengenski informacijski sistem (SIS) razvil iz večstranskih sporazumov in je bil pozneje vključen v pravo EU. Vizumski informacijski sistem (VIS), Eurodac, Eurosur in carinski informacijski sistem (CIS) so bili vzpostavljeni kot instrumenti, urejeni s pravom EU.

Nacionalni nadzorni organi in ENVP skupaj izvajajo nadzor nad temi sistemi. Da bi zagotavljali visoko raven varstva, sodelujejo v okviru skupin za usklajevanje nadzora, ki se nanašajo na naslednje obsežne informacijske sisteme: 1) Eurodac, 2) vizumski informacijski sistem, 3) schengenski informacijski sistem, 4) carinski informacijski sistem in 5) informacijski sistem za notranji trg.[844] Skupine za usklajevanje nadzora se običajno sestanejo dvakrat letno pod vodstvom izvoljenega predsednika in sprejemajo smernice, razpravljajo o čezmejnih zadevah ali sprejemajo skupne okvire za inšpekcijske preglede.

Evropska agencija za obsežne informacijske sisteme (eu-LISA),[845] ustanovljena leta 2012, je odgovorna za operativno upravljanje druge generacije schengenskega informacijskega sistema (SIS II), vizumskega informacijskega sistema (VIS) in sistema

844 Glej spletišče Evropskega nadzornika za varstvo podatkov o usklajevanju nadzora.

845 Uredba (EU) št. 1077/2011 Evropskega parlamenta in Sveta z dne 25. oktobra 2011 o ustanovitvi Evropske agencije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (UL L 286, 1.11.2011, str. 1).

Eurodac. Glavna naloga agencije eu-LISA je zagotavljati učinkovito, varno in neprekinjeno delovanje informacijskih sistemov. Odgovorna je tudi za sprejetje potrebnih ukrepov za zagotovitev varnosti sistemov in osebnih podatkov.

Schengenski informacijski sistem

Leta 1985 je več držav članic tedanje Evropske skupnosti sklenilo sporazum med državami Gospodarske unije Beneluks, Nemčije in Francije o postopni odpravi kontrol na skupnih mejah (Schengenski sporazum), katerega cilj je bil vzpostaviti območje prostega gibanja ljudi brez nadzora na mejah znotraj schengenskega območja.[846] Kot protiutež grožnji za javno varnost, ki bi jo lahko povzročile odprte meje, sta bila uvedena okrepljen nadzor na zunanjih mejah schengenskega območja in tesno sodelovanje med nacionalnimi policijskimi in pravosodnimi organi.

Zaradi pristopa novih držav k Schengenskemu sporazumu je bil schengenski sistem z Amsterdamsko pogodbo vključen v pravni okvir EU.[847] Ta se je začela izvajati leta 1999. Najnovejša različica schengenskega informacijskega sistema, t. i. SIS II, je začela delovati 9. aprila 2013. Zdaj ga uporablja večina držav članic EU[848] ter Islandija, Lihtenštajn, Norveška in Švica.[849] Dostop do sistema SIS II imata tudi Europol in Eurojust.

Sistem SIS II sestavljajo centralni sistem (C-SIS), nacionalni sistem (N-SIS) v vsaki državi članici in komunikacijska infrastruktura med centralnim sistemom in nacionalnimi sistemi. Sistem C-SIS vsebuje nekatere podatke o osebah in stvareh, ki so jih vanj vnesle države članice. Sistem SIS uporabljajo nacionalni organi za nadzor meja ter carinski, vizumski in pravosodni organi na celotnem schengenskem območju. Vsaka država članica upravlja nacionalno kopijo sistema C-SIS, ki se imenuje nacionalni schengenski informacijski sistem (N-SIS) in se nenehno posodablja, s tem pa

846 Sporazum med vladami držav Gospodarske unije Beneluks, Zvezne republike Nemčije in Francoske republike o postopni odpravi kontrol na skupnih mejah (UL L 239, 22.9.2000, str. 13).

847 Evropske skupnosti (1997), Amsterdamska pogodba, ki spreminja Pogodbo o Evropski uniji, pogodbe o ustanovitvi Evropskih skupnosti in nekatere z njimi povezane akte (UL C 340, 10.11.1997, str. 1).

848 Ciper, Hrvaška in Islandija izvajajo pripravljalne dejavnosti za vključitev v SIS II, vendar vanj še niso vključene. Glej informacije o schengenskem informacijskem sistemu, ki so na voljo na spletišču Generalnega direktorata Evropske komisije za migracije in notranje zadeve.

849 Uredba (ES) št. 1987/2006 Evropskega parlamenta in Sveta z dne 20. decembra 2006 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) (UL L 381, 28.12.2006, str. 4) in Svet Evropske unije (2007), Sklep Sveta 2007/533/PNZ z dne 12. junija 2007 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) (UL L 205, 7.8.2007, str. 63).

se posodablja tudi sistem C-SIS. V sistemu SIS se uporabljajo različne vrste razpisov ukrepov:

- oseba nima pravice vstopiti na schengensko območje ali na njem prebivati;
- osebo ali predmet iščejo pravosodni organi ali organi pregona (npr. evropski nalogi za prijetje, zahteve za prikrito kontrolo);
- oseba je bila prijavljena kot pogrešana ali
- blago, na primer bankovci, avtomobili, kombiji, orožje ali osebni dokumenti, je prijavljeno kot ukradena ali izgubljena lastnina.

Ob razpisu ukrepa je treba nadaljnje dejavnosti začeti prek uradov SIRENE. Sistem SIS II ima nove funkcije, na primer možnost vnosa: biometričnih osebnih podatkov, kot so na primer prstni odtisi in fotografije, novih kategorij razpisov ukrepov, kot so na primer ukradena plovila, zrakoplovi, zabojniki ali plačilna sredstva, izboljšanih razpisov ukrepov o osebah in predmetih ter kopij evropskih nalogov za prijetje oseb, za katere se zahteva prijetje, predaja ali izročitev.

Sistem SIS II temelji na dveh aktih, ki se dopolnjujeta, in sicer Sklepu SIS II[850] in Uredbi SIS II[851]. Zakonodajalec EU je za sprejetje zadevnega sklepa in uredbe uporabil različni pravni podlagi. S sklepom je urejena uporaba sistema SIS II za namene policijskega in pravosodnega sodelovanja v kazenskih zadevah (nekdanji tretji steber EU). Uredba se uporablja za postopke razpisov ukrepov, ki spadajo na področje vizumov, azila, priseljevanja in drugih politik v zvezi s prostim gibanjem oseb (nekdanji prvi steber). Postopke razpisov ukrepov za vsak steber je bilo treba urediti z ločenimi akti, saj sta bila zadevna pravna akta sprejeta pred Lizbonsko pogodbo in odpravo stebrne strukture.

Oba pravna akta vsebujeta pravila o varstvu podatkov. S Sklepom SIS II je prepovedana obdelava občutljivih podatkov.[852] Obdelava osebnih podatkov spada na podro-

850 Sklep Sveta 2007/533/PNZ z dne 12. junija 2007 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) (UL L 205, 7.8.2007, str. 63).

851 Uredba (ES) št. 1987/2006 Evropskega parlamenta in Sveta z dne 20. decembra 2006 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) (UL L 381, 28.12.2006, str. 4).

852 Sklep SIS II, člen 56; Uredba SIS II, člen 40.

čje uporabe posodobljene Konvencije št. 108.[853] Poleg tega imajo osebe pravico do vpogleda v osebne podatke, ki se nanašajo nanje in so vneseni v SIS II.[854]

Z Uredbo SIS II so urejeni pogoji in postopki za vnos in obdelavo razpisov ukrepov v zvezi z zavrnitvijo vstopa ali prepovedjo prebivanja za državljane tretjih držav. V njej so določena tudi pravila za izmenjavo dopolnilnih in dodatnih podatkov zaradi zavrnitve vstopa ali prepovedi prebivanja na ozemlju držav članic.[855] Ta uredba vsebuje tudi pravila o varstvu podatkov. Prepovedana je obdelava občutljivih kategorij podatkov iz člena 9(1) SUVP.[856] Uredba SIS II vsebuje tudi nekatere pravice posameznika, na katerega se nanašajo osebni podatki, in sicer:

- pravico do vpogleda v osebne podatke, ki se nanašajo nanj;[857]
- pravico do popravka netočnih podatkov;[858]
- pravico do izbrisa nezakonito shranjenih podatkov[859] in
- pravico biti obveščen, če je zoper njega izdan razpis ukrepa. To obvestilo je pisno, priložena pa mu je kopija ali sklic na nacionalno odločitev o izdaji razpisa ukrepa.[860]

Pravica do obveščenosti se ne zagotovi, če: 1) osebni podatki niso bili pridobljeni od posameznika, na katerega se nanašajo, in če teh informacij ni mogoče posredovati ali če bi bil za njihovo posredovanje potreben nesorazmeren napor, 2) če posameznik, na katerega se nanašajo osebni podatki, že ima te informacije, ali 3) če nacionalno pravo omogoča omejitev, med drugim na podlagi varovanja nacionalne varnosti ali preprečevanja kaznivih dejanj.[861]

853 Sklep SIS II, člen 57.
854 Sklep SIS II, člen 58; Uredba SIS II, člen 41.
855 Uredba SIS II, člen 2.
856 Prav tam, člen 40.
857 Prav tam, člen 41(1).
858 Prav tam, člen 41(5).
859 Prav tam, člen 41(5).
860 Prav tam, člen 42(1).
861 Prav tam, člen 42(2).

V zvezi s Sklepom SIS II in Uredbo SIS II se lahko pravice dostopa posameznikov v zvezi s sistemom SIS II uveljavljajo v kateri koli državi članici in se obravnavajo v skladu z nacionalnim pravom zadevne države članice.[862]

Primer: v zadevi *Dalea proti Franciji*[863] je bila pritožniku zavrnjena izdaja vizuma za obisk Francije, saj so francoski organi v schengenski informacijski sistem sporočili, da mu je treba zavrniti vstop. Pritožnik je pred francosko komisijo za varstvo osebnih podatkov in nazadnje pred državnim svetom neuspešno zahteval dostop do osebnih podatkov in njihov popravek ali izbris. ESČP je razsodilo, da je bila prijava pritožnika v schengenski informacijski sistem v skladu z zakonom in da je imela zakonit cilj varstva nacionalne varnosti. Ker pritožnik ni dokazal, da je bil zaradi zavrnitve vstopa v schengensko območje dejansko oškodovan, in ker so bili uvedeni zadostni ukrepi za preprečitev samovoljnih odločitev v zvezi z njim, je bilo poseganje v njegovo pravico do spoštovanja zasebnega življenja sorazmerno. Pritožba, ki jo je pritožnik vložil na podlagi člena 8 EKČP, je bila zato razglašena za nedopustno.

Pristojni nacionalni nadzorni organ vsake države članice nadzoruje nacionalni sistem N-SIS. Nacionalni nadzorni organ mora zagotoviti, da se vsaj vsaka štiri leta izvede revizija postopkov obdelave osebnih podatkov v nacionalnem sistemu N-SIS.[864] Nacionalni nadzorni organi in ENVP sodelujejo ter zagotavljajo usklajen nadzor nad sistemom N-SIS, ENVP pa je odgovoren za nadzor nad sistemom C-SIS. Zaradi preglednosti se Evropskemu parlamentu, Svetu in agenciji eu-LISA vsaki dve leti pošlje skupno poročilo o dejavnostih. Da bi se zagotovilo usklajevanje nadzora nad sistemom SIS, je bila ustanovljena skupina za usklajevanje nadzora nad SIS II, ki se sestane do dvakrat letno. To skupino sestavljajo ENVP in predstavniki nadzornih organov tistih držav članic, ki so uvedle sistem SIS II, ter Islandije, Lihtenštajna, Norveške in Švice, saj se sistem SIS uporablja tudi zanje, ker so članice schengenskega območja.[865] Ciper, Hrvaška in Irska še niso del sistema SIS II, zato v skupini za usklajevanje nadzora sodelujejo le kot opazovalke. ENVP in nacionalni nadzorni organi v okviru skupine za usklajevanje nadzora dejavno sodelujejo tako, da si izmenjujejo informacije, si pomagajo pri izvajanju revizij in inšpekcijskih pregledov, oblikujejo usklajene predloge za skupno rešitev morebitnih težav in spodbujajo ozaveščenost o pravicah

862 Uredba SIS II, člen 41(1), in Sklep SIS II, člen 58.

863 ESČP, *Dalea proti Franciji*, pritožba št. 964/07, 2. februar 2010.

864 Sklep SIS II, člen 60(2).

865 Glej spletno stran Evropskega nadzornika za varstvo podatkov o schengenskem informacijskem sistemu.

glede varstva osebnih podatkov.[866] Skupina za usklajevanje nadzora nad SIS II sprejema tudi smernice za pomoč posameznikom, na katere se nanašajo osebni podatki. Primer je priročnik za pomoč posameznikom, na katere se nanašajo osebni podatki, pri uveljavljanju njihovih pravic do dostopa.[867]

Obeti

Evropska komisija je leta 2016 opravila oceno sistema SIS,[868] iz katere je razvidno, da so bili vzpostavljeni nacionalni mehanizmi, ki posameznikom, na katere se nanašajo osebni podatki, omogočajo, da dostopajo do svojih osebnih podatkov v sistemu SIS II, jih popravijo ali izbrišejo ali prejmejo odškodnino zaradi netočnih podatkov. Da bi izboljšala učinkovitost in uspešnost sistema SIS II, je predstavila tri predloge uredb:

- uredbe o vzpostavitvi, delovanju in uporabi sistema SIS na področju na področju mejnih kontrol, s katero bo razveljavljena Uredba SIS II;

- uredbe o vzpostavitvi, delovanju in uporabi sistema SIS na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, s katero bo med drugim razveljavljen Sklep SIS II, in

- uredbe o uporabi sistema SIS za vračanje nezakonito prebivajočih državljanov tretjih držav.

Pomembno je, da je s predlogi poleg fotografij in prstnih odtisov, ki so že del sedanje ureditve sistema SIS II, dovoljena tudi obdelava drugih vrst biometričnih podatkov. V podatkovni zbirki SIS bodo shranjeni tudi podobe obraza, odtisi dlani in profili DNK. Uredba SIS II in Sklep SIS II že omogočata iskanje s prstnimi odtisi za identifikacijo osebe, v skladu s predlogi pa bo takšno iskanje obvezno, če identitete osebe ne bo mogoče ugotoviti kako drugače. Podobe obraza, fotografije in odtisi dlani se bodo uporabljali za iskanje po sistemu in ugotavljanje identitete ljudi, ko bo to postalo tehnično izvedljivo. Nova pravila o biometričnih lastnostih pomenijo posebna tveganja

866 Uredba SIS II, člen 46, in Sklep SIS II, člen 62.

867 Glej Skupina za usklajevanje nadzora nad SIS II, *Schengenski informacijski sistem. Priročnik za uveljavljanje pravice do dostopa*, na voljo na spletišču ENVP.

868 Evropska komisija (2016), Poročilo Komisije Evropskemu parlamentu in Svetu o oceni druge generacije schengenskega informacijskega sistema (SIS II) v skladu s členom 24(5), členom 43(3) in členom 50(5) Uredbe (ES) št. 1987/2006 ter členom 59(3) in členom 66(5) Sklepa Sveta 2007/533/PNZ, COM(2016) 880 final, Bruselj, 21. december 2016.

za pravice posameznikov. ENVP je v svojem mnenju o predlogih Komisije[869] ugotovil, da so biometrični podatki zelo občutljivi in da bi moral njihov vnos v tako obsežno podatkovno zbirko temeljiti na z dokazi podprti oceni potrebe po njihovi vključitvi v sistem SIS. Z drugimi besedami, dokazati bi bilo treba potrebo po obdelavi novih lastnosti. ENVP je menil tudi, da je treba dodatno pojasniti, katere vrste informacij se lahko vključijo v profil DNK. Ker lahko profil DNK vključuje občutljive informacije (najizrazitejši primer bi bile informacije, ki razkrivajo zdravstvene težave), bi morali profili DNK, ki se hranijo v sistemu SIS, vsebovati le minimalne informacije, ki so nujno potrebne za identifikacijo pogrešanih oseb, ter izrecno izključevati informacije o zdravju in rasi ter vse druge občutljive informacije.[870] Vendar so v predlogih uvedeni dodatni zaščitni ukrepi za omejitev zbiranja in nadaljnje obdelave osebnih podatkov na tisto, kar je nujno potrebno in operativno zahtevano, poleg tega je dostop do osebnih podatkov omejen na tiste osebe, ki imajo operativno potrebo za njihovo obdelavo.[871] Z zadevnimi predlogi je agencija eu-LISA tudi pooblaščena, da državam članicam redno posreduje poročila o kakovosti podatkov, da se lahko redno pregledujejo razpisi ukrepov, s čimer se zagotavlja kakovost podatkov.[872]

Vizumski informacijski sistem

Vizumski informacijski sistem (VIS), ki ga prav tako upravlja agencija eu-LISA, je bil razvit v podporo izvajanju skupne vizumske politike EU.[873] Sistem VIS državam schengenskega območja omogoča izmenjavo podatkov o prosilcih za vizum prek popolnoma centraliziranega sistema, ki konzulate in veleposlaništva držav schengenskega območja v državah, ki niso članice EU, povezuje z zunanjimi mejnimi prehodi vseh držav schengenskega območja. V njem se obdelujejo osebni podatki o vlogah

869 ENVP (2017), EDPS Opinion on the new legal basis of the Schengen Information System (Mnenje ENVP o novi pravni podlagi schengenskega informacijskega sistema), Mnenje št. 7/2017, 2. maj 2017.

870 Prav tam, točka 22.

871 Evropska komisija (2016), Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, o spremembi Uredbe (EU) št. 515/2014 ter razveljavitvi Uredbe (ES) št. 1986/2006, Sklepa Sveta 2007/533/PNZ in Sklepa Komisije 2010/261/EU, COM(2016) 883 final, Bruselj, 21. december 2016.

872 Prav tam, str. 15.

873 Svet Evropske unije (2004), Odločba Sveta 2004/512/ES z dne 8. junija 2004 o vzpostavitvi vizumskega informacijskega sistema (VIS) (UL L 213, 15.6.2004, str. 5); Uredba (ES) št. 767/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov med državami članicami o vizumih za kratkoročno prebivanje (Uredba VIS) (UL L 218, 13.8.2008, str. 60); Svet Evropske unije (2008), Sklep Sveta 2008/633/PNZ z dne 23. junija 2008 o dostopu imenovanih organov držav članic in Europola do vizumskega informacijskega sistema (VIS) za iskanje podatkov za namene preprečevanja, odkrivanja in preiskovanja terorističnih dejanj in drugih hudih kaznivih dejanj (UL L 218, 13.8.2008, str. 129).

za izdajo vizumov za kratkoročno prebivanje zaradi obiska ali tranzita prek schengenskega območja. Sistem VIS mejnim organom omogoča, da na podlagi biometričnih značilnosti, zlasti prstnih odtisov, preverijo, ali je oseba, ki predloži vizum, zakoniti imetnik dokumenta ali ne, in identificirajo osebe, ki nimajo dokumentov ali katerih dokumenti so ponarejeni.

Z Uredbo (ES) št. 767/2008 Evropskega parlamenta in Sveta o vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov med državami članicami o vizumih za kratkoročno prebivanje (Uredba VIS) so urejeni pogoji in postopki za prenos osebnih podatkov v zvezi z vlogami za izdajo vizumov za kratkoročno bivanje. Z njo so urejene tudi odločitve za njihovo reševanje, vključno z odločitvami o razveljavitvi, preklicu ali podaljšanju vizumov.[874] Uredba VIS zajema predvsem podatke o prosilcu, njegove vizume, fotografije, prstne odtise, povezave na predhodne vloge za izdajo vizuma in dosjeje oseb, ki spremljajo prosilca, ali podatke v zvezi z osebami, ki izdajo povabilo.[875] Dostop do sistema VIS za vnos, spremembo ali izbris podatkov je omejen izključno na vizumske organe; dostop za vpogled v podatke pa je zagotovljen vizumskim organom in organom, pristojnim za preverjanje na mejnih prehodih na zunanjih mejah, za nadzor priseljevanja in za azil.

Pod določenimi pogoji lahko pristojni nacionalni policijski organi in Europol zaprosijo za dostop do podatkov, vnesenih v sistem VIS, in sicer za namene preprečevanja, odkrivanja in preiskovanja terorističnih in drugih kaznivih dejanj.[876] Ker je bil sistem VIS oblikovan kot instrument za podporo izvajanju skupne vizumske politike, bi bilo načelo omejitve namena, v skladu s katerim je treba, kot je pojasnjeno v razdelku 3.2, osebne podatke obdelovati le za določene, izrecne in zakonite namene, pri čemer morajo biti osebni podatki ustrezni, relevantni in ne prekomerni glede na namene, za katere se obdelujejo, kršeno, če bi se sistem VIS uporabljal kot orodje kazenskega pregona. Zato nacionalni organi kazenskega pregona in Europol nimajo rutinskega dostopa do podatkovne zbirke sistema VIS. Dostop se lahko odobri le za vsak primer posebej in ob upoštevanju strogih zaščitnih ukrepov. Pogoji in zaščitni

874 Uredba VIS, člen 1.

875 Člen 5 Uredbe (ES) št. 767/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov med državami članicami o vizumih za kratkoročno prebivanje (Uredba VIS) (UL L 218, 13.8.2008, str. 60).

876 Svet Evropske unije (2008), Sklep Sveta 2008/633/PNZ z dne 23. junija 2008 o dostopu imenovanih organov držav članic in Europola do vizumskega informacijskega sistema (VIS) za iskanje podatkov za namene preprečevanja, odkrivanja in preiskovanja terorističnih dejanj in drugih hudih kaznivih dejanj (UL L 218, 13.8.2008, str. 129).

ukrepi za dostop teh organov do sistema VIS in vpogled vanj so urejeni s Sklepom Sveta 2008/633/PNZ.[877]

Poleg tega so v Uredbi VIS določene pravice posameznikov, na katere se nanašajo osebni podatki. To so:

- pravica, da jih odgovorna država članica obvesti o identiteti in kontaktnih podatkih upravljavca osebnih podatkov, ki je odgovoren za obdelavo osebnih podatkov v tej državi članici, o namenih, za katere bodo njihovi osebni podatki obdelani v sistemu VIS, o kategorijah oseb, ki se jim osebni podatki lahko posredujejo (uporabniki), in o obdobju hrambe osebnih podatkov. Poleg tega je treba prosilce za vizum obvestiti o dejstvu, da je zbiranje njihovih osebnih podatkov v okviru sistema VIS obvezno za obravnavo njihove vloge, pri čemer jih morajo države članice obvestiti tudi o njihovi pravici, da dostopajo do svojih osebnih podatkov in zahtevajo njihov popravek ali izbris, ter o postopkih za uveljavljanje teh pravic;[878]

- pravica do vpogleda v osebne podatke, ki se nanašajo nanje in so bili vneseni v sistem VIS;[879]

- pravica do popravka netočnih podatkov;[880]

- pravica do izbrisa nezakonito shranjenih podatkov.[881]

Za zagotovitev nadzora nad sistemom VIS je bila vzpostavljena skupina za usklajevanje nadzora nad sistemom VIS. Sestavljena je iz predstavnikov ENVP in nacionalnih nadzornih organov, ki se sestajajo dvakrat letno. To skupino sestavljajo predstavniki 28 držav članic EU ter Islandije, Lihtenštajna, Norveške in Švice.

Eurodac

Ime Eurodac je kratica za evropsko daktiloskopijo (angl. European Dactyloscopy)[882]. Gre za centraliziran sistem, ki vsebuje podatke o prstnih odtisih državljanov tretjih

877 Prav tam.

878 Uredba VIS, člen 37.

879 Prav tam, člen 38(1).

880 Prav tam, člen 38(2).

881 Prav tam, člen 38(2).

882 Glej spletno stran Evropskega nadzornika za varstvo podatkov o sistemu Eurodac.

držav in oseb brez državljanstva, ki zaprosijo za azil v eni od držav članic EU.[883] Sistem je začel delovati leta 2003, ko je bila sprejeta Uredba Sveta št. 2725/2000; prenovitev te uredbe je začela veljati leta 2015. Njegov namen je predvsem pomagati pri določanju, katera država članica je odgovorna za obravnavanje posamezne prošnje za azil na podlagi Uredbe (ES) št. 604/2013. Navedena uredba določa merila in mehanizme za določitev države članice, odgovorne za obravnavanje prošnje za mednarodno zaščito, ki jo v eni od držav članic vloži državljan tretje države ali oseba brez državljanstva (Uredba Dublin III).[884] Osebni podatki v sistemu Eurodac se uporabljajo predvsem za lažjo uporabo uredbe Dublin III.[885]

Nacionalni organi kazenskega pregona in Europol lahko prstne odtise, povezane s kazenskimi preiskavami, primerjajo s prstnimi odtisi v sistemu Eurodac, vendar le za preprečevanje, odkrivanje ali preiskovanje terorističnih dejanj ali drugih hudih kaznivih dejanj. Ker je bil sistem Eurodac zasnovan kot instrument za podporo izvajanju azilne politike EU, ne pa kot orodje kazenskega pregona, imajo organi kazenskega pregona dostop do te podatkovne zbirke le v posebnih primerih, v posebnih okoliščinah in pod strogimi pogoji.[886] Za nadaljnjo uporabo podatkov za namene kazenskega pregona se uporablja direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja; osebni podatki, ki se uporabljajo predvsem za lažjo uporabo uredbe Dublin III, pa so zaščiteni v skladu s SUVP. Prepovedan je nadaljnji prenos osebnih podatkov, ki jih država članica ali Europol pridobi v skladu s prenovljeno uredbo Eurodac, kateri koli tretji državi, mednarodni organizaciji ali zasebnemu subjektu s sedežem v EU ali zunaj nje.[887]

883 Uredba Sveta (ES) št. 2725/2000 z dne 11. decembra 2000 o vzpostavitvi sistema „Eurodac" za primerjavo prstnih odtisov zaradi učinkovite uporabe Dublinske konvencije (uredba Eurodac) (UL L 316, 15.12.2000, str. 1); Uredba Sveta (ES) št. 407/2002 z dne 28. februarja 2002 o pravilih za izvedbo Uredbe (ES) št. 2725/2000 o vzpostavitvi sistema „Eurodac" za primerjavo prstnih odtisov zaradi učinkovite uporabe Dublinske konvencije (UL L 62, 5.3.2002, str. 1); Uredba (EU) št. 603/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o vzpostavitvi sistema Eurodac za primerjavo prstnih odtisov zaradi učinkovite uporabe Uredbe (EU) št. 604/2013 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za mednarodno zaščito, ki jo v eni od držav članic vloži državljan tretje države ali oseba brez državljanstva, in o zahtevah za primerjavo s podatki iz sistema Eurodac, ki jih vložijo organi kazenskega pregona držav članic in Europol za namene kazenskega pregona, ter o spremembi Uredbe (EU) št. 1077/2011 o ustanovitvi Evropske agencije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (prenovljena uredba Eurodac) (UL L 180, 29.6.2013, str. 1).

884 Uredba (EU) št. 604/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za mednarodno zaščito, ki jo v eni od držav članic vloži državljan tretje države ali oseba brez državljanstva (uredba Dublin III) (UL L 180, 29.6.2013, str. 31).

885 Prenovljena uredba Eurodac (UL L 180, 29.6.2013, str. 1), člen 1(1).

886 Prav tam, člen 1(2).

887 Prav tam, člen 35.

Sistem Eurodac je sestavljen iz centralne enote za shranjevanje in primerjavo prstnih odtisov, ki jo upravlja agencija eu-LISA, ter sistema za elektronski prenos podatkov med državami članicami in centralno podatkovno zbirko. Države članice odvzamejo in posredujejo prstne odtise vsake osebe, stare vsaj 14 let, ki zaprosi za azil na njihovem ozemlju, in vsakega državljana tretje države ali osebe brez državljanstva, stare vsaj 14 let, ki je prijeta zaradi nezakonitega prehoda njihove zunanje meje. Države članice lahko odvzamejo in posredujejo tudi prstne odtise državljanov tretjih držav ali oseb brez državljanstva, v zvezi s katerimi se izkaže, da na ozemlju teh držav članic prebivajo brez dovoljenja.

Čeprav lahko katera koli država članica išče podatke po sistemu Eurodac in zahteva primerjave s podatki o prstnih odtisih, ima le država članica, ki je odvzela prstne odtise in jih je posredovala v centralno enoto, pravico, da jih spremeni, in sicer tako, da jih popravi, dopolni ali izbriše.[888] Agencija eu-LISA vodi evidentirane zapise o vseh postopkih obdelave osebnih podatkov, da nadzira varstvo osebnih podatkov in zagotavlja njihovo varnost.[889] Nacionalni nadzorni organi posameznikom, na katere se nanašajo osebni podatki, nudijo pomoč in jim svetujejo pri uveljavljanju njihovih pravic.[890] Zbiranje in posredovanje podatkov o prstnih odtisih sta predmet sodnega nadzora, ki ga izvajajo nacionalna sodišča.[891] Za dejavnosti obdelave v centralnem sistemu, ki ga v zvezi s sistemom Eurodac upravlja agencija eu-LISA, se uporabljata uredba o varstvu osebnih podatkov v institucijah EU[892] in nadzor, ki ga izvaja ENVP.[893] Če oseba utrpi škodo zaradi nezakonite obdelave osebnih podatkov ali drugega dejanja, ki je nezdružljivo z uredbo Eurodac, ima pravico prejeti odškodnino od države članice, ki je odgovorna za nastalo škodo.[894] Vendar je treba poudariti, da so prosilci za azil posebej ranljiva skupina ljudi, ki so se praviloma podali na dolgo in tvegano pot. Zaradi njihove ranljivosti in negotovega položaja, v katerem se pogosto znajdejo, ko se obravnava njihova prošnja za azil, se lahko v praksi uveljavljanje njihovih pravic, vključno s pravico do odškodnine, izkaže za težavno.

888 Prav tam, člen 27.

889 Prav tam, člen 28.

890 Prav tam, člen 29.

891 Prav tam, člen 29.

892 Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

893 Prenovljena uredba Eurodac (UL L 180, 29.6.2013, str. 1), člen 31.

894 Prav tam, člen 37.

Da lahko države članice uporabljajo sistem Eurodac za namene kazenskega pregona, morajo imenovati organe, ki bodo imeli pravico zahtevati dostop, in organe, ki bodo preverili, da so zahteve za primerjavo zakonite.[895] Za dostop nacionalnih organov in Europola do podatkov o prstnih odtisih v sistemu Eurodac veljajo zelo strogi pogoji. Organ prosilec mora predložiti utemeljeno elektronsko zahtevo šele po tem, ko zadevne podatke primerja s podatki v drugih razložljivih informacijskih sistemih, kot so nacionalne podatkovne zbirke prstnih odtisov in sistem VIS. Obstajati mora prevladujoča skrb za javno varnost, zaradi katere je primerjava sorazmerna. Primerjava mora biti resnično potrebna in povezana s konkretno zadevo, poleg tega morajo obstajati utemeljeni razlogi za sklepanje, da bi primerjava znatno pripomogla k preprečevanju, odkrivanju ali preiskovanju katerega koli zadevnega kaznivega dejanja, zlasti kadar obstaja utemeljen sum, da osumljenec, storilec ali žrtev terorističnega dejanja ali drugega hudega kaznivega dejanja spada v eno od kategorij, za katere velja obveznost zbiranja prstnih odtisov v sistemu Eurodac. Primerjavo je treba opraviti le s podatki o prstnih odtisih. Europol mora pridobiti tudi odobritev države članice, ki je zbrala podatke o prstnih odtisih.

Osebni podatki, shranjeni v sistemu Eurodac, ki se nanašajo na prosilce za azil, se hranijo deset let od datuma odvzema prstnih odtisov, razen če posameznik, na katerega se nanašajo osebni podatki, pridobi državljanstvo države članice EU. V takem primeru je treba osebne podatke nemudoma izbrisati. Osebni podatki, ki se nanašajo na tujce, prijete zaradi nezakonitega prečkanja zunanje meje, se hranijo 18 mesecev. Te podatke je treba nemudoma izbrisati, če posameznik, na katerega se nanašajo osebni podatki, dobi dovoljenje za prebivanje, zapusti ozemlje EU ali pridobi državljanstvo države članice. Osebni podatki o osebah, ki jim je bil podeljen azil, ostanejo tri leta na voljo za primerjavo v okviru preprečevanja, odkrivanja in preiskovanja terorističnih dejanj in drugih hudih kaznivih dejanj.

Sistem Eurodac poleg vseh držav članic EU uporabljajo tudi Islandija, Norveška, Lihtenštajn in Švica, in sicer na podlagi mednarodnih sporazumov.

Za zagotovitev nadzora nad sistemom Eurodac je bila vzpostavljena skupina za usklajevanje nadzora nad sistemom Eurodac. Sestavljena je iz predstavnikov ENVP in nacionalnih nadzornih organov, ki se sestajajo dvakrat letno. To skupino sestavljajo predstavniki 28 držav članic EU ter Islandije, Lihtenštajna, Norveške in Švice.[896]

895 Roots, L. (2015), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination", *Baltic Journal of European Studies*, Univerza za tehnologijo v Talinu, zvezek 5, št. 2, str. 108–129.

896 Glej spletno stran Evropskega nadzornika za varstvo podatkov o sistemu Eurodac.

Obeti

Komisija je maja 2016 v okviru reforme, katere namen je izboljšati delovanje skupnega evropskega azilnega sistema (CEAS), objavila predlog o novi prenovljeni uredbi Eurodac.[897] Predlagana prenovitev je pomembna, saj se bo z njo znatno razširilo področje uporabe izvirne podatkovne zbirke Eurodac. Sistem Eurodac je bil prvotno vzpostavljen v podporo izvajanju skupnega evropskega azilnega sistema, in sicer z zagotavljanjem dokazov v obliki prstnih odtisov, ki omogočajo določitev države članice, odgovorne za obravnavanje prošnje za azil, vložene v EU. S predlagano prenovitvijo se bo razširilo področje uporabe podatkovne zbirke, kar bo olajšalo vračanje migrantov brez urejenega statusa.[898] Nacionalni organi bodo lahko dostopali do podatkovne zbirke za ugotavljanje istovetnosti državljanov tretjih držav, ki v EU prebivajo nezakonito ali ki so nezakonito vstopili na njeno območje, da se pridobijo dokazi za pomoč državam članicam pri vračanju teh posameznikov. V skladu z veljavno pravno ureditvijo je treba zbirati in hraniti le prstne odtise, v predlogu pa se uvaja pridobivanje podobe obraza posameznikov,[899] ki je še ena vrsta biometričnih podatkov. V skladu z zadevnim predlogom bi se tudi znižala najnižja starost otrok, od katerih se lahko odvzamejo ali pridobijo biometrični podatki, in sicer na šest let[900] namesto 14 let, kar je najnižja starost na podlagi zadevne uredbe iz leta 2013. Razširjeno področje uporabe predloga pomeni, da bo pomenil poseg v pravici do zasebnosti in varstva osebnih podatkov več posameznikov, ki so lahko vključeni v podatkovno zbirko. Da bi se ta poseg uravnotežil, se s predlogom in predlaganimi spremembami, ki jih je predložil odbor Evropskega parlamenta za državljanske svoboščine,

897 Evropska komisija, Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi sistema Eurodac za primerjavo prstnih odtisov zaradi učinkovite uporabe [Uredbe (EU) št. 604/2013 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za mednarodno zaščito, ki jo v eni od držav članic vloži državljan tretje države ali oseba brez državljanstva], za ugotavljanje istovetnosti nezakonito prebivajočih državljanov tretjih držav ali oseb brez državljanstva in o zahtevah za primerjavo s podatki iz sistema Eurodac, ki jih vložijo organi kazenskega pregona držav članic in Europol za namene kazenskega pregona (prenovitev), COM(2016) 272 final, 4. maj 2016.

898 Glej obrazložitveni memorandum k predlogu, str. 3.

899 Evropska komisija, Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi sistema Eurodac za primerjavo prstnih odtisov zaradi učinkovite uporabe [Uredbe (EU) št. 604/2013 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za mednarodno zaščito, ki jo v eni od držav članic vloži državljan tretje države ali oseba brez državljanstva], za ugotavljanje istovetnosti nezakonito prebivajočih državljanov tretjih držav ali oseb brez državljanstva in o zahtevah za primerjavo s podatki iz sistema Eurodac, ki jih vložijo organi kazenskega pregona držav članic in Europol za namene kazenskega pregona (prenovitev), COM(2016) 272 final, 4. maj 2016, člen 2(1).

900 Prav tam, člen 2(2).

pravosodje in notranje zadeve (LIBE),[901] poskušajo okrepiti zahteve glede varstva osebnih podatkov. V času pisanja tega priročnika so v Parlamentu in Svetu potekale razprave o tem predlogu.

Eurosur

Evropski sistem varovanja meja (Eurosur)[902] je namenjen krepitvi nadzora nad zunanjimi schengenskimi mejami z odkrivanjem in preprečevanjem nezakonitega priseljevanja in čezmejnega kriminala ter bojem proti njima. Uporablja se za krepitev izmenjave informacij in operativnega sodelovanja med nacionalnimi koordinacijskimi centri in agencijo Frontex, agencijo EU, ki je pristojna za razvoj in uporabo novega koncepta integriranega upravljanja meja.[903] Njegovi splošni cilji so:

- zmanjšati število migrantov brez urejenega statusa, ki neopaženo vstopijo v EU;
- zmanjšati število smrtnih primerov med migranti brez urejenega statusa z rešitvijo večjega števila življenj na morju;
- povečati notranjo varnost EU kot celote s prizadevanji za preprečevanje čezmejnega kriminala.[904]

Sistem je v vseh državah članicah z zunanjimi mejami začel delovati 2. decembra 2013, 1. decembra 2014 pa še v vseh drugih. Uredba o sistemu Eurosur se uporablja za varovanje zunanjih kopenskih, morskih in zračnih meja držav članic. Osebni

901 Evropski parlament, *Poročilo o predlogu uredbe Evropskega parlamenta in Sveta o vzpostavitvi sistema Eurodac za primerjavo prstnih odtisov zaradi učinkovite uporabe Uredbe (EU) št. 604/2013 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za mednarodno zaščito, ki jo v eni od držav članic vloži državljan tretje države ali oseba brez državljanstva, za ugotavljanje istovetnosti nezakonito prebivajočih državljanov tretjih držav ali oseb brez državljanstva in o zahtevah za primerjavo s podatki iz sistema Eurodac, ki jih vložijo organi kazenskega pregona držav članic in Europol za namene kazenskega pregona (prenovitev)*, PE 597.620v03-00, 9. junij 2017.

902 Uredba (EU) št. 1052/2013 Evropskega parlamenta in Sveta z dne 22. oktobra 2013 o vzpostavitvi Evropskega sistema varovanja meja (EUROSUR) (UL L 295, 6.11.2013, str. 11).

903 Uredba (EU) 2016/1624 Evropskega parlamenta in Sveta z dne 14. septembra 2016 o evropski mejni in obalni straži ter spremembi Uredbe (EU) 2016/399 Evropskega parlamenta in Sveta ter razveljavitvi Uredbe (ES) št. 863/2007 Evropskega parlamenta in Sveta, Uredbe Sveta (ES) št. 2007/2004 in Odločbe Sveta 2005/267/ES (UL L 251, 16.9.2016, str. 1).

904 Glej tudi: Evropska komisija (2008), Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij,Proučitev vzpostavitve evropskega sistema nadzorovanja meja (EUROSUR), COM(2008) 68 final, Bruselj, 13. februar 2008; Evropska komisija (2011), Ocena učinka, priložena predlogu uredbe Evropskega parlamenta in Sveta o vzpostavitvi Evropskega sistema varovanja meja (EUROSUR), delovni dokument služb Komisije, SEC(2011) 1536 final, Bruselj,12. december 2011, str. 18.

podatki se v okviru sistema Eurosur izmenjujejo in obdelujejo v zelo omejenem obsegu, saj si lahko države članice in agencija Frontex izmenjujejo le identifikacijske številke ladij. V njegovem okviru se izmenjujejo operativne informacije, kot so lokacija patrulj in incidentov, informacije, ki se izmenjujejo, pa praviloma ne smejo vsebovati osebnih podatkov.[905] V izjemnih primerih, ko se v okviru sistema Eurosur izmenjujejo osebni podatki, je v zadevni uredbi določeno, da se v celoti uporablja splošni pravni okvir EU o varstvu osebnih podatkov.[906]

Sistem Eurosur tako zagotavlja pravico do varstva osebnih podatkov, in sicer je v uredbi o sistemu Eurosur določeno, da morajo biti izmenjave osebnih podatkov v skladu z merili in zaščitnimi ukrepi iz direktive o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, ter SUVP.[907]

Carinski informacijski sistem

Še en pomemben informacijski sistem, vzpostavljen na ravni EU, je carinski informacijski sistem (CIS).[908] Med vzpostavljanjem notranjega trga so bile odpravljene vse kontrole in formalnosti v zvezi s pretokom blaga na ozemlju EU, zato se je povečalo tveganje goljufij. Tveganje se je izničilo z okrepljenim sodelovanjem med carinskimi upravami držav članic. Sistem CIS naj bi državam članicam pomagal pri preprečevanju, preiskovanju in pregonu hudih kršitev nacionalne in evropske carinske in kmetijske zakonodaje. Vzpostavljen je bil z dvema pravnima aktoma, ki sta bila sprejeta na različnih pravnih podlagah: Uredba Sveta (ES) št. 515/97 se nanaša na sodelovanje med različnimi nacionalnimi upravnimi organi za boj proti goljufijam v okviru carinske unije in skupne kmetijske politike, cilj Sklepa Sveta 2009/917/PNZ pa je pomagati pri preprečevanju, preiskovanju in pregonu hudih kršitev carinske zakonodaje. To pomeni, da se sistem CIS ne uporablja le za kazenski pregon.

Informacije, ki jih vsebuje sistem CIS, vključujejo osebne podatke v zvezi s proizvodi, prevoznimi sredstvi, podjetji, osebami ter zadržanim, zaseženim ali zarubljenim

905 Evropska komisija, *EUROSUR: Varovanje zunanjih meja schengenskega območja – zaščita življenja migrantov. EUROSUR na kratko*, 29. november 2013.

906 Uredba (EU) št. 1052/2013, uvodna izjava 13 in člen 13.

907 Prav tam, uvodna izjava 13 in člen 13.

908 Svet Evropske unije (1995), Akt Sveta z dne 26. julija 1995 o sestavitvi Konvencije o uporabi informacijske tehnologije za carinske namene (UL C 316, 27.11.1995, str. 33), spremenjen z Uredbo Sveta (ES) št. 515/97 z dne 13. marca 1997 o medsebojni pomoči med upravnimi organi držav članic in o sodelovanju med njimi in Komisijo zaradi zagotavljanja pravilnega izvajanja carinske in kmetijske zakonodaje (UL L 82, 22.3.1997, str. 1); Sklep Sveta 2009/917/PNZ o uporabi informacijske tehnologije za carinske namene (Sklep CIS) (UL L 323, 10.12.2009, str. 20).

blagom in denarjem. Kategorije podatkov, ki se lahko obdelujejo, so jasno opredeljene, vključujejo pa imena, državljanstvo, spol, kraj in datum rojstva zadevnih posameznikov, razlog za vnos njihovih podatkov v sistem in registracijsko številko prevoznega sredstva.[909] Te informacije se lahko uporabljajo le za vpogled, poročanje ali izvajanje posebnih inšpekcijskih pregledov ali za strateške ali operativne analize v zvezi z osebami, osumljenimi kršitve carinskih predpisov.

Dostop do sistema CIS imajo nacionalni carinski, davčni in kmetijski organi, organi, pristojni za javno zdravje, policija ter Europol in Eurojust.

Osebne podatke je treba obdelovati v skladu s posebnimi pravili Uredbe (ES) št. 515/97 in Sklepa Sveta 2009/917/PNZ ter določbami SUVP, uredbe o varstvu osebnih podatkov v institucijah EU, posodobljene Konvencije št. 108 in Priporočila o uporabi osebnih podatkov v policijskem sektorju. ENVP je odgovoren za nadzor nad skladnostjo sistema CIS z Uredbo (ES) št. 45/2001 in vsaj enkrat na leto skliče sestanek z vsemi nacionalnimi nadzornimi organi za varstvo podatkov, pristojnimi za vprašanja, povezana z nadzorom sistema CIS.

Interoperabilnost informacijskih sistemov EU

Upravljanje migracij, integrirano upravljanje zunanjih meja EU ter boj proti terorizmu in čezmejnemu kriminalu so pomembni izzivi, ki postajajo v globaliziranem svetu vse bolj zapleteni. EU v zadnjih letih oblikuje nov celovit pristop k ohranjanju in vzdrževanju varnosti, ne da bi bile pri tem ogrožene vrednote in temeljne svoboščine EU. Pri teh prizadevanjih je ključna učinkovita izmenjava informacij med nacionalnimi organi kazenskega pregona ter med državami članicami in ustreznimi agencijami EU.[910] Obstoječi informacijski sistemi EU za upravljanje meja in notranjo varnost imajo vsak svoje cilje, institucionalno ureditev, posameznike, na katere se nanašajo osebni podatki, in uporabnike. EU si prizadeva odpraviti pomanjkljivosti v funkcionalnostih razdrobljene arhitekture EU za upravljanje podatkov, ki zajema različne informacijske sisteme, kot so SIS II, VIS in Eurodac, in sicer s proučevanjem možnosti

909 Glej Sklep CIS, členi 24, 25 in 28.

910 Evropska komisija (2016), Sporočilo Komisije Evropskemu parlamentu in Svetu z dne 6. aprila 2016 z naslovom Trdnejši in pametnejši informacijski sistemi za meje in varnost, COM(2016) 205 final, Bruselj; Evropska komisija (2016), Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu in Svetu z dne 14. septembra 2016 z naslovom Krepitev varnosti v svetu mobilnosti: boljša izmenjava informacij na področju boja proti terorizmu in trdnejše zunanje meje, COM(2016) 602 final, Bruselj; Evropska komisija (2016), Predlog uredbe Evropskega parlamenta in Sveta o uporabi schengenskega informacijskega sistema za vračanje nezakonito prebivajočih državljanov tretjih držav. Glej tudi Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu in Svetu, z dne 16. maja 2017 z naslovom Sedmo poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije, COM(2017) 261 final, Bruselj.

za interoperabilnost.[911] Glavni cilj je zagotoviti, da imajo pristojni policijski, carinski in pravosodni organi sistematično na voljo potrebne informacije za opravljanje svojih nalog, ob tem pa ohranjati ravnovesje v zvezi s pravicama do zasebnosti in varstva osebnih podatkov ter drugimi temeljnimi pravicami.

Interoperabilnost je „zmožnost informacijskih sistemov, da si izmenjujejo podatke in omogočajo souporabo informacij".[912] Ta izmenjava ne sme ogroziti nujno strogih pravil o dostopu in uporabi, ki jih zagotavljajo SUVP, direktiva o varstvu osebnih podatkov, ki jih obdelujejo policija in organi kazenskega pravosodja, Listina EU o temeljnih pravicah in vsa druga ustrezna pravila. Nobena integrirana rešitev za upravljanje podatkov ne sme vplivati na načela omejitve namena, vgrajenega varstva osebnih podatkov ali privzetega varstva osebnih podatkov.[913]

Komisija je poleg izboljšanja funkcionalnosti treh glavnih informacijskih sistemov – SIS II, VIS in Eurodac – predlagala tudi vzpostavitev četrtega centraliziranega sistema za upravljanje meja, s katerim bi se obravnavali državljani tretjih držav: sistem vstopa/izstopa (SVI),[914] ki naj bi se začel izvajati do leta 2020.[915] Komisija je poleg tega objavila predlog o vzpostavitvi evropskega sistema za potovalne informacije in odobritve (ETIAS),[916] v okviru katerega se bodo zbirale informacije o osebah, ki v EU potujejo brez vizuma, da se omogočijo predhodna preverjanja nedovoljenih migracij in varnostna preverjanja.

911 Svet Evropske Unije (2005), Haaški program: krepitev svobode, varnosti in pravice v Evropski uniji (UL C 53, 3.3.2005, str. 1); Evropska komisija (2010), Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu in Svetu„ Pregled upravljanja informacij na območju svobode, varnosti in pravice, COM(2010) 385 final; Evropska komisija (2016), Sporočilo Komisije Evropskemu parlamentu in Svetu z dne 6. aprila 2016 z naslovom Trdnejši in pametnejši informacijski sistemi za meje in varnost, COM(2016) 205 final, Bruselj; Evropska komisija (2016), Sklep Komisije z dne 17. junija 2016 o ustanovitvi strokovne skupine na visoki ravni za informacijske sisteme in interoperabilnost (UL C 257, 15.7.2016, str. 3).

912 Evropska komisija (2016), Sporočilo Komisije Evropskemu parlamentu in Svetu z dne 6. aprila 2016 z naslovom Trdnejši in pametnejši informacijski sistemi za meje in varnost, COM(2016) 205 final, Bruselj, str. 14.

913 Prav tam, str. 4 in 5.

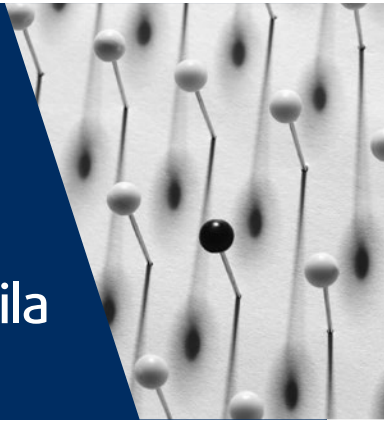
914 Evropska komisija (2016), Predlog uredbe Evropskega parlamenta in Sveta z dne 6. aprila 2016 o vzpostavitvi sistema vstopa/izstopa (SVI) za evidentiranje podatkov o vstopu in izstopu ter zavrnitvi vstopa državljanov tretjih držav pri prehajanju zunanjih meja držav članic Evropske unije in določitvi pogojev za dostop do SVI zaradi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter spremembi Uredbe (ES) št. 767/2008 in Uredbe (EU) št. 1077/2011, COM(2016) 194 final, Bruselj.

915 Evropska komisija (2016), Sporočilo Komisije Evropskemu parlamentu in Svetu z dne 6. aprila 2016 z naslovom Trdnejši in pametnejši informacijski sistemi za meje in varnost, COM(2016) 205 final, Bruselj, str. 5.

916 Evropska komisija (2016), Predlog uredbe Evropskega parlamenta in Sveta z dne 16. novembra 2016 o vzpostavitvi evropskega sistema za potovalne informacije in odobritve (ETIAS) ter spremembi uredb (EU) št. 515/2014, (EU) 2016/399, (EU) 2016/794 in (EU) 2016/1624, COM(2016) 731 final.

9

Posebne vrste osebnih podatkov in zadevna pravila o njihovem varstvu



EU	Obravnavane teme	Svet Evrope
SUVP Direktiva o zasebnosti in elektronskih komunikacijah	**Elektronske komunikacije**	Posodobljena Konvencija št. 108 Priporočilo o telekomunikacijskih storitvah
SUVP, člen 88	**Odnosi med delodajalci in delojemalci**	Posodobljena Konvencija št. 108 Priporočilo o zaposlovanju ESČP, *Copland proti Združenemu kraljestvu*, pritožba št. 62617/00, 2007
SUVP, člen 9(2)(h) in (i)	**Zdravstveni podatki**	Posodobljena Konvencija št. 108 Priporočilo o zdravstvenih podatkih ESČP, *Z proti Finski*, pritožba št. 22009/93, 1997
Uredba o kliničnem preskušanju	**Klinično preskušanje**	
SUVP, člen 6(4) in člen 89	**Statistični podatki**	Posodobljena Konvencija št. 108 Priporočilo o statističnih podatkih

EU	Obravnavane teme	Svet Evrope
Uredba (ES) št. 223/2009 o evropski statistiki SEU, C-524/06, *Huber proti Bundesrepublik Deutschland* (veliki senat), 2008	**Uradni statistični podatki**	Posodobljena Konvencija št. 108 Priporočilo o statističnih podatkih
Direktiva 2014/65/EU o trgih finančnih instrumentov Uredba (EU) št. 648/2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov Uredba (ES) št. 1060/2009 o bonitetnih agencijah Direktiva 2007/64/ES o plačilnih storitvah na notranjem trgu	**Finančni podatki**	Posodobljena Konvencija št. 108 Priporočilo 90(19), ki se uporablja za plačila in druge s tem povezane transakcije ESČP, *Michaud proti Franciji*, pritožba št. 12323/11, 2012

V več primerih so bili na evropski ravni sprejeti posebni pravni instrumenti, s katerimi se splošna pravila iz posodobljene Konvencije št. 108 ali SUVP izvajajo podrobneje za posebne primere.

9.1 Elektronske komunikacije

Ključni poudarki

- Posebna pravila o varstvu osebnih podatkov na področju telekomunikacij, zlasti telefonskih storitev, so vključena v priporočilo Sveta Evrope iz leta 1995.
- Obdelava osebnih podatkov v zvezi z zagotavljanjem komunikacijskih storitev na ravni EU je urejena v Direktivi o zasebnosti in elektronskih komunikacijah.
- Zaupnost elektronskih komunikacij se ne nanaša le na vsebino komunikacije, temveč tudi na metapodatke, na primer informacije o tem, kdo je komuniciral s kom, kdaj in kako dolgo, in lokacijske podatke, na primer od kod so bili podatki poslani.

Pri komunikacijskih omrežjih je možnost neupravičenega poseganja v zasebnost uporabnikov večja, saj ponujajo dodatne tehnične možnosti za prisluškovanje in spremljanje komunikacij, ki potekajo v takih omrežjih. Tako se je pokazala potreba po posebnih predpisih o varstvu osebnih podatkov, da bi obravnavali posebna tveganja za uporabnike komunikacijskih storitev.

Svet Evrope je leta 1995 izdal Priporočilo za varstvo osebnih podatkov na področju telekomunikacij, zlasti telefonskih storitev.[917] V skladu s tem priporočilom morajo biti nameni zbiranja in obdelave osebnih podatkov v okviru telekomunikacij omejeni na: povezovanje uporabnika v omrežje, zagotavljanje določene telekomunikacijske storitve, obračunavanje, preverjanje, zagotavljanje optimalnega tehničnega delovanja ter razvoj omrežja in storitve.

Posebna pozornost je bila namenjena tudi uporabi komunikacijskih omrežij za pošiljanje sporočil, namenjenih neposrednemu trženju. Splošno pravilo je, da se sporočila, namenjena neposrednemu trženju, ne smejo pošiljati naročniku, ki je izrecno odklonil njihovo prejemanje. Avtomatizirane klicne naprave za pošiljanje vnaprej posnetih oglaševalskih sporočil se lahko uporabijo samo, če je naročnik v to izrecno privolil. Podrobna pravila na tem področju se določijo z nacionalno zakonodajo.

V **pravnem okviru EU** je bila Direktiva o zasebnosti in elektronskih komunikacijah po prvem poskusu leta 1997 sprejeta leta 2002 in spremenjena leta 2009. Namen je bil dopolniti določbe prejšnje direktive o varstvu osebnih podatkov in jih prilagoditi telekomunikacijskemu sektorju.[918]

Uporaba Direktive o zasebnosti in elektronskih komunikacijah je omejena na komunikacijske storitve v javnih elektronskih omrežjih.

V Direktivi o zasebnosti in elektronskih komunikacijah se razlikuje med tremi glavnimi kategorijami podatkov, ustvarjenih med komunikacijo:

- podatki o vsebini sporočil, poslanih med komunikacijo – ti podatki so strogo zaupni;

917 Svet Evrope, Odbor ministrov (1995), Priporočilo Rec(95)4 državam članicam o varstvu osebnih podatkov na področju telekomunikacijskih storitev, zlasti telefonskih storitev, 7. februar 1995.

918 Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov (UL L 337, 18.12.2009, str. 11).

- podatki, ki so potrebni za vzpostavitev in ohranjanje komunikacije – t. i. metapodatki, ki se v navedeni direktivi imenujejo „podatki o prometu“ –, kot so informacije o sogovornikih ter njenem času in trajanju;

- med metapodatki so podatki, ki se posebej nanašajo na lokacijo komunikacijske naprave, t. i. lokacijski podatki – to so hkrati tudi podatki o lokaciji uporabnikov komunikacijskih naprav, zlasti pri uporabnikih mobilnih komunikacijskih naprav.

Ponudnik storitve lahko podatke o prometu uporablja samo za obračunavanje in tehnično zagotavljanje storitve. Vendar se lahko ti podatki s privolitvijo posameznika, na katerega se nanašajo, posredujejo drugim upravljavcem, ki ponujajo storitve z dodano vrednostjo, kot je na primer zagotavljanje informacij na podlagi lokacije uporabnika o naslednji postaji podzemne železnice ali lekarni ali vremenske napovedi za to lokacijo.

V skladu s členom 15 Direktive o zasebnosti in elektronskih komunikacijah morajo biti za drug dostop do podatkov o komunikacijah v elektronskih omrežjih izpolnjene zahteve za upravičeno poseganje v pravico do varstva osebnih podatkov, kot je določeno v členu 8(2) EKČP ter potrjeno v členih 8 in 52 Listine EU o temeljnih pravicah. Tak dostop lahko vključuje dostop za preiskovanje kaznivih dejanj.

S spremembami iz leta 2009 je bilo v Direktivo o zasebnosti in elektronskih komunikacijah[919] uvedeno naslednje:

- omejitve v zvezi s pošiljanjem e-sporočil zaradi neposrednega trženja so bile razširjene na storitve kratkih sporočil, storitve večpredstavnih sporočil in druge vrste podobnih aplikacij; oglaševalska e-sporočila so prepovedana, razen če se pridobi predhodna privolitev. Če take privolitve ni, se lahko oglaševalska e-sporočila pošiljajo samo prejšnjim strankam, če so dale na voljo svoj e-naslov in temu ne nasprotujejo;

- državam članicam je bila naložena obveznost zagotovitve pravnih sredstev zoper kršitve prepovedi neželenih sporočil;[920]

919 Direktiva 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov (UL L 337, 18.12.2009, str. 11).

920 Glej spremenjeno direktivo, člen 13.

- nameščanje piškotkov, programske opreme, ki spremlja in beleži dejanja računalniškega uporabnika, ni več dovoljeno brez njegove privolitve. Z nacionalno zakonodajo se podrobneje določi, kako mora biti privolitev izražena in pridobljena, da se zagotovi zadostno varstvo.[921]

Če pride do kršitve varnosti osebnih podatkov zaradi nedovoljenega dostopa, izgube ali uničenja podatkov, je treba o tem nemudoma obvestiti pristojni nadzorni organ. Naročnike je treba obvestiti, če so bili morda oškodovani zaradi kršitve varnosti osebnih podatkov.[922]

Ponudniki komunikacijskih storitev so morali v skladu z direktivo o hrambi podatkov[923] hraniti metapodatke, vendar je SEU to direktivo razveljavilo (za več podrobnosti glej razdelek 8.3).

Obeti

Evropska komisija je januarja 2017 sprejela nov predlog uredbe o zasebnosti in elektronskih komunikacijah, ki bi nadomestila staro Direktivo o zasebnosti in elektronskih komunikacijah. Cilj naj bi bil še naprej varstvo „temeljnih pravic in svoboščin fizičnih in pravnih oseb pri zagotavljanju in uporabi elektronskih komunikacijskih storitev in zlasti pravic do spoštovanja zasebnega življenja in komunikacij ter varstv[o] posameznikov pri obdelavi osebnih podatkov“. Hkrati je namen novega predloga zagotoviti prosti pretok elektronskih komunikacijskih podatkov in storitev v Uniji.[924] V SUVP je obravnavan predvsem člen 8 Listine EU o temeljnih pravicah, cilj predlagane uredbe pa je vključiti člen 7 Listine v sekundarno zakonodajo EU.

Z uredbo naj bi se določbe prejšnje direktive prilagodile novim tehnologijam in dejanskemu stanju na trgu, poleg tega naj bi se z njo vzpostavil celovit okvir, skladen

921 Glej prav tam, člen 5; glej tudi Delovna skupina za varstvo podatkov iz člena 29 (2012), *Mnenje 04/2012 o piškotkih, ki so izvzeti iz zahteve po soglasju*, WP 194, Bruselj, 7. junij 2012.

922 Glej tudi Delovna skupina za varstvo podatkov iz člena 29 (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* (Delovni dokument št. 1/2011 o sedanjem okviru EU za kršitve osebnih podatkov in priporočilih o prihodnjem razvoju politike), WP 184, Bruselj, 5. april 2011.

923 Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13.4.2006, str. 54).

924 Predlog uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah) (COM(2017) 10 final), člen 1.

s SUVP. V tem smislu bi bila uredba o zasebnosti in elektronskih komunikacijah *lex specialis* glede na SUVP, pri čemer bi jo prilagodila elektronskim komunikacijskim podatkom, ki se štejejo za osebne podatke. Nova uredba zajema obdelavo elektronskih komunikacijskih podatkov, vključno z vsebino elektronskih komunikacij in elektronskimi komunikacijskimi metapodatki, ki niso nujno osebni podatki. Ozemeljska veljavnost je omejena na EU, pri čemer vključuje primere, kadar se podatki, pridobljeni v EU, obdelujejo zunaj nje, in ponudnike storitev OTT. To so ponudniki storitev, ki zagotavljajo vsebine, storitve ali aplikacije prek interneta, in sicer brez neposredne vključenosti omrežnega operaterja ali ponudnika internetnih storitev. Taki ponudniki so na primer Skype (govorni in video klici), WhatsApp (pošiljanje sporočil), Google (iskanje), Spotify (glasba) in Netflix (video vsebine). Za novo uredbo bi se uporabljali mehanizmi za izvrševanje iz SUVPv.

Uredba o zasebnosti in elektronskih komunikacijah naj bi bila sprejeta pred 25. majem 2018, do takrat pa se bo v vseh 28 državah članicah začela uporabljati SUVP. Vendar je to odvisno od soglasja Evropskega parlamenta in Sveta.[925]

9.2 Osebni podatki o zaposlitvi

Ključni poudarki

- Posebna pravila za varstvo osebnih podatkov pri odnosih med delodajalci in delojemalci so navedena v Priporočilu Sveta Evrope o osebnih podatkih o zaposlitvi.
- V SUVP so odnosi med delodajalci in delojemalci izrecno navedeni samo v okviru obdelave občutljivih osebnih podatkov.
- Veljavnost privolitve, ki mora biti prostovoljna, kot pravne podlage za obdelavo osebnih podatkov o zaposlenih je lahko sporna glede na ekonomsko neravnovesje med delodajalcem in delojemalcem. Okoliščine privolitve je treba presojati previdno.

Za obdelavo podatkov v okviru zaposlitve se uporablja splošna zakonodaja EU o varstvu osebnih podatkov. Vendar je v eni uredbi[926] izrecno obravnavano varstvo

925 Za več informacij glej Evropska komisija (2017), Komisija predlaga predpise za visoko raven varstva zasebnosti za vse elektronske komunikacije in posodobitev predpisov za varstvo podatkov v institucijah EU, sporočilo za medije z dne 10. januarja 2017.

926 Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

posameznikov pri obdelavi osebnih podatkov v institucijah Skupnosti (med drugim) v okviru zaposlitve. V SUVP so odnosi med delodajalci in delojemalci izrecno navedeni v členu 9(2), ki določa, da se osebni podatki lahko obdelujejo za namene izpolnjevanja obveznosti in izvajanja posebnih pravic upravljavca ali posameznika, na katerega se nanašajo osebni podatki, na področju delovnega prava.

V skladu s SUVP bi bilo treba zaposlenemu omogočiti, da jasno prepozna osebne podatke, v zvezi s katerimi je prostovoljno privolil, da se obdelujejo/hranijo, in namene, za katere se njegovi osebni podatki hranijo. Pred privolitvijo bi bilo zaposlene treba seznaniti tudi z njihovimi pravicami in obdobjem hrambe osebnih podatkov. Če bi se zgodila kršitev varstva osebnih podatkov, ki bi lahko povzročila veliko tveganje za pravice in svoboščine posameznikov, mora delodajalec o tej kršitvi obvestiti zaposlenega. Države članice lahko v skladu s členom 88 zadevne uredbe določijo podrobnejša pravila za zagotovitev varstva pravic in svoboščin zaposlenih v zvezi z njihovimi osebnimi podatki v okviru zaposlitve.

Primer: v zadevi *Worten*[927] so podatki iz evidence delovnega časa vključevali podatke o dnevnem času dela in času premora, ki pomenijo osebne podatke. V skladu z nacionalnim pravom se lahko od delodajalca zahteva, da nacionalnim organom, pristojnim za nadzor delovnih razmer, omogoči vpogled v evidenco delovnega časa. To bi omogočalo takojšen dostop do zadevnih osebnih podatkov. Vendar je dostop do osebnih podatkov potreben, da se nacionalnemu organu omogoči, da izvaja nadzor uporabe predpisov s področja delovnih razmer.[928]

Kar zadeva **Svet Evrope**, je bilo leta 1989 izdano Priporočilo o osebnih podatkih o zaposlitvi, ki je bilo revidirano leta 2015.[929] V njem je obravnavana obdelava osebnih podatkov za namene zaposlitve v zasebnem in javnem sektorju. Obdelava mora biti v skladu z nekaterimi načeli in omejitvami, kot sta načelo preglednosti in posvetovanje s predstavniki zaposlenih, preden se na delovnem mestu vzpostavijo sistemi nadzora. V priporočilu je poleg tega navedeno, da bi morali delodajalci izvajati preventivne ukrepe, kot so filtri, namesto da nadzirajo uporabo interneta med zaposlenimi.

927 SEU, *Worten – Equipamentos para o Lar SA proti Autoridade para as Condições de Trabalho (ACT)*, C-342/12, 30. maj 2013, točka 19.

928 Prav tam, točka 43.

929 Svet Evrope, Odbor ministrov (2015), Priporočilo Rec(2015)5 državam članicam o obdelavi osebnih podatkov v okviru zaposlitve, april 2015.

Pregled najpogostejših težav v zvezi z varstvom osebnih podatkov, ki so značilne za okvir zaposlitve, je na voljo v delovnem dokumentu Delovne skupine iz člena 29.[930] Delovna skupina je analizirala pomen privolitve kot pravne podlage za obdelavo podatkov o zaposlitvi.[931] Ugotovila je, da ekonomsko neravnovesje med delodajalcem, ki zaprosi za privolitev, in zaposlenim, ki privolitev daje, pogosto vzbudi dvome o tem, ali je bila privolitev prostovoljna ali ne. Pri presoji veljavnosti privolitve v okviru zaposlitve je treba zato pozorno proučiti okoliščine, v katerih je privolitev pravna podlaga za obdelavo osebnih podatkov.

Pogosta težava v zvezi z varstvom osebnih podatkov v današnjem značilnem delovnem okolju je obseg, v katerem je spremljanje elektronskih komunikacij zaposlenega na delovnem mestu zakonito. Pogosto se trdi, da bi to težavo zlahka rešili, če bi na delovnem mestu prepovedali zasebno uporabo komunikacijskih naprav. Vendar bi lahko bila taka splošna prepoved nesorazmerna in nerealna. V zvezi s tem sta zlasti pomembni sodbi ESČP v zadevah *Copland proti Združenemu kraljestvu* in *Bărbulescu proti Romuniji*.

Primer: v zadevi *Copland proti Združenemu kraljestvu*[932] se je pri uslužbenki visokošolske ustanove na skrivaj spremljala uporaba telefona, elektronske pošte in interneta, da bi se ugotovilo, ali naprave visokošolske ustanove pretirano uporablja za zasebne namene. ESČP je menilo, da so telefonski klici iz poslovnih prostorov zajeti s pojmoma zasebno življenje in dopisovanje. Zato so bili taki klici in elektronska pošta, poslana z delovnega mesta, ter vse informacije, pridobljene s spremljanjem zasebne uporabe interneta, varovani s členom 8 EKČP. V pritožničinem primeru ni bilo predpisano, v katerih okoliščinah lahko delodajalci nadzorujejo uporabo telefona, elektronske pošte in interneta svojih zaposlenih. Tak poseg zato ni bil v skladu z zakonom. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Primer: v zadevi *Bărbulescu proti Romuniji*[933] je bil pritožnik odpuščen, ker je v nasprotju z internimi pravili med delovnim časom uporabljal internet na delovnem mestu. Njegov delodajalec je nadziral njegovo komunikacijo.

930 Delovna skupina za varstvo podatkov iz člena 29 (2017), *Mnenje št. 2/2017 o obdelavi podatkov pri delu*, WP 249, Bruselj, 8. junij 2017.

931 Delovna skupina za varstvo podatkov iz člena 29 (2005), *Delovni dokument o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995*, WP 114, Bruselj, 25. november 2005.

932 ESČP, *Copland proti Združenemu kraljestvu*, pritožba št. 62617/00, 3. april 2007.

933 ESČP, *Bărbulescu proti Romuniji* (veliki senat), pritožba št. 61496/08, 5. september 2017, točka 121.

V nacionalnem postopku je bila predložena evidenca komunikacije, v kateri so bila povsem zasebna sporočila. ESČP, ki je ugotovilo, da zadeva spada na področje uporabe člena 8 EKČP, ni odgovorilo na vprašanje, ali so omejevalni predpisi delodajalca pritožniku dopuščali primerno raven zasebnosti, menilo pa je, da delodajalčeva navodila ne smejo povsem prepovedati zasebnega družbenega življenja na delovnem mestu.

Kar zadeva vsebino zadeve, je bilo treba pogodbenicam podeliti široko polje proste presoje pri ocenjevanju potrebe po vzpostavitvi pravnega okvira, ki bi urejal pogoje, s katerimi bi lahko delodajalec urejal neslužbeno elektronsko ali drugo komunikacijo zaposlenih na delovnem mestu. Kljub temu bi morali nacionalni organi zagotoviti, da ukrepe za nadzor dopisovanja in druge komunikacije, ki jih uvede delodajalec, in sicer ne glede na njihov obseg in trajanje, spremljajo ustrezni in zadostni zaščitni ukrepi pred zlorabo. Načelo sorazmernosti in procesna jamstva, ki preprečujejo samovoljnost, so bistvena, pri čemer je ESČP opredelilo več dejavnikov, ki bi jih bilo treba upoštevati v okoliščinah obravnavane zadeve. Ti so se med drugim nanašali na obseg nadzora, ki ga je uvedel delodajalec, in stopnjo posega v zasebnost delavca, posledice nadzora za zaposlenega ter to, ali so bili sprejeti ustrezni zaščitni ukrepi. Poleg tega bi morali nacionalni organi zagotoviti, da ima delavec, čigar komunikacija se je nadzirala, dostop do pravnega sredstva pred sodnim organom, ki je pristojen, da vsaj vsebinsko odloča, kako so bila upoštevana navedena merila in ali so bili izpodbijani ukrepi zakoniti.

ESČP je v tem primeru ugotovilo kršitev člena 8 EKČP, saj nacionalni organi niso zagotovili ustreznega varstva pritožnikove pravice do spoštovanja zasebnega življenja in dopisovanja ter posledično niso vzpostavili pravičnega ravnotežja med zadevnimi interesi.

V skladu s Priporočilom Sveta Evrope o osebnih podatkih o zaposlitvi bi bilo treba osebne podatke, zbrane zaradi zaposlitve, pridobiti neposredno od zadevnega zaposlenega.

Osebni podatki, zbrani z namenom zaposlitve, morajo biti omejeni na informacije, ki so nujne za oceno primernosti kandidatov in njihovih poklicnih zmožnosti.

V priporočilu so tudi posebej navedene subjektivne informacije v zvezi z uspešnostjo ali potencialom posameznih zaposlenih. Subjektivne informacije morajo izhajati iz

poštenih in pravičnih ocen ter ne smejo biti žaljive. To se zahteva z načeloma poštene obdelave in točnosti podatkov.

Poseben vidik prava o varstvu osebnih podatkov v odnosu med delodajalcem in zaposlenim je vloga predstavnikov zaposlenih. Ti lahko osebne podatke o zaposlenih prejmejo le, če je to nujno za zastopanje njihovih interesov ali če so taki podatki potrebni za izpolnjevanje ali nadzor izpolnjevanja obveznosti, določenih v kolektivnih pogodbah.

Občutljivi osebni podatki, zbrani zaradi zaposlitve, se lahko obdelujejo samo v posameznih primerih in v skladu z zaščitnimi ukrepi, določenimi z nacionalno zakonodajo. Delodajalci lahko zaposlene ali kandidate za delovna mesta povprašajo o njihovem zdravstvenem stanju ali zdravstveno pregledajo le, če je to nujno. To je lahko potrebno za ugotovitev njihove primernosti za zaposlitev, izpolnitev zahtev preventivne medicine, varovanje življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugih zaposlenih in posameznikov, odobritev socialnih prejemkov ali izpolnitev sodnih odredb. Zdravstveni osebni podatki se lahko pridobijo le od zadevnega zaposlenega, razen če je bila pridobljena izrecna in informirana privolitev ali če je tako določeno z nacionalno zakonodajo.

Na podlagi Priporočila o osebnih podatkih o zaposlitvi morajo biti zaposleni obveščeni o namenu obdelave njihovih osebnih podatkov, vrsti osebnih podatkov, ki se zbirajo, subjektih, ki se jim podatki redno sporočajo, ter namenu in pravni podlagi takih razkritij. Do elektronske komunikacije se lahko na delovnem mestu dostopa le zaradi varnosti ali drugih zakonitih razlogov, pri čemer je tak dostop dovoljen le po tem, ko so bili zaposleni obveščeni, da ima lahko delodajalec dostop do tovrstne komunikacije.

Zaposleni morajo imeti pravico do dostopa do svojih osebnih podatkov o zaposlitvi in pravico do njihovega popravka ali izbrisa. Če se obdelujejo subjektivne informacije, morajo imeti zaposleni tudi pravico do njihovega izpodbijanja. Vendar se lahko te pravice zaradi notranjih preiskav začasno omejijo. Če se zaposlenemu zavrne dostop, popravek ali izbris osebnih podatkov o zaposlitvi, morajo biti z nacionalnim pravom določeni ustrezni postopki za ugovarjanje taki zavrnitvi.

9.3 Zdravstveni osebni podatki

Ključni poudarek

- Zdravstveni podatki so občutljivi osebni podatki, zato zanje velja posebno varstvo.

Osebni podatki o zdravstvenem stanju posameznika, na katerega se nanašajo, se štejejo za občutljive na podlagi člena 9(1) SUVP in člena 6 posodobljene Konvencije št. 108. Za zdravstvene osebne podatke zato velja strožja ureditev obdelave osebnih podatkov kot za neobčutljive osebne podatke. V skladu s SUVP je prepovedana obdelava osebnih podatkov v zvezi z zdravjem (za katere šteje, da obsegajo „vse podatke o zdravstvenem stanju posameznika, na katerega se nanašajo osebni podatki, ki razkrivajo informacije o njegovem preteklem, sedanjem ali prihodnjem telesnem ali duševnem zdravstvenem stanju“)[934], ter genskih podatkov in biometričnih podatkov, razen če je obdelava dovoljena v skladu s členom 9(2) navedene uredbe. Obe vrsti podatkov sta bili dodani na seznam „posebnih vrst podatkov“.[935]

Primer: v zadevi *Z proti Finski*[936] je pritožničin nekdanji mož, ki je bil okužen z virusom HIV, storil več kaznivih dejanj zoper spolno nedotakljivost. Pozneje je bil obsojen poskusa uboja, ker naj bi svoje žrtve zavestno izpostavil tveganju okužbe z virusom HIV. Nacionalno sodišče je odredilo, da celotna sodba in spis ostaneta zaupna deset let, čeprav je pritožnica večkrat zaprosila za daljše obdobje zaupnosti. Pritožbeno sodišče je te prošnje zavrnilo, v sodbi pa sta bila pritožnica in njen nekdanji mož navedena s polnimi imeni. ESČP je razsodilo, da se tako vmešavanje ne šteje za nujno v demokratični družbi, ker je varstvo zdravstvenih osebnih podatkov bistvenega pomena za uživanje pravice do spoštovanja zasebnega in družinskega življenja, zlasti kadar gre za informacije o okužbah z virusom HIV, saj je ta bolezen v številnih družbah stigmatizirana. Zato je menilo, da bi odobritev dostopa do sodbe pritožbenega sodišča, v kateri sta navedena identiteta pritožnice in njeno zdravstveno stanje, po zgolj desetih letih po izdaji sodbe pomenila kršitev člena 8 EKČP.

934 SUVP, uvodna izjava 35.

935 Prav tam, člen 9.

936 ESČP, *Z proti Finski*, pritožba št. 22009/93, 25. februar 1997, točki 94 in 112; glej tudi ESČP, *M. S. proti Švedski*, pritožba št. 20837/92, 27. avgust 1997; ESČP, *L. L. proti Franciji*, pritožba št. 7508/02, 10. oktober 2006; ESČP, *I proti Finski*, pritožba št. 20511/03, 17. julij 2008; ESČP, *K. H. in drugi proti Slovaški*, pritožba št. 32881/04, 28. april 2009, in ESČP, *Szuluk proti Združenemu kraljestvu*, pritožba št. 36936/05, 2. junij 2009.

V okviru **prava EU** člen 9(2)(h) SUVP omogoča obdelavo zdravstvenih osebnih podatkov, kadar je to potrebno za namene preventivne medicine, zdravstvene diagnoze, zagotovitev oskrbe ali zdravljenja ali upravljanje storitev zdravstvenega varstva. Vendar je obdelava dovoljena samo, če podatke obdeluje zdravstveni delavec, za katerega velja obveznost varovanja poklicne skrivnosti ali druga oseba, ki jo prav tako zavezuje ta obveznost.

V okviru **prava Sveta Evrope** je v Priporočilu Sveta Evrope o zdravstvenih podatkih iz leta 1997 podrobneje določena uporaba načel iz posodobljene Konvencije št. 108 za obdelavo osebnih podatkov na zdravstvenem področju.[937] Predlagana pravila so skladna s pravili iz SUVP glede zakonitih namenov obdelave zdravstvenih osebnih podatkov, obveznosti varovanja poklicne skrivnosti za osebe, ki uporabljajo zdravstvene osebne podatke, ter pravic posameznikov, na katere se nanašajo osebni podatki, do preglednosti, dostopa, popravka in izbrisa. Poleg tega se lahko zdravstveni osebni podatki, ki jih zdravstveni delavci zakonito obdelujejo, organom pregona posredujejo samo, če so zagotovljeni zadostni zaščitni ukrepi za preprečitev razkritja, ki ni v skladu s spoštovanjem zasebnega življenja, varovanega na podlagi člena 8 EKČP.[938] Nacionalno pravo mora biti oblikovano tudi dovolj natančno in zagotavljati ustrezno pravno varstvo pred samovoljnim ravnanjem.[939]

Priporočilo o zdravstvenih podatkih vsebuje tudi posebne določbe o zdravstvenih podatkih nerojenih otrok in oseb, ki niso sposobne odločati o sebi, ter obdelavi genskih podatkov. Znanstvene raziskave se izrecno priznavajo kot razlog za daljšo hrambo osebnih podatkov, kot je nujno, čeprav se pri tem običajno zahteva anonimizacija. V členu 12 Priporočila o zdravstvenih podatkih je predlagana podrobna ureditev za primere, kadar raziskovalci potrebujejo osebne podatke in anonimizirani podatki ne zadostujejo.

Psevdonimizacija je lahko ustrezen način za izpolnitev znanstvenih zahtev in hkratno zaščito interesov zadevnih pacientov. Pojem psevdonimizacije v okviru varstva osebnih podatkov je podrobneje pojasnjen v razdelku 2.1.1.

937 Svet Evrope, Odbor ministrov (1997), Priporočilo Rec(97)5 državam članicam o varstvu zdravstvenih podatkov, 13. februar 1997. Upoštevati je treba, da je to priporočilo v postopku revizije.

938 ESČP, *Avilkina in drugi proti Rusiji*, pritožba št. 1585/09, 6. junij 2013, točka 53. Glej tudi ESČP, *Biriuk proti Litvi*, pritožba št. 23373/03, 25. november 2008.

939 ESČP, *L. H. proti Latviji*, pritožba št. 52019/07, 29. april 2014, točka 59.

Za obdelavo osebnih podatkov na zdravstvenem področju se uporablja tudi Priporočilo Sveta Evrope iz leta 2016 o podatkih, pridobljenih z genetskimi testi.[940] To priporočilo je zelo pomembno za e-zdravje, saj se v njegovem okviru informacijske in komunikacijske tehnologije uporabljajo za omogočanje zdravstvene oskrbe. Primer je pošiljanje rezultatov testa starševstva pacienta od enega izvajalca zdravstvene dejavnosti drugemu. Namen tega priporočila je zaščititi pravice oseb, katerih osebni podatki se obdelujejo za namene zavarovanja, in sicer za zavarovanje pred tveganji v zvezi z zdravjem osebe, njeno telesno celovitostjo, starostjo ali smrtjo. Zavarovatelji morajo utemeljiti obdelavo osebnih podatkov v zvezi z zdravjem, ki bi morala biti sorazmerna z naravo in pomembnostjo obravnavanega tveganja. Za obdelavo tovrstnih podatkov je potrebna privolitev zadevnega posameznika. Zavarovatelji bi morali poleg tega imeti vzpostavljene zaščitne ukrepe za shranjevanje osebnih podatkov v zvezi z zdravjem.

Klinična preskušanja, ki vključujejo ocenjevanje učinkov novih zdravil na paciente v dokumentiranih raziskovalnih okoljih, imajo pomembne posledice za varstvo osebnih podatkov. Klinično preskušanje zdravil za uporabo v humani medicini je urejeno z Uredbo (EU) št. 536/2014 Evropskega parlamenta in Sveta z dne 16. aprila 2014 o kliničnem preskušanju zdravil za uporabo v humani medicini in razveljavitvi Direktive 2001/20/ES (uredba o kliničnem preskušanju).[941] Glavni elementi uredbe o kliničnem preskušanju so:

- poenostavljen postopek predložitve vlog prek portala EU;[942]
- roki za oceno vloge za klinična preskušanja;[943]
- odbor za etiko, ki v skladu s pravom držav članic (in evropskim pravom, s katerim so opredeljena zadevna časovna obdobja) sodeluje pri oceni,[944] in
- boljša preglednost kliničnih preskušanj in njihovih rezultatov.[945]

940 Svet Evrope, Odbor ministrov (2016), Priporočilo Rec(2016)8 državam članicam o obdelavi osebnih podatkov v zvezi z zdravjem za namene zavarovanja, vključno z osebnimi podatki, pridobljenimi z genetskimi testi, 26. oktober 2016.

941 Uredba (EU) št. 536/2014 Evropskega parlamenta in Sveta z dne 16. aprila 2014 o kliničnem preskušanju zdravil za uporabo v humani medicini in razveljavitvi Direktive 2001/20/ES (uredba o kliničnem preskušanju) (UL L 158, 27.5.2014, str. 1).

942 Uredba o kliničnem preskušanju, člen 5(1).

943 Prav tam, člen 5(2)–(5).

944 Prav tam, člen 2(2)(11).

945 Prav tam, člen 9(1) in uvodna izjava 67.

SUVP določa, da se za namene privolitve v udeležbo pri znanstvenoraziskovalnih dejavnostih v okviru kliničnega preskušanja uporabljajo določbe Uredbe (EU) št. 536/2014.[946]

Na ravni EU poteka še veliko drugih zakonodajnih in ostalih pobud v zvezi z osebnimi podatki v zdravstvu.[947]

Elektronski zdravstveni zapisi

Elektronski zdravstveni zapis je opredeljen kot „obsežen zdravstveni zapis ali podobn[a] dokumentacij[a] preteklega in sedanjega fizičnega ter psihičnega zdravstvenega stanja posameznika v elektronski obliki, katere podatki so na voljo za zdravniško zdravljenje in za druge z njim tesno povezane namene".[948] Elektronski zdravstveni zapisi so elektronske različice zdravstvene anamneze pacientov in lahko vključujejo klinične podatke v zvezi s temi posamezniki, kot je pretekla zdravstvena anamneza, težave in bolezni, zdravila in zdravljenje, pa tudi rezultate pregledov in laboratorijskih preiskav ter poročila o njih. Dostop do teh elektronskih kartotek, ki lahko segajo od celotnih zapisov do zgolj odlomkov ali povzetkov podatkov, imajo splošni zdravnik, farmacevt in drugi zdravstveni delavci. Tudi pojem e-zdravje se dotika teh zdravstvenih zapisov.

Primer: oseba A je sklenila zavarovalno pogodbo z družbo B, ki je zavarovalnica. Ta bo od osebe A zbrala nekaj informacij, povezanih z njenim zdravjem, na primer o sedanjih zdravstvenih težavah ali boleznih. Zavarovalnica bi morala osebne podatke osebe A, povezane z zdravjem, hraniti ločeno od drugih podatkov. Zavarovalnica bi poleg tega morala osebne podatke, povezane z zdravjem, hraniti ločeno od drugih osebnih podatkov. To pomeni, da bo dostop do osebnih podatkov osebe A, povezanih z zdravjem, imel le delavec, odgovoren za primer osebe A.

946 SUVP, uvodni izjavi 156 in 161.

947 ENVP (2013), *Opinion of the European Data Protection Supervisor on the Communication from the Commission on ‚eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century'* (Mnenje Evropskega nadzornika za varstvo podatkov o sporočilu Komisije z naslovom Akcijski načrt za e-zdravje za obdobje 2012–2020 – Inovativno zdravstveno varstvo za 21. stoletje), Bruselj, 27. marec 2013.

948 Priporočilo Komisije z dne 2. julija 2008 o čezmejni medobratovalnosti sistemov za vodenje elektronskih zdravstvenih zapisov, točka 3(c).

Vseeno se glede elektronskih zdravstvenih kartotek porajajo nekatera vprašanja v zvezi varstvom osebnih podatkov, kot so njihova dostopnost, ustrezno shranjevanje in dostop posameznika, na katerega se nanašajo osebni podatki, do njih.

Poleg Priporočila o elektronskih zdravstvenih zapisih je Evropska komisija 10. aprila 2014 objavila Zeleno knjigo o mobilnem zdravju (m-zdravju), saj meni, da je to nastajajoče in hitro razvijajoče se področje, ki bi lahko preoblikovalo zdravstveno varstvo ter povečalo njegovo učinkovitost in kakovost. Izraz mobilno zdravje zajema medicinsko prakso in prakso na področju javnega zdravja, podprto z mobilnimi napravami, kot so mobilni telefoni, naprave za spremljanje pacientov, dlančniki in druge brezžične naprave, pa tudi aplikacije (na primer za dobro počutje), ki se lahko povežejo z medicinskimi pripomočki ali senzorji.[949] V dokumentu so opisana tveganja za pravico do varstva osebnih podatkov, ki bi jih lahko pomenil razvoj m-zdravja, pri čemer je v njem navedeno, da bi bilo treba v razvoj zaradi občutljive narave zdravstvenih podatkov vključiti posebne in ustrezne varnostne zaščitne ukrepe za podatke o pacientih, kot je na primer šifriranje, in ustrezne mehanizme za avtentikacijo pacientov za zmanjšanje varnostnih tveganj. Zato je za vzpostavitev zaupanja v rešitve m-zdravja ključna skladnost s pravili o varstvu osebnih podatkov, vključno z obveznostjo zagotavljanja informacij posamezniku, na katerega se nanašajo osebni podatki, varnostjo osebnih podatkov in načelom zakonite obdelave osebnih podatkov.[950] V ta namen je panoga pripravila kodeks ravnanja, ki temelji na prispevkih najrazličnejših deležnikov, vključno s strokovnjaki s področja varstva osebnih podatkov, samo in sourejanja, informacijske in komunikacijske tehnologije ter zdravstvenega varstva.[951] V času pisanja tega priročnika je bil osnutek kodeksa ravnanja predložen Delovni skupini za varstvo podatkov iz člena 29, da bi o njem predložila pripombe, in še ni bil uradno potrjen.

949 Evropska komisija (2014), *Zelena knjiga o mobilnem zdravju („m-zdravju")*, COM(2014) 219 final, Bruselj, 10. april 2014.

950 Prav tam, str. 8.

951 Osnutek kodeksa ravnanja o zasebnosti za mobilne aplikacije za zdravje, 7. junij 2016.

9.4 Obdelava osebnih podatkov za raziskovalne in statistične namene

Ključna poudarka

- Osebni podatki, ki se zbirajo za statistične, znanstveno- ali zgodovinskoraziskovalne namene, se ne smejo uporabljati za noben drug namen.
- Osebni podatki, ki se zakonito zbirajo za kateri koli namen, se lahko nadalje uporabijo za statistične, znanstveno- ali zgodovinskoraziskovalne namene, če so vzpostavljeni ustrezni zaščitni ukrepi. Ti zaščitni ukrepi se lahko v tem primeru zagotovijo z anonimizacijo ali psevdonimizacijo pred prenosom osebnih podatkov tretjim osebam.

V skladu s **pravom EU** je dovoljena obdelava osebnih podatkov za statistične in znanstveno- ali zgodovinskoraziskovalne namene, če so vzpostavljeni ustrezni zaščitni ukrepi za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Ti lahko vključujejo psevdonimizacijo.[952] V pravu EU ali nacionalnem pravu so lahko določena nekatera odstopanja od pravic posameznikov, na katere se lahko nanašajo osebni podatki, če je verjetno, da bi te pravice onemogočile ali resno ovirale uresničevanje zakonitega namena raziskave.[953] Uvedejo se lahko odstopanja od pravice posameznika, na katerega se nanašajo osebni podatki, do dostopa, pravice do popravka, pravice do omejitve obdelave in pravice do ugovora.

Čeprav lahko upravljavec osebne podatke, ki jih je zakonito zbral za kateri koli namen, znova uporabi za lastne statistične, znanstveno- ali zgodovinskoraziskovalne namene, bi jih bilo treba pred prenosom tretji osebi, ki bi jih prav tako uporabila za statistične, znanstveno- ali zgodovinskoraziskovalne namene, anonimizirati ali v zvezi z njimi izvesti ukrepe, kot je psevdonimizacija, odvisno od okoliščin, razen če posameznik, na katerega se nanašajo osebni podatki, v prenos privoli ali če je ta izrecno določen z nacionalno zakonodajo. V nasprotju z anonimiziranimi osebni podatki se za psevdonimizirane osebne podatke še naprej uporablja SUVP.[954]

S to uredbo je za raziskave določena posebna obravnava v zvezi s splošnimi pravili o varstvu osebnih podatkov, da bi se preprečile omejitve za razvoj raziskav in izpolnil cilj oblikovanja evropskega raziskovalnega prostora, kot je določeno v členu 179 PDEU. Uredba določa, da je treba obdelavo osebnih podatkov

952 SUVP, člen 89(1).

953 Prav tam, člen 89(2).

954 Prav tam, uvodna izjava 26.

v znanstveno-raziskovalne namene razlagati široko, tako da vključuje tehnološki razvoj, predstavitvene dejavnosti, temeljne raziskave, uporabne raziskave in zasebno financirane raziskave. V njej sta priznana tudi pomen zbiranja podatkov v registre za raziskovalne namene in morebitna težava glede tega, da v fazi zbiranja podatkov ni mogoče vedno v celoti opredeliti poznejšega namena obdelave osebnih podatkov v znanstvenoraziskovalne namene.[955] Zato ta uredba omogoča obdelavo osebnih podatkov v te namene brez privolitve posameznikov, na katere se nanašajo osebni podatki, če so uvedeni ustrezni zaščitni ukrepi.

Pomemben primer uporabe osebnih podatkov za statistične namene so uradne statistike, ki jih nacionalni statistični uradi in statistični urad EU pridobijo na podlagi nacionalnih zakonov in zakonov EU o uradni statistiki. Državljani in podjetja so v skladu s temi zakoni podatke običajno dolžni razkriti ustreznim statističnim organom. Za uradnike, zaposlene v statističnih uradih, veljajo posebne obveznosti varovanja poklicne skrivnosti, ki jih je treba ustrezno izpolnjevati, saj so bistvenega pomena za visoko raven zaupanja državljanov, ki je nujna, če se osebni podatki dajejo na voljo statističnim organom.[956]

Uredba (ES) št. 223/2009 o evropski statistiki (uredba o evropski statistiki) vsebuje bistvena pravila za varstvo osebnih podatkov v okviru uradne statistike, zato je lahko pomembna tudi za določbe o uradni statistiki, sprejete na nacionalni ravni.[957] V uredbi se zagovarja načelo, da je za dejavnosti uradne statistike potrebna dovolj jasna pravna podlaga.[958]

Primer: v zadevi *Huber proti Bundesrepublik Deutschland*[959] se je avstrijski poslovnež, ki se je preselil v Nemčijo, pritožil, da nemški organi s tem, ko zbirajo in shranjujejo osebne podatke tujih državljanov v centralnem registru (AZR) tudi za statistične namene, kršijo njegove pravice na podlagi direktive

955 Prav tam, uvodne izjave 33, 157 in 159.

956 Prav tam, člen 90.

957 Uredba (ES) št. 223/2009 Evropskega parlamenta in Sveta z dne 11. marca 2009 o evropski statistiki ter razveljavitvi Uredbe (ES, Euratom) št. 1101/2008 Evropskega parlamenta in Sveta o prenosu zaupnih podatkov na Statistični urad Evropskih skupnosti, Uredbe Sveta (ES) št. 322/97 o statističnih podatkih Skupnosti in Sklepa Sveta 89/382/EGS, Euratom, o ustanovitvi Odbora za statistične programe Evropskih skupnosti (UL L 87, 31.3.2009, str. 164), kakor je bila spremenjena z Uredbo (EU) 2015/759 Evropskega parlamenta in Sveta z dne 29. aprila 2015 o spremembi Uredbe (ES) št. 223/2009 o evropski statistiki (UL L 123, 19.5.2015, str. 90).

958 To načelo naj bi bilo nadalje opredeljeno v Eurostatovem kodeksu ravnanja, v katerem bodo v skladu s členom 11 uredbe o evropski statistiki zagotovljene etične smernice o vodenju uradnih statistik, vključno s premišljeno uporabo osebnih podatkov.

959 SEU, *Heinz Huber proti Bundesrepublik Deutschland* (veliki senat), C-524/06, 16. december 2008,; glej zlasti točko 68.

o varstvu osebnih podatkov. Ker je cilj Direktive 95/46/ES zagotoviti enakovredno raven varstva osebnih podatkov v vseh državah članicah, je SEU menilo, da se zaradi zagotavljanja visoke ravni varstva v EU pomen pojma nujnosti iz člena 7(e) navedene direktive med državami članicami ne more razlikovati. Gre torej za samostojen pojem prava EU, ki ga je treba razlagati na način, ki v celoti izraža cilj Direktive 95/46/ES. SEU je ugotovilo, da bi bilo treba za statistične namene uporabljati le anonimizirane informacije, zato je odločilo, da nemški register ni v skladu z zahtevo glede potrebnosti iz člena 7(e) navedene direktive.

V okviru **prava Sveta Evrope** se lahko osebni podatki nadalje obdelujejo za znanstvene, zgodovinske ali statistične namene, če je to v javnem interesu, pri čemer za nadaljnjo obdelavo veljajo ustrezni zaščitni ukrepi.[960] Pravice posameznikov, na katere se nanašajo osebni podatki, so lahko omejene tudi, kadar se osebni podatki obdelujejo za statistične namene, če ne obstaja nobeno prepoznavno tveganje za kršitev njihovih pravic in svoboščin.[961]

V Priporočilu o statističnih podatkih, ki je bilo izdano leta 1997, je obravnavano izvajanje statistične dejavnosti v javnem in zasebnem sektorju.[962]

Osebni podatki, ki jih upravljavec zbira za statistične namene, se ne smejo uporabiti za noben drug namen. Osebni podatki, ki se zbirajo za nestatistične namene, so na voljo za nadaljnjo statistično uporabo. V skladu s Priporočilom o statističnih podatkih je dovoljeno tudi posredovanje osebnih podatkov tretjim osebam, če je to izključno za statistične namene. V takih primerih se morajo stranke dogovoriti o obsegu zakonite nadaljnje uporabe za statistiko in ga zapisati. Ker to ne more nadomestiti privolitve posameznika, na katerega se nanašajo osebni podatki, če je ta potrebna, morajo biti v nacionalnem pravu določeni ustrezni zaščitni ukrepi, da se zmanjšajo tveganja zlorabe osebnih podatkov, na primer obveznost, da se osebni podatki pred razkritjem anonimizirajo ali psevdonimizirajo.

Za strokovnjake s področja statističnih raziskav morajo v skladu z nacionalnim pravom veljati posebne obveznosti varovanja poklicne skrivnosti, kot običajno velja za uradno statistiko. Enako mora veljati tudi za anketarje in druge zbiratelje osebnih

960 Posodobljena Konvencija št. 108, člen 5(4)(b).

961 Prav tam, člen 11(2).

962 Svet Evrope, Odbor ministrov (1997), Priporočilo Rec(97)18 državam članicam o varstvu osebnih podatkov, zbranih in obdelanih v statistične namene, 30. september 1997.

podatkov, če zbirajo osebne podatke od posameznikov, na katere se nanašajo osebni podatki, ali drugih oseb.

Da bi bila statistična raziskava, pri kateri se uporabljajo osebni podatki in ki ni dovoljena z zakonom, zakonita, bodo posamezniki, na katere se nanašajo osebni podatki, morda morali privoliti v uporabo svojih podatkov ali imeti možnost, da ji ugovarjajo. Če osebne podatke za statistične namene zbirajo anketarji, morajo biti anketiranci jasno obveščeni o tem, ali je v skladu z nacionalnim pravom razkritje osebnih podatkov obvezno ali ne.

Če statistične raziskave ni mogoče izvesti z anonimnimi podatki in so potrebni osebni podatki, je treba osebne podatke, zbrane za ta namen, čim prej anonimizirati. Osnovni pogoj je, da na podlagi rezultatov statistične raziskave ni mogoče določiti nobenega posameznika, na katerega se nanašajo osebni podatki, razen če to očitno ne bi povzročilo nikakršnega tveganja.

Uporabljene osebne podatke je treba po koncu statistične analize izbrisati ali anonimizirati. V takih primerih je treba identifikacijske podatke v skladu s Priporočilom o statističnih podatkih hraniti ločeno od drugih osebnih podatkov. To na primer pomeni, da je treba šifrirni ključ ali seznam, ki vsebuje identifikacijske sinonime, hraniti ločeno od drugih podatkov.

9.5 Finančni podatki

Ključni poudarki

- Čeprav se finančni osebni podatki ne štejejo za občutljive osebne podatke v smislu posodobljene Konvencije št. 108 ali SUVP, so za njihovo obdelavo potrebni posebni zaščitni ukrepi za zagotovitev točnosti in varnosti osebnih podatkov.
- Pri elektronskih plačilnih sistemih je zlasti potrebno varovanje osebnih podatkov tj. vgrajeno in privzeto varstvo zasebnosti oziroma osebnih podatkov.
- Na tem področju se lahko zaradi potrebe po vzpostavitvi ustreznih mehanizmov avtentikacije pojavijo posebne težave v zvezi z varstvom osebnih podatkov.

Primer: v zadevi *Michaud proti Franciji*[963] je pritožnik, francoski odvetnik, izpodbijal obveznost, ki jo je imel po francoskem pravu, da prijavi sum pranja denarja svojih strank. ESČP je ugotovilo, da zahteva, da morajo odvetniki upravnim organom sporočiti informacije o drugi osebi, ki so jih pridobili v okviru poklicnih dejavnosti, pomeni poseganje v pravico odvetnikov do spoštovanja njihovega dopisovanja in zasebnega življenja na podlagi člena 8 EKČP, saj so s tem pojmom zajete poklicne ali poslovne dejavnosti. Vendar je bilo poseganje v skladu z zakonom in je imelo zakonit cilj, tj. preprečevanje nereda in kriminala. Ker obveznost prijave sumljivih dejavnosti za odvetnike velja le v točno določenih okoliščinah, je ESČP menilo, da je ta obveznost sorazmerna. Ugotovilo je, da člen 8 EKČP ni bil kršen.

Primer: v zadevi *M. N. in drugi proti San Marinu*[964] je pritožnik, italijanski državljan, sklenil fiduciarno pogodbo z družbo v preiskavi. To pomeni, da je bila v zadevni družbi izvedena preiskava, v okviru katere so bile zasežene kopije (elektronske) dokumentacije. Pritožnik je pri sodišču v San Marinu vložil pritožbo, v kateri je trdil, da med njim in očitanimi kaznivimi dejanji ni nobene povezave. Vendar je sodišče njegovo pritožbo razglasilo za nedopustno, saj pritožnik ni bil stranka v postopku. ESČP je menilo, da je bil pritožnik v primerjavi s strankami v postopku v precej slabšem položaju glede sodnega varstva in da so bili kljub temu njegovi osebni podatki predmet preiskave in zasega. Sodišče je zato menilo, da je bil kršen člen 8 EKČP.

Primer: v zadevi *G. S. B. proti Švici*[965] so bili na podlagi sporazuma med Švico in ZDA o upravnem sodelovanju podatki o bančnem računu pritožnika poslani davčnim organom ZDA. ESČP je menilo, da prenos ni bil v nasprotju s členom 8 EKČP, saj je bil poseg v pravico pritožnika do zasebnosti določen z zakonom, imel je zakonit cilj in je bil sorazmeren z zadevnim javnim interesom.

Svet Evrope je v Priporočilu Rec(90)19 iz leta 1990 opredelil uporabo splošnega pravnega okvira za varstvo osebnih podatkov (kot je bil določen v Konvenciji št. 108) na področju plačil.[966] V tem priporočilu je pojasnjen obseg zakonitega zbiranja in upo-

963 ESČP, *Michaud proti Franciji*, pritožba št. 12323/11, 6. december 2012. Glej tudi ESČP, *Niemietz proti Nemčiji*, pritožba št. 13710/88, 16. december 1992, točka 29, in ESČP, *Halford proti Združenemu kraljestvu*, pritožba št. 20605/92, 25. junij 1997, točka 42.

964 ESČP, *M. N. in drugi proti San Marinu*, pritožba št. 28005/12, 7. julij 2015.

965 ESČP, *G. S. B. proti Švici*, pritožba št. 28601/11, 22. december 2015.

966 Svet Evrope, Odbor ministrov (1990), Priporočilo R(90)19 o varstvu osebnih podatkov, ki se uporabljajo za plačila in druge povezane finančne transakcije, 13. september 1990.

rabe osebnih podatkov na področju plačil, zlasti plačil s plačilnimi karticami. Poleg tega so v njem nacionalnim zakonodajalcem zagotovljena podrobna priporočila o razkritju podatkov o plačilih tretjim osebam, rokih za hrambo osebnih podatkov, preglednosti, varnosti osebnih podatkov in čezmejnem prenosu osebnih podatkov ter nadzoru in pravnih sredstvih. Svet Evrope je pripravil tudi Mnenje o prenosu davčnih podatkov,[967] v katerem so navedena priporočila in vidiki, ki jih je treba upoštevati pri prenosu davčnih podatkov.

ESČP dovoljuje prenos finančnih podatkov – zlasti podatkov o bančnem računu posameznika – v skladu s členom 8 EKČP, če je določen z zakonom, uresničuje zakonit cilj in je sorazmeren z zadevnim javnim interesom.[968]

Kar zadeva **pravo EU**, morajo biti elektronski plačilni sistemi, ki vključujejo obdelavo osebnih podatkov, v skladu s SUVP. Ti sistemi morajo zato zagotavljati vgrajeno in privzeto varstvo osebnih podatkov. V skladu z vgrajenim varstvom osebnih podatkov mora upravljavec sprejeti ustrezne tehnične in organizacijske ukrepe za izvajanje načel varstva osebnih podatkov. Privzeto varstvo osebnih podatkov pomeni, da mora upravljavec zagotoviti, da se lahko privzeto obdelujejo le osebni podatki, ki so potrebni za določen namen (glej razdelek 4.4). V zvezi s finančnimi podatki je SEU menilo, da preneseni davčni podatki lahko pomenijo osebne podatke.[969] Delovna skupina iz člena 29 je v zvezi s tem izdala smernice za države članice, vključno z merili za zagotavljanje skladnosti s pravili o varstvu osebnih podatkov pri samodejni izmenjavi osebnih podatkov za davčne namene z avtomatiziranimi sredstvi.[970] Poleg tega je bilo sprejetih več pravnih instrumentov za ureditev finančnih trgov ter dejavnosti kreditnih institucij in investicijskih podjetij.[971] Drugi pravni instrumenti

967 Svet Evrope, Posvetovalni odbor po Konvenciji št. 108 (2014), Mnenje o posledicah za varstvo osebnih podatkov, ki jih imajo mehanizmi za samodejne meddržavne izmenjave podatkov za upravne in davčne namene, 4. junij 2014.

968 ESČP, *G. S. B. proti Švici*, pritožba št. 28601/11, 22. december 2015.

969 SEU, *Smaranda Bara in drugi proti Președintele Casei Naționale de Asigurări de Sănătate in drugim*, C-201/14, 1. oktober 2015, točka 29.

970 Delovna skupina za varstvo podatkov iz člena 29 (2015), *Izjava Delovne skupine iz člena 29 o avtomatičnih meddržavnih izmenjavah osebnih podatkov za davčne namene*, 14/SL WP 230.

971 Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU (UL L 173, 12.6.2014, str. 349); Uredba (EU) št. 600/2014 Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov in spremembi Uredbe (EU) št. 648/2012 (UL L 173, 12.6.2014, str. 84); Direktiva 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES (UL L 176, 27.6.2013, str. 338).

pomagajo v boju proti trgovanju z notranjimi informacijami in tržni manipulaciji.[972] Glavna področja, ki vplivajo na varstvo osebnih podatkov, so:

- hramba evidenc o finančnih transakcijah;
- prenos osebnih podatkov v tretje države;
- snemanje elektronskih komunikacij ali evidentiranje elektronskih komunikacij, vključno s pravico pristojnih organov, da zahtevajo telefonske evidence in podatke o prometu;
- razkritje osebnih informacij, vključno z objavo sankcij;
- nadzorna in preiskovalna pooblastila pristojnih organov, vključno s pregledi na kraju samem in vstopom v zasebne prostore zaradi zasega dokumentov;
- mehanizmi za prijavo kršitev, tj. sistemi za prijavljanje nepravilnosti, ter
- sodelovanje med pristojnimi organi držav članic in Evropskim organom za vrednostne papirje in trge (ESMA).

Na teh področjih so posebej obravnavana tudi druga vprašanja, vključno z zbiranjem osebnih podatkov o finančnem stanju posameznikov, na katere se nanašajo osebni podatki,[973] ali čezmejnimi plačili z bančnimi nakazili, ki nujno vključujejo prenos osebnih podatkov.[974]

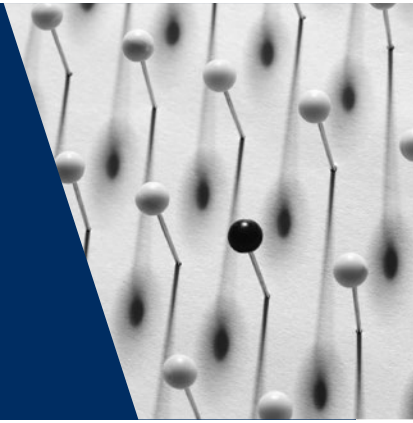
---

972 Uredba (EU) št. 596/2014 Evropskega parlamenta in Sveta z dne 16. aprila 2014 o zlorabi trga (uredba o zlorabi trga) ter razveljavitvi Direktive 2003/6/ES Evropskega parlamenta in Sveta ter direktiv Komisije 2003/124/ES, 2003/125/ES in 2004/72/ES (UL L 173, 12.6.2014, str. 1).

973 Uredba (ES) št. 1060/2009 Evropskega parlamenta in Sveta z dne 16. septembra 2009 o bonitetnih agencijah (UL L 302, 17.11.2009, str. 1), nazadnje spremenjena z Direktivo 2014/51/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o spremembi direktiv 2003/71/ES in 2009/138/ES ter uredb (ES) št. 1060/2009, (EU) št. 1094/2010 in (EU) št. 1095/2010 glede pristojnosti Evropskega nadzornega organa (Evropski organ za zavarovanja in poklicne pokojnine) ter Evropskega nadzornega organa (Evropski organ za vrednostne papirje in trge) (UL L 153, 22.5.2014, str. 1); Uredba (EU) št. 462/2013 Evropskega parlamenta in Sveta z dne 21. maja 2013 o spremembi Uredbe (ES) št. 1060/2009 o bonitetnih agencijah (UL L 146, 31.5.2013, str. 1).

974 Direktiva 2007/64/ES Evropskega parlamenta in Sveta z dne 13. novembra 2007 o plačilnih storitvah na notranjem trgu in o spremembah direktiv 97/7/ES, 2002/65/ES, 2005/60/ES in 2006/48/ES ter o razveljavitvi Direktive 97/5/ES (UL L 319, 5.12.2007, str. 1), kakor je bila spremenjena z Direktivo 2009/111/ES Evropskega parlamenta in Sveta z dne 16. septembra 2009 o spremembi direktiv 2006/48/ES, 2006/49/ES in 2007/64/ES glede bank, ki so odvisne od centralnih institucij, nekaterih postavk lastnih sredstev, velikih izpostavljenosti, nadzornih režimov in kriznega upravljanja (UL L 302, 17.11.2009, str. 97).

10 Sodobni izzivi v zvezi z varstvom osebnih podatkov



Za digitalno dobo ali dobo informacijske tehnologije je značilna vsesplošna uporaba računalnikov, interneta in digitalnih tehnologij. Ta vključuje zbiranje in obdelavo velikih količin podatkov, vključno z osebnimi podatki. Zbiranje in obdelava osebnih podatkov v globaliziranem gospodarstvu pomenita, da se povečuje število čezmejnih tokov podatkov. Taka obdelava lahko prinaša pomembne in očitne koristi v vsakdanjem življenju: iskalniki lajšajo dostop do velikih količin informacij in znanja, storitve družbenih omrežij ljudem po vsem svetu omogočajo, da komunicirajo, izražajo svoja mnenja in pridobivajo podporo za družbene, okoljske in politične cilje, podjetja in potrošniki pa imajo koristi od uspešnih in učinkovitih trženjskih tehnik, ki spodbujajo gospodarstvo. Tehnologija in obdelava osebnih podatkov sta poleg tega nepogrešljivi orodji za državne organe v boju proti kriminalu in terorizmu. Podobno so lahko masovni podatki – zbiranje, shranjevanje in analiza velikih količin informacij za prepoznavanje vzorcev in napovedovanje ravnanja – zelo pomemben vir za družbo, ki spodbuja produktivnost, uspešnost javnega sektorja in družbeno udeležbo.[975]

Digitalna doba kljub številnim koristim prinaša tudi izzive v zvezi z zasebnostjo in varstvom osebnih podatkov, saj se ogromne količine osebnih podatkov zbirajo in obdelujejo na vse bolj zapletene in nepregledne načine. Tehnološki napredek je privedel do razvoja masovnih naborov podatkov, ki jih je mogoče zlahka navzkrižno preverjati in nadalje analizirati za prepoznavanje vzorcev ali sprejemanje odločitev na podlagi algoritmov, s čimer se lahko zagotovi doslej najboljši vpogled v človeško vedenje in zasebno življenje.[976]

975 Svet Evrope, Posvetovalni odbor po Konvenciji št. 108, *Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov*, T-PD(2017)01, Strasbourg, 23. januar 2017.

976 Evropski parlament (2017), Resolucija o posledicah velepodatkov za temeljne pravice: zasebnost, varstvo podatkov, nediskriminacija, varnost in kazenski pregon (P8_TA-PROV(2017)0076), Strasbourg, 14. marec 2017.

Nove tehnologije so zmogljive in so lahko še posebej nevarne, če pridejo v napačne roke. Dejavnosti množičnega nadzora, ki jih izvajajo državni organi in pri katerih se lahko uporabljajo te tehnologije, so primer znatnega vpliva, ki ga lahko imajo te tehnologije na pravice posameznikov. Leta 2013 so razkritja Edwarda Snowdna o obsežnih programih internetnega nadzora in telefonskega prisluškovanja, ki jih v nekaterih državah izvajajo obveščevalne agencije, vzbudila resne pomisleke glede tveganj, ki jih dejavnosti nadzora pomenijo za zasebnost, demokratično upravljanje in svobodo izražanja. Množični nadzor in tehnologije, ki omogočajo globalizirano shranjevanje in obdelavo osebnih podatkov ter masovni dostop do podatkov, lahko posegajo v samo bistvo pravice do zasebnosti.[977] Poleg tega lahko negativno vplivajo na politično kulturo, na demokracijo, ustvarjalnost in inovativnost pa odvračilno.[978] Že strah, da država stalno spremlja in analizira ravnanje in dejanja državljanov, lahko te odvrne od izražanja mnenj o nekaterih zadevah ter ima za posledico nezaupljivost in previdnost.[979] Ti izzivi so več javnih organov, raziskovalnih središč in organizacij civilne družbe spodbudili, da so analizirali morebitne učinke novih tehnologij na družbo. Evropski nadzornik za varstvo podatkov je leta 2015 začel izvajati več pobud za oceno učinka, ki ga imajo masovni podatki in internet stvari na etiko. Zlasti je ustanovil svetovalno skupino za etiko, katere cilj je spodbujanje „odprte in poučne razprave o digitalni etičnosti, kar bo EU omogočilo izkoristiti tehnološke prednosti za družbo in gospodarstvo, ob sočasni krepitvi pravic in svoboščin posameznikov, zlasti njihovih pravic do zasebnosti in varstva osebnih podatkov".[980]

Obdelava osebnih podatkov je močno orodje tudi v rokah korporacij. Danes se z njo lahko razkrijejo podrobne informacije o zdravstvenem ali finančnem stanju posameznika, ki jih nato korporacije uporabijo za sprejemanje pomembnih odločitev za posameznike, kot sta višina njihove premije za zdravstveno zavarovanje in njihova kreditna sposobnost. Tehnike obdelave osebnih podatkov lahko vplivajo tudi na demokratične procese, kadar jih uporabijo politiki ali korporacije, da vplivajo na volitve, na primer z mikrociljanjem komunikacij volivcev. Z drugimi besedami, zasebnost se je sprva dojemala kot pravica posameznikov, ki jo je treba zaščititi pred neupravičenim vmešavanjem javnih organov, v današnjem času pa jo lahko ogrožajo tudi zasebni akterji. To poraja vprašanja o uporabi tehnologije in napovedne analitike pri

977 Glej ZN, Generalna skupščina, *Poročilo posebnega poročevalca za spodbujanje in varstvo človekovih pravic in temeljnih svoboščin v boju proti terorizmu*, Ben Emmerson, A/69/397, 23. september 2014, odstavek 59. Glej tudi ESČP, informativni pregled *Množični nadzor*, julij 2017.

978 ENVP (2015), Mnenje št. 7/2015 o soočanju z izzivi masovnih podatkov, Bruselj, 19. november 2015.

979 Glej zlasti SEU, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim* in Kärntner Landesregierung in drugi (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014, točka 37.

980 ENVP, Sklep z dne 3. decembra 2015 o ustanovitvi zunanje svetovalne skupine za etične razsežnosti varstva podatkov (svetovalna skupina za etiko), uvodna izjava 5.

odločitvah, ki vplivajo na vsakdanje življenje posameznikov, in krepi potrebo po zagotavljanju, da se pri obdelavi osebnih podatkov spoštujejo zahteve glede temeljnih pravic.

Varstvo osebnih podatkov je neločljivo povezano s tehnološkimi, družbenimi in političnimi spremembami, zato bi bilo nemogoče pripraviti izčrpen seznam prihodnjih izzivov. V tem poglavju so obravnavana izbrana področja v zvezi z masovnimi podatki, spletnimi družbenimi omrežji in enotnim digitalnim trgom EU. Ne gre za izčrpno oceno teh področij z vidika varstva osebnih podatkov, temveč so poudarjeni številni možni medsebojni vplivi med novimi ali spremenjenimi človekovimi dejavnostmi in varstvom osebnih podatkov.

10.1 Masovni podatki, algoritmi in umetna inteligenca

Ključni poudarki

- S prelomnimi inovacijami na področju IKT se oblikuje nov način življenja, v katerem so družbeni odnosi ter poslovne, zasebne in javne storitve digitalno medsebojno povezani, s čimer se ustvarja vse večja količina podatkov, številni od katerih so osebni podatki.
- Vlade, podjetja in državljani vse bolj delujejo v podatkovno vodenemu gospodarstvu, v katerem so podatki postali dragoceno sredstvo.
- Pojem masovnih podatkov se nanaša na podatke in analitiko podatkov.
- Za osebne podatke, ki se obdelujejo na podlagi analitike masovnih podatkov, se uporabljata zakonodaji EU in Sveta Evrope.
- Odstopanja od pravil o varstvu osebnih podatkov in pravic so omejena na izbrane pravice in posebne primere, v katerih bi bilo uveljavljanje neke pravice nemogoče ali bi zahtevalo nesorazmeren napor upravljavcev osebnih podatkov.
- Povsem avtomatizirano sprejemanje odločitev je načeloma prepovedano, razen v posebnih primerih.
- Ozaveščenost posameznikov in možnost, da izvajajo nadzor, sta ključna za zagotavljanje uveljavljanja pravic.

V vse bolj digitaliziranem svetu vsaka dejavnost pusti digitalno sled, ki jo je mogoče zbrati, obdelati in ovrednotiti ali analizirati. Z novimi informacijskimi in

komunikacijskimi tehnologijami se zbira in evidentira vse več podatkov.[981] Do nedavnega ni nobena tehnologija omogočala analize ali vrednotenja mase podatkov oziroma oblikovanja uporabnih zaključkov. Podatki, ki jih je bilo preprosto preveč, da bi jih bilo mogoče ovrednotiti, so bili prezapleteni in slabo strukturirani ter so se prehitro spreminjali, zato ni bilo mogoče opredeliti trendov in navad.

10.1.1 Opredelitev masovnih podatkov, algoritmov in umetne inteligence

Masovni podatki

Masovni podatki so moden izraz, ki se lahko nanaša na več pojmov, odvisno od konteksta. Običajno zajema vse večjo tehnološko sposobnost za zbiranje, obdelavo in izluščenje novega in napovedovalnega znanja iz velike količine, hitrosti in raznolikosti podatkov.[982] Pojem masovnih podatkov se torej nanaša na same podatke in na podatkovno analitiko.

Viri podatkov so različnih vrst, vključujejo pa ljudi in njihove osebne podatke, stroje ali senzorje, podnebne informacije, satelitske posnetke, digitalne slike in videoposnetke ali signale GPS. Veliko podatkov in informacij pa je osebnih podatkov, ki so lahko ime, fotografija, elektronski naslov, bančni podatki, podatki GPS za sledenje, objave na spletnih družbenih omrežjih, zdravstveni podatki ali IPnaslov računalnika.[983]

Izraz masovni podatki se nanaša tudi na **obdelavo**, analizo in vrednotenje velikih količin podatkov in razpoložljivih informacij, da bi se pridobile koristne informacije za namene analize masovnih podatkov. To pomeni, da se zbrani podatki in informacije lahko uporabijo za namene, ki niso prvotno predvideni nameni, na primer za analizo

981 Evropska komisija, Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Uspešnemu podatkovno vodenemu gospodarstvu naproti, COM(2014) 442 final, Bruselj, 2. julij 2014.

982 Svet Evrope, Posvetovalni odbor po Konvenciji št. 108, Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov, 23. januar 2017, str. 2; Evropska komisija, Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Uspešnemu podatkovno vodenemu gospodarstvu naproti, COM(2014) 442 final, Bruselj, 2. julij 2014, str. 4; Mednarodna telekomunikacijska zveza (2015), Priporočilo Y.3600. Big Data – Cloud computing based requirements and capabilities (Masovni podatki – Zahteve in zmogljivosti v zvezi z računalništvom v oblaku).

983 Evropska komisija, Reforma varstva podatkov v EU in masovni podatki, informativni pregled; Svet Evrope, Posvetovalni odbor po Konvenciji št. 108, Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov, 23. januar 2017, str. 2.

statističnih trendov ali za bolj prilagojene storitve, na primer v oglaševanju. Če so na voljo tehnologije za zbiranje, obdelavo in vrednotenje masovnih podatkov, je dejansko mogoče združiti in ponovno ovrednotiti najrazličnejše vrste informacij v zvezi s finančnimi transakcijami, kreditno sposobnostjo, zdravljenjem, zasebno potrošnjo, poklicno dejavnostjo, sledenjem in opravljenimi potmi, uporabo interneta, elektronskimi karticami in pametnimi telefoni ter videonadzorom in nadzorom komunikacije. Iz analize masovnih podatkov izhaja nova kvantitativna razsežnost podatkov, ki jo je mogoče ovrednotiti in uporabiti v realnem času, na primer za zagotavljanje prilagojenih storitev potrošnikom.

Algoritmi in umetna inteligenca

Z izrazom umetna inteligenca označujemo inteligenco strojev, ki delujejo kot „inteligentni agenti". Nekatere naprave lahko kot inteligentni agenti ob podpori programske opreme zaznavajo svoje okolje in ravnajo v skladu z algoritmi. Izraz umetna inteligenca se uporablja, kadar stroj posnema kognitivne funkcije – kot sta učenje in reševanje težav –, ki se običajno povezujejo z ljudmi.[984] Da bi posnemale sprejemanje odločitev, sodobne tehnologije in programska oprema uporabljajo algoritme, na podlagi katerih naprave sprejemajo „avtomatizirane odločitve". Algoritem je mogoče najbolje opisati kot postopek po korakih za izračun, obdelavo podatkov, ovrednotenje ter avtomatizirano sklepanje in sprejemanje odločitev.

Podobno kot pri analitiki masovnih podatkov sta za umetno inteligenco in iz nje izhajajoče avtomatizirano sprejemanje odločitev potrebna zbiranje in obdelava velikih količin podatkov. Ti podatki lahko izvirajo iz same naprave (toplota zavor, gorivo itd.) ali iz okolice. Oblikovanje profilov je na primer postopek, ki se lahko opira na avtomatizirano sprejemanje odločitev v skladu z vnaprej določenimi vzorci ali dejavniki.

Primer: oblikovanje profilov in ciljno oglaševanje

Oblikovanje profilov na podlagi masovnih podatkov vključuje iskanje vzorcev, ki izražajo značilnosti neke vrste osebnosti, na primer kadar podjetja za spletno nakupovanje predlagajo izdelke, ki bi vam lahko prav tako bili všeč, na podlagi informacij, pridobljenih z izdelki, ki ste jih pred tem kot stranka dali

984 Stuart Russel in Peter Norvig, *Artificial Intelligence: A Modern Approach (2. izdaja)*, Prentice Hall, Upper Saddle River, New Jersey, 2003, str. 27, 32–58, 968–972; Stuart Russel in Peter Norvig, *Artificial Intelligence: A Modern Approach (3. izdaja)*, Prentice Hall, Upper Saddle River, New Jersey, 2009, str. 2.

v košarico. Več ko je osebnih podatkov, jasnejši je mozaik. Pametni telefon je na primer učinkovit vprašalnik, ki ga posamezniki izpolnijo z vsako uporabo, zavestno in nezavestno.

V sodobni psihografiji – vedi, ki se ukvarja s proučevanjem osebnosti – se uporablja metoda OCEAN (angl. **o**penness (odprtost), **c**onscientiousness (vestnost), **e**xtraversion (ekstravertnost), **a**greeableness (prijetnost), **n**euroticism (nevroticizem)), s katero se opredeli vrsta zadevnega značaja. „Velikih pet" razsežnosti značaja se nanaša na odprtost (kako odprta je oseba za novosti), vestnost (v kolikšni meri je oseba nagnjena k perfekcionizmu), ekstravertnost (kako družabna je oseba), prijetnost (kako prijetna je oseba) in nevroticizem (kako ranljiva je oseba). Na podlagi teh informacij se profilirajo zadevna oseba, njene potrebe in bojazni, njeno obnašanje itd. Te informacije so nato dopolnjene z drugimi informacijami o osebi, pridobljenimi iz vseh razpoložljivih virov, od posrednikov podatkov in družbenih omrežij (vključno z „všečki" na objavah in objavljenih fotografijah) do glasbe, ki jo oseba posluša na spletu, ali podatkov GPS in podatkov za sledenje.

Velika količina profilov, ustvarjenih s tehnikami analize masovnih podatkov, se nato primerja, da se opredelijo podobni vzorci in razložijo vzorčne skupine osebnosti. Informacije o vedenju in naravnanosti posameznih tipov osebnosti so zato obrnjene. Z dostopom do masovnih podatkov in njihovo uporabo se osebnostni test obrne, saj se za opis osebnosti posameznika zdaj uporabljajo informacije o vedenju in naravnanosti. Z združitvijo informacij o „všečkih" na družbenih omrežjih, podatkih za sledenje, poslušani glasbi ali gledanih filmih se lahko izoblikuje jasna slika o osebnosti posameznika, ki podjetjem omogoča prikazovanje prilagojenih oglasov in/ali sporočanje informacij v skladu z „osebnostjo" te osebe. Predvsem pa je te informacije mogoče obdelovati v realnem času.[985]

985 S tehnikami za obdelavo in novo programsko opremo se v realnem času ovrednotijo informacije o tem, kaj je osebi všeč, kaj gleda med spletnim nakupovanjem ali kaj doda v spletno nakupovalno košarico, poleg tega se lahko z njimi na podlagi zbranih informacij predlagajo „izdelki", ki bi lahko bili zanimivi za zadevno osebo.

10.1.2 Uravnoteženje koristi in tveganj masovnih podatkov

S sodobnimi tehnikami obdelave je mogoče obdelovati velike količine podatkov, hitro uvažati nove podatke, zagotavljati obdelavo informacij v realnem času v smislu kratkega odzivnega časa (tudi v primeru zapletenih zahtev), omogočati večkratne in hkratne zahteve ter analizirati različne vrste informacij (fotografije, besedila ali številke). Te tehnološke inovacije omogočajo strukturiranje, obdelavo in vrednotenje velikih količin podatkov in informacij v realnem času.[986] Z eksponentnim povečanjem količine razpoložljivih in analiziranih podatkov je zdaj mogoče doseči rezultate, ki jih ne bi bilo mogoče doseči z analizo manjšega obsega. Masovni podatki so prispevali k razvoju novega področja poslovanja, na katerem se bodo lahko pojavile nove storitve za podjetja in potrošnike. Vrednost osebnih podatkov državljanov EU se lahko do leta 2020 povzpne na skoraj bilijon evrov letno.[987] Masovni podatki lahko zato ponudijo nove **priložnosti**, ki izhajajo iz vrednotenja masovnih podatkov za nova družbena, gospodarska ali znanstvena spoznanja, ki koristijo posameznikom, podjetjem in vladam.[988]

Z analitiko masovnih podatkov se lahko razkrijejo vzorci med različnimi viri in nabori podatkov, kar omogoča koristna spoznanja na področjih, kot sta znanost in medicina. Tako je na primer na področjih, kot so zdravstvo, prehranska varnost, inteligentni prometni sistemi, energijska učinkovitost ali urbanistično načrtovanje. Ta analiza informacij v realnem času se lahko uporabi za izboljšanje sistemov, ki se izvajajo. Na področju raziskav je mogoče pridobiti nova spoznanja z združevanjem velikih količin podatkov in statističnega ovrednotenja, zlasti v panogah, v katerih se je velika količina podatkov do zdaj vrednotila samo ročno. Razvijejo se lahko nove oblike

986 Razvoj programske opreme za obdelavo masovnih podatkov je še vedno v zgodnji fazi. Kljub temu so bili v zadnjem času razviti analitični programi, zlasti za analizo masovnih podatkov in informacij v realnem času, ki se nanašajo na dejavnosti posameznikov. Možnost strukturirane analize in obdelave masovnih podatkov pomeni nova sredstva za oblikovanje profilov in ciljno oglaševanje. Evropska komisija, Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij,Uspešnemu podatkovno vodenemu gospodarstvu naproti, COM(2014) 442 final, Bruselj, 2. julij 2014; Evropska komisija, Reforma varstva podatkov v EU in masovni podatki, informativni pregled, in Svet Evrope, Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov, 23. januar 2017, str. 2.

987 Evropska komisija, Reforma varstva podatkov v EU in masovni podatki, informativni pregled.

988 Mednarodna konferenca pooblaščencev za varstvo podatkov in zasebnost (2014), Resolution on Big Data (Resolucija o masovnih podatkih); Evropska komisija, Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Uspešnemu podatkovno vodenemu gospodarstvu naproti, COM(2014) 442 final, Bruselj, 2. julij 2014, str. 2; Evropska komisija, Reforma varstva podatkov v EU in masovni podatki, informativni pregled, in Svet Evrope, Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov, 23. januar 2017, str. 1.

zdravljenja, ki so prilagojene posameznim pacientom in temeljijo na primerjavah z veliko količino informacij, ki so na voljo. Podjetja upajo, da bodo lahko z analizo masovnih podatkov pridobila konkurenčno prednost, ustvarila morebitne prihranke in z neposrednimi individualiziranimi storitvami za stranke oblikovala nova poslovna področja. Vladne agencije upajo, da bodo lahko dosegle izboljšave na področju kazenskega pravosodja. Komisija v svoji strategiji za enotni digitalni trg za Evropo priznava potencial podatkovno vodenih tehnologij, storitev in masovnih podatkov kot gonilne sile za gospodarsko rast, inovacije in digitalizacijo v EU.[989]

Vendar masovni podatki prinašajo tudi **tveganja**, ki so na splošno povezana z njihovimi tremi značilnostmi, in sicer obsegom, hitrostjo in raznolikostjo obdelanih podatkov. Obseg se nanaša na količino obdelanih podatkov, raznolikost na število in raznovrstnost podatkov, hitrost pa se nanaša na naglost obdelave podatkov. Posebni pomisleki glede varstva osebnih podatkov se pojavijo, zlasti kadar se analitika masovnih podatkov uporablja za velike nabore podatkov, da bi se pridobilo novo in napovedno znanje za sprejemanje odločitev v zvezi s posamezniki in/ali skupinami.[990] Tveganja za varstvo osebnih podatkov in zasebnost, povezana z masovnimi podatki, so bila poudarjena v mnenjih ENVP in Delovne skupine iz člena 29, resolucijah Evropskega parlamenta in Sveta ter dokumentih Sveta Evrope.[991]

Tveganja vključujejo neustrezno ravnanje z masovnimi podatki s strani tistih, ki imajo dostop do velike količine informacij, z manipulacijo, diskriminacijo ali zatiranjem posameznikov ali posebnih skupin v družbi.[992] Kadar se zbirajo, obdelujejo ali vrednotijo velike količine osebnih podatkov ali informacij o vedenju posameznika, lahko njihovo izkoriščanje privede do hudih kršitev temeljnih pravic in svoboščin, ne samo pravice do zasebnosti. Obsega, v katerem se lahko poseže v zasebnost in osebne podatke, ni mogoče natančno izmeriti. Evropski parlament je ugotovil, da še ne obstaja metodologija za oceno vseh vplivov masovnih podatkov, podprto z dokazi, vendar da so

989 Resolucija Evropskega parlamenta z dne 14. marca 2017 o posledicah velepodatkov za temeljne pravice: zasebnost, varstvo podatkov, nediskriminacija, varnost in kazenski pregon (2016/2225(INI)).

990 Svet Evrope, Posvetovalni odbor po Konvenciji št. 108, Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov, 23. januar 2017, str. 2.

991 Glej na primer ENVP (2015), Mnenje št. 7/2015 o soočanju z izzivi masovnih podatkov, 19. november 2015; ENVP (2016), Mnenje št. 8/2016 o učinkovitem izvrševanju temeljnih pravic v dobi masovnih podatkov, 23. september 2016; Evropski parlament (2016), Resolucija o posledicah velepodatkov za temeljne pravice: zasebnost, varstvo podatkov, nediskriminacija, varnost in kazenski pregon, P8_TA(2017)0076, Strasbourg, 14. marec 2017; Svet Evrope, Posvetovalni odbor po Konvenciji št. 108, Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov, T-PD(2017)01, Strasbourg, 23. januar 2017.

992 Mednarodna konferenca pooblaščencev za varstvo podatkov in zasebnost (2014), Resolution on Big Data (Resolucija o masovnih podatkih).

na voljo dokazi, da ima lahko analitika masovnih podatkov velik horizontalen učinek v javnem in zasebnem sektorju.[993]

SUVP vključuje določbe o pravici posameznika, na katerega se nanašajo osebni podatki, da se zanj ne uporablja avtomatizirano sprejemanje odločitev, vključno z oblikovanjem profilov.[994] Vprašanje zasebnosti se pojavi, kadar je za uveljavljanje pravice do ugovora potrebno osebno posredovanje, da se posameznikom, na katere se nanašajo osebni podatki, omogoči izražanje njihovih stališč in izpodbijanje odločitve.[995] To lahko povzroči izzive pri zagotavljanju ustrezne ravni varstva osebnih podatkov, če na primer ni mogoče človeško posredovanje ali če so algoritmi preveč zapleteni in je količina zadevnih podatkov prevelika, da bi se posameznikom lahko zagotovile utemeljitve za posamezne odločitve in/ali predhodne informacije za pridobitev njihove privolitve. Primer uporabe umetne inteligence in avtomatiziranega sprejemanja odločitev je mogoče najti v nedavnem razvoju v zvezi z vlogami za hipotekarni kredit ali postopki zaposlovanja. Vloge za kredite in prijave za delovno mesto se zavrnejo, ker prosilci za kredit ali kandidati za delovno mesto ne izpolnjujejo vnaprej določenih parametrov ali dejavnikov.

10.1.3 Vprašanja, povezana z varstvom osebnih podatkov

Kar zadeva varstvo osebnih podatkov, se glavna vprašanja na eni strani nanašajo na obseg in raznolikost obdelanih osebnih podatkov, na drugi strani pa na obdelavo in njene posledice. Uvedba zapletenih algoritmov in programske opreme za preoblikovanje množičnih podatkov v vir za sprejemanje odločitev vpliva predvsem na posameznike in skupine, zlasti v primeru oblikovanja profilov ali označevanja, in navsezadnje odpira številna vprašanja v zvezi z varstvom osebnih podatkov.[996]

Opredelitev upravljavcev in obdelovalcev ter njihova odgovornost

V zvezi z masovnimi podatki in umetno inteligenco se poraja več vprašanj glede opredelitve upravljavcev in obdelovalcev ter njihove odgovornosti: kdo je lastnik

993 Resolucija Evropskega parlamenta z dne 14. marca 2017 o posledicah velepodatkov za temeljne pravice: zasebnost, varstvo podatkov, nediskriminacija, varnost in kazenski pregon (2016/2225(INI)).

994 SUVP, člen 22.

995 Prav tam, člen 22(3).

996 Svet Evrope, Posvetovalni odbor po Konvenciji št. 108, Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov, 23. januar 2017, str. 2.

osebnih podatkov, kadar se zbira in obdeluje tako velika količina osebnih podatkov? Kdo je upravljavec, kadar se osebni podatki obdelujejo z inteligentnimi stroji in programsko opremo? Katere so natančne odgovornosti vsakega akterja pri obdelavi? In za katere namene se lahko uporabljajo masovni podatki?

Vprašanje odgovornosti v okviru umetne inteligence bo postalo še toliko bolj zapleteno, ko bo umetna inteligenca sprejela odločitev na podlagi obdelave osebnih podatkov, ki jo je sama razvila. SUVP določa pravni okvir za odgovornost upravljavca in obdelovalca osebnih podatkov. Nezakonita obdelava osebnih podatkov povzroči odgovornost upravljavca in obdelovalca osebnih podatkov.[997] Z umetno inteligenco in avtomatiziranim sprejemanjem odločitev se porajajo vprašanja o tem, kdo je odgovoren za kršitve, ki vplivajo na zasebnost posameznikov, na katere se nanašajo osebni podatki, kadar zaradi zapletenosti in količine obdelanih osebnih podatkov odgovornosti ni mogoče z gotovostjo pripisati nikomur. Če se umetna inteligenca in algoritmi štejejo za izdelke, se s tem odpirajo vprašanja glede osebne odgovornosti, ki je urejena s SUVP, in odgovornosti za izdelek, ki ni.[998] Za to bi bila potrebna pravila o odgovornosti, da bi se zapolnila vrzel med osebno odgovornostjo in odgovornostjo za izdelek za robotiko in umetno inteligenco, med drugim za avtomatizirano sprejemanje odločitev.[999]

Vpliv na načela varstva osebnih podatkov

Zgoraj opisane narava, analiza in uporaba masovnih podatkov otežujejo uporabo nekaterih tradicionalnih temeljnih načel evropskega prava o varstvu osebnih podatkov.[1000] Taki izzivi se nanašajo predvsem na načela zakonitosti, najmanjšega obsega podatkov, omejitve namena in preglednosti.

V skladu z načelom najmanjšega obsega podatkov morajo biti osebni podatki primerni, ustrezni in omejeni na tisto, kar je potrebno za namene, za katere se obdelujejo. Vendar je lahko poslovni model masovnih podatkov popolno nasprotje najmanjšega obsega podatkov, saj je pri njem potrebnih vedno več osebnih podatkov, pogosto za nedoločene namene.

997 SUVP, členi 77–79 in 82.

998 Evropski parlament, European Civil Law Rules in Robotics (Pravila evropskega civilnega prava o robotiki), Generalni direktorat za notranjo politiko Unije, 2016, str. 14.

999 Govor Roberta Viole na seminarju za medije o evropskem pravu o robotiki, ki je potekal v Evropskem parlamentu 16. februarja 2017; Sporočilo Evropskega parlamenta o zahtevi, naj Komisija pripravi predlog o pravilih civilne odgovornosti na področju robotike in umetne inteligence.

1000 Svet Evrope, *Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov*, T-PD(2017)01, Strasbourg, 2017.

Enako velja za načelo omejitve namena, v skladu s katerim je treba osebne podatke obdelovati za določene namene in jih ni mogoče uporabljati za namene, ki niso združljivi s prvotnim namenom zbiranja, razen če taka obdelava temelji na pravni podlagi, kot je med drugim privolitev posameznika, na katerega se nanašajo osebni podatki (glej razdelek 4.1.1).

Nenazadnje masovni podatki postavljajo pod vprašaj tudi načelo točnosti podatkov, saj aplikacije za masovne podatke običajno zbirajo osebne podatke iz najrazličnejših virov, ne da bi se lahko preverila in/ali ohranjala točnost zbranih podatkov.[1001]

Posebna pravila in pravice

Splošno pravilo je, da osebni podatki, ki se obdelujejo v okviru analitike masovnih podatkov, spadajo na področje uporabe zakonodaje o varstvu osebnih podatkov. Vseeno so bila v pravo EU in Sveta Evrope uvedena posebna pravila ali odstopanja za posebne primere, povezane z algoritemsko kompleksno obdelavo osebnih podatkov.

V okviru prava Sveta Evrope so s posodobljeno Konvencijo št. 108 posamezniku, na katerega se nanašajo osebni podatki, podeljene nove pravice, da se omogoči učinkovitejši nadzor nad njegovimi osebnimi podatki v dobi masovnih podatkov. Prav to velja za na primer člen 9(1)(a), (c) in (d) posodobljene Konvencije št. 108 o pravici, da za zadevnega posameznika ne veljajo odločitve, ki bi lahko nanj znatno vplivale in temeljijo zgolj na avtomatizirani obdelavi osebnih podatkov, ne da bi se upoštevala njegova stališča, o pravici tega posameznika, da se na zahtevo seznani z razlogi, na katerih temelji obdelava osebnih podatkov, če se rezultati take obdelave uporabljajo zanj, in o njegovi pravici do ugovora. Druge določbe posodobljene Konvencije št. 108, zlasti tiste o preglednosti in dodatnih obveznostih, so dopolnilni elementi zaščitnega mehanizma, vzpostavljenega z zadevno posodobljeno Konvencijo za obvladovanje digitalnih izzivov.

V skladu s pravom EU je treba **preglednost** poleg v primerih iz člena 23 SUVP zagotoviti tudi pri vsaki obdelavi osebnih podatkov. Zlasti pomembna je v zvezi z internetnimi storitvami in drugo zapleteno avtomatizirano obdelavo osebnih podatkov, kot je uporaba algoritmov za sprejemanje odločitev. V zvezi z njimi morajo sistemi za obdelavo osebnih podatkov omogočati, da posamezniki, na katere se nanašajo osebni podatki, dejansko razumejo, kaj se dogaja z njihovimi osebnimi podatki. Da

1001 ENVP (2016), Mnenje št. 8/2016 o učinkovitem izvrševanju temeljnih pravic v dobi masovnih podatkov, 23. september 2016, str. 8.

bi zagotovili pošteno in pregledno obdelavo, mora upravljavec v skladu s SUVP posamezniku, na katerega se nanašajo osebni podatki, zagotoviti smiselne informacije o razlogih za avtomatizirano sprejemanje odločitev, vključno z oblikovanjem profilov.[1002] Odbor ministrov Sveta Evrope je v svojem Priporočilu o varstvu in spodbujanju pravice do svobode izražanja in pravice do zasebnega življenja v zvezi z omrežno nevtralnostjo priporočil, naj ponudniki internetnih storitev uporabnikom zagotovijo jasne, popolne in javno dostopne informacije v zvezi z vsemi praksami upravljanja spletnega prometa, ki bi lahko vplivale na njihov dostop do vsebin, aplikacij ali storitev in na njihovo razširjanje.[1003] Poročila o praksah upravljanja spletnega prometa, ki jih pripravijo pristojni organi v vseh državah članicah, bi morala biti oblikovana odprto in pregledno ter biti na voljo javnosti brezplačno.[1004]

Upravljavci osebnih podatkov morajo posameznikom, na katere se nanašajo osebni podatki, ne glede na to, ali so bili osebni podatki pridobljeni od njih ali ne, **sporočiti** specifične informacije o zbranih osebnih podatkih in predvideni obdelavi (glej razdelek 6.1.1) ter jih poleg tega po potrebi obvestiti o obstoju postopkov avtomatiziranega sprejemanja odločitev, pri čemer jim zagotovijo „smiselne informacije o razlogih zanj[e]“[1005] ter informacije o ciljih in morebitnih posledicah takih postopkov. V SUVP je poleg tega pojasnjeno, da (le v primerih, ko osebni podatki niso bili pridobljeni od posameznika, na katerega se nanašajo) upravljavcu takih informacij ni treba zagotoviti posamezniku, na katerega se nanašajo osebni podatki, če „se izkaže, da je zagotavljanje takih informacij nemogoče ali bi vključevalo nesorazmeren napor“.[1006] Vendar, kot je poudarila Delovna skupina iz člena 29 v svojih *Smernicah o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679*, zaradi zapletenosti obdelave kot take upravljavcu osebnih podatkov ne bi smelo biti onemogočeno, da posameznikom, na katere se nanašajo osebni podatki, zagotovijo jasna pojasnila glede ciljev obdelave osebnih podatkov in uporabljene analitike.[1007]

Pravice posameznikov, na katere se nanašajo osebni podatki, do **dostopa** do svojih osebnih podatkov ter njihovega **popravka** in **izbrisa**, pa tudi njihova pravica do

1002 SUVP, člen 13(2)(f).

1003 Svet Evrope, Odbor ministrov (2016), Priporočilo Rec(2016)1 državam članicam o varstvu in spodbujanju pravice do svobode izražanja in pravice do zasebnega življenja v zvezi z omrežno nevtralnostjo, 13. januar 2016, točka 5.1.

1004 Prav tam, točka 5.2.

1005 SUVP, člen 13(2)(f) in člen 14(2)(g).

1006 Prav tam, člen 14(5)(b).

1007 Delovna skupina za varstvo podatkov iz člena 29, *Smernice o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679*, WP251, 3. oktober 2017, str. 14.

omejitve obdelave, ne vključujejo podobne izjeme. Vendar se lahko obveznost upravljavca osebnih podatkov, da posameznika, na katerega se nanašajo osebni podatki, obvesti o popravku ali izbrisu njegovih osebnih podatkov (razdelek 6.1.4), odpravi tudi, če bi se taka obvestitev „izka[zala] za nemogoč[o] ali vključ[evala] nesorazmeren napor".[1008]

Posamezniki, na katere se nanašajo osebni podatki, imajo poleg tega v skladu s členom 21 SUVP (glej razdelek 6.1.6) pravico, da **ugovarjajo** obdelavi svojih osebnih podatkov, med drugim v primeru analitike masovnih podatkov. Upravljavci osebnih podatkov so lahko iz te obveznosti izvzeti, če lahko dokažejo obstoj prevladujočih zakonitih interesov, do takega izvzetja pa niso upravičeni pri obdelavi za namene neposrednega trženja.

Upravljavci osebnih podatkov lahko uveljavljajo posebna odstopanja od teh pravic tudi, kadar se osebni podatki obdelujejo za namene arhiviranja v javnem interesu, v znanstveno- ali zgodovinskoraziskovalne namene oziroma v statistične namene.[1009]

V SUVP so uvedena posebna pravila v zvezi z **oblikovanjem profilov in avtomatiziranim sprejemanjem odločitev**. Člen 22(1) določa, da ima posameznik, na katerega se nanašajo osebni podatki, „pravico, da zanj ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva". Kot je poudarjeno v smernicah Delovne skupina iz člena 29, ta člen določa splošno prepoved popolnoma avtomatiziranega sprejemanja odločitev.[1010] Upravljavci osebnih podatkov so lahko iz take prepovedi izvzeti le v treh posebnih primerih, in sicer če je odločitev: 1) nujna za sklenitev ali izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov, 2) dovoljena v pravu EU ali nacionalnem pravu ali 3) utemeljena z izrecno privolitvijo posameznika, na katerega se nanašajo osebni podatki.[1011]

Posameznikov nadzor

Zaradi zapletenosti analitike masovnih podatkov in njene nepreglednosti bo morda treba ponovno razmisliti o nadzoru posameznika nad osebnimi podatki. Ta nadzor bi

1008 SUVP, člen 19.

1009 Prav tam, člen 89(2) in (3).

1010 Delovna skupina za varstvo podatkov iz člena 29, *Smernice o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679*, WP251, 3. oktober 2017, str. 9.

1011 SUVP, člen 22(2).

bilo treba prilagoditi družbenemu in tehnološkemu okviru, pri čemer je treba upoštevati pomanjkanje znanja pri posameznikih. Zato bi bilo treba pri varstvu osebnih podatkov v zvezi z masovnimi podatki sprejeti širši pojem nadzora nad uporabo podatkov, v skladu s katerim se posameznikov nadzor razvije v bolj zapleten proces večkratnih ocen učinka tveganj, povezanih z uporabo podatkov.[1012]

Kako učinkovita je aplikacija za masovne podatke, je odvisno od tega, kako dobro lahko napove želje ali vedenje posameznikov, ki sodelujejo v preizkusu (ali potrošnikov). Sedanji modeli napovedovanja, ki temeljijo na analitiki masovnih podatkov, se vseskozi izpopolnjujejo. Nedavni napredek vključuje ne le uporabo podatkov za kategorizacijo osebnosti (tj. vedenja in stališč), temveč tudi analizo vedenja z analiziranjem vzorcev glasu in intenzivnosti, s katero se natipkajo sporočila, ali telesne temperature. Vse te informacije se lahko uporabijo v realnem času glede na spoznanja, pridobljena z vrednotenjem masovnih podatkov, da se na primer oceni kreditna sposobnost na sestanku s predstavnikom banke. Ocena se ne opravi na podlagi sposobnosti posameznika, ki zaprosi za kredit, temveč na podlagi vedenjskih značilnosti, pridobljenih z analizo in ovrednotenjem informacij iz masovnih podatkov, tj. na podlagi tega, ali prosilec govori odločno ali laskavo, njegove govorice telesa ali telesne temperature.

Oblikovanje profilov in ciljno oglaševanje morda nista nujno problematična, če se posamezniki **zavedajo**, da se zanje uporabljajo prilagojeni oglasi. Oblikovanje profilov postane težava, če se uporablja za manipulacijo posameznikov, tj. za iskanje določenih osebnosti ali skupin ljudi za politične kampanje. Skupine neodločenih volivcev lahko na primer oglaševalci nagovarjajo s političnimi sporočili, prilagojenimi njihovi osebnosti in stališčem. Druga težava bi lahko bila uporaba takega oblikovanja profilov za zavrnitev dostopa do blaga in storitev nekaterim posameznikom. Eden od zaščitnih ukrepov, ki lahko zagotovijo zaščito pred zlorabo masovnih in osebnih podatkov, je psevdonimizacija (glej razdelek 2.1.1).[1013] Če so osebni podatki resnično anonimizirani, tj. ni informacij, ki bi puščale sledi do posameznika, na katerega se nanašajo osebni podatki, ti primeri ne spadajo na področje uporabe SUVP. Izziv za pravo o varstvu osebnih podatkov je tudi privolitev posameznikov, na katere se nanašajo osebni podatki, v okviru obdelave masovnih podatkov. To zajema privolitev, da se uporabljajo prilagojeni oglasi in oblikovanje profilov, ki so lahko upravičeni iz razlogov v zvezi z uporabniško izkušnjo, in privolitev v uporabo velikih količin osebnih

1012 Svet Evrope, Posvetovalni odbor po Konvenciji št. 108, *Smernice o varstvu posameznikov pri obdelavi osebnih podatkov v svetu masovnih podatkov*, T-PD(2017)01, Strasbourg, 23. januar 2017.

1013 Prav tam, str. 2.

podatkov za izpopolnitev in razvoj analitičnih orodij, ki temeljijo na informacijah. V zvezi s seznanjenostjo ali neseznanjenostjo z obdelavo masovnih podatkov se poraja več vprašanj glede načinov, kako lahko posamezniki, na katere se nanašajo osebni podatki, uveljavljajo svoje pravice, saj se je pri obdelavi masovnih podatkov mogoče hkrati opirati na psevdonimizirane in anonimizirane informacije, za katere se uporabljajo algoritmi. Psevodnimizirani podatki sicer spadajo na področje uporabe SUVP, vendar pa se navedena uredba ne uporablja za anonimizirane podatke. Nadzor posameznikov nad obdelavo svojih osebnih podatkov in njihova seznanjenost z njo sta bistvenega pomena v analitiki masovnih podatkov – posamezniki brez njiju nimajo jasne predstave o tem, kdo je upravljavec ali obdelovalec osebnih podatkov, kar jim preprečuje učinkovito uveljavljanje svojih pravic.

10.2 Splet 2.0 in 3.0: družbena omrežja in internet stvari

Ključni poudarki

- Storitve družbenih omrežij so spletne komunikacijske platforme, ki posameznikom omogočajo, da se pridružijo mrežam enako mislečih uporabnikov ali jih oblikujejo.
- Internet stvari je povezovanje predmetov z internetom in njihovo medsebojno povezovanje.
- Privolitev posameznikov, na katere se nanašajo osebni podatki, je najpogostejša pravna podlaga za zakonito obdelavo osebnih podatkov, ki jo upravljavci osebnih podatkov izvajajo na družbenih omrežjih.
- Uporabniki družbenih omrežij so na splošno zaščiteni z izjemo obdelave za domače potrebe, vendar se lahko to odstopanje v posebnih okoliščinah odpravi.
- Ponudniki družbenih omrežij niso zaščiteni z izjemo obdelave za domače potrebe.
- Vgrajena in privzeta zasebnost sta ključni za zagotavljanje varnosti osebnih podatkov na tem področju.

10.2.1 Opredelitev spleta 2.0 in 3.0

Storitve družbenih omrežij

Internet je bil sprva zasnovan kot omrežje za povezovanje računalnikov in prenos sporočil z omejenimi zmogljivostmi za izmenjavo podatkov, pri čemer so spletišča posameznikom omogočala le pasivno ogledovanje objavljenih vsebin.[1014] V dobi spleta 2.0 se je internet preoblikoval v forum, na katerem uporabniki komunicirajo, sodelujejo in ustvarjajo prispevke. Za to dobo sta značilna izjemen uspeh in razširjena uporaba storitev družbenih omrežij, ki so zdaj bistven del vsakdanjega življenja milijonov ljudi.

Storitve družbenih omrežij ali družbene medije bi lahko na široko opredelili kot „spletne komunikacijske platforme, ki posameznikom omogočajo, da se pridružijo ali ustvarijo mreže podobno mislečih uporabnikov".[1015] Da bi se posamezniki pridružili omrežju ali ga vzpostavili, so pozvani, naj predložijo osebne podatke in ustvarijo svoj profil. Storitve družbenih omrežij uporabnikom omogočajo ustvarjanje digitalne vsebin, ki segajo od fotografij ter videoposnetkov do povezav na časopise in osebnih objav za izražanje svojih stališč. Uporabniki lahko prek teh spletnih komunikacijskih platform sodelujejo in komunicirajo z več drugimi uporabniki. Pomembno je, da je pri večini priljubljenih storitev družbenih omrežij registracija brezplačna. Namesto da bi ponudniki teh storitev od uporabnikov zahtevali plačilo za pridružitev omrežju, večino svojih prihodkov ustvarijo s ciljnim oglaševanjem. Oglaševalcem lahko zelo koristijo osebni podatki, ki se vsak dan razkrivajo na teh spletnih mestih. Informacije o starosti, spolu, lokaciji in interesih uporabnika jim omogočajo, da s svojimi oglasi dosežejo „prave" osebe.

Odbor ministrov Sveta Evrope je sprejel Priporočilo o varstvu človekovih pravic v zvezi s storitvami družbenih omrežij,[1016] v katerem je v posebnem oddelku obravnavano varstvo osebnih podatkov in ki je bilo leta 2018 dopolnjeno s Priporočilom o vlogah in odgovornostih internetnih posrednikov.[1017]

1014 Evropska komisija (2016), *Advancing the Internet of Things in Europe* (Nadaljnji razvoj interneta stvari v Evropi), SWD(2016) 110 final.

1015 Delovna skupina za varstvo podatkov iz člena 29 (2009), *Mnenje 5/2009 o spletnem socialnem mreženju*, WP 163, 12. junij 2009, str. 4.

1016 Svet Evrope, Odbor ministrov, Priporočilo Rec(2012)4 državam članicam o varstvu človekovih pravic v zvezi s storitvami družbenih omrežij, 4. april 2012.

1017 Svet Evrope, Odbor ministrov, Priporočilo Rec(2018)2 državam članicam o vlogah in odgovornostih internetnih posrednikov, 7. marec 2018.

Primer: Nora je zelo srečna, ker jo je partner zaprosil za roko. Dobro novico želi deliti s prijatelji in družino, zato se odloči, da na družbenem omrežju napiše čustveno objavo, v kateri izrazi svojo radost, in spremeni svoj status razmerja v „zaročena". Ko se v naslednjih dneh prijavi v svoj račun, vidi oglase o poročnih oblekah in cvetličarnah. Zakaj se to zgodi?

Ko so družbe, ki prodajajo poročne obleke, in cvetličarne ustvarile oglas na Facebooku, so izbrale nekatere parametre, da bi lahko dosegle ljudi, kot je Nora. Če je iz Norinega profila razvidno, da je ženska, zaročena ter živi v Parizu v bližini trgovin s poročnimi oblekami in cvetličarn, ki so objavile oglase, so Nori ti oglasi takoj vidni.

Internet stvari

Internet stvari je naslednji korak v razvoju interneta: doba spleta 3.0. Z internetom stvari so naprave lahko povezane in prek interneta komunicirajo z drugimi napravami. To omogoča, da so predmeti in ljudje medsebojno povezani prek komunikacijskih omrežij ter poročajo o svojem stanju in/ali stanju okolice.[1018] Internet stvari in povezane naprave so že realnost, po pričakovanjih pa se bodo v naslednjih nekaj letih občutno razširili z oblikovanjem in nadaljnjim razvojem pametnih naprav, ki bodo privedle do oblikovanja pametnih mest, pametnih domov in pametnih podjetij.

Primer: internet stvari je lahko še posebej koristen za zdravstveno varstvo. Podjetja so že ustvarila naprave, senzorje in aplikacije, ki omogočajo spremljanje zdravstvenega stanja pacienta. Z nosljivim alarmnim gumbom in drugimi brezžičnimi senzorji, nameščenimi v stanovanju, je mogoče spremljati vsakodnevno rutino starejših, ki živijo sami, in sprožiti opozorila, če se v njihovih vsakodnevnih navadah zaznajo velika odstopanja. Med starejšimi je razširjena uporaba senzorjev za zaznavanje padcev. Ti lahko natančno zaznajo padec in o njem obvestijo zdravnika in/ali družinske člane zadevnega posameznika.

Primer: Barcelona je eden od najbolj znanih primerov pametnega mesta. To mesto od leta 2012 uporablja inovativne tehnologije za vzpostavitev pametnega sistema javnega prevoza, ravnanja z odpadki, parkiranja in ulične

1018 Evropska komisija, delovni dokument služb Komisije, *Advancing the Internet of Things in Europe* (Nadaljnji razvoj interneta stvari v Evropi), SWD(2016) 110 final, 19. april 2016.

razsvetljave. Za izboljšanje ravnanja z odpadki na primer uporablja pametne smetnjake, ki omogočajo spremljanje ravni odpadkov za optimizacijo poti odvoza odpadkov. Ko so smetnjaki skoraj polni, prek mobilnega komunikacijskega omrežja oddajo signale, ki se pošljejo programski aplikaciji, ki jo uporablja podjetje za ravnanje z odpadki. Podjetje lahko tako načrtuje najboljšo pot za odvoz odpadkov, pri čemer prednostno ali celo izključno odvozi odpadke iz smetnjakov, ki jih je dejansko treba izprazniti.

10.2.2 Uravnoteževanje koristi in tveganj

Obsežna širitev in uspešnost storitev družbenih omrežij v zadnjem desetletju kažeta, da zagotavljajo **precejšnje koristi**. Ciljno oglaševanje (kot je opisano v primeru, ponazorjenem v besedilnem polju) je posebej inovativen način, ki podjetjem omogoča, da dosežejo svoje občinstvo, in jim ponuja bolj specifičen trg. Tudi v interesu potrošnikov je lahko, da so jim predstavljeni oglasi, ki so zanje ustreznejši in zanimivejši. Še pomembneje pa je, da lahko storitve družbenih omrežij in družbeni mediji pozitivno vplivajo na družbo in uvajanje sprememb. Uporabnikom omogočajo, da komunicirajo, sodelujejo ter organizirajo skupine in dogodke o vprašanjih, ki jih zadevajo.

Podobno naj bi internet stvari, ki je del strategije EU za razvoj enotnega digitalnega trga, prinesel pomembne koristi za gospodarstvo. Ocenjuje se, da bo število povezav interneta stvari v EU leta 2020 naraslo na šest milijard. Ta širitev povezljivosti naj bi prinesla pomembne gospodarske koristi z razvojem inovativnih storitev in aplikacij, boljšim zdravstvenim varstvom, boljšim razumevanjem potreb potrošnikov in večjo učinkovitostjo.

Hkrati širitev storitev družbenih omrežij zaradi velike količine osebnih podatkov, ki jih ustvarijo uporabniki družbenih medijev in jih nato obdelajo izvajalci storitev, vzbuja **vse večjo zaskrbljenost** glede načinov, kako se lahko zaščitijo zasebnost in osebni podatki. Storitve družbenih omrežij lahko ogrozijo pravico do zasebnega življenja in pravico do svobode izražanja. Take grožnje lahko vključujejo: pomanjkanje pravnih in procesnih jamstev v zvezi s postopki, ki lahko privedejo do izključitve uporabnikov; neustrezna zaščita otrok in mladih pred škodljivimi vsebinami ali vedenji; nespoštovanje pravic drugih oseb; dejstvo, da privzete nastavitve ne varujejo zasebnosti; nepreglednost glede namenov, za katere se zbirajo in obdelujejo osebni podatki.[1019] Evropsko pravo o varstvu osebnih podatkov se je poskusilo odzvati na izzive glede

1019 Svet Evrope, Priporočilo Rec(2012)4 državam članicam o varstvu človekovih pravic v zvezi s storitvami družbenih omrežij, 4. april 2012.

varstva zasebnosti in osebnih podatkov, ki so jih povzročili družbeni mediji. V okviru družbenih medijev in storitev družbenih omrežij so zlasti pomembna načela, kot so privolitev, vgrajena in privzeta zasebnost/varstvo osebnih podatkov ter pravice posameznikov.

V okviru interneta stvari so tveganja za zasebnost in varstvo osebnih podatkov povezana tudi z veliko količino osebnih podatkov, ustvarjenih z različnimi medsebojno povezanimi napravami. Čeprav je preglednost pomembno načelo evropskega prava o varstvu osebnih podatkov, zaradi množice povezanih naprav ni vedno jasno, kdo lahko zbira podatke, pridobljene iz naprav interneta stvari, dostopa do njih in jih uporablja.[1020] Vendar morajo v okviru prava EU in Sveta Evrope upravljavci v skladu z načelom preglednosti posameznike, na katere se nanašajo osebni podatki, v jasnem in preprostem jeziku redno obveščati o tem, kako se uporabljajo njihovi osebni podatki. Zadevnim posameznikom je treba pojasniti tveganja, pravila, zaščitne ukrepe in pravice v zvezi z obdelavo njihovih osebnih podatkov. Izziv za izpolnjevanje zahteve glede jasne in informirane privolitve v obdelavo osebnih podatkov, kadar taka obdelava temelji na privolitvi, bi lahko pomenile tudi naprave, povezane z internetom stvari, ter številna dejanja obdelave in zadevni osebni podatki. Posamezniki pogosto ne razumejo tehničnega poteka take obdelave in s tem posledic, ki jih ima njihova privolitev.

Pomemben pomislek je tudi varnost, saj so povezane naprave še posebej izpostavljene varnostnim tveganjem. Povezane naprave imajo različne ravni varnosti. Ker delujejo zunaj običajne informacijske infrastrukture, morda nimajo ustrezne zmogljivosti za obdelavo in shranjevanje, da bi lahko imele nameščeno varnostno programsko opremo ali uporabljale tehnike, kot so šifriranje, psevdonimizacija ali anonimizacija, za varstvo osebnih podatkov uporabnikov.

Primer: v Nemčiji so se regulativni organi odločili, da bodo prepovedali igračo, povezano z internetom, zaradi resnih pomislekov glede njenega vpliva na spoštovanje zasebnega življenja otrok. Menili so, da je z internetom povezana punčka Cayla dejansko skrita vohunska naprava. Punčka je delovala tako, da je zvočna vprašanja otroka, ki se je z njo igral, poslala aplikaciji na digitalni napravi, ki jih je pretvorila v besedilo in odgovore nanje poiskala na internetu. Aplikacija je nato odgovore poslala punčki, ki jih je izgovorila otroku. S to punčko se je lahko otrokova komunikacija in komunikacija odraslih

1020 Evropski nadzornik za varstvo podatkov (2017), *Understanding the Internet of Things* (Razumevanje interneta stvari).

v bližini snemala in posredovala aplikaciji. Če proizvajalci te punčke ne bi sprejeli ustreznih varnostnih ukrepov, bi lahko punčko kdor koli uporabljal za poslušanje pogovorov.

10.2.3 Vprašanja, povezana z varstvom osebnih podatkov

Privolitev

V Evropi je obdelava osebnih podatkov zakonita le, če je dovoljena v skladu z evropskim pravom o varstvu osebnih podatkov. Za ponudnike storitev družbenih omrežij je privolitev posameznikov, na katere se nanašajo osebni podatki, na splošno zakonita podlaga za obdelavo osebnih podatkov. Privolitev mora biti prostovoljna, konkretna, informirana in nedvoumna (glej razdelek 4.1.1).[1021] „Prostovoljna" pomeni, da morajo imeti posamezniki, na katere se nanašajo osebni podatki, možnost resnične in dejanske izbire. Privolitev je „konkretna" in „informirana", če je razumljiva ter vsebuje jasno in natančno sklicevanje na celoten obseg, namene in posledice obdelave osebnih podatkov. V zvezi z družbenimi mediji bi se lahko spraševali o tem, ali je privolitev prostovoljna, konkretna in informirana za vse vrste obdelave, ki jih izvajajo ponudniki storitev družbenih medijev in tretje osebe.

Primer: da bi se posamezniki lahko pridružili storitvi družbenega omrežja in dostopali do njega, morajo običajno privoliti v različne oblike obdelave svojih osebnih podatkov, pogosto ne da bi bili seznanjeni s potrebnimi specifikacijami ali drugimi možnostmi. Primer je potreba po privolitvi posameznikov v prejemanje vedenjskih oglasov, da bi se lahko registrirali v družbeno omrežje. Delovna skupina iz člena 29 je v svojem mnenju o opredelitvi privolitve navedla: „Glede na to, kako pomembna so postala nekatera socialna omrežja, nekatere vrste uporabnikov (kot so najstniki) privolijo v prejemanje vedenjskih oglasov, da bi se izognili tveganju delne izključenosti iz socialnih interakcij. Uporabnik bi moral imeti možnost dati prostovoljno in posebno privolitev v prejemanje vedenjskih oglasov neodvisno od njegovega dostopa do storitve socialnega omrežja."[1022]

1021 SUVP, člena 4 in 7; posodobljena Konvencija št. 108, člen 5.

1022 Delovna skupina iz člena 29 (2011), *Mnenje št. 15/2011 o opredelitvi privolitve*, WP 187, 13. julij 2011, str. 18.

V skladu s SUVP osebnih podatkov otrok, mlajših od 16 let, načeloma ni mogoče obdelovati na podlagi njihove privolitve.[1023] Če je za obdelavo potrebna privolitev, jo mora dati otrokov starš ali skrbnik. Otrokom je treba zagotoviti posebno varstvo, saj se lahko manj zavedajo tveganj in posledic, povezanih z obdelavo osebnih podatkov. To je zelo pomembno v okviru družbenih medijev, saj so otroci občutljivejši na nekatere negativne učinke, ki jih lahko ima uporaba teh medijev, kot so kibernetsko nadlegovanje, kibernetsko zalezovanje ali kraja identitete.

Varnost ter vgrajena in privzeta zasebnost/varstvo osebnih podatkov

Obdelava osebnih podatkov sama po sebi vključuje varnostna tveganja zaradi stalne možnosti, da pride do kršitve varnosti, ki privede do nenamernega ali nezakonitega uničenja, izgube ali spremembe obdelanih osebnih podatkov oziroma nepooblaščenega dostopa do njih ali njihovega razkritja. V skladu z evropskim pravom o varstvu osebnih podatkov morajo upravljavci in obdelovalci izvajati ustrezne tehnične in organizacijske ukrepe za preprečitev nepooblaščenega poseganja v dejanja obdelave osebnih podatkov. To obveznost morajo izpolnjevati tudi ponudniki storitev družbenih omrežij, za katere veljajo evropska pravila o varstvu osebnih podatkov.

Upravljavci morajo v skladu z načeli vgrajene in privzete zasebnosti/varstva osebnih podatkov zagotavljati varnost pri načrtovanju svojih izdelkov ter samodejno uporabljati ustrezne nastavitve glede zasebnosti in varstva osebnih podatkov. To pomeni, da če se oseba odloči, da se bo pridružila družbenemu omrežju, ponudnik zadevne storitve informacij o novem uporabniku storitve ne sme samodejno dati na voljo vsem svojim uporabnikom. Ob pridružitvi zadevni storitvi bi morale biti privzete nastavitve glede zasebnosti in varstva osebnih podatkov take, da so informacije na voljo le izbranim stikom posameznika. Razširitev dostopa na osebe, ki niso na tem seznamu, bi morala biti mogoča šele po tem, ko uporabnik ročno spremeni privzeto nastavitev glede zasebnosti in varstva osebnih podatkov. To bi lahko imelo vpliv tudi v primerih, ko kljub sprejetim varnostnim ukrepom pride do kršitve varnosti osebnih podatkov. V takih primerih morajo ponudniki storitev prizadete uporabnike obvestiti o kršitvi varnosti osebnih podatkov, kadar je verjetno, da bo ta povzročila veliko tveganje za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki.[1024]

1023 Glej SUVP, člen 8. Države članice EU lahko z zakonom določijo nižjo starost, vendar ta ne sme biti nižja od 13 let.

1024 Prav tam, člen 34.

V okviru storitev družbenih omrežij sta vgrajena in privzeta zasebnost/varstvo osebnih podatkov še posebej pomembna, saj poleg tveganj nepooblaščenega dostopa, ki obstajajo pri večini vrst obdelave, izmenjava osebnih podatkov na družbenih medijih pomeni dodatna varnostna tveganja. Ta pogosto nastanejo, ker posamezniki ne razumejo, *kdo* lahko dostopa do njihovih informacij in kako jih lahko te osebe uporabijo. Z razširjeno uporabo družbenih medijev se je povečalo število primerov in žrtev kraje identitete.

Primer: kraja identitete je pojav, pri katerem oseba pridobi informacije, podatke ali dokumente, ki pripadajo drugi osebi (žrtvi), in nato te informacije uporabi, da se izdaja za žrtev in tako pridobi blago in storitve v imenu žrtve. Vzemimo za primer Paula, ki ima račun na spletišču družbenega medija. Učitelja Paula, ki je dejaven član skupnosti in zelo družaben, ne zanimajo preveč nastavitve glede zasebnosti in varstva osebnih podatkov na njegovem računu na družbenem mediju. Ima obsežen seznam stikov, na katerem so tudi osebe, ki jih ne pozna osebno. Ker je zaposlen v veliki šoli in je zelo priljubljen, ker je trener šolske nogometne ekipe, meni, da so te osebe najverjetneje starši ali podporniki. Na njegovem računu na družbenem mediju sta navedena njegov elektronski naslov in rojstni datum. Poleg tega Paul redno objavlja fotografije svojega psa Tobyja s komentarji, kot na primer „S Tobyjem na najinem jutranjem teku". Paul se ne zaveda, da je eno najpogostejših varnostnih vprašanj za zaščito elektronskega poštnega predala ali mobilnega telefonskega računa „Kako je ime vašemu ljubljenčku?". Nick uporabi informacije, ki so na voljo v Paulovem profilu na družbenem mediju, in zlahka vdre v Paulove račune.

Pravice posameznikov

Ponudniki storitev družbenega omrežja morajo spoštovati pravice posameznikov (glej razdelek 6.1), med drugim pravico, da so obveščeni o namenu obdelave in morebitni uporabi osebnih podatkov za namene neposrednega trženja. Posameznikom je poleg tega treba zagotoviti pravico, da dostopajo do svojih osebnih podatkov, ki so jih ustvarili na platformi družbenega omrežja, in zahtevajo njihov izbris. Tudi če so osebe privolile v obdelavo osebnih podatkov in naložile informacije na splet, bi morale imeti možnost zahtevati, da so „pozabljene", če ne želijo več uporabljati storitev družbenega omrežja. Pravica do prenosljivosti podatkov poleg tega uporabnikom omogoča, da prejmejo kopijo osebnih podatkov, ki so jih zagotovili ponudniku storitev družbenega omrežja, v strukturirani, splošno uporabljani in strojno berljivi

obliki, ter da svoje osebne podatke prenesejo od enega ponudnika storitev družbenega omrežja na drugega.[1025]

Upravljavci

Zahtevno vprašanje, ki se pogosto pojavi v okviru družbenih medijev, je vprašanje, kdo je upravljavec, torej kdo je oseba, ki ima obveznost in odgovornost, da ravna v skladu s pravili o varstvu osebnih podatkov. Ponudniki storitev družbenega omrežja se v skladu z evropskim pravom o varstvu osebnih podatkov štejejo za upravljavce. To je razvidno iz široke opredelitve pojma upravljavec in dejstva, da ti ponudniki storitev določijo namen in sredstva obdelave osebnih podatkov, ki jih delijo posamezniki. Če upravljavci ponujajo storitve posameznikom, na katere se nanašajo osebni podatki, v EU, morajo v skladu s pravom EU izpolnjevati določbe SUVP, tudi če niso ustanovljeni v EU.

Vendar ali je mogoče za upravljavce šteti tudi uporabnike storitev družbenega omrežja? Pravila o varstvu osebnih podatkov se ne uporabljajo, kadar posamezniki osebne podatke obdelujejo „med potekom popolnoma osebne ali domače dejavnosti". V evropskem pravu o varstvu osebnih podatkov je to znano kot izjema obdelave za domače potrebe. Vendar uporabnik storitve družbenega omrežja v nekaterih primerih morda ni zajet z izjemo obdelave za domače potrebe.

Uporabniki prostovoljno delijo svoje osebne podatke na spletu. Vendar informacije, ki se delijo na spletu, pogosto vključujejo osebne podatke drugih posameznikov.

Primer: Paul ima račun na zelo priljubljeni platformi za družbeno mreženje. Ker si prizadeva postati igralec, na svojem računu objavlja fotografije, videoposnetke in objave, v katerih pojasnjuje svojo ljubezen do umetnosti. Priljubljenost je pomembna za njegovo prihodnost, zato se je odločil, da njegov profil ne bo na voljo le njegovemu ožjemu seznamu stikov, temveč vsem internetnim uporabnikom, ne glede na to, ali so člani omrežja ali ne. Ali lahko Paul objavlja fotografije in videoposnetke, na katerih je s prijateljico Sarah, brez njene privolitve? Sarah kot osnovnošolska učiteljica poskuša svoje zasebno življenje varovati pred očmi svojega delodajalca, učencev in njihovih staršev. Predstavljajte si, da Sarah, ki družbenih omrežij ne uporablja,

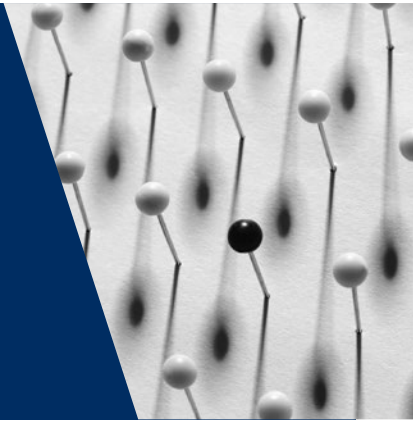
1025 SUVP, člen 20.

od skupnega prijatelja Nicka izve, da je bila na spletu objavljena fotografija nje in Paula na zabavi. V tem primeru obdelava osebnih podatkov ne spada na področje prava EU, saj je zajeta z izjemo obdelave za domače potrebe.

Vendar pa je za uporabnike ključno, da se zavedajo, da lahko objavljanje informacij o drugih posameznikih brez njihove privolitve posega v zasebnost teh posameznikov in njihovo pravico do varstva osebnih podatkov. Tudi če se uporablja izjema obdelave za domače potrebe, na primer če ima uporabnik profil, ki je dostopen le osebam s seznama stikov, ki jih je izbral sam, lahko uporabnik še vedno nosi odgovornost za objavo osebnih podatkov o drugih osebah. Čeprav se pravila o varstvu osebnih podatkov ne uporabljajo, če se uporablja izjema obdelave za domače potrebe, bi lahko odgovornost izhajala iz uporabe drugih nacionalnih predpisov, na primer v zvezi z obrekovanjem ali kršitvijo osebnostnih pravic. Nenazadnje so z izjemo obdelave za domače potrebe zaščiteni le uporabniki storitev družbenih omrežij: za upravljavce in obdelovalce, ki zagotavljajo sredstva za tovrstno zasebno obdelavo, veljajo določbe prava EU o varstvu osebnih podatkov.[1026]

V skladu z reformo Direktive o zasebnosti in elektronskih komunikacijah bi se pravila o varstvu osebnih podatkov, zasebnosti in varnosti, ki se v skladu z veljavnim pravnim okvirom uporabljajo za ponudnike telekomunikacijskih storitev, uporabljala tudi za komunikacijo stroj-stroj in elektronske komunikacijske storitve, vključno s storitvami OTT.

1026 Prav tam, uvodna izjava 18.



Dodatna literatura

Poglavje 1

Araceli Mangas, M. (ur.) (2008), *Carta de los derechos fundamentales de la Unión Europea, Bilbao*, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Dunaj, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C., „Four fundamental rights: finding the balance", *International Data Privacy Law*, zv. 6, št. 3, str. 195–209.

EDRi, *An introduction to data protection*, Bruselj.

Frowein, J., in Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G., in Gellert, G. (2012), „The fundamental right of data protection in the European Union: in search of an uncharted right", *International Review of Law, Computers and Technology*, zv. 26 (1), str. 73–82.

Grabenwarter, C., in Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C., in Nouwt, S. (ur.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C., in Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), „EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation".

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Kokott, J., in Sobotta, C. (2013), „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR", *International Data Privacy Law*, zv. 3, št. 4, str. 222–228.

Kranenborg, H. (2015), „Google and the Right to be Forgotten", *European Data Protection Law Review*, zv. 1, št. 1, str. 70–79.

Lynskey, O. (2014), „Deconstructing data protection: the ‚added-value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, zv. 63, št. 3, str. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K., in Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerpen, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C., in Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bruselj, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?“, *Neue Juristische Wochenschrift*, zv. 5, str. 281–288.

Warren, S., in Brandeis, L. (1890), „The right to privacy“, *Harvard Law Review,* zv. 4, št. 5, str. 193–220.

White, R., in Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Poglavje 2

Acquisty, A., in Gross R. (2009), „Predicting Social Security numbers from public data“, *Proceedings of the National Academy of Science*, 7. julij 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., in Blondel V. D. (2013), „Unique in the Crowd: the Privacy Bounds of Human Mobility“, *Nature Scientific Reports*, zv. 3, 2013.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Pariz, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R., in Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization“, *UCLA Law Review*, zv. 57, št. 6, str. 1701–1777.

Samarati, P., in Sweeney, L. (1998), „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression“, Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), „K-Anonymity: A Model for Protecting Privacy“, *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, zv. 10, št. 5, str. 557–570.

Tinnefeld, M., Buchner, B., in Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*.

Poglavja 3 do 6

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ v: Grabitz, E., Hilf, M., in Nettesheim, M. (ur.), *Das Recht der Europäischen Union*, Band IV, A. 30, München, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Curren, L., in Kaye, J. (2010), „Revoking consent: a ‚blind spot' in data protection law?“, *Computer Law & Security Review*, zv. 26, št. 3, str. 273–283.

Dammann, U., in Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P., in Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis“, *Computers & Law Magazine of SCL*, zv. 22, št. 6, str. 1–5.

De Hert, P., in Papakonstantinou, V. (2012), „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals“, *Computer Law & Security Review*, zv. 28, št. 2, str. 130–142.

Feretti, F. (2012), „A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously", *European Review of Private Law*, zv. 20, št. 2, str. 473–506.

FRA (Agencija Evropske unije za temeljne pravice) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Urad za publikacije Evropske unije (Urad za publikacije).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (konferenčna izdaja), Dunaj, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Urad za publikacije.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I., in Saxby, S. (2011), „30 years on – The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Review*, zv. 27, št. 3, str. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, Privacy Impact Assessment.

Poglavje 7

Delovna skupina za varstvo podatkov iz člena 29 (2005), *Delovni dokument o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995*.

Evropski nadzornik za varstvo podatkov (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C., in Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Kuner, C. (2013), *European data protection law*, Oxford, Oxford University Press.

Poglavje 8

Blasi Casagran, C. (2016), *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

De Hert, P., in Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, zv. 22, št. 6, str. 1–5.

Drewer, D., in Ellermann, J. (2012), „Europol's data protection framework as an asset in the fight against cybercrime", *ERA Forum*, zv. 13, št. 3, str. 381–395.

Eurojust (2014), *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

Europol (2012), *Data Protection at Europol*, Luxembourg, Urad za publikacije.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y., in De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P., in Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, zv. 36, št. 5, str. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2.

Poglavje 9

Büllesbach, A., Gijrath, S., Poullet, Y., in Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Poullet, Y., in De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P., in Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Gutwirth, S., Leenes, R., De Hert, P., in Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, zv. 36, št. 5, str. 722–776.

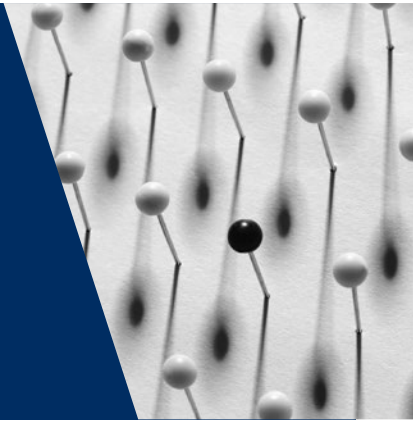
Rosemary, J., in Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Poglavje 10

El Emam, K., in Álvarez, C. (2015), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, zv. 5, št. 1, str. 73–87.

Mayer-Schönberger, V., in Cate, F. (2013), „Notice and consent in a world of Big Data", *International Data Privacy Law*, zv. 3, št. 2, str. 67–73.

Rubistein, I. (2013), „Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, zv. 3, št. 2, str. 74–87.



Sodna praksa

Izbrana sodna praksa Evropskega sodišča za človekove pravice

Dostop do osebnih podatkov
Gaskin proti Združenemu kraljestvu, pritožba št. 10454/83, 7. julij 1989
Godelli proti Italiji, pritožba št. 33783/09, 25. september 2012
K. H. in drugi proti Slovaški, pritožba št. 32881/04, 28. april 2009
Leander proti Švedski, pritožba št. 9248/81, 26. marec 1987
M. K. proti Franciji, pritožba št. 19522/09, 18. april 2013
Odièvre proti Franciji (veliki senat), pritožba št. 42326/98, 13. februar 2003

Uravnoteženje varstva osebnih podatkov s svobodo izražanja in pravico do obveščenosti
Axel Springer AG proti Nemčiji (veliki senat), pritožba št. 39954/08, 7. februar 2012
Bohlen proti Nemčiji, pritožba, 19. februar 2015
Couderc in Hachette Filipacchi Associés proti Franciji (veliki senat), pritožba št. 40454/07, 10. november 2015
Magyar Helsinki Bizottság proti Madžarski (veliki senat), pritožba št. 18030/11, 8. november 2016
Müller in drugi proti Švici, pritožba št. 10737/84, 24. maj 1988
Satakunnan Markkinapörssi Oy in Satamedia Oy proti Finski (veliki senat), pritožba št. 931/13, 27. junij 2017
Vereinigung Bildender Künstler proti Avstriji, pritožba št. 68354/01, 25. januar 2007

Združeni zadevi *Von Hannover proti Nemčiji (št. 2)* (veliki senat), pritožbi št. 40660/08 in 60641/08, 7. februar 2012

Uravnoteženje varstva osebnih podatkov s svobodo vere
Sinan Işık proti Turčiji, pritožba št. 21924/05, 2. februar 2010

Izzivi varstva osebnih podatkov na spletu
K. U. proti Finski, pritožba št. 2872/02, 2. december 2008

Privolitev posameznika, na katerega se nanašajo osebni podatki
Elberte proti Latviji, pritožba št. 61243/08, 13. januar 2015
Sinan Işık proti Turčiji, pritožba št. 21924/05, 2. februar 2010
Y proti Turčiji, pritožba št. 648/10, 17. februar 2015

Dopisovanje
Amann proti Švici (veliki senat), pritožba št. 27798/95, 16. februar 2000
Association for European Integration and Human Rights in Ekimdzhiev proti Bolgariji, pritožba št. 62540/00, 28. junij 2007
Bernh Larsen Holding AS in drugi proti Norveški, pritožba št. 24117/08, 14. marec 2013
Cemalettin Canli proti Turčiji, pritožba št. 22427/04, 18. november 2008
D. L. proti Bolgariji, pritožba št. 7472/14, 19. maj 2016
Dalea proti Franciji, pritožba št. 964/07, 2. februar 2010
Gaskin proti Združenemu kraljestvu, pritožba št. 10454/83, 7. julij 1989
Haralambie proti Romuniji, pritožba št. 21737/03, 27. oktober 2009
Khelili proti Švici, pritožba št. 16188/07, 18. oktober 2011
Leander proti Švedski, pritožba št. 9248/81, 26. marec 1987
Malone proti Združenemu kraljestvu, pritožba št. 8691/79, 2. avgust 1984
Rotaru proti Romuniji (veliki senat), pritožba št. 28341/95, 4. maj 2000
Združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 4. december 2008
Shimovolos proti Rusiji, pritožba št. 30194/09, 21. junij 2011
Združene zadeve *Silver in drugi proti Združenemu kraljestvu*, pritožbe št. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 in 7113/75, 25. marec 1983
The Sunday Times proti Združenemu kraljestvu, pritožba št. 6538/74, 26. april 1979

Podatkovne zbirke kazenskih evidenc
Aycaguer proti Franciji, pritožba št. 8806/12, 22. junij 2017
B. B. proti Franciji, pritožba št. 5335/06, 17. december 2009

Brunet proti Franciji, pritožba št. 21010/10, 18. september 2014
M. K. proti Franciji, pritožba št. 19522/09, 18. april 2013
M. M. proti Združenemu kraljestvu, pritožba št. 24029/07, 13. november 2012

Varnost podatkov
Haralambie proti Romuniji, pritožba št. 21737/03, 27. oktober 2009
K. H. in drugi proti Slovaški, pritožba št. 32881/04, 28. april 2009

Podatkovne zbirke DNK
Združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 4. december 2008

Podatki GPS
Uzun proti Nemčiji, pritožba št. 35623/05, 2. september 2010

Zdravstveni osebni podatki
Avilkina in drugi proti Rusiji, pritožba št. 1585/09, 6. junij 2013
Biriuk proti Litvi, pritožba št. 23373/03, 25. november 2008
I proti Finski, pritožba št. 20511/03, 17. julij 2008
L. H. proti Latviji, pritožba št. 52019/07, 29. april 2014
L. L. proti Franciji, pritožba št. 7508/02, 10. oktober 2006
M. S. proti Švedski, pritožba št. 20837/92, 27. avgust 1997
Szuluk proti Združenemu kraljestvu, pritožba št. 36936/05, 2. junij 2009
Y proti Turčiji, pritožba št. 648/10, 17. februar 2015
Z proti Finski, pritožba št. 22009/93, 25. februar 1997

Identiteta
Ciubotaru proti Moldaviji, pritožba št. 27138/04, 27. april 2010
Godelli proti Italiji, pritožba št. 33783/09, 25. september 2012
Odièvre proti Franciji (veliki senat), pritožba št. 42326/98, 13. februar 2003

Informacije o poklicnih dejavnostih
G. S. B. proti Švici, pritožba št. 28601/11, 22. december 2015
M. N. in drugi proti San Marinu, pritožba št. 28005/12, 7. julija2015
Michaud proti Franciji, pritožba št. 12323/11, 6. december 2012
Niemietz proti Nemčiji, pritožba št. 13710/88, 16. december 1992

Prestrezanje komunikacij
Amann proti Švici (veliki senat), pritožba št. 27798/95, 16. februar 2000

Brito Ferrinho Bexiga Villa-Nova proti Portugalski, pritožba št. 69436/10, 1. december 2015
Copland proti Združenemu kraljestvu, pritožba št. 62617/00, 3. april 2007
Halford proti Združenemu kraljestvu, pritožba št. 20605/92, 25. junij 1997
Iordachi in drugi proti Moldaviji, pritožba št. 25198/02, 10. februar 2009
Kopp proti Švici, pritožba št. 23224/94, 25. marec 1998
Liberty in drugi proti Združenemu kraljestvu, pritožba št. 58243/00, 1. julij 2008
Malone proti Združenemu kraljestvu, pritožba št. 8691/79, 2. avgust 1984
Mustafa Sezgin Tanrıkulu proti Turčiji, pritožba št. 27473/06, 18. julij 2017
Pruteanu proti Romuniji, pritožba št. 30181/05, 3. februar 2015
Szuluk proti Združenemu kraljestvu, pritožba št. 36936/05, 2. junij 2009

Obveznosti nosilcev dolžnosti
B. B. proti Franciji, pritožba št. 5335/06, 17. december 2009
I proti Finski, pritožba št. 20511/03, 17. julij 2008
Mosley proti Združenemu kraljestvu, pritožba št. 48009/08, 10. maj 2011

Osebni podatki
Amann proti Švici (veliki senat), pritožba št. 27798/95, 16. februar 2000
Bernh Larsen Holding AS in drugi proti Norveški, pritožba št. 24117/08, 14. marec 2013
Uzun proti Nemčiji, pritožba št. 35623/05, 2. september 2010

Fotografije
Sciacca proti Italiji, pritožba št. 50774/99, 11. januar 2005
Von Hannover proti Nemčiji, pritožba št. 59320/00, 24. junij 2004

Pravica do pozabe
Satakunnan Markkinapörssi Oy in Satamedia Oy proti Finski (veliki senat), pritožba št. 931/13, 27. junij 2017
Segerstedt-Wiberg in drugi proti Švedski, pritožba št. 62332/00, 6. junij 2006

Pravica do ugovora
Leander proti Švedski, pritožba št. 9248/81, 26. marec 1987
M. S. proti Švedski, pritožba št. 20837/92, 27. avgust 1997
Mosley proti Združenemu kraljestvu, pritožba št. 48009/08, 10. maj 2011
Rotaru proti Romuniji (veliki senat), pritožba št. 28341/95, 4. maj 2000
Sinan Işık proti Turčiji, pritožba št. 21924/05, 2. februar 2010

Občutljive vrste osebnih podatkov
Brunet proti Franciji, pritožba št. 21010/10, 18. september 2014
I proti Finski, pritožba št. 20511/03, 17. julij 2008
Michaud proti Franciji, pritožba št. 12323/11, 6. december 2012
Združeni zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), pritožbi št. 30562/04 in 30566/04, 4. december 2008

Nadzor in pregon (vloga različnih akterjev, vključno z nadzornimi organi)
I proti Finski, pritožba št. 20511/03, 17. julij 2008
K. U. proti Finski, pritožba št. 2872/02, 2. december 2008
Von Hannover proti Nemčiji, pritožba št. 59320/00, 24. junij 2004
Združeni zadevi *Von Hannover proti Nemčiji (št. 2)* (veliki senat), pritožbi št. 40660/08 in 60641/08, 7. februar 2012

Metode nadzora
Allan proti Združenemu kraljestvu, pritožba št. 48539/99, 5. november 2002
Association for European Integration and Human Rights in Ekimdzhiev proti Bolgariji, pritožba št. 62540/00, 28. juni 2007
Bărbulescu proti Romuniji (veliki senat), pritožba št. 61496/08, 5. september 2017
D. L. proti Bolgariji, pritožba št. 7472/14, 19. maj 2016
Dragojević proti Hrvaški, pritožba št. 68955/11, 15. januar 2015
Karabeyoğlu proti Turčiji, pritožba št. 30083/10, 7. junij 2016
Klass in drugi proti Nemčiji, pritožba št. 5029/71, 6. september 1978
Roman Zakharov proti Rusiji (veliki senat), pritožba št. 47143/06, 4. december 2015
Rotaru proti Romuniji (veliki senat), pritožba št. 28341/95, 4. maj 2000
Szabó in Vissy proti Madžarski, pritožba št. 37138/14, 12. januar 2016
Taylor-Sabori proti Združenemu kraljestvu, pritožba št. 47114/99, 22. oktober 2002
Uzun proti Nemčiji, pritožba št. 35623/05, 2. september 2010
Versini-Campinchi in Crasnianski proti Franciji, pritožba št. 49176/11, 16. junij 2016
Vetter proti Franciji, pritožba št. 59842/00, 31. maj 2005
Vukota-Bojić proti Švici, pritožba št. 61838/10, 18. oktober 2016

Videonadzor
Köpke proti Nemčiji, pritožba št. 420/07, sklep z dne 5. oktobra 2010
Peck proti Združenemu kraljestvu, pritožba št. 44647/98, 28. januar 2003

Glasovni vzorci
P. G. in J. H. proti Združenemu kraljestvu, pritožba št. 44787/98, 25. september 2001
Wisse proti Franciji, pritožba št. 71611/01, 20. december 2005

Izbrana sodna praksa Sodišča Evropske unije

Sodna praksa v zvezi z direktivo o varstvu osebnih podatkov

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado, združeni zadevi C-468/10 in C-469/10, 24. november 2011

(Pravilno izvajanje člena 7(f) direktive o varstvu osebnih podatkov – zakoniti interesi drugih – v nacionalnem pravu)

Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) proti Netlog NV, C-360/10, 16. februar 2012

(Obveznost ponudnikov družbenih omrežij, da uporabnikom omrežja preprečijo nezakonito uporabo glasbenih in avdiovizualnih del)

Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatoreju Manniju, C-398/15, 9. marec 2017

(Pravica do izbrisa osebnih podatkov; pravica do ugovora obdelavi)

College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer, C-553/07, 7. maj 2009

(Pravica posameznika, na katerega se nanašajo osebni podatki, do dostopa)

Deutsche Telekom AG proti Bundesrepublik Deutschland, C-543/09, 5. maj 2011

(Potreba po ponovni privolitvi)

Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim in Kärntner Landesregierung in drugim (veliki senat), združeni zadevi C-293/12 in C-594/12, 8. april 2014

(Neskladnost direktive o hrambi podatkov s primarno zakonodajo EU; zakonita obdelava; omejitev namena in shranjevanja)

Evropska komisija proti Zvezni republiki Nemčiji (veliki senat), C-518/07, 9. marec 2010

(Neodvisnost nacionalnega nadzornega organa)

Evropska komisija proti Madžarski (veliki senat), C-288/12, 8. april 2014

(Zakonitost predčasne prekinitve mandata nacionalnega nadzornega organa za varstvo podatkov)

Evropska komisija proti Republiki Avstriji (veliki senat), C-614/10, 16. oktober 2012
(Neodvisnost nacionalnega nadzornega organa)

František Ryneš proti Úřad pro ochranu osobních údajů, C-212/13,
11. december 2014
(Pojma obdelava podatkov in upravljavec)

Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeju Gonzálezu (veliki senat), C-131/12, 13. maj 2014
(Obveznosti ponudnikov spletnih iskalnikov, da na zahtevo posameznika, na katerega se nanašajo osebni podatki, v zadetkih iskanja ne prikazujejo osebnih podatkov; uporaba direktive o varstvu osebnih podatkov; pojem obdelava podatkov; pomen upravljavca; uravnoteženje varstva osebnih podatkov s svobodo izražanja; pravica do pozabe)

Heinz Huber proti Bundesrepublik Deutschland (veliki senat), C-524/06,
16. december 2008
(Zakonitost hrambe podatkov o tujih državljanih v statističnem registru)

Institut professionnel des agents immobiliers (IPI) proti Geoffreyju Englebertu in drugim, C-473/12, 7. november 2013
(Pravica do obveščenosti o obdelavi osebnih podatkov

Kazenski postopek proti Bodil Lindqvist, C-101/01, 6. november 2003
(Posebne kategorije osebnih podatkov)

Maximillian Schrems proti Data Protection Commissioner (veliki senat), C-362/14,
6. oktober 2015
(Načelo zakonite obdelave; temeljne pravice; neveljavnost odločbe o varnem pristanu; pooblastila neodvisnih nadzornih organov)

Michael Schwarz proti Stadt Bochum, C-291/12, 17. oktober 2013
(Predlog za sprejetje predhodne odločbe; območje svobode, varnosti in pravice; biometrični potni list; prstni odtisi; pravna podlaga; sorazmernost)

Patrick Breyer proti Bundesrepublik Deutschland, C-582/14, 19. oktober 2016
(Opredelitev pojma osebni podatki; IP-naslovi; shranjevanje podatkov s strani ponudnika storitev spletnih medijev; nacionalna zakonodaja, ki ne dopušča, da bi se upošteval legitimni interes upravljavca)

Peter Nowak proti Data Protection Commissioner, C-434/16, sklepni predlogi generalne pravobranilke Juliane Kokott z dne 20. julija 2017

(Pojem osebni podatki; dostop do lastnega izpitnega izdelka; komentarji popravljavca)

Pilkington Group Ltd proti Evropski komisiji, T-462/12 R, sklep predsednika Splošnega sodišča z dne 11. marca 2013

Productores de Música de España (Promusicae) proti Telefónica de España SAU (veliki senat), C-275/06, 29. januar 2008

(Pojem osebni podatki; obveznost ponudnikov dostopa do interneta, da združenju za varstvo intelektualne lastnine razkrijejo identiteto uporabnikov programa KaZaA za izmenjavo datotek)

Rechnungshof proti Österreichischer Rundfunk in drugim in *Christa Neukomm in Joseph Lauermann proti Österreichischer Rundfunk*, združene zadeve C-465/00, C-138/01 in C-139/01, 20. maj 2003

(Sorazmernost pravne obveznosti glede objave osebnih podatkov o plačah zaposlenih v nekaterih kategorijah institucij, povezanih z javnim sektorjem)

Scarlet Extended SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, 24. november 2011

(Informacijska družba; avtorska pravica; internet; programska oprema „peer-to-peer"; ponudniki internetnih storitev; vzpostavitev sistema za filtriranje elektronskih komunikacij z namenom preprečitve izmenjave datotek, ki pomeni kršitev avtorske pravice; neobstoj splošne obveznosti nadzora informacij, ki se prenašajo)

Smaranda Bara in drugi proti Președintele Casei Naționale de Asigurări de Sănătate in drugim, C-201/14, 1. oktober 2015

(Pravica do obveščenosti o obdelavi osebnih podatkov)

Tele2 Sverige AB proti Post- och telestyrelsen in *Secretary of State for the Home Department proti Tomu Watsonu in drugim* (veliki senat), združeni zadevi C-203/15 in C-698/15, 21. december 2016

(Zaupnost elektronskih komunikacij; ponudniki elektronskih komunikacijskih storitev; obveznost splošne in neselektivne hrambe podatkov o prometu in lokaciji; neobstoj predhodnega nadzora s strani sodišča ali neodvisnega upravnega organa; Listina Evropske unije o temeljnih pravicah; združljivost s pravom EU)

Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy in Satamedia Oy (veliki senat), C-73/07, 16. december 2008

(Pojem novinarski nameni v smislu člena 9 direktive o varstvu osebnih podatkov)

Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde proti Rīgas pašvaldības SIA „Rīgas satiksme“, C-13/16, 4. maj 2017
(Načelo zakonite obdelave: zakonit interes, za katerega si prizadeva tretja oseba)

Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen (veliki senat), združeni zadevi C-92/09 in C-93/09, 9. november 2010
(Pojem osebni podatki; sorazmernost pravne obveznosti glede objave osebnih podatkov upravičencev do sredstev iz nekaterih kmetijskih skladov EU)

Weltimmo s.r.o. proti Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1. oktober 2015
(Pooblastila nacionalnih nadzornih organov)

Worten – Equipamentos para o Lar SA proti Autoridade para as Condições de Trabalho (ACT), C-342/12, 30. maj 2013
(Pojem osebni podatki; evidenca delovnega časa; načela v zvezi s kakovostjo podatkov in merila za zakonitost obdelave podatkov; dostop nacionalnega organa, pristojnega za nadzor delovnih razmer; obveznost delodajalca, da omogoči dostop do evidence delovnega časa, in sicer tako, da je mogoč takojšen vpogled vanjo)

YS proti Minister voor Immigratie, Integratie en Asiel in Minister voor Immigratie, Integratie en Asiel proti M in S, združeni zadevi C-141/12 in C-372/12, 17. julij 2014
(Obseg pravice do dostopa, ki jo ima posameznik, na katerega se nanašajo osebni podatki; varstvo posameznikov pri obdelavi osebnih podatkov; pojem osebni podatki; podatki, ki se nanašajo na prosilca za dovoljenje za prebivanje, in pravna analiza, vsebovani v pripravljalnem upravnem dokumentu za odločbo; Listina Evropske unije o temeljnih pravicah)

Sodna praksa v zvezi z Direktivo (EU) 2016/681

Mnenje Sodišča 1/15 (veliki senat) z dne 26. julija 2017
(Pravna podlaga; osnutek sporazuma med Kanado in Evropsko unijo o prenosu in obdelavi podatkov iz evidence podatkov o potnikih; združljivost osnutka sporazuma s členom 16 PDEU ter členoma 7 in 8 ter členom 52(1) Listine Evropske unije o temeljnih pravicah)

Sodna praksa v zvezi z uredbo o varstvu osebnih podatkov v institucijah EU

ClientEarth in Pesticide Action Network Europe (PAN Europe) proti Evropski agenciji za varno hrano in Evropski komisiji, C-615/13 P, 16. julij 2015
(Dostop do dokumentov)

Evropska komisija proti The Bavarian Lager Co. Ltd. (veliki senat), C-28/08 P, 29. junij 2010
(Dostop do dokumentov)

Sodna praksa v zvezi z Direktivo 2002/58/ES

Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB proti Perfect Communication Sweden AB, C-461/10, 19. april 2012
(Avtorska pravica in sorodne pravice; internetna obdelava podatkov; poseg v izključno pravico; zvočne knjige, ki so prek strežnika FTP z uporabo specifičnega IPnaslova, ki ga je dodelil ponudnik internetnih storitev, postale dostopne na internetu; odredba sodišča, naj ponudnik internetnih storitev razkrije ime in naslov uporabnika IPnaslova)

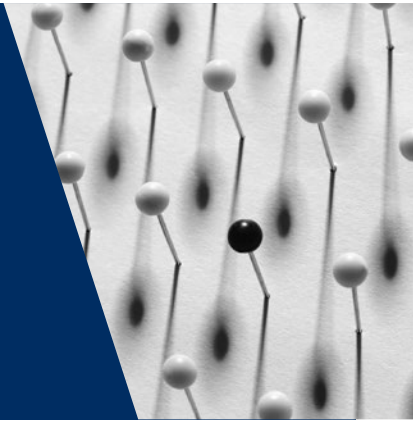
Scarlet Extended SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, 24. november 2011
(Informacijska družba; avtorska pravica; internet; programska oprema „peer-to-peer"; ponudniki internetnih storitev; vzpostavitev sistema za filtriranje elektronskih komunikacij z namenom preprečitve izmenjave datotek, ki pomeni kršitev avtorske pravice; neobstoj splošne obveznosti nadzora informacij, ki se prenašajo)

Tele2 (Netherlands) BV in drugi proti Autoriteit Consument en Markt (ACM), C-536/15, 15. marec 2017
(Načelo prepovedi diskriminacije; dajanje na razpolago osebnih podatkov o naročnikih za namene zagotavljanja javno dostopnih telefonskih imeniških storitev in imenikov; soglasje naročnika; razlikovanje glede na državo članico, v kateri se opravljajo storitve zagotavljanja javno dostopnih telefonskih imeniških storitev in imenikov)

Tele2 Sverige AB proti Post- och telestyrelsen in *Secretary of State for the Home Department proti Tomu Watsonu in drugim* (veliki senat), združeni zadevi C-203/15 in C-698/15, 21. december 2016
(Zaupnost elektronskih komunikacij; ponudniki elektronskih komunikacijskih storitev; obveznost splošne in neselektivne hrambe podatkov o prometu in lokaciji; neobstoj predhodnega nadzora s strani sodišča ali neodvisnega upravnega organa; Listina Evropske unije o temeljnih pravicah; združljivost s pravom EU)

Pasquale Foglia proti Marielli Novello (št. 2), C-244/80, 16. december 1981

Kazenski postopek proti Gasparinijuin drugim, C-467/04, 28. september 2006



Kazalo zadev

Sodna praksa Sodišča Evropske unije

Sodna praksa Evropskega sodišča za človekove pravice

Sodna praksa nacionalnih sodišč

Veliko informacij o Agenciji Evropske unije za temeljne pravice je na voljo na spletu. Do njih je mogoče dostopati na njenem spletišču fra.europa.eu.

Dodatne informacije v zvezi s sodno prakso Evropskega sodišča za človekove pravice so na voljo na njegovem spletišču: echr.coe.int. Iskalnik HUDOC omogoča dostop do sodnih odločb in sklepov v angleškem in/ali francoskem jeziku, prevodov v nekatere druge jezike, mesečnih poročil o sodni praksi, sporočil za javnost in drugih informacij o delu sodišča.

Kako do publikacij Sveta Evrope

Založništvo Sveta Evrope deluje na vseh področjih organizacije, vključno s človekovimi pravicami, pravnimi znanostmi, zdravjem, etiko, socialnimi zadevami, okoljem, izobraževanjem, kulturo, športom, mladino in arhitekturno dediščino. Knjige in elektronske publikacije iz obsežnega kataloga lahko naročite na spletu (http://book.coe.int/).

Virtualna bralnica uporabnikom omogoča brezplačen dostop do odlomkov iz pravkar objavljenih glavnih publikacij ali do celotnih besedil nekaterih uradnih dokumentov.

Informacije o konvencijah Sveta Evrope in njihovo polno besedilo je na voljo na spletišču Urada za mednarodne pogodbe: http://conventions.coe.int/.

Stik z EU

Osebno

Po vsej Evropski uniji je na stotine informacijskih točk Europe Direct. Naslov najbližje lahko najdete na spletni strani: https://europa.eu/european-union/contact_sl.

Po telefonu ali elektronski pošti

Europe Direct je služba, ki odgovarja na vaša vprašanja o Evropski uniji. Nanjo se lahko obrnete:
— s klicem na brezplačno telefonsko številko: 00 800 6 7 8 9 10 11 (nekateri ponudniki lahko klic zaračunajo),
— s klicem na navadno telefonsko številko: +32 22999696 ali
— po elektronski pošti s spletne strani: https://europa.eu/european-union/contact_sl.

Iskanje informacij o EU

Na spletu

Informacije o Evropski uniji v vseh uradnih jezikih EU so na voljo na spletišču Europa: https://europa.eu/european-union/index_sl.

Publikacije EU

Brezplačne in plačljive publikacije EU lahko prenesete s https://op.europa.eu/sl/publications ali jih tam naročite. Za več izvodov brezplačnih publikacij se obrnite na Europe Direct ali najbližjo informacijsko točko (https://europa.eu/european-union/contact_sl).

Zakonodaja EU in drugi dokumenti

Do pravnih informacij EU, vključno z vso zakonodajo EU od leta 1951 v vseh uradnih jezikovnih različicah, lahko dostopate na spletišču EUR-Lex: http://eur-lex.europa.eu.

Odprti podatki EU

Do podatkovnih zbirk EU lahko dostopate na portalu odprtih podatkov EU (http://data.europa.eu/euodp/sl). Podatke lahko brezplačno prenesete in uporabite tudi v komercialne namene.

doi:10.2811/972846 TK-05-17-225-SI-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Hiter razvoj informacijske tehnologije stopnjuje potrebo po trdnem varstvu osebnih podatkov, kar je pravica, ki je zaščitena z instrumenti Evropske unije (EU) in Sveta Evrope. Varovanje te pomembne pravice prinaša nove in pomembne izzive, saj se s tehnološkim napredkom širijo meje področij, kot so nadzor, prestrezanje komunikacij in shranjevanje podatkov. Ta priročnik je bil oblikovan, da bi delavce v pravni stroki, ki niso specializirani za varstvo osebnih podatkov, seznanil s tem nastajajočim področjem prava. V njem je na voljo pregled veljavnih pravnih okvirov EU in Sveta Evrope. Vključuje tudi pojasnila ključne sodne prakse ter povzema pomembne odločbe Sodišča Evropske unije in Evropskega sodišča za človekove pravice. Poleg tega so v njem predstavljeni hipotetični scenariji za praktično ponazoritev različnih vprašanj, ki se pojavljajo na tem razvijajočem se področju.

FRA – AGENCIJA EVROPSKE UNIJE ZA TEMELJNE PRAVICE
Schwarzenbergplatz 11 – 1040 Dunaj – Avstrija
Tel. +43 158030-0 – Faks +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EVROPSKO SODIŠČE ZA ČLOVEKOVE PRAVICE
SVET EVROPE
67075 Strasbourg Cedex – Francija
Tel. +33 388412018 – Faks +33 388412730
echr.coe.int – publishing@echr.coe.int – twitter.com/ECHR_CEDH

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV
Rue Wiertz 60 – 1047 Bruselj – Belgija
Tel. +32 22831900
edps.europa.eu – edps@edps.europa.eu – twitter.com/EU_EDPS

Urad za publikacije Evropske unije

ISBN 978-92-871-9815-0 (Svet Evrope)
ISBN 978-92-9474-785-3 (FRA)