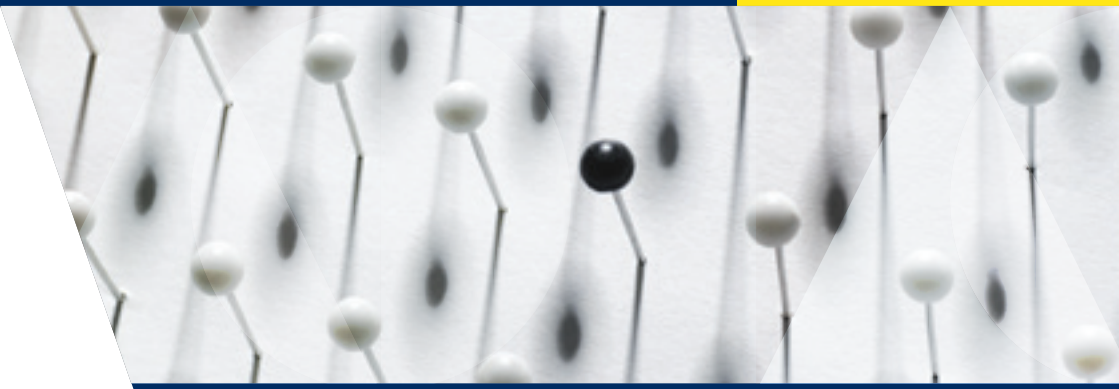
PRIROČNIK



# Priročnik o evropskem pravu varstva osebnih podatkov

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

Rokopis tega priročnika je bil dokončan aprila 2014.
Posodobitve bodo v prihodnje na voljo na spletišču Agencije Evropske unije za temeljne pravice (FRA) na spletnem naslovu fra.europa.eu, na spletišču Sveta Evrope na spletnem naslovu coe.int/dataprotection in na spletišču Evropskega sodišča za človekove pravice v meniju Sodna praksa na spletnem naslovu echr.coe.int.



***Europe Direct je služba za pomoč pri iskanju odgovorov na vprašanja v zvezi z Evropsko unijo.***

**Brezplačna telefonska številka (*):**

**00 800 6 7 8 9 10 11**

(*) Informacije so brezplačne, kakor tudi večina klicev (nekateri operaterji, telefonske govorilnice ali hoteli lahko klic zaračunajo).

Fotografija (naslovnica in notranja stran): © iStockphoto

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

Kataloški podatki so navedeni na koncu te publikacije.

Luxembourg: Urad za publikacije Evropske unije, 2014

ISBN 978-92-871-9936-2 (Svet Evrope)
ISBN 978-92-9239-341-0 (FRA)
doi:10.2811/55931

*Printed in Belgium*

TISKANO NA PAPIRJU, RECIKLIRANEM BREZ KLORA (PCF)


Priročnik je bil pripravljen v angleščini. Svet Evrope (SE) in Evropsko sodišče za človekove pravice (ESČP) ne prevzemata odgovornosti za kakovost prevodov v druge jezike. Stališča, izražena v tem priročniku, za SE in ESČP niso zavezujoča. Priročnik vsebuje sklicevanja na izbrane razlage in druge priročnike. SE in ESČP ne prevzemata odgovornosti za njihovo vsebino, poleg tega pa njihova vključitev na ta seznam ne pomeni, da jih je potrdil. Več publikacij je navedenih na spletnih straneh digitalne knjižnice ESČP na spletnem naslovu: echr.coe.int.

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

# Priročnik o evropskem pravu varstva osebnih podatkov

# Predgovor

Priročnik o evropskem pravu varstva osebnih podatkov sta skupaj pripravila Agencija Evropske unije za temeljne pravice (FRA) in Svet Evrope v sodelovanju s sodno pisarno Evropskega sodišča za človekove pravice. Je tretji v seriji pravnih priročnikov, ki sta jih skupaj pripravila ti dve organizaciji. Marca 2011 je bil objavljen prvi priročnik o evropskem pravu o nediskriminaciji,junija 2013 pa še drugi priročnik o evropskem pravu v zvezi z azilom, mejami in priseljevanjem.

Odločili smo se, da sodelovanje nadaljujemo z zelo aktualno temo, ki vsak dan vpliva na vse nas, to je varstvo osebnih podatkov. Evropa ima na tem področju enega od najbolj zaščitnih sistemov, ki temelji na Konvenciji Sveta Evrope št. 108, instrumentih Evropske unije ter na sodni praksi Evropskega sodišča za človekove pravice in Sodišča Evropske unije.

Namen tega priročnika je povečati ozaveščenost in izboljšati poznavanje pravil o varstvu osebnih podatkov v državah članicah Evropske unije in Sveta Evrope, da bi ga lahko bralci uporabljali kot glavno referenčno točko. Namenjen je nespecializiranim pravosodnim delavcem, sodnikom, nacionalnim organom za varstvo osebnih podatkov in drugim osebam, ki delajo na področju varstva osebnih podatkov.

Z začetkom veljavnosti Lizbonske pogodbe decembra 2009 je Listina Evropske unije o temeljnih pravicah postala pravno zavezujoča, pravica do varstva osebnih podatkov pa je tako dobila status samostojne temeljne pravice. Za varstvo te temeljne pravice je ključnega pomena boljše razumevanje Konvencije Sveta Evrope št. 108 in instrumentov Evropske unije (EU), ki so utrli pot varstvu podatkov v Evropi, ter sodne prakse Sodišča Evropske unije in Evropskega sodišča za človekove pravice.

Za pomoč pri pripravi priročnika bi se radi zahvalili Ludwig Boltzmann inštitutu. Zahvaljujemo pa se tudi uradu Evropskega nadzornika za varstvo podatkov za njihov prispevek pri njegovem snovanju. Za pomoč pri pripravi priročnika bi se radi zlasti zahvalili oddelku Evropske komisije za varstvo podatkov.Zahvalo želimo izraziti tudi Informacijskemu pooblaščencu Republike Slovenije za strokovni pregled prevedenega besedila Priročnika v slovenščino.

**Philippe Boillat**

Generalni direktor za človekove pravice in pravno državo Sveta Evrope

**Morten Kjaerum**

Direktor Agencije Evropske unije za temeljne pravice

# Kazalo

# Okrajšave in kratice

| | |
|---|---|
| **BCR** | Zavezujoče poslovno pravilo |
| **CCTV** | Televizija zaprtega kroga (videonadzor) |
| **CETS** | Zbirka pogodb Sveta Evrope |
| **CIS** | Carinski informacijski sistem |
| **CRM** | Upravljanje odnosov s strankami |
| **C-SIS** | Centralni schengenski informacijski sistem |
| **EFTA** | Evropsko združenje za prosto trgovino |
| **EGP** | Evropski gospodarski prostor |
| **EKČP** | Evropska konvencija o človekovih pravicah |
| **ENISA** | Evropska agencija za varnost omrežij in informacij |
| **ENP** | Evropski nalog za prijetje |
| **ENU** | Nacionalna enota Europola |
| **ENVP** | Evropski nadzornik 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 obsežne informacijske sisteme |
| **EuroPriSe** | Evropski pečat zaupnosti |
| **FRA** | Agencija Evropske unije za temeljne pravice |
| **GPS** | Globalni sistem za določanje položaja |
| **JSB** | Skupni nadzorni organ |
| **Konvencija št. 108** | Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Svet Evrope) |

| | |
|---|---|
| **Listina** | Listina Evropske unije o temeljnih 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 o človekovih pravicah |
| **SE** | Svet Evrope |
| **SEPA** | Enotno območje plačil v eurih |
| **SEU** | Sodišče Evropske unije (pred decembrom 2009 se je imenovalo Sodišče Evropskih skupnosti, SES) |
| **SIS** | Schengenski informacijski sistem |
| **SWIFT** | Združenje za svetovne finančne telekomunikacije med bankami |
| **VIS** | Vizumski informacijski sistem |
| **ZN** | Združeni narodi |

# Kako uporabljati priročnik

Priročnik vsebuje pregled zakonodaje na področju varstva podatkov v zvezi z Evropsko unijo (EU) in Svetom Evrope.

Namenjen je delavcem v pravni stroki, ki niso specializirani za varstvo osebnih podatkov; uporabljali naj bi ga odvetniki, sodniki in drugi pravosodni delavci, pa tudi uslužbenci drugih organov, vključno z nevladnimi organizacijami (NVO), ki se lahko srečujejo s pravnimi vprašanji, povezanimi z varstvom osebnih podatkov.

Priročnik je prva referenčna točka v zvezi s pravom EU in Evropsko konvencijo o človekovih pravicah (EKČP) o varstvu osebnih podatkov, v njem pa je pojasnjeno, kako je to področje urejeno s pravom EU in EKČP ter Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108) in drugimi instrumenti Sveta Evrope. Vsako poglavje najprej vsebuje enotno preglednico veljavnih zakonskih določb, vključno z izborom pomembne sodne prakse v okviru obeh ločenih evropskih pravnih sistemov. Zadevni zakoni obeh evropskih pravnih redov so nato predstavljeni po vrstnem redu, kot se uporabljajo na posameznem področju. Bralec tako lahko vidi, v čem oba pravna sistema sovpadata in v čem se razlikujeta.

V preglednicah na začetku vsakega poglavja so navedene teme, obravnavane v njem, ter veljavne pravne določbe in drugo pomembno gradivo, kot je na primer sodna praksa. Zaradi jedrnate predstavitve vsebine poglavja se lahko vrstni red tem nekoliko razlikuje od zgradbe besedila poglavja. V preglednicah sta zajeta pravo Sveta Evrope in pravo EU. Uporabniki naj bi tako lažje poiskali ključne informacije, ki se nanašajo na njihov primer, zlasti če se zanje uporablja samo pravo Sveta Evrope.

Za delavce v pravni stroki iz držav, ki niso članice EU, vendar so članice Sveta Evrope ter podpisnice EKČP in Konvencije št. 108, so informacije v zvezi z njihovo državo navedene v razdelkih, ki se nanašajo na Svet Evrope. Delavci v pravni stroki iz držav članic EU bodo morali uporabiti oba razdelka, saj sta za te države zavezujoča oba pravna reda. Za vse, ki o določeni temi potrebujejo več informacij, je v razdelku z naslovom „Dodatna literatura“ naveden seznam virov bolj specializiranega gradiva.

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

Pravo EU izhaja iz sprejetih zakonodajnih ukrepov, zadevnih določb Pogodb in Listine Evropske unije o temeljnih pravicah, kot se razlagajo v sodni praksi Sodišča Evropske unije (Sodišče EU, ki se je pred letom 2009 imenovalo Sodišče Evropskih skupnosti (SES)).

Sodna praksa, opisana ali navedena v tem priročniku, vključuje primere iz obsežnega korpusa sodne prakse ESČP in Sodišča EU. S smernicami na koncu tega priročnika naj bi si bralec pomagal pri iskanju sodne prakse na spletu.

Poleg tega so v besedilnih poljih navedene praktične ponazoritve hipotetičnih scenarijev za dodatno ponazoritev izvajanja evropskih pravil za varstvo podatkov v praksi, zlasti če za zadevno temo ni na voljo posebna sodna praksa ESČP ali Sodišča EU.

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

- izrazi s področja varstva osebnih podatkov;
- ključna načela evropskega prava o varstvu osebnih podatkov;
- pravila evropskega prava o varstvu osebnih podatkov;
- pravice posameznikov, na katere se nanašajo osebni podatki, in njihovo uveljavljanje;
- čezmejni prenos osebnih podatkov;
- varstvo osebnih podatkov v okviru policije in kazenskega pravosodja;
- druga posebna evropska zakonodaja o varstvu osebnih podatkov.

# 1

# Okvir in ozadje evropskega prava o varstvu osebnih podatkov

| EU | Obravnavane teme | Svet Evrope |
|---|---|---|
| **Pravica do varstva osebnih podatkov** | | |
| Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (*Direktiva o varstvu osebnih podatkov*), UL 1995, L 281 | | EKČP, člen 8 (pravica do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja)<br>Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108) |
| **Uravnoteženje pravic** | | |
| Sodba Sodišča EU v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, in, 2010 | **Splošno** | |
| Sodba Sodišča EU v zadevi *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy in Satamedia Oy*, C-73/07, 2008 | **Svoboda izražanja** | Sodba ESČP v zadevi *Axel Springer AG proti Nemčiji*, 2012<br>Sodba ESČP v zadevi *Mosley proti Združenemu kraljestvu*, 2011 |
| | **Svoboda umetnosti in znanosti** | Sodba ESČP v zadevi *Vereinigung bildender Künstler proti Avstriji*, 2007 |
| Sodba Sodišča EU v zadevi *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, C-275/06, 2008 | **Varstvo lastnine** | |
| Sodba Sodišča EU v zadevi *Evropska komisija proti The Bavarian Lager Co. Ltd.*, C-28/08 P, 2010 | **Dostop do dokumentov** | Sodba ESČP v zadevi *Társaság a Szabadságjogokért proti Madžarski*, 2009 |

# 1.1. Pravica do varstva osebnih podatkov

**Ključne točke**

- 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.
- Varstvo osebnih podatkov je bilo v pravu EU prvič urejeno z Direktivo o varstvu osebnih podatkov.
- Varstvo osebnih podatkov je v pravu EU priznano kot temeljna pravica.

Pravica do varstva posameznikovega zasebnega življenja pred vmešavanjem drugih, zlasti države, je bila v mednarodnem pravnem instrumentu prvič določena v členu 12 Splošne deklaracije o človekovih pravicah (SDČP) Združenih narodov (ZN) iz leta 1948, ki se je nanašal na spoštovanje zasebnega in družinskega življenja.[1] SDČP je vplivala na razvoj drugih instrumentov o človekovih pravicah v Evropi.

## 1.1.1. Evropska konvencija o človekovih pravicah

Svet Evrope je bil ustanovljen v obdobju po drugi svetovni vojni, da bi združil 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.

Države 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.

Za zagotovitev, da pogodbenice izpolnjujejo svoje obveznosti na podlagi EKČP, je bilo leta 1959 v Strasbourgu v Franciji ustanovljeno Evropsko sodišče za človekove pravice (ESČP). ESČP 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. Svet Evrope je leta 2013 sestavljalo 47 držav članic, od tega jih je bilo 28 tudi držav članic EU. Ni

1 Združeni narodi (ZN), Splošna deklaracija o človekovih pravicah z dne 10. decembra 1948.

nujno, da je pritožnik pred ESČP državljan ene od držav članic. ESČP obravnava tudi meddržavne zadeve, ki jih ena ali več držav članic Sveta Evrope sproži zoper drugo državo članico.

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.[2]

ESČP je v svoji sodni praksi obravnavalo že veliko zadev, ki so se nanašale na vprašanje varstva osebnih podatkov, zlasti v zvezi s prestrezanjem komunikacij[3], različnimi oblikami nadzora[4] in varstvom pred hrambo osebnih podatkov s strani javnih organov.[5] Pojasnilo je, da se morajo države na podlagi člena 8 EKČP ne samo vzdržati ukrepov, s katerimi bi lahko bila kršena ta pravica iz Konvencije, ampak so jim v nekaterih okoliščinah naložene tudi pozitivne obveznosti, da dejavno zagotovijo učinkovito spoštovanje zasebnega in družinskega življenja.[6] Veliko teh zadev bo podrobneje obravnavanih v ustreznih poglavjih.

## 1.1.2. 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.[7] Leta 1981 je bila na voljo za podpis Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov

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

3 Glej na primer sodbi ESČP z dne 2. avgusta 1984 v zadevi *Malone proti Združenemu kraljestvu*, pritožba št. 8691/79, in z dne 3. aprila 2007 v zadevi *Copland proti Združenemu kraljestvu*, pritožba št. 62617/00.

4 Glej na primer sodbi ESČP z dne 6 septembra 1978 v zadevi *Klass in drugi proti Nemčiji*, pritožba št. 5029/71, in z dne 2 septembra 2010 v zadevi *Uzun proti Nemčiji*, pritožba št. 35623/05.

5 Glej na primer sodbi ESČP z dne 26 marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81, in z dne 4. decembra 2008 v zadevi *S. in Marper proti Združenemu kraljestvu*, pritožbi št 30562/04 in 30566/04.

6 Glej na primer sodbi ESČP z dne 17. julija 2008 v zadevi *I. proti Finski*, pritožba št. 20511/03, in z dne 2. decembra 2008 v zadevi *K. U. proti Finski*, pritožba št. 2872/02.

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

(Konvencija št. 108).[8] 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 v javnem sektorju, kot je obdelava osebnih podatkov v pravosodju in policiji. Posameznike varuje pred zlorabami, ki lahko spremljajo zbiranje in obdelavo osebnih podatkov, hkrati pa naj bi bil z njo urejen tudi čezmejni prenos osebnih podatkov. Kar zadeva zbiranje in 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 in niso namenjeni uporabi, ki ni v skladu s temi nameni, niti se ne hranijo dlje, kot je potrebno. Nanašajo se tudi na kakovost osebnih podatkov, ki morajo biti primerni, ustrezni in ne pretirani (sorazmernost) ter točni.

Konvencija določa jamstva glede zbiranja in obdelave osebnih podatkov, hkrati pa je z njo tudi prepovedana (če ni ustreznih zakonskih zaščitnih ukrepov) obdelava „občutljivih" podatkov o osebi, na primer o njeni rasi, političnem prepričanju, zdravju, verski pripadnosti, 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.

Čeprav Konvencija določa prosti prenos osebnih podatkov med državami, ki so njene pogodbenice, pa so z njo naložene tudi nekatere omejitve tega prenosa v države, katerih pravna ureditev ne zagotavlja ustreznega varstva.

Da bi natančneje izoblikovali splošna načela in pravila, določena v Konvenciji št. 108, je Odbor ministrov Sveta Evrope sprejel več priporočil, ki pa niso pravno zavezujoča (glej poglavji 7 in 8).

Konvencijo št. 108 so ratificirale vse države članice EU. Leta 1999 je bila spremenjena tako, da je lahko pogodbenica postala tudi EU.[9] Leta 2001 je bil sprejet Dodatni

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

9 Svet Evrope, Spremembe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (ETS št. 108), ki jih je Odbor ministrov sprejel v Strasbourgu 15. junija 1999 in ki Evropskim skupnostim dovoljujejo, da pristopijo k spremenjeni Konvenciji št. 108 (člen 23(2)).

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.[10]

### Obeti

Po odločitvi za posodobitev Konvencije št. 108 je javno posvetovanje, izvedeno leta 2011, omogočilo, da sta bila potrjena oba glavna cilja posodobitve: okrepiti varstvo zasebnosti v digitalni dobi in utrditi mehanizem spremljanja na podlagi Konvencije.

H Konvenciji št. 108 lahko pristopijo tudi države, ki niso članice Sveta Evrope, vključno z neevropskimi državami. Možnost, da se Konvencija uveljavi kot splošni standard, in njena odprtost bi lahko bili podlaga za spodbujanje varstva osebnih podatkov na svetovni ravni.

Za zdaj je 45 od 46 pogodbenic Konvencije št. 108 tudi držav članic Sveta Evrope. Urugvaj, prva neevropska država, je h Konvenciji št. 108 pristopil avgusta 2013, Maroko, ki ga je k pristopu povabil Odbor ministrov, pa je v postopku formaliziranja pristopa.

## 1.1.3. Pravo Evropske unije o varstvu osebnih podatkov

Pravo EU sestavljajo Pogodbi in sekundarna zakonodaja EU. Pogodbi, in sicer Pogodbo o Evropski uniji (PEU) in Pogodbo o delovanju Evropske unije (PDEU), so potrdile vse države članice EU in se imenujeta tudi „primarna zakonodaja EU“. Uredbe, direktive in sklepe EU sprejemajo institucije EU, ki so tako pristojnost dobile na podlagi Pogodb; ti dokumenti se pogosto imenujejo „sekundarna zakonodaja EU“.

Najpomembnejši pravni instrument EU o varstvu osebnih podatkov je 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*).[11] Sprejeta je bila leta 1995, ko je več držav članic že sprejelo nacionalne zakone o varstvu osebnih podatkov. Za prosti pretok

10 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.

11 Direktiva o varstvu osebnih podatkov, UL 1995, L 281, str. 31.

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.

Ker je bil cilj sprejetja Direktive o varstvu osebnih podatkov uskladitev[12] zakonodaje o varstvu osebnih podatkov na nacionalni ravni, je podobno natančna kot (takrat) veljavni nacionalni zakoni o varstvu teh podatkov. Za SEU »je namen Direktive 95/46 (...) zagotoviti, da je raven varstva pravic in svoboščin v zvezi z obdelavo osebnih podatkov ustrezna v vseh državah članicah. (...) Približevanje nacionalne zakonodaje na tem področju se ne sme odražati v zniževanju zaščite, temveč mora nasprotno, stremeti k visoki ravni varstva v EU. Zato (...) harmonizacija teh nacionalnih zakonov ne more biti omejena na izpolnjevanje minimuma zahtev, temveč mora biti celovita. Zaradi tega države članice nimajo popolnoma prostih rok pri njenem izvajanju.[13]

Namen Direktive o varstvu osebnih podatkov je uresničiti načela v zvezi s pravico do zasebnosti, ki jih je vsebovala že Konvencija št. 108, in jih razširiti. Ker je bilo vseh 15 držav članic EU leta 1995 tudi pogodbenic Konvencije št. 108, je bila izključena možnost, da bi bila v obeh pravnih instrumentih sprejeta nasprotujoča si pravila. Vendar navedena direktiva izhaja iz možnosti iz člena 11 Konvencije št. 108, da se dodajo novi instrumenti varstva. Zlasti uvedba neodvisnega nadzora kot instrumenta za izboljšanje upoštevanja pravil o varstvu osebnih podatkov se je izkazala za pomemben prispevek k učinkovitemu delovanju evropske zakonodaje o varstvu osebnih podatkov. (Ta značilnost je bila zato v pravo Sveta Evrope leta 2001 prevzeta z Dodatnim protokolom h Konvenciji št. 108.)

Ozemeljska uporaba Direktive o varstvu osebnih podatkov ne zajema samo 28 držav članic EU, temveč vključuje tudi države, ki niso članice EU, vendar so del Evropskega gospodarskega prostora (EGS)[14] – in sicer Islandijo, Lihtenštajn in Norveško.

Sodišče EU v Luxembourgu je pristojno za ugotavljanje, ali je država članica izpolnila obveznosti na podlagi Direktive o varstvu osebnih podatkov, ter predhodno odločanje o njeni veljavnosti in razlagi, da se zagotovi njena učinkovita in enotna uporaba v državah članicah. Pomembna izjema glede uporabe navedene direktive je t. i. izjema

12 Glej na primer Direktivo o varstvu osebnih podatkov, uvodne izjave 1, 4, 7 in 8.

13 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) v. Administración del Estado*, 24 November 2011, para. 28-29.

14 Sporazum o Evropskem gospodarskem prostoru, UL 1994, L 1, ki je začel veljati 1. januarja 1994.

obdelave za domače potrebe, in sicer obdelava osebnih podatkov, ki jo fizične osebe izvajajo za izključno osebn ali domačepotrebe.[15] Taka obdelava se na splošno pojmuje kot sestavni del svoboščin posameznika.

V skladu s primarno zakonodajo EU, ki se je uporabljala ob sprejetju Direktive o varstvu osebnih podatkov, je vsebinsko področje njene uporabe omejeno na zadeve, povezane z notranjim trgom. Zunaj njenega področja uporabe so, kar je najpomembneje, zadeve s področja policijskega in pravosodnega sodelovanja v kazenskih zadevah. Varstvo osebnih podatkov v teh zadevah temelji na drugih pravnih instrumentih, ki so podrobno opisani v poglavju 7.

Ker so lahko bile naslovnice Direktive o varstvu osebnih podatkov samo 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*).[16]

Poleg tega so celo na področjih, zajetih z Direktivo o varstvu osebnih podatkov, pogosto potrebne natančnejše določbe o varstvu podatkov, da bi se dosegla potrebna jasnost pri uravnoteženju drugih zakonitih interesov. Taka primera sta Direktiva 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (*Direktiva o zasebnosti in elektronskih komunikacijah*)[17] in Direktiva 2006/24/ES 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 (*Direktiva o hrambi podatkov,* ki je bila razveljavljena 8. aprila 2014).[18] Drugi primeri bodo obravnavani v poglavju 8. Take določbe morajo biti v skladu z Direktivo o varstvu osebnih podatkov.

15 Direktiva o varstvu osebnih podatkov, člen 3(2), druga alinea.

16 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 2001, L 8.

17 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 2002, L 201.

18 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 (*Direktiva o hrambi podatkov*), UL 2006, L 105, razveljavljena 8. Aprila 2014.

## Listina Evropske unije o temeljnih pravicah

Prvotne pogodbe Evropskih skupnosti niso vsebovale sklicevanja na človekove pravice ali njihovo varstvo. Ko pa so bile tedanjemu Sodišču Evropskih skupnosti (SES) predložene zadeve, v katerih so stranke zatrjevale, da so jim bile kršene človekove pravice na področjih, zajetih s pravom EU, se je razvil nov pristop. Da bi se posameznikom zagotovilo varstvo, so bile temeljne pravice vključene med t. i. splošna načela evropskega prava. Po mnenju Sodišča EU se v teh splošnih načelih izraža vsebina varstva človekovih pravic, ki je vključena v nacionalne ustave in pogodbe o človekovih pravicah, zlasti EKČP. Sodišče EU 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 listina 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.

Čeprav je bila Listina prvotno samo politični dokument, je kot primarna zakonodaja EU (glej člen 6(1) PEU) postala pravno zavezujoča[19] z začetkom veljavnosti Lizbonske pogodbe 1. decembra 2009.[20]

Primarna zakonodaja EU vključuje tudi splošno pristojnost EU za sprejemanje zakonov o zadevah v zvezi z varstvom osebnih podatkov (člen 16 PDEU).

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

19 EU (2012), Listina Evropske unije o temeljnih pravicah, UL 2012, C 326.

20 Glej prečiščeni različici pogodb o Evropskih skupnostih (2012), Pogodbe o Evropski uniji, UL 2012, C 326, in Pogodbe o delovanju Evropske unije (2012), UL 2012, C 326.

v členu 8(1), ampak je v členu 8(2) navedeno tudi sklicevanje na ključna načela varstva osebnih podatkov. Nazadnje, s členom 8(3) Listine je zagotovljeno, da bo izvajanje navedenih načel nadzoroval neodvisni organ.

### Obeti

Evropska komisija je januarja 2012 predlagala sveženj reform varstva osebnih podatkov, pri čemer je navedla, da je treba veljavna pravila o varstvu osebnih podatkov posodobiti ob upoštevanju hitrega tehnološkega razvoja in globalizacije. Sveženj reform sestavljata predlog Splošne uredbe o varstvu osebnih podatkov[21], ki naj bi nadomestila Direktivo o varstvu osebnih podatkov, in nova direktiva o varstvu osebnih podatkov[22], ki bo določala varstvo teh podatkov na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah. Ob objavi tega priročnika je razprava o svežnju reform še potekala.

## 1.2. Uravnoteženje pravic

### Ključne točke

- Pravica do varstva osebnih podatkov ni absolutna pravica; uravnotežiti jo je treba z drugimi pravicami.

Temeljna pravica do varstva osebnih podatkov na podlagi člena 8 Listine „ni absolutna, temveč jo je treba obravnavati glede na vlogo, ki jo ima v družbi“.[23] Na podlagi člena 52(1) Listine je tako dovoljeno uvesti omejitve uresničevanja pravic, določenih v členih 7 in 8 Listine, če so te omejitve predpisane z zakonom, spoštujejo bistveno vsebino pravic in svoboščin ter so ob upoštevanju načela sorazmernosti potrebne in dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Evropska unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.[24]

21 Evropska komisija (2012), predlog Uredbe Evropskega parlamenta in Sveta z dne 25. januarja 2012 o varstvu posameznikov v zvezi z obdelavo osebnih podatkov in prostem pretoku takih podatkov (*Splošna uredba o varstvu podatkov*), COM(2012) 11 final, Bruselj.

22 Evropska komisija (2012), predlog Direktive Evropskega parlamenta in Sveta z dne 25. januarja 2012 o varstvu posameznikov v zvezi z obdelavo osebnih podatkov, ki jo pristojni organi izvajajo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazni, in prostim pretokom takih podatkov (*Splošna direktiva o varstvu podatkov*), COM(2012) 10 final, Bruselj.

23 Glej na primer sodbo Sodišča EU z dne 9. novembra 2010 v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, točka 48.

24 Prav tam, točka 50.

Varstvo osebnih podatkov je v ureditvi na podlagi EKČP zagotovljeno s členom 8 (pravica do spoštovanja zasebnega in družinskega življenja), pri čemer je treba to pravico, tako kot v ureditvi na podlagi Listine, izvajati ob upoštevanju področja uporabe drugih povezanih pravic. V skladu s členom 8(2) EKČP se „[j]avna oblast [...] ne sme vmešavati v izvrševanje te pravice, razen [...] če je to določeno z zakonom in nujno v demokratični družbi[,] [...] da se zavarujejo pravice in svoboščine drugih ljudi".

ESČP in Sodišče EU sta tako že večkrat navedli, da je pri uporabi in razlagi člena 8 EKČP in člena 8 Listine nujno uravnoteženje z drugimi pravicami.[25] Kako to ravnotežje doseči, bo ponazorjeno z več ključnimi primeri.

## 1.2.1. Svoboda izražanja

Ena od pravic, ki bi lahko bile v navzkrižju 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". Člen 11 ustreza členu 10 EKČP. V skladu s členom 52(3) Listine, če ta vsebuje pravice, ki ustrezajo pravicam, zagotovljenim z EKČP, „sta 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, to pomeni, da morajo biti določene z zakonom in nujne v demokratični družbi „[...] za varovanje ugleda ali pravic drugih ljudi". S tem pojmom je zajeta pravica do varstva osebnih podatkov.

Razmerje med varstvom osebnih podatkov in svobodo izražanja je urejeno s členom 9 Direktive o varstvu osebnih podatkov z naslovom „Obdelava osebnih

25 Sodba ESČP z dne 7. februarja 2012 v združenih zadevah *Von Hannover proti Nemčiji (št. 2)* [veliki senat], pritožbi št. 40660/08 in 60641/08; sodbi Sodišča EU z dne 24. novembra 2011 v združenih zadevah *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, C-468/10 in C-469/10, točka 48, in z dne 29. januarja 2008 v zadevi *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, C-275/06, točka 68. Glej tudi Svet Evrope (2013), Sodna praksa Evropskega sodišča za človekove pravice v zvezi z varstvom osebnih podatkov, DP (2013) Sodna praksa, ki je na voljo na: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

podatkov in svoboda izražanja".[26] Ta člen določa, da morajo države članice opredeliti določene izjeme in omejitve varstva osebnih podatkov in torej temeljne pravice do zasebnosti, določene v poglavjih II, IV in VI te direktive. Te izjeme je treba določiti zgolj v novinarske namene ali zaradi umetniškega ali literarnega izražanja, ki spadajo pod temeljno pravico do svobode izražanja, le če so potrebne za uskladitev pravice do zasebnosti s predpisi, ki urejajo svobodo izražanja.

Primer: Sodišče EU je bilo v zadevi *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy in Satamedia Oy*[27] pozvano, naj razloži člen 9 Direktive o varstvu osebnih podatkov in opredeli razmerje med varstvom osebnih podatkov in svobodo tiska. Obravnavati je moralo družbi Markkinapörssi in Satamedia, ki sta razširjali davčne podatke o približno 1,2 milijona fizičnih osebah, zakonito pridobljene od finskih davčnih organov. Sodišče 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 fizičnih osebah, šteti za dejavnost, ki se izvaja zgolj v novinarske namene. Sodišče je najprej ugotovilo, da se dejavnosti družbe Satakunnan štejejo za „obdelavo osebnih podatkov" v smislu člena 3(1) Direktive o varstvu osebnih podatkov, nato pa je razložilo člen 9 navedene direktive. 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 novinarstvo, 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 nujno. Sodišče je v teh okoliščinah ugotovilo, da je mogoče dejavnosti, ki sta jih družbi Markkinapörssi in Satamedia 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 za prenos. Razsodilo 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 v obravnavani zadevi.

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

26 Direktiva o varstvu osebnih podatkov, člen 9.

27 Sodba Sodišča EU z dne 16. decembra 2008 v zadevi *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy in Satamedia Oy*, C-73/07, točke 56, 61 in 62.

Primer: ESČP je v zadevi *Axel Springer AG proti Nemčiji*[28] ugotovilo, da je nacionalno sodišče s prepovedjo, naloženo lastniku časopisa, ki je želel objaviti članek o aretaciji in obsodbi znanega igralca, kršilo člen 10 EKČP. Opozorilo je na merila, ki jih je v svoji sodni praksi določilo pri uravnoteženju pravice do svobodnega izražanja s pravico do spoštovanja zasebnega življenja:

- prvič, ali je bil dogodek, na katerega se je objavljeni članek nanašal, v splošnem interesu: aretacija in obsodba osebe je bilo javno pravno dejstvo in je bilo zato v javnem interesu;
- drugič, ali je bila zadevna oseba javna osebnost: zadevna oseba je bila igralec, ki je bil dovolj znan, da se je štel za javno osebnost, in
- tretjič, kako so bile informacije pridobljene in ali so bile zanesljive: informacije je zagotovil urad državnega tožilca, točnost informacij iz obeh objav pa med strankama ni bila sporna.

ESČP je zato razsodilo, da prepovedi objave, naložene družbi, niso bile razumno sorazmerne z zakonitim ciljem varstva pritožnikovega zasebnega življenja. Ugotovilo je, da je bil kršen člen 10 EKČP.

Primer: ESČP je v sodbi v zadevi *Von Hannover proti Nemčiji (št. 2)*[29] ugotovilo, da ni bila kršena pravica do spoštovanja zasebnega življenja na podlagi člena 8 EKČP, ko monaška princesa Caroline ni dosegla sodne prepovedi objave fotografije, na kateri je skupaj z možem na smučanju. Fotografijo je spremljal članek, v katerem se je med drugim poročalo o slabem zdravju princa Rainierja. ESČP je ugotovilo, da so nacionalna sodišča pravico založniških družb do svobodnega izražanja skrbno uravnotežila s pravico pritožnikov do spoštovanja njunega zasebnega življenja. Dejstva, da so nacionalna sodišča bolezen princa Rainierja štela za dogodek, ki je pomemben za sodobno družbo, ni bilo mogoče šteti za nerazumno dejanje in ESČP se je strinjalo, da je fotografija v povezavi s člankom vsaj deloma pripomogla k razpravi, ki je v splošnem interesu. Sodišče je ugotovilo, da člen 8 EKČP ni bil kršen.

28 Sodba ESČP z dne 7. februarja 2012 v zadevi *Axel Springer AG proti Nemčiji* [veliki senat], pritožba št. 39954/08, točki 90 in 91.

29 Sodba ESČP z dne 7. februarja 2012 v združenih zadevah *Von Hannover proti Nemčiji (št. 2)* [veliki senat], pritožbi št. 40660/08 in 60641/08, točki 118 in 124.

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

Primer: Nacionalni tednik je v zadevi *Mosley proti Združenemu kraljestvu*[30] objavil pritožnikove intimne fotografije. Ta je nato trdil, da je bil kršen člen 8 EKČP, ker pred objavo spornih fotografij ni imel možnosti zahtevati sodne prepovedi, saj časopisu ni bilo treba zagotoviti predhodnega obvestila o objavi gradiva, s katerim bi se lahko kršila posameznikova pravica do zasebnosti. Čeprav se je tako gradivo na splošno razširjalo za razvedritev in ne toliko za poučevanje, je bilo nedvomno varovano s členom 10 EKČP, tako da bi lahko obveljale zahteve iz člena 8 EKČP, če so bile informacije zasebne in intimne ter ni bilo javnega interesa za njihovo razširjanje. Vendar je bilo treba še posebno skrbno proučiti omejitve, ki bi lahko delovale kot oblika cenzure pred objavo. ESČP je glede 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 se na podlagi člena 8 EKČP ne zahteva obstoj pravno zavezujoče zahteve po predhodnem obveščanju. Sodišče je tako ugotovilo, da člen 8 EKČP ni bil kršen.

Primer: Pritožnica je v zadevi *Biriuk proti Litvi*[31] od dnevnika zahtevala odškodnino, ker je objavil članek, v katerem je poročal, da je HIV pozitivna. To so domnevno potrdili zdravniki v tamkajšnji bolnišnici. ESČP je menilo, da zadevni članek ni pripomogel k razpravi v splošnem interesu, zato je opozorilo, da je varstvo osebnih podatkov, zlasti zdravstvenih podatkov, temeljnega pomena za to, da lahko oseba uveljavlja pravico do spoštovanja zasebnega in družinskega življenja, ki je zagotovljena s členom 8 EKČP. 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. Država pritožnici tako ni zagotovila pravice do spoštovanja njenega zasebnega življenja. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

30 Sodba ESČP z dne 10. maja 2011 v zadevi *Mosley proti Združenemu kraljestvu*, pritožba št. 48009/08, točki 129 in 130.

31 Sodba ESČP z dne 25. novembra 2008 v zadevi *Biriuk proti Litvi*, pritožba št. 23373/03.

## 1.2.2. Dostop do dokumentov

S svobodo obveščanja v skladu s členom 11 Listine in členom 10 EKČP ni varovana le pravica do sporočanja informacij, ampak tudi pravica do njihovega *prejemanja*. Vse večje je zavedanje, kako pomembna je preglednost javne uprave za delovanje demokratične družbe. 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 tam registrirani sedež.

**Po pravu 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*).[32] **Po pravu EU** je pravica do dostopa do dokumentov zagotovljena z Uredbo št. 1049/2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (*Uredba o dostopu do dokumentov*).[33] S členom 42 Listine in členom 15(3) PDEU je bila ta pravica do dostopa razširjena na „dokument[e] institucij, organov, uradov in agencij Unije, ne glede na nosilec dokumenta". V skladu s členom 52(2) Listine se pravica do dostopa do dokumentov uresničuje tudi v skladu s pogoji in v mejah, opredeljenih v členu 15(3) PDEU. 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. Zahteve za dostop do dokumentov ali informacij javnih organov je morda treba zato uravnotežiti s pravico oseb, katerih podatke vsebujejo zahtevani dokumenti, do varstva osebnih podatkov.

Primer: Sodišče EU je v sodbi v zadevi *Komisija proti Bavarian Lager*[34] opredelilo obseg varstva osebnih podatkov v okviru dostopa do dokumentov institucij EU ter razmerje med uredbama št. 1049/2001 (*Uredba o dostopu do dokumentov*) in št. 45/2001 (*Uredba o varstvu podatkov*). Družba Bavarian Lager, ustanovljena leta 1992, v Združeno kraljestvo uvaža ustekleničeno nemško pivo, predvsem za pivnice in bare. Naletela pa je na težave, ker je britanska zakonodaja *de facto* bolj naklonjena nacionalnim proizvajalcem. Evropska komisija se je v

32 Svet Evrope, Odbor ministrov (2002), Priporočilo Rec(2002)2 državam članicam o dostopu do uradnih dokumentov z dne 21. februarja 2002; Svet Evrope, Konvencija o dostopu do uradnih dokumentov z dne 18. junija 2009, CETS št. 205.

33 Uredba (ES) št. 1049/2001 Evropskega parlamenta in Sveta z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije, UL 2001, L145.

34 Sodba Sodišča EU z dne 29. junija 2010 v zadevi *Evropska komisija proti The Bavarian Lager Co. Ltd.*, C-28/08 P, točke 60, 63, 76, 78 in 79.

odgovor na pritožbo družbe Bavarian Lager odločila, da bo proti Združenemu kraljestvu začela postopek 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 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. Ker družba Bavarian Lager s tem ni bila zadovoljna, je vložila tožbo pri Sodišču prve stopnje, ki je odločbo Komisije s sodbo z dne 8. novembra 2007 v zadevi *Bavarian Lager proti Komisiji* (T-194/04) razglasilo za nično, pri čemer je zlasti menilo, 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.

Sodišče EU je sodbo Sodišča prve stopnje na podlagi pritožbe Komisije razveljavilo. Ugotovilo je, da se z Uredbo o dostopu do dokumentov „uvaja posebna ureditev in krepi varstvo osebe, katere osebni podatki bi se v nekaterih primerih lahko posredovali javnosti“. Po mnenju Sodišča EU postanejo določbe Uredbe o varstvu osebnih podatkov v celoti upoštevne, če se poskuša s prošnjo na podlagi Uredbe o dostopu do dokumentov pridobiti dostop do dokumentov, ki vsebujejo osebne podatke. Sodišče EU 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.

Sodišče EU je še 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. Prav tako 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 Direktivo o varstvu osebnih podatkov.

V skladu s to sodbo je za poseganje v pravico do varstva osebnih podatkov v zvezi z dostopom do dokumentov potreben poseben in upravičen razlog. Pravica do dostopa do dokumentov ne more samodejno prevladati nad pravico do varstva osebnih podatkov.[35]

Poseben vidik prošnje za dostop je bil obravnavan v naslednji sodbi ESČP.

> Primer: V zadevi *Társaság a Szabadságjogokért proti Madžarski*[36] je pritožnik, nevladna organizacija za človekove pravice, ustavno sodišče zaprosil za dostop do informacij o še nerešeni zadevi. Ustavno sodišče je prošnjo za dostop, ne da bi se posvetovalo s poslancem, ki mu je zadevo predložil, zavrnilo z obrazložitvijo, da lahko tretje osebe pritožbe pred njim vlagajo samo z odobritvijo tožeče stranke. Nacionalna sodišča so to zavrnitev potrdila z obrazložitvijo, da nad varstvom takih osebnih podatkov ne morejo prevladati drugi zakoniti interesi, vključno z dostopnostjo javnih informacij. Pritožnik je deloval kot „družbeni nadzornik", katerega dejavnosti so upravičene do enakega varstva, kot je zagotovljeno tisku. ESČP je v zvezi s svobodo tiska dosledno razsojalo, da ima javnost pravico prejeti informacije, ki so v splošnem interesu. Informacije, ki jih je zahteval pritožnik, so bile „pripravljene in na voljo", zbiranje podatkov pa ni bilo potrebno. Država v takih okoliščinah ne bi smela ovirati prenosa informacij, ki jih je zahteval pritožnik. Skratka, ESČP je ugotovilo, da bi lahko oviranje dostopa do informacij v javnem interesu zaposlene v medijih odvračale od opravljanja ključne vloge „javnega nadzornika". Ugotovilo je, da je bil kršen člen 10 EKČP.

Pomen preglednosti (transparentnosti) je **v pravu EU** trdno ukoreninjen. Načelo preglednosti je vključeno v člena 1 in 10 PEU ter člen 15(1) PDEU.[37] V skladu z uvodno izjavo 2 Uredbe (ES) št. 1049/2001 državljanom omogoča, da tesneje sodelujejo v postopku odločanja, in zagotavlja, da je uprava deležna večje zakonitosti ter je učinkovitejša in bolj odgovorna državljanu v demokratičnem sistemu.[38]

35 Glej podrobna posvetovanja evropskega nadzornika za varstvo podatkov z dne 24. marca 2011, Dostop javnosti do dokumentov, ki vsebujejo osebne podatke, po odločitvi Sodišča v zadevi Bavarian Lager, na voljo na: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 Sodba ESČP z dne 14. aprila 2009 v zadevi *Társaság a Szabadságjogokért proti Madžarski*, pritožba št. 37374/05, glej točke 27, 36–38.

37 EU (2012), prečiščena različica Pogodbe o Evropski uniji in Pogodbe o delovanju Evropske unije, UL 2012, C 326.

38 Sodbi Sodišča EU z dne 6. marca 2003 v zadevi *Interporc Im- und Export GmbH proti Komisiji Evropskih skupnosti*, C-41/00 P, točka 39, in z dne 29. junija 2010 v zadevi *Evropska komisija proti The Bavarian Lager Co. Ltd.*, C-28/08 P, točka 54.

V skladu s tem se z Uredbo Sveta (ES) št. 1290/2005 o financiranju skupne kmetijske politike in Uredbo Komisije (ES) št. 259/2008 o podrobnih pravilih za njeno uporabo zahteva objava informacij o upravičencih do sredstev iz nekaterih skladov EU v kmetijskem sektorju in zneskih, ki jih prejme vsak upravičenec.[39] Objava bi morala prispevati k javnemu nadzoru nad tem, ali upravni organi javna sredstva uporabljajo primerno. Sorazmernost te objave je izpodbijalo več upravičencev.

Primer: Sodišče EU je moralo v združenih zadevah *Volker und Markus Schecke in Hartmut Eifert proti Land Hessen*[40] odločiti o sorazmernosti objave – zahtevane z zakonodajo EU – imen upravičencev do kmetijskih subvencij EU in zneskov, ki so jih prejeli.

Poudarilo je, 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.

Sodišče 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 vključno s povečanjem preglednosti porabe sredstev Skupnosti. Vendar je odločilo, da poimenska objava fizičnih oseb, 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. Sodišče je zato razglasilo delno ničnost zakonodaje EU o objavi informacij v zvezi z upravičenci do sredstev iz evropskih kmetijskih skladov.

## 1.2.3. Svoboda umetnosti in znanosti

Še ena pravica, ki jo je treba uravnotežiti s pravico do spoštovanja zasebnega življenja in varstva osebnih podatkov, je svoboda umetnosti in znanosti, ki je izrecno varovana s členom 13 Listine. Ta pravica je izpeljana predvsem iz pravice do svobode

39 Uredba Sveta (ES) št. 1290/2005 z dne 21. junija 2005 o financiranju skupne kmetijske politike, UL 2005, L 209, in 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 2008, L 76.

40 Sodba Sodišča EU z dne 9. novembra 2010 v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, C-92/09 in C-93/09, točke 47–52, 58, 66–67, 75, 86 in 92.

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.[41] Tudi pravica, zagotovljena s členom 13 Listine, je lahko predmet omejitev, ki so dovoljene s členom 10 EKČP.[42]

Primer: Avstrijska sodišča so v zadevi *Vereinigung bildender Künstler proti Avstriji*[43] združenju, ki je vložilo pritožbo, prepovedala nadaljnje razstavljanje slike, na kateri so bile upodobljene glave različnih javnih osebnosti v spolnih položajih. Avstrijski poslanec, katerega fotografija 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 in s tem ugodilo njegovi zahtevi. ESČP je opozorilo, da se člen 10 EKČP uporablja 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] v tej funkciji pokazati večjo strpnost do kritike“. EKČP je ob tehtanju različnih vpletenih interesov ugotovilo, da neomejena prepoved nadaljnjega razstavljanja slike ni sorazmerna. Ugotovilo je, da je bil kršen člen 10 EKČP.

Kar zadeva znanost, se evropska zakonodaja o varstvu podatkov zaveda posebne vrednosti znanosti za družbo. Splošne omejitve uporabe osebnih podatkov so zato manj stroge. Z Direktivo o varstvu osebnih podatkov in Konvencijo št. 108 je dovoljena hramba osebnih podatkov za znanstvene raziskave, tudi ko ti niso več potrebni za prvotni namen zbiranja. Poleg tega se poznejša uporaba osebnih podatkov za znanstvene raziskave ne šteje za nezdružljiv namen. Naloga nacionalnega prava je, da izoblikuje podrobnejše določbe, vključno s potrebnimi zaščitnimi ukrepi, na podlagi katerih bo mogoče interes za znanstvene raziskave uskladiti s pravico do varstva osebnih podatkov (glej tudi razdelka 3.3.3 in 8.4).

41 Sodba ESČP z dne 24. maja 1988 v zadevi *Müller in drugi proti Švici*, pritožba št. 10737/84.

42 Pojasnila k Listini o temeljnih pravicah, UL 2007, C 303.

43 Sodba ESČP z dne 25. januarja 2007 v zadevi *Vereinigung bildender Künstler proti Avstriji*, pritožba št. 68345/01, glej zlasti točki 26 in 34.

## 1.2.4. Varstvo lastnine

Pravica do varstva lastnine je vključena v člen 1 Prvega protokola k EKČP in člen 17(1) Listine. Pomemben vidik lastninske pravice 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 pojasnjeno s sodno prakso Sodišča EU, je treba varstvo temeljne lastninske pravice uravnotežiti z varstvom drugih temeljnih pravic, zlasti s pravico do varstva osebnih podatkov.[44] Institucije za varstvo avtorskih pravic so že večkrat zahtevale, naj ponudniki spletnih storitev razkrijejo identiteto uporabnikov platform za izmenjavo datotek. Take platforme uporabnikom spleta omogočajo brezplačen prenos glasbenih del, tudi če so ta zaščitena z avtorskimi pravicami.

Primer: V zadevi *Promusicae proti Telefónica de España*[45] španski ponudnik internetnega dostopa, Telefónica, združenju Promusicae, nepridobitnemu združenju glasbenih producentov ter založnikov glasbenih in avdiovizualnih posnetkov, ni hotel razkriti osebnih podatkov nekaterih oseb, ki jim je zagotavljal internetni dostop. Združenje Promusicae si je prizadevalo za razkritje informacij, da bi lahko sprožilo sodne postopke proti navedenim osebam, 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 Sodišču EU, pri čemer mu je postavilo vprašanje, ali je treba take osebne podatke v skladu s pravom Skupnosti posredovati v okviru civilnih postopkov, da bi zagotovili učinkovito varstvo avtorskih pravic. Sklicevalo se je na direktive 2000/31, 2001/29 in 2004/48 v povezavi s členoma 17 in 47 Listine. Sodišče je ugotovilo, da navedene tri direktive, pa tudi Direktiva o zasebnosti in elektronskih komunikacijah (Direktiva 2002/58), državam članicam ne preprečujejo, da bi določile obveznost razkritja osebnih podatkov v okviru civilnih postopkov in tako zagotovile učinkovito varstvo avtorskih pravic.

44 Sodba ESČP z dne 10. januarja 2013 v zadevi *Ashby Donald in drugi proti Franciji*, pritožba št. 36769/08.

45 Sodba Sodišča EU z dne 29. januarja 2008 v zadevi *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, C-275/06, točki 54 in 60.

Sodišče EU 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 sodnega varstva.

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.“[46]

46 Prav tam, točki 65 in 68; glej tudi sodbo Sodišča EU z dne 16. februarja 2012 v zadevi *SABAM proti Netlog N.V.*, C-360/10.

# 2

# Izrazi s področja varstva osebnih podatkov

| EU | Obravnavane teme | Svet Evrope |
|---|---|---|
| **Osebni podatki** | | |
| Direktiva o varstvu osebnih podatkov, člen 2(a)<br>Sodba Sodišča EU z dne 9. novembra 2010 v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, C-92/09 in C-93/09<br>Sodba Sodišča EU z dne 29. januarja 2008 v zadevi *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, C-275/06 | **Pravna opredelitev** | Konvencija št. 108, člen 2(a)<br>Sodba ESČP z dne 14. marca 2013 v zadevi *Bernh Larsen Holding AS in drugi proti Norveški*, pritožba št. 24117/08 |
| Direktiva o varstvu osebnih podatkov, člen 8(1)<br>Sodba Sodišča EU z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01 | **Posebne kategorije osebnih podatkov (občutljivi osebni podatki)** | Konvencija št. 108, člen 6 |
| Direktiva o varstvu osebnih podatkov, člen 6(1)(e) | **Anonimizirani in psevdonimizirani podatki** | Konvencija št. 108, člen 5(e)<br>Konvencija št. 108, pojasnjevalno poročilo, člen 42 |
| **Obdelava osebnih podatkov** | | |
| Direktiva o varstvu osebnih podatkov, člen 2(b)<br>Sodba Sodišča EU z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01 | **Opredelitve** | Konvencija št. 108, člen 2(c) |

| | | |
|---|---|---|
| **Uporabniki osebnih podatkov** | | |
| Direktiva o varstvu osebnih podatkov, člen 2(d) | **Upravljavec** | Konvencija št. 108, člen 2(d)<br>Priporočilo o profiliranju, člen 1(g)* |
| Direktiva o varstvu osebnih podatkov, člen 2(e)<br>Sodba Sodišča EU z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01 | **Obdelovalec** | Priporočilo o profiliranju, člen 1(h) |
| Direktiva o varstvu osebnih podatkov, člen 2(g) | **Prejemnik** | Konvencija št. 108, Dodatni protokol, člen 2(1) |
| Direktiva o varstvu osebnih podatkov, člen 2(f) | **Tretja stranka** | |
| **Privolitev** | | |
| Direktiva o varstvu osebnih podatkov, člen 2(h)<br>Sodba Sodišča EU z dne 5. maja 2011 v zadevi *Deutsche Telekom AG proti Nemčiji*, C-543/09 | **Opredelitev in zahteve za veljavno privolitev** | Priporočilo o zdravstvenih podatkih, člen 6, in različna poznejša priporočila |

*Opomba: * Svet Evrope, Odbor ministrov (2010), Priporočilo Rec(2010)13 državam članicam o varstvu posameznikov v zvezi z avtomatsko obdelavo osebnih podatkov pri profiliranju (Priporočilo o profiliranju), 23. november 2010.*

## 2.1. Osebni podatki

### Ključne točke

- Podatki so osebni, če se nanašajo na določeno ali vsaj določljivo osebo, to je posameznika, na katerega se nanašajo osebni podatki.
- Oseba je določljiva, če je mogoče brez nerazumnega napora dobiti dodatne informacije, tako da je mogoče določiti posameznika, na katerega se nanašajo osebni podatki.
- Avtentikacija pomeni dokazati, da ima določena oseba določeno istovetnost in/ali da je pooblaščena za izvajanje nekaterih dejavnosti.
- V Konvenciji št. 108 in Direktivi 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 ne vsebujejo več identifikatorjev; psevdonimizirani pa so, če so identifikatorji zakodirani.
- Psevdonimizirani podatki so v nasprotju z anonimiziranimi podatki osebni podatki.

## 2.1.1. Glavni vidiki pojma osebni podatki

**Po pravu EU** in **pravu Sveta Evrope** so „osebni podatki" opredeljeni kot informacije, ki se nanašajo na določeno ali določljivo fizično osebo[47], to pomeni informacije o osebi, katere istovetnost je bodisi očitna bodisi jo je mogoče vsaj ugotoviti na podlagi dodatnih informacij.

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

### Oseba

Pravica do varstva podatkov se je razvila iz pravice do spoštovanja zasebnega življenja. Pojem zasebno življenje se navezuje na človeška bitja. Glavni upravičenci do varstva podatkov so zato fizične osebe. Poleg tega je v skladu z mnenjem Delovne skupine iz člena 29 z evropsko zakonodajo o varstvu osebnih podatkov varovano samo *živo bitje*.[48]

Sodna praksa ESČP v zvezi s členom 8 EKČP kaže, da je včasih težko popolnoma razlikovati med zadevami zasebnega in poklicnega življenja.[49]

Primer: Organi so v zadevi *Amann proti Švici*[50] prestregli poslovni telefonski klic pritožniku. Na podlagi tega klica so pritožnika preiskali in njegove podatke vnesli v register nacionalne varnosti. Čeprav se je zadevno prestrezanje nanašalo na poslovni telefonski klic, je ESČP menilo, da se shranjevanje podatkov o tem klicu nanaša na pritožnikovo zasebno življenje. Poudarilo je, da se pojem „zasebno življenje" ne sme razlagati ozko, zlasti ker spoštovanje zasebnega življenja vključuje pravico do oblikovanja in razvijanja odnosov z drugimi ljudmi. Poleg tega načeloma ni bilo razlogov, da bi poklicne ali poslovne dejavnosti izključili iz pojma „zasebno življenje". Tako široka razlaga ustreza razlagi iz Konvencije št. 108. ESČP je še ugotovilo, da vmešavanje v pritožnikove zadeve ni bilo v

47 Direktiva o varstvu osebnih podatkov, člen 2(a), Konvencija št. 108, člen 2(a).

48 Mnenje 4/2007 delovne skupine iz člena 29 z dne 20. junija 2007 o pojmu osebnih podatkov, WP 136, str. 22.

49 Glej na primer sodbi ESČP z dne 4. maja 2000 v zadevi *Rotaru proti Romuniji* [veliki senat], pritožba št. 28341/95, točka 43, in z dne 16. decembra 1992 v zadevi *Niemietz proti Nemčiji*, pritožba št. 13710/88, točka 29.

50 Sodba ESČP z dne 16. februarja 2000 v zadevi *Amann proti Švici* [veliki senat], pritožba št. 27798/95, točka 65.

skladu z zakonom, saj nacionalna zakonodaja ne vsebuje posebnih in podrobnih določb o zbiranju, evidentiranju in shranjevanju informacij. Zato je ugotovilo, da je bil kršen člen 8 EKČP.

Če se lahko varstvo osebnih podatkov nanaša tudi na zadeve iz poklicnega življenja, se poleg tega zdi sporno, da bi lahko varstvo imele samo fizične osebe. Pravice na podlagi EKČP niso zagotovljene samo fizičnim osebam, ampak vsakomur.

Sodna praksa ESČP vključuje sodbe o pritožbah pravnih oseb, ki trdijo, da so jim bile kršene pravice do varstva pred uporabo njihovih osebnih podatkov na podlagi člena 8 EKČP. Sodišče je zadevo kljub temu proučilo na podlagi pravice do spoštovanja doma in dopisovanja in ne na podlagi pravice do zasebnega življenja:

Primer: Zadeva *Bernh Larsen Holding AS in drugi proti Norveški*[51] 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 vsa tri podjetja skupaj.

ESČP je ugotovilo, da obveznost, naložena tožečim podjetjem, pomeni posega-nje v njihove pravice do spoštovanja „doma" in „dopisovanja" za namen člena 8 EKČP. Vendar je Sodišče je kljub temu ugotovilo, da imajo 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 ravnotežje 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 Konvencijo št. 108** nanaša predvsem na varstvo fizičnih oseb, vendar lahko pogodbenice varstvo osebnih podatkov razširijo tudi na pravne osebe, kot so podjetja in združenja v njihovem notranjem pravu. **Zakonodaja EU o varstvu osebnih podatkov** na splošno ne zajema varstva pravnih

51 Sodba ESČP z dne 14. marca 2013 v zadevi *Bernh Larsen Holding AS in drugi proti Norveški*, pritožba št. 24117/08. Glej tudi sodbo ESČP z dne 1. julija 2008 v zadevi *Liberty in drugi proti Združenemu kraljestvu*, pritožba št 58243/00.

oseb v zvezi z obdelavo podatkov, ki se nanje nanašajo. Nacionalni regulativni organi imajo pri urejanju tega področja proste roke.[52]

Primer: Sodišče EU je v združenih zadevah *Volker und Markus Schecke in Hartmut Eifert proti Land Hessen*[53] 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. [...] [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 [...]".[54]

## Določljivost osebe

Informacije **po pravu EU** in **pravu Sveta Evrope** vsebujejo podatke o osebi, če:

- je posameznik v teh informacijah določen ali
- če je posameznik, tudi če ni določen, v teh informacijah opisan tako, da je mogoče z dodatnim raziskovanjem ugotoviti, kdo je posameznik, na katerega se nanašajo osebni podatki.

Obe vrsti informacij sta z evropsko zakonodajo o varstvu osebnih podatkov varovani enako. ESČP je večkrat navedlo, da je pojem „osebni podatki" v okviru EKČP enak kot v Konvenciji št. 108, zlasti v zvezi s pogojem, da se podatki nanašajo na določene ali določljive osebe.[55]

V pravnih opredelitvah osebnih podatkov ni dodatno pojasnjeno, kdaj se šteje, da je oseba določena.[56] Očitno so za določitev potrebni elementi, s katerimi je oseba opisana tako, da jo je mogoče razlikovati od vseh drugih oseb in je prepoznavna kot posameznik. Dober primer takih opisnih elementov je ime osebe. Izjemoma lahko

52 Direktiva o varstvu podatkov, uvodna izjava 24.

53 Sodba Sodišča EU z dne 9. novembra 2010 v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, C-92/09 in C-93/09, točka 53.

54 Prav tam, točka 52.

55 Glej sodbo ESČP z dne 16. februarja 2000 v zadevi *Amann proti Švici* [veliki senat], pritožba št. 27798/95, točka 65 in naslednje.

56 Glej tudi sodbi ESČP z dne 13. februarja 2003 v zadevi *Odièvre proti Franciji* [veliki senat], pritožba št. 42326/98, in z dne 25. septembra 2012 v zadevi *Godelli proti Italiji*, pritožba št. 33783/09.

imajo tudi drugi identifikatorji podoben učinek kot ime. Pri javnih osebnostih lahko na primer zadostuje sklicevanje na položaj osebe, na primer predsednika Evropske komisije.

Primer: Sodišče EU je v zadevi *Promusicae*[57] navedlo, da „ni sporno, da posredovanje imen in naslovov določenih uporabnikov [določene platforme za izmenjavo datotek], za katero je zaprosilo Promusicae, v postopku v glavni stvari vključuje uporabo osebnih podatkov, to je podatkov o določenih ali določljivih fizičnih osebah, v skladu z opredelitvijo iz člena 2(a) Direktive 95/46 [...]. To posredovanje informacij, ki so po mnenju Promusicae shranjene pri Telefónica – čemur slednja ne ugovarja –, pomeni obdelavo osebnih podatkov v skladu s prvim pododstavkom člena 2 Direktive 2002/58 v povezavi s členom 2(b) Direktive 95/46".

Ker veliko imen ni izvirnih, so lahko za ugotovitev istovetnosti osebe potrebni dodatni identifikatorji, da osebe ne bi zamenjali s kom drugim. Pogosto se uporabljata datum in kraj rojstva. Poleg tega so bile za boljše razlikovanje med državljani v nekaterih državah uvedene osebne identifikacijske številke. Biometrični podatki, na primer prstni odtisi, digitalne fotografije ali slikanje šarenice postajajo v tehnološki dobi vse pomembnejši za identifikacijo oseb.

Vendar za uporabo evropske zakonodaje o varstvu osebnih podatkov ni potrebna visokokakovostna identifikacija osebe, na katero se nanašajo osebni podatki; zadostuje že, da je zadevna oseba določljiva. Oseba se šteje za določljivo, če informacija vsebuje identifikacijske elemente, na podlagi katerih je mogoče osebo neposredno ali posredno identificirati.[58] V skladu z uvodno izjavo 26 Direktive o varstvu osebnih podatkov je odločilnega pomena, ali se pričakuje, da bodo imeli predvidljivi uporabniki informacij na voljo sredstva za identifikacijo in bodo ta sredstva uporabili; to vključuje prejemnike, ki so tretje osebe (glej razdelek 2.3.2).

Primer: Lokalni organ se odloči zbirati 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

57 Sodba Sodišča EU z dne 29. januarja 2008 v zadevi *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, C-275/06, točka 45.

58 Direktiva o varstvu podatkov, člen 2(a).

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 podatki o anonimnih osebah. 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 Direktive o varstvu osebnih podatkov. 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 tudi izrecno predviden scenarij, po katerem lahko tudi nadaljnji prejemniki podatkov in ne samo njihovi neposredni uporabniki poskušajo ugotoviti identiteto posameznika. V skladu z uvodno izjavo 26 je dejanje lokalnega organa enako zbiranju podatkov o določljivih osebah, zato je potrebna pravna podlaga v zakonodaji o varstvu podatkov.

**Po pravu Sveta Evrope** se določljivost razume podobno. Člen 1(2) Priporočila o plačilnih podatkih[59] na primer določa, da se oseba ne šteje za „določljivo“, če je za identifikacijo potrebnega preveč časa, denarja ali dela.

## 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, ali 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, včasih skupaj s številkami PIN, so elektronski podpisi še posebno primeren instrument za identifikacijo in avtentikacijo osebe v elektronskih komunikacijah.

59 Svet Evrope, Odbor ministrov (1990), Priporočilo št. R Rec(90)19 z dne 13. septembra 1990 o varstvu osebnih podatkov, ki se uporabljajo za plačila in druge povezane finančne transakcije.

## Vrsta podatkov

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

Primer: Ocena delovne uspešnosti zaposlenega, ki jo izvede nadrejeni in je shranjena v osebnem spisu zaposlenega, je osebni podatek o zaposlenem, 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“.

Osebni podatki vključujejo informacije, ki se nanašajo na zasebno življenje osebe, in informacije o njenem poklicnem ali javnem življenju.

ESČP je v zadevi *Amann*[60] pojem „osebni podatki“ razlagalo, kot da ni omejen na zadeve iz zasebnega življenja posameznika (glej razdelek 2.1.1). Ta pomen pojma „osebni podatki“ je pomemben tudi za Direktivo o varstvu osebnih podatkov:

Primer: Sodišče EU je v združenih zadevah *Volker und Markus Schecke in Hartmut Eifert proti Land Hessen*[61] navedlo, da „[v] zvezi s tem dejstvo, da se objavljeni podatki nanašajo na poklicne dejavnosti, ni pomembno [...]. Evropsko sodišče za človekove pravice je v zvezi s tem s sklicevanjem na razlago člena 8 Konvencije navedlo, da se pojem ‚zasebno življenje‘ ne sme razlagati ozko in da poklicnih [...] dejavnosti načeloma ni mogoče izključiti iz pojma zasebno življenje“.

Podatki se na osebe nanašajo tudi, če se z vsebino informacij posredno razkrijejo podatki o osebi. V nekaterih primerih, kadar obstaja tesna povezava med predmetom ali dogodkom (na primer mobilnim telefonom, avtomobilom, nesrečo) na eni strani in osebo (na primer kot njegovim lastnikom, uporabnikom, žrtvijo) na drugi, bi bilo treba tudi informacije o predmetu ali dogodku šteti za osebne podatke.

Primer: V zadevi *Uzun proti Nemčiji*[62] sta bila pritožnik in nek drug moški zaradi domnevne vpletenosti v bombne napade nadzorovana prek naprave z

60 Glej sodbo ESČP z dne 16. februarja 2000 v zadevi *Amann proti Švici*, pritožba št. 27798/95, točka 65.

61 Sodba Sodišča z dne 9. novembra 2010 v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, C-92/09 in C-93/09, točka 59.

62 Sodba ESČP z dne 2. septembra 2010 v zadevi *Uzun proti Nemčiji*, pritožba št. 35623/05.

globalnim sistemom za določanje položaja (GPS), ki je bila nameščena v avtomobilu drugega moškega. ESČP je v tej zadevi ugotovilo, da opazovanje pritožnika s sistemom GPS pomeni poseganje v njegovo zasebno življenje, ki je varovano s členom 8 EKČP. Vendar je bil nadzor s sistemom GPS v skladu z zakonom in sorazmeren z zakonitim ciljem preiskovanja več primerov poskusa umora, zato je bil v demokratični družbi nujen. Sodišče je ugotovilo, da člen 8 EKČP ni bil kršen.

### Pojavna oblika osebnih podatkov

Za uporabo zakonodaje o varstvu osebnih podatkov ni pomembno, v kakšni obliki se osebni podatki hranijo ali uporabljajo. Pisna ali govorna sporočila lahko vsebujejo osebne podatke in slike[63], vključno s posnetki televizije zaprtega kroga (CCTV)[64] ali zvokom.[65] Elektronsko zabeležene informacije in informacije na papirju so lahko osebni podatki; celo celični vzorci človeškega tkiva so lahko osebni podatki, saj je v njih zapisana DNK osebe.

## 2.1.2. Posebne kategorije osebnih podatkov

**Po pravu EU** in **pravu Sveta Evrope** obstajajo posebne kategorije osebnih podatkov, ki lahko glede na svojo naravo pomenijo tveganje za posameznike, na katere se nanašajo, zato potrebujejo okrepljeno varstvo. Obdelava teh posebnih kategorij osebnih podatkov („občutljivih osebnih podatkov“) mora biti zato dovoljena samo s posebnimi zaščitnimi ukrepi.

V zvezi z opredelitvijo osebnih podatkov so v Konvenciji št. 108 (člen 6) in Direktivi o varstvu osebnih podatkov (člen 8) navedene naslednje kategorije:

- osebni podatki, ki kažejo na rasno ali etnično poreklo;
- osebni podatki, ki razkrivajo politična stališča, verska ali druga prepričanja, ter

63 Sodbi ESČP z dne 24. junija 2004 v zadevi *Von Hannover proti Nemčiji*, pritožba št. 59320/00, in z dne 11. januarja 2005 v zadevi *Sciacca proti Italiji*, pritožba št. 50774/99.

64 Sodbi ESČP z dne 28. januarja 2003 v zadevi *Peck proti Združenem kraljestvu*, pritožba št. 44647/98, in z dne 5. oktobra 2010 v zadevi *Köpke proti Nemčiji*, pritožba št. 420/07.

65 Direktiva o varstvu osebnih podatkov, uvodni izjavi 16 in 17; sodbi ESČP z dne 25. septembra 2001 v zadevi *P. G. in J. H. proti Združenemu kraljestvu*, pritožba št. 44787/98, točki 59 in 60, ter z dne 20. decembra 2005 v zadevi *Wisse proti Franciji*, pritožba št. 71611/01.

- osebni podatki v zvezi z zdravjem ali spolnim življenjem.

> Primer: Sodišče EU je v zadevi *Bodil Lindqvist*[66] navedlo, da je „navedba, da si je oseba poškodovala nogo in je delno odsotna z dela zaradi bolezni, osebni podatek v zvezi z zdravjem v smislu člena 8(1) Direktive 95/46."

V Direktivi o varstvu osebnih podatkov je poleg tega med občutljivimi osebnih podatki navedena „pripadnost sindikatu", saj je lahko močan kazalnik političnega prepričanja ali pripadnosti.

V Konvenciji št. 108 se za občutljive osebnih podatke štejejo tudi osebni podatki v zvezi s kazenskimi obsodbami.

Države članice EU so s členom 8(7) Direktive o varstvu osebnih podatkov pooblaščene, da „določijo pogoje, pod katerimi se lahko obdela nacionalna identifikacijska številka ali kateri koli drug identifikator splošne uporabe."

## 2.1.3. Anonimizirani in psevdonimizirani podatki

V skladu z načelom omejene hrambe osebnih podatkov, vključenim v Direktivo o varstvu osebnih podatkov in Konvencijo št. 108 (in podrobneje obravnavanim v poglavju 3), morajo biti osebnih podatki shranjeni „v obliki, ki dopušča identifikacijo posameznikov, na katere se osebni podatki nanašajo, le toliko časa, kolikor je potrebno za namene, za katere so bili osebnih podatki zbrani ali za katere se naprej obdelujejo."[67] Osebne podatke bi bilo treba zato anonimizirati, če bi jih upravljavec želel shraniti, potem ko bi zastarali in ne bi več služili prvotnemu namenu.

### Anonimizirani podatki

Podatki so anonimizirani, če so bili iz niza osebnih podatkov odstranjeni vsi identifikacijski elementi. V informacijah ne sme ostati noben element, na podlagi katerega bi bilo mogoče ob razumnem naporu znova ugotoviti identiteto zadevne osebe ali več oseb.[68] Podatki, ki so bili uspešno anonimizirani, niso več osebni podatki.

66 Sodba Sodišča EU z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01, točka 51.

67 Direktiva o varstvu osebnih podatkov, člen 6(1)(e), Konvencija št. 108, člen 5(e).

68 Prav tam, uvodna izjava 26.

Če osebni podatki ne služijo več prvotnemu namenu, vendar se v personalizirani obliki še naprej hranijo za zgodovinsko, statistično ali znanstveno uporabo, je ta možnost z Direktivo o varstvu podatkov in Konvencijo št. 108 dovoljena, če so uvedeni ustrezni zaščitni ukrepi pred zlorabo.[69]

## Psevdonimizirani podatki

Osebni podatki vsebujejo identifikatorje, kot so ime, datum rojstva, spol in naslov. Če se osebni podatki psevdonimizirajo, se identifikatorji nadomestijo s psevdonimom. Psevdonimizacija se izvede na primer s šifriranjem identifikatorjev v osebnih podatkih.

Psevdonimizirani podatki v pravnih opredelitvah v Konvenciji št. 108 ali Direktivi o varstvu osebnih podatkov niso izrecno navedeni. Vendar je v členu 42 pojasnjevalnega poročila h Konvenciji št. 108 navedeno, da „[z]ahteva [...] v zvezi s časovnimi omejitvami hrambe osebnih podatkov v poimenski obliki ne pomeni, da bi bilo treba podatke po določenem času nepreklicno ločiti od imena osebe, na katero se nanašajo, temveč samo, da podatkov in identifikatorjev ne bi bilo mogoče zlahka povezati“. To je mogoče doseči s psevdonimizacijo osebnih podatkov. Psevdonimizirane podatke je mogoče razvozlati samo z uporabo ključa za dešifriranje, zato je identifikacija brez ključa možna le s težavo. Ker pa povezava z identiteto še vedno obstaja v obliki psevdonima in ključa za dešifriranje, je ponovna identifikacija zlahkamogoča za vse, ki imajo pravico uporabljati takšen ključ. Zlasti je treba preprečiti, da bi šifrirne ključe uporabljale nepooblaščene osebe.

Psevdonimizacija osebnih podatkov je eden od najpomembnejših načinov za zagotovitev varstva osebnih podatkov v velikem obsegu; če se uporabi osebnih podatkov ni mogoče v celoti odreči, je treba podrobneje pojasniti logiko in učinek takega ravnanja.

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“.

69 Prav tam, člen 6(1)(e), Konvencija št. 108, člen 5(e).

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

Vendar je prvi primer 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. Na učinkovitost varstva osebnih podatkov vpliva metoda psevdonimizacije.

Osebni podatki s šifriranimi identifikatorji 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 imeti 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 podatke o zgodovini primerov. Psevdonimizacija je torej pomembno orodje na področju tehnologije za boljše varovanje zasebnosti. Lahko je pomemben dejavnik pri izvajanju vgrajene zasebnosti. To pomeni, da je varstvo osebnih podatkov vgrajeno v ogrodje naprednih sistemov za obdelavo osebnih podatkov.

## 2.2. Obdelava osebnih podatkov

### Ključne točke

- Pojem „obdelava“ se nanaša predvsem na avtomatizirano obdelavo.
- Po pravu EU se „obdelava“ nanaša tudi na ročno obdelavo v strukturiranih zbirkah.
- Po pravu Sveta Evrope je mogoče pomen „obdelave“ z nacionalnim pravom razširiti tako, da vključuje ročno obdelavo.

Varstvo osebnih podatkov na podlagi Konvencije št. 108 in Direktive o varstvu osebnih podatkov je osredotočeno predvsem na avtomatizirano obdelavo podatkov.

Po **pravu Sveta Evrope** se z opredelitvijo avtomatske obdelave kljub temu dopušča, da so med avtomatiziranimi postopki nujne določene faze ročne uporabe osebnih podatkov. Podobno je po **pravu EU** avtomatizirana obdelava osebnih podatkov

opredeljena kot „postopki, ki se izvajajo v zvezi z osebnimi podatki, in sicer v celoti ali delno z avtomatskimi sredstvi“.[70]

> Primer: Sodišče EU je v zadevi *Bodil Lindqvist*[71] razsodilo, 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.“

Tudi pri ročni obdelavi osebnih podatkovje treba zagotoviti varstvo osebnih podatkov.

Varstvo osebnih podatkov **po pravu EU** nikakor ni omejeno samo na avtomatizirano obdelavo osebnih podatkov. V skladu s tem se varstvo osebnih podatkov po pravu EU nanaša na obdelavo osebnih podatkov v ročni zbirki, to pomeni v posebej strukturirani natisnjeni zbirki.[72] Razlog za to razširitev varstva osebnih podatkov je, da:

- je mogoče natisnjeno zbirko strukturirati tako, da je iskanje informacij hitro in preprosto, ter
- je mogoče s shranjevanjem osebnih podatkov v strukturirani natisnjeni zbirki zlahka zaobiti omejitve, ki so z zakonom predpisane za avtomatizirano obdelavo osebnih podatkov.[73]

**Po pravu Sveta Evrope** je s Konvencijo št. 108 urejena predvsem obdelava osebnih podatkov v avtomatiziranih podatkovnih datotekah.[74] Določa pa tudi možnost, da se varstvo v nacionalni zakonodaji razširi na ročno obdelavo. To možnost je izkoristilo več pogodbenic Konvencije št. 108, ki so zato podale izjave generalnemu sekretarju Sveta Evrope.[75] Razširitev varstva osebnih podatkov na podlagi take izjave mora

70 Direktiva o varstvu osebnih podatkov, člen 2(c), Konvencija št. 108, člena 2(b) in 3(1).

71 Sodba Sodišča EU z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01, točka 27.

72 Direktiva o varstvu osebnih podatkov, člen 3(1).

73 Prav tam, uvodna izjava 27.

74 Konvencija št. 108, člen 2(b).

75 Glej izjave iz Konvencije št. 108, člen 3(2)(c).

veljati za vsakršno ročno obdelavo osebnih podatkov in je ni mogoče omejiti na obdelavo v ročnih zbirkah.[76]

Kar zadeva vrsto vključenih postopkov obdelave, je pojem obdelava **po pravu EU in po pravu Sveta Evrope** izčrpen: „‚obdelava osebnih podatkov' […] pomeni kakršen koli postopek […], kakršno je zbiranje, beleženje, urejanje, shranjevanje, prilagajanje ali predelava, iskanje, posvetovanje, uporaba, posredovanje s prenosom, širjenje ali drugo razpolaganje, prilagajanje ali kombiniranje, blokiranje, izbris ali uničenje"[77], ki se izvaja v zvezi z osebnimi podatki. Pojem „obdelava" vključuje tudi dejanja, pri katerih za osebne podatke ni več odgovoren en upravljavec, ampak se odgovornost prenese na drugega upravljavca.

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 Konvenciji št. 108 in navedeni direktivi. Vendar pravna podlaga za tako 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 nacionalnih davčnih zakonodaj. Prenos osebnih podatkov bi se brez takih določb štel za nezakonito obdelavo.

## 2.3. Uporabniki osebnih podatkov

### Ključne točke

- Kdor se odloči obdelovati osebne podatke drugih, je v skladu z zakonodajo o varstvu osebnih podatkov „upravljavec"; če tako odločitev skupaj sprejme več oseb, so lahko „skupni upravljavci".
- „Obdelovalec" je pravno ločen subjekt, ki v imenu upravljavca obdeluje osebne podatke.

76 Glej besedilo Konvencije št. 108, člen 3(2).

77 Direktiva o varstvu osebnih podatkov, člen 2(b). Glej, podobno, Konvencijo št. 108, člen 2(c).

- Obdelovalec postane upravljavec, če uporablja osebne podatke za lastne namene, pri čemer ne upošteva navodil upravljavca.
- „Prejemnik" je vsak, ki prejme osebne podatke od upravljavca.
- „Tretja oseba" je fizična ali pravna oseba, ki ne ravna po navodilih upravljavca (in ni posameznik, na katerega se nanašajo osebni podatki).
- „Prejemnik, ki je tretja oseba," je oseba ali subjekt, ki je pravno ločen od upravljavca, vendar od njega prejme osebne podatke.

## 2.3.1. Upravljavci in obdelovalci

Pri upravljavcih in obdelovalcih je najpomembneje, da so pravno zavezani izpolnjevanju zadevnih obveznosti na podlagi zakonodaje o varstvu osebnih podatkov. Te položaje torej lahko prevzamejo samo osebe, ki jim je mogoče na podlagi upoštevne zakonodaje naložiti tako odgovornost. V zasebnem sektorju je to običajno fizična ali pravna oseba, v javnem sektorju pa organ. Drugi subjekti, kot so organi ali institucije, ki nimajo pravne osebnosti, so lahko upravljavci ali obdelovalci samo, če je tako določeno s posebnimi zakonskimi določbami.

Primer: Če oddelek za trženje družbe Sonček načrtuje obdelavo osebnih podatkov za tržno raziskavo, je upravljavec take obdelave podjetje Sonček in ne oddelek za trženje. Oddelek za trženje ne more biti upravljavec, saj ni ločena pravna oseba.

V skupini družb se matična družba in posamezna odvisna družba kot ločeni pravni osebi štejeta za ločena upravljavca ali obdelovalca. Posledica tega pravno ločenega statusa je, da je za prenos osebnih podatkov med člani skupine družb potrebna posebna pravna podlaga. Nikakršne pravice ni, ki bi omogočala izmenjavo osebnih podatkov kot takih med ločenimi pravnimi subjekti v skupini družb.

Pri tem je treba omeniti vlogo fizičnih oseb. **Po pravu EU** pravila iz Direktive o varstvu osebnih podatkov ne veljajo za fizične osebe, ki obdelujejo osebne podatke o drugih med popolnoma osebno ali domačo dejavnostjo; te se ne štejejo za upravljavce.[78]

78 Direktiva o varstvu osebnih podatkov, uvodna izjava 12 in člen 3(2), zadnja alinea.

Vendar je bilo s sodno prakso ugotovljeno, da se zakonodaja o varstvu osebnih podatkov kljub temu uporablja, če fizična oseba pri uporabi interneta objavi osebne podatke o drugih.

Primer: Sodišče EU je v zadevi *Bodil Lindqvist*[79] navedlo, 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".[80]

Taka obdelava osebnih podatkov ne spada med popolnoma osebne ali domače dejavnosti, za katere se Direktiva o varstvu osebnih podatkov ne uporablja, 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."[81]

## Upravljavec

**Po pravu EU** je upravljavec opredeljen kot oseba, ki „sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov".[82] V odločitvi upravljavca je pojasnjeno, zakaj in kako se bodo osebni podatki obdelovali. **Po pravu Sveta Evrope** je v opredelitvi „upravljavca" navedeno še, da upravljavec odloči, katere kategorije osebnih podatkov je treba shraniti.[83]

Konvencija št. 108 se v opredelitvi upravljavca navezuje še na dodaten vidik upravljanja, ki ga je treba obravnavati. Ta opredelitev se nanaša na vprašanje, kdo lahko zakonito obdeluje določene osebne podatke za določen namen. Vendar se ob domnevno nezakonitih postopkih obdelave, ko je treba najti odgovornega upravljavca, za upravljavca šteje oseba ali subjekt, na primer družba ali organ, ki je odločil, da je treba osebne podatke obdelati, ne glede na to, ali je imel za to zakonsko

79 Sodba Sodišča EU z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01.

80 Prav tam, točka 27.

81 Prav tam, točka 47.

82 Direktiva o varstvu osebnih podatkov, člen 2(d).

83 Konvencija št. 108, člen 2(d).

pravico ali ne.[84] Zahtevo za izbris je treba zato vedno nasloviti na „dejanskega“ upravljavca.

## Skupno upravljanje

Opredelitev „upravljavca“ v Direktivi o varstvu osebnih podatkov določa, da je lahko tudi več pravno ločenih subjektov, ki skupaj ali v povezavi z drugimi delujejo kot upravljavci. To pomeni, da se skupaj odločijo za obdelavo osebnih podatkov za skupni namen.[85] Vendar je to pravno mogoče samo, kadar je s posebno pravno podlago predvidena skupna obdelava osebnih podatkov za skupni namen.

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 premišljeno odločitev o kreditni sposobnosti prosilca.

V uredbah 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. Vendar na evropski ravni še ni na voljo zadevne sodne prakse, niti niso jasne posledice v zvezi z odgovornostjo. Delovna skupina iz člena 29 zagovarja širšo razlago pojma skupno upravljanje, da bi se omogočilo nekaj prožnosti, ki je v trenutnih razmerah nujna, saj postaja obdelava osebnih podatkov vse bolj zapletena.[86] 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 združenje SWIFT, prvotno kot obdelovalca, uporabljale za prenos podatkov med bančnimi transakcijami. Združenje SWIFT je take podatke o bančnih transakcijah, shranjene v računalniškem storitvenem centru v Združenih državah, razkrilo ministrstvu za finance ZDA, ne da bi mu evropske bančne institucije, ki so ga uporabljale, to izrecno naročile. Delovna skupina iz člena 29 je med oceno zakonitosti takega položaja ugotovila, da je treba evropske bančne institucije, ki so uporabljale

84 Glej tudi Mnenje 1/2010 delovne skupine iz člena 29 z dne 16. februarja 2010 o pojmih „upravljavec“ in „obdelovalec“, WP 169, Bruselj, str. 15.

85 Direktiva o varstvu osebnih podatkov, člen 2(d).

86 Mnenje 1/2010 delovne skupine iz člena 29 z dne 16. februarja 2010 o pojmih „upravljavec“ in „obdelovalec“, WP 169, Bruselj, str. 19.

združenje SWIFT, in samo združenje SWIFT šteti za skupne upravljavce, ki so evropskim strankam odgovorni za razkritje njihovih osebnih podatkov.[87] Združenje SWIFT je z odločitvijo za razkritje (nezakonito) prevzelo vlogo upravljavca; bančne institucije očitno niso izpolnile svoje obveznosti, da nadzorujejo svojega obdelovalca, zato jih ni bilo mogoče popolnoma razbremeniti njihove odgovornosti kot upravljavcev. Ta primer pomeni skupno upravljanje.

## Obdelovalec

Obdelovalec je **po pravu EU** opredeljen kot oseba, ki obdeluje osebne podatke v imenu upravljavca.[88] Dejavnosti, zaupane obdelovalcu, so lahko omejene na zelo posebno nalogo ali okoliščine ali pa so lahko precej splošne in obsežne.

**Po pravu Sveta Evrope** je pomen obdelovalca enak kot po pravu EU.

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 upravljanje svojih zaposlenih, prodaje in računov.

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 zaradi izpolnjevanja svojih obveznosti kot delodajalec.

## Razmerje med upravljavcem in obdelovalcem

Kot smo videli, je upravljavec opredeljen kot oseba, ki določi namene in sredstva obdelave.

Primer: Direktor družbe Sonček odloči, naj družba Mesečina, ki je specializirana za tržne analize, izvede tržno analizo podatkov Sončkovih strank. Čeprav se bo naloga določitve sredstev obdelave tako prenesla na družbo Mesečina,

87 Mnenje 10/2006 delovne skupine iz člena 29 z dne 22. novembra 2006 o obdelavi osebnih podatkov Družbe za svetovne medbančne finančne telekomunikacije (SWIFT), WP 128, Bruselj.

88 Direktiva o varstvu osebnih podatkov, člen 2(e).

upravljavec ostaja družba Sonček, družba Mesečina pa je samo obdelovalec, saj lahko družba Mesečina v skladu s pogodbo podatke o strankah družbe Sonček uporablja samo za namene, ki jih določi slednja.

Če se pristojnost za določitev sredstev obdelave prenese na obdelovalca, mora imeti upravljavec kljub temu pravico poseči v odločitve 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 z zakonodajo o varstvu osebnih podatkov. Pogodba, s katero bi bilo upravljavcu prepovedano posegati v odločitve obdelovalca, bi bila zato verjetno sestavljena v smislu skupnega upravljanja, pri čemer bi si obe stranki delili pravno obveznost upravljavca.

Dalje, če obdelovalec ne upošteva omejitev uporabe 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. Delovna skupina iz člena 29 v takih primerih dejansko največkrat predpostavlja skupno upravljanje, saj se tako najbolje zavarujejo interesi posameznikov, na katere se nanašajo osebni podatki.[89] Pomembna posledica skupnega upravljanja bi morala biti solidarna odgovornost za škodo, kar posameznikom, na katere se nanašajo osebni podatki, zagotavlja najrazličnejša pravna sredstva.

Pojavijo se lahko tudi vprašanja porazdelitve odgovornosti, če je upravljavec majhno 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.[90]

Zaradi jasnosti in preglednosti bi morale biti podrobnosti razmerja med upravljavcem in obdelovalcem določene v pisni pogodbi.[91] Če take pogodbe ni, to pomeni kršitev

89 Mnenje 1/2010 delovne skupine iz člena 29 z dne 16. februarja 2010 o pojmih „upravljavec“ in „obdelovalec“, WP 169, Bruselj, str. 25, in Mnenje 10/2006 z dne 22. novembra 2006 o obdelavi osebnih podatkov Družbe za svetovne medbančne finančne telekomunikacije (SWIFT), WP 128, Bruselj.

90 Mnenje 1/2010 delovne skupine iz člena 29 z dne 16. februarja 2010 o pojmih „upravljavec“ in „obdelovalec“, WP 169, Bruselj, str. 26.

91 Direktiva o varstvu podatkov, člen 17(3) in (4).

obveznosti upravljavca, da zagotovi pisno dokumentacijo o vzajemnih odgovornostih, in lahko se naložijo sankcije.[92]

Obdelovalci morda želijo nekatere naloge prenesti na druge podobdelovalce. To je zakonsko dopustno, podrobnosti pa so odvisne od pogodbenih določil med upravljavcem in obdelovalcem, vključno s tem, ali je dovoljenje upravljavca vedno nujno ali pa zadostuje že obveščanje.

**Po pravu Sveta Evrope** je razlaga pojmov upravljavec in obdelovalec, kot sta pojasnjena zgoraj, v celoti upoštevna, kar dokazujejo priporočila, sprejeta na podlagi Konvencije št. 108.[93]

## 2.3.2. Prejemniki in tretje osebe

Razlika med obema 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 pravno gledano razlikuje od upravljavca. Za razkritje osebnih podatkov tretji osebi je zato vedno potrebna posebna pravna podlaga. Tretja oseba v skladu s členom 2(f) Direktive o varstvu osebnih podatkov „pomeni katero koli fizično ali pravno osebo, javni organ, agencijo ali kateri koli drug organ, ki ni posameznik, na katerega se osebni podatki nanašajo, upravljavec, obdelovalec in oseba, ki je pod neposredno oblastjo upravljavca ali obdelovalca pooblaščena za obdelavo podatkov". To pomeni, da se osebe, zaposlene pri organizaciji, ki je pravno ločena od upravljavca – čeprav je del iste skupine ali holdinga –, štejejo za „tretje osebe" (ali spadajo mednje). Nasprotno pa se podružnice banke, ki obdelujejo račune strank pod neposrednim nadzorom glavne poslovalnice, ne bi štele za „tretje osebe".[94]

„Prejemnik" je širši pojem kot „tretja oseba". Prejemnik v smislu člena 2(g) Direktive o varstvu osebnih podatkov pomeni „fizično ali pravno osebo, javni organ, agencijo ali kateri koli drug organ, ki se mu posreduje podatke, bodisi da je tretja [oseba] ali ne". Prejemnik je lahko tudi oseba, ki ni del upravljavca ali obdelovalca – to bi

92 Mnenje 1/2010 delovne skupine iz člena 29 z dne 16. februarja 2010 o pojmih „upravljavec" in „obdelovalec", WP 169, Bruselj, str. 27.

93 Glej na primer priporočilo o profiliranju, člen 1.

94 Mnenje 1/2010 delovne skupine iz člena 29 z dne 16. februarja 2010 o pojmih „upravljavec" in „obdelovalec", WP 169, Bruselj, str. 31.

bila potem tretja oseba –, ali nekdo, ki je del upravljavca ali obdelovalca, na primer zaposleni ali drug oddelek v isti družbi ali organu.

Razlikovanje med prejemniki in tretjimi osebami je pomembno samo zaradi pogojev za zakonito razkritje osebnih podatkov. Zaposleni pri upravljavcu ali obdelovalcu so lahko brez dodatne pravne zahteve prejemniki osebnih podatkov, če sodelujejo pri postopkih obdelave upravljavca ali obdelovalca. Nasprotno pa tretja oseba, ki je pravno ločena od upravljavca ali obdelovalca, ni pooblaščena za uporabo osebnih podatkov, ki jih obdeluje upravljavec, razen če v posameznem primeru obstaja posebna pravna podlaga. „Prejemniki osebnih podatkov, ki so tretje osebe," zato vedno potrebujejo pravno podlago za zakonito prejemanje osebnih podatkov.

Primer: Oseba, ki je zaposlena pri obdelovalcu in uporablja osebne podatke v okviru nalog, ki ji jih je zaupal delodajalec, je prejemnik osebnih podatkov, vendar ni tretja oseba, saj uporablja podatke v imenu in po navodilih obdelovalca.

Če pa se isti zaposleni odloči, da bo podatke, do katerih ima dostop, ker je zaposlen pri obdelovalcu, uporabil za lastne namene in jih proda drugemu podjetju, potem zaposleni deluje kot tretja oseba. Ta oseba več ne ravna po navodilih obdelovalca (delodajalca). Zaposleni bi kot tretja oseba potreboval pravno podlago za pridobitev in prodajo osebnih podatkov. V tem primeru zaposleni take pravne podlage nikakor nima, zato so ta dejanja nezakonita.

## 2.4. Privolitev

### Ključne točke

- Privolitev kot pravna podlaga za obdelavo osebnih podatkov mora biti prostovoljna, informirana in posebna.
- Privolitev mora biti nedvoumna. Privolitev je lahko izrecna ali implicitna na podlagi ravnanja, ki ne dopušča dvoma, da se posameznik, na katerega se nanašajo osebni podatki, strinja z obdelavo svojih podatkov.
- Za obdelavo občutljivih osebnih podatkov na podlagi privolitve je potrebna izrecna privolitev.
- Privolitev se lahko kadar koli prekliče.

Privolitev pomeni „vsako prostovoljno dano posebno in informirano izjavo volje posameznika, na katerega se nanašajo osebni podatki“.[95] Pogosto je to pravna podlaga za zakonito obdelavo osebnih podatkov (glej razdelek 4.1).

## 2.4.1. Dejavniki veljavne privolitve

**Pravo EU** določa tri dejavnike, na podlagi katerih je privolitev veljavna in katerih namen je zagotoviti, da so posamezniki, na katere se nanašajo osebni podatki, dejansko soglašali z uporabo svojih podatkov:

- posameznik, na katerega se nanašajo osebni podatki, med dajanjem privolitve ne sme biti pod nikakršnim pritiskom;
- posameznik, na katerega se nanašajo osebni podatki, je moral biti ustrezno seznanjen s ciljem in posledicami privolitve, ter
- vsebina privolitve mora biti dovolj konkretna.

Privolitev je v smislu zakonodaje o varstvu osebnih podatkov veljavna samo, če so izpolnjene vse te zahteve.

Konvencija št. 108 ne vsebuje opredelitve privolitve; to je prepuščeno nacionalni zakonodaji. Vendar **po pravu Sveta Evrope** dejavniki veljavne privolitve ustrezajo tistim, ki so bili pojasnjeni zgoraj, saj so določeni s priporočili, sprejetimi na podlagi Konvencije št. 108.[96] Zahteve za privolitev so enake kot za veljavno izjavo o nameri na podlagi evropskega civilnega prava.

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.

Privolitev je lahko izrecna[97] ali neizrecna. Pri prvi ni nikakršnega dvoma o nameri posameznika, na katerega se nanašajo osebni podatki, in je lahko ustna ali pisna;

95 Direktiva o varstvu osebnih podatkov, člen 2(h).

96 Glej na primer Konvencijo št. 108, priporočilo o statističnih podatkih, točka 6.

97 Direktiva o varstvu osebnih podatkov, člen 8(2).

pri drugi se sklepa na podlagi okoliščin. Vsaka privolitev mora biti nedvoumna.[98] To pomeni, da ne sme biti nikakršnega razumnega dvoma o tem, da je želel posameznik, na katerega se nanašajo osebni podatki, sporočiti svoje strinjanje z obdelavo svojih podatkov. Nedvoumne privolitve na primer ni mogoče izpeljati zgolj na podlagi neukrepanja (molka). Če so osebni podatki, ki naj bi se obdelovali, občutljivi, je izrecna privolitev obvezna in mora biti nedvoumna.

## Prostovoljna privolitev

Prostovoljna privolitev je veljavna samo, če „je posamezniku, na katerega se nanašajo osebni podatki, omogočena dejanska izbira in ni nevarnosti zavajanja, ustrahovanja, prisile ali znatnih negativnih posledic, če ne privoli".[99]

Primer: Na številnih letališčih morajo potniki pred vstopom na območje za vkrcanje skozi telesne skenerje.[100] Ker se med skeniranjem obdelujejo osebnih podatki o potnikih, mora biti obdelava v skladu z eno od pravnih podlag iz člena 7 Direktive o varstvu osebnih podatkov (glej razdelek 4.1.1). Včasih se pregled s telesnimi skenerji potnikom ponudi kot možnost, kar pomeni, da bi lahko njihova privolitev upravičila obdelavo. Vendar bi se lahko potniki bali, da bodo s tem, ko ne bodo hoteli skozi telesne skenerje, vzbudili sum ali povzročili dodatne preglede, na primer telesne preglede. Številni potniki privolijo v skeniranje, ker se s tem izognejo morebitnim težavam ali zamudam. Taka privolitev verjetno ni dovolj prostovoljna.

Trdna zakonita podlaga zato lahko izhaja samo iz akta zakonodajalca na podlagi člena 7(e) Direktive o varstvu osebnih podatkov, kar pomeni, da morajo potniki sodelovati zaradi prevladujočega javnega interesa. Taka zakonodaja bi lahko še vedno omogočala izbiro med skeniranjem in telesnim pregledom, vendar samo kot del dodatnih ukrepov pri nadzoru meje, ki so v določenih okoliščinah nujni. Evropska komisija je to leta 2011 določila v dveh uredbah, ki sta se nanašali na varnostne skenerje.[101]

98 Prav tam, člena 7(a) in 26(1).

99 Glej tudi Mnenje 15/2011 delovne skupine iz člena 29 z dne 13. julija 2011 o pojmu privolitve, WP 187, Bruselj, str. 12.

100 Ta primer je vzet iz prav tam, str. 15.

101 Uredba Komisije (EU) št. 1141/2011 z dne 10. novembra 2011 o spremembi Uredbe (ES) št. 272/2009 o dopolnitvi skupnih osnovnih standardov na področju varovanja v civilnem letalstvu v zvezi z uporabo varnostnih skenerjev na letališčih EU, UL 2011, L 293, in Izvedbena uredba Komisije (EU) št. 1147/2011 z dne 11. novembra 2011 o spremembi Uredbe (EU) št. 185/2010 za izvajanje skupnih osnovnih standardov za varnost letalstva v zvezi z uporabo varnostnih skenerjev na letališčih EU, UL 2011, L 294.

Prostovoljna privolitev bi lahko bila ogrožena tudi v podrejenih položajih, ko je med upravljavcem, ki mora dobiti privolitev, in posameznikom, na katerega se nanašajo osebni podatki in ki mora podati privolitev, precejšnje ekonomsko ali drugo neravnovesje.[102]

Primer: Veliko podjetje namerava izključno zaradi izboljšanja komunikacije znotraj podjetja ustvariti imenik, ki bo vseboval imena vseh zaposlenih, njihov položaj v podjetju in naslov sedeža. Vodja kadrovske službe predlaga, naj se v imenik doda fotografija vsakega zaposlenega, da bo na primer 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 je jasno, da objava fotografije v imeniku kot taka nima negativnih posledic, poleg tega se zaposleni pri delodajalcu verjetno ne bo znašel v nemilosti, če se ne bo strinjal z objavo svoje fotografije v imeniku.

To pa ne pomeni, da privolitev nikoli ne more biti veljavna v okoliščinah, ko bi zavrnitev privolitve imela negativne posledice. Če na primer zavrnitev pridobitve trgovske kartice zvestobe pomeni samo, da kupec ne bo prejemal popustov za določeno blago, je 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.

Kadar pa je mogoče dovolj pomembno blago ali storitve pridobiti samo in izključno z razkritjem nekaterih osebnih podatkov tretjim osebam, privolitve posameznika, na katerega se nanašajo osebni podatki, da se razkrijejo njegovi podatki, običajno ni mogoče šteti za svobodno izbiro, zato na podlagi zakonodaje o varstvu osebnih podatkov ni veljavna.

Primer: Soglasja, ki ga potniki dajo letalski družbi, da t. i. evidence podatkov o potnikih (PNR), to je podatke o njihovi identiteti, prehranjevalnih navadah

102 Glej tudi Mnenje 8/2001 delovne skupine iz člena 29 z dne 13. septembra 2001 o obdelavi osebnih podatkov na področju delovnega prava, WP 48, Bruselj, in delovni dokument delovne skupine iz člena 29 z dne 25. novembra 2005 o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995, WP 114, Bruselj.

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 poleg privolitve potrebna še druga pravna podlaga: najverjetneje poseben zakon.

## Informirana privolitev

Posameznik, na katerega se nanašajo osebni podatki, mora imeti dovolj informacij, preden sprejme odločitev. Ali so informacije zadostne ali ne, je mogoče ugotoviti izključno za vsak primer posebej. Informirana privolitev običajno vključuje natančen in preprosto razumljiv opis vsebine, za katero je potrebna privolitev, poleg tega pa so na kratko predstavljene tudi posledice privolitve ali neprivolitve. Jezik, v katerem se te informacije navedejo, mora biti prilagojen predvidljivim naslovnikom informacij.

Informacije morajo biti posamezniku, na katerega se nanašajo osebni podatki, tudi zlahka na voljo. Dostopnost in vidnost informacij sta pomembna dejavnika. V spletnem okolju so lahko dobra rešitev večplastna informativna obvestila, saj ima posameznik, na katerega se nanašajo osebni podatki, poleg dostopa do strnjene različice informacij tudi dostop do bolj izčrpne različice.

## Posebna privolitev

Da je privolitev veljavna, mora biti posebna (določna oz. specificirana). To je neločljivo povezano s kakovostjo informacij o predmetu 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 postopki obdelave dodali ali spremenili tako, da tega ob prvotni privolitvi ni bilo mogoče razumno predvideti.

Primer: Sodišče EU je v zadevi *Deutsche Telekom AG*[103] obravnavalo vprašanje, ali ponudnik telekomunikacijskih storitev, ki je moral posredovati podatke na podlagi člena 12 *Direktive o zasebnosti in elektronskih komunikacijah*[104], pot-

103 Sodba Sodišča EU z dne 5. maja 2011 v zadevi *Deutsche Telekom AG proti Nemčiji*, C-543/09, glej zlasti točki 53 in 54.

104 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 2002, L 201.

rebuje novo privolitev posameznikov, na katere se nanašajo osebni podatki, saj prejemniki ob privolitvi prvotno niso bili poimensko navedeni.

Sodišče EU je ugotovilo, da na podlagi navedenega člena nova privolitev pred posredovanjem podatkov ni nujna, ker imajo posamezniki, na katere se nanašajo osebni podatki, na podlagi te določbe možnost privoliti samo v obdelavo, tj. objavo njihovih podatkov, in ne morejo izbirati med različnimi imeniki, v katerih bi se lahko ti podatki objavili.

Kot je poudarilo Sodišče, „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“.[105] Poleg tega „bi naročniku utegnila škoditi sama objava osebnih podatkov v imeniku, katerega namen je poseben,“[106] in ne podatek, kdo je odgovoren za objavo.

## 2.4.2. Pravica, da se privolitev kadar koli prekliče

V Direktivi o varstvu osebnih podatkov ni navedena splošna pravica, da se lahko privolitev kadar koli prekliče. Kljub temu se na splošno domneva, da taka pravica obstaja in da je treba posamezniku, na katerega se nanašajo osebni podatki, omogočiti, da jo 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.

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. Kazni, na primer globe, se ne smejo naložiti.

Če je stranka v zameno za privolitev v uporabo svojih podatkov za pošiljanje reklamne pošte prejemala 5odstotni popust na stroške hotelske sobe, poznejši preklic privolitve v prejemanje reklamne pošte ne bi smel pomeniti, da mora povrniti te popuste.

105 Sodba Sodišča EU z dne 5. maja 2011 v zadevi *Deutsche Telekom AG proti Nemčiji*, C-543/09, glej zlasti točko 61.

106 Prav tam, glej zlasti točko 62.

# 3

# Ključna načela evropske zakonodaje o varstvu podatkov

| EU | Obravnavane teme | Svet Evrope |
|---|---|---|
| Direktiva o varstvu osebnih podatkov, člen 6(1)(a) in (b)<br>Sodba Sodišča EU z dne 16. decembra 2008 v zadevi *Huber proti Bundesrepublik Deutschland*, C-524/06<br>Sodba Sodišča EU z dne 9. novembra 2010 v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, C-92/09 in C-93/09 | **Načelo zakonite obdelave** | Konvencija št. 108, člen 5(a) in (b)<br>Sodba ESČP z dne 4. maja 2000 v zadevi *Rotaru proti Romuniji* [veliki senat], pritožba št. 28341/95<br>Sodba ESČP z dne 22. oktobra 2002 v zadevi *Taylor-Sabori proti Združenemu kraljestvu*, pritožba št. 47114/99<br>Sodba ESČP z dne 28. januarja 2003 v zadevi *Peck proti Združenemu kraljestvu*, pritožba št. 44647/98<br>Sodba ESČP z dne 18. oktobra 2011 v zadevi *Khelili proti Švici*, pritožba št. 16188/07<br>Sodba ESČP z dne 26. marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81 |
| Direktiva o varstvu osebnih podatkov, člen 6(1)(b) | **Načelo opredelitve in omejitve namena** | Konvencija št. 108, člen 5(b) |

| | Načela kakovosti osebnih podatkov: | |
|---|---|---|
| Direktiva o varstvu osebnih podatkov, člen 6(1)(c) | Ustreznost osebnih podatkov | Konvencija št. 108, člen 5(c) |
| Direktiva o varstvu osebnih podatkov, člen 6(1)(d) | Točnost osebnih podatkov | Konvencija št. 108, člen 5(d) |
| Direktiva o varstvu osebnih podatkov, člen 6(1)(e) | Omejena hramba osebnih podatkov | Konvencija št. 108, člen 5(e) |
| Direktiva o varstvu osebnih podatkov, člen 6(1)(e) | Izvzetje za znanstvene raziskave in statistiko | Konvencija št. 108, člen 9(3) |
| Direktiva o varstvu osebnih podatkov, člen 6(1)(a) | Načelo poštene obdelave | Konvencija št. 108, člen 5(a)<br>Sodba ESČP z dne 27. oktobra 2009 v zadevi *Haralambie proti Romuniji*, pritožba št. 21737/03<br>Sodba ESČP z dne 6. novembra 2009 v zadevi *K. H. in drugi proti Slovaški*, pritožba št. 32881/04 |
| Direktiva o varstvu osebnih podatkov, člen 6(2) | Načelo odgovornosti | |

Načela, določena v členu 5 Konvencije št. 108, vključujejo bistvo evropske zakonodaje o varstvu osebnih podatkov. Pojavijo se tudi v členu 6 Direktive o varstvu osebnih podatkov, in sicer kot izhodišče za podrobnejše določbe v naslednjih členih navedene direktive. 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 razlagi take zakonodaje. Morebitne izjeme od teh ključnih načel in njihove omejitve se lahko določijo na nacionalni ravni;[107] biti morajo določene z zakonom, imeti morajo zakonit cilj in biti nujne v demokratični družbi. Izpolnjeni morajo biti vsi trije pogoji.

107 Konvencija št. 108, člen 9(2), Direktiva o varstvu osebnih podatkov, člen 13.

# 3.1. Načelo zakonite obdelave osebnih podatkov

## Ključne točke

- Pri razumevanju načela zakonite obdelave je treba izhajati iz pogojev za zakonito omejevanje pravice do varstva osebnih podatkov glede na člen 52(1) Listine in zahtev za upravičeno poseganje na podlagi člena 8(2) EKČP.
- V skladu s tem je obdelava osebnih osebnih podatkov zakonita samo, če:
  - je v skladu z zakonom,
  - uresničuje zakoniti cilj in
  - je v demokratični družbi nujna za dosego zakonitega cilja.

**V zakonodaji o varstvu osebnih podatkov EU in Sveta Evrope** je načelo zakonite obdelave prvo navedeno načelo; s skoraj enakimi besedami je izraženo v členu 5 Konvencije št. 108 in členu 6 Direktive o varstvu osebnih podatkov.

V nobeni od teh določb ni opredeljeno, kaj pomeni „zakonita obdelava“. Pri razumevanju tega pravnega pojma je treba izhajati iz pojma upravičeno poseganje na podlagi EKČP, kot je pojasnjen v sodni praksi ESČP, in pogojev za zakonito omejevanje na podlagi člena 52 Listine.

## 3.1.1. Zahteve za upravičeno poseganje na podlagi EKČP

Z obdelavo osebnih podatkov se lahko posega v pravico do spoštovanja zasebnega življenja posameznika, na katerega se nanašajo osebni podatki. Vendar pravica do spoštovanja zasebnega življenja ni absolutna pravica, temveč jo je treba uravnotežiti in uskladiti z drugimi zakonitimi interesi, bodisi drugih oseb (zasebni interesi) bodisi družbe kot celote (javni interesi).

Pogoji, pod katerimi je poseganje države upravičeno, so naslednji:

## V skladu z zakonom

V skladu s sodno prakso ESČP je poseganje v skladu z zakonom, če temelji na določbi nacionalnega zakona, ki ima določene značilnosti. Zakon mora biti „dostopen zadevnim osebam in imeti predvidljive učinke".[108] Predpis je predvidljiv, „če je opredeljen dovolj natančno, da lahko vsak posameznik (če je treba, ob ustreznem nasvetu) usmerja svoje ravnanje".[109] „Stopnja natančnosti, ki se v zvezi s tem zahteva za ‚zakonodajo', je odvisna od zadevne vsebine."[110]

Primer: ESČP je v zadevi *Rotaru proti Romuniji*[111] ugotovilo kršitev člena 8 EKČP, ker je bilo z romunskim zakonom dovoljeno zbiranje in snemanje informacij, ki vplivajo na nacionalno varnost, ter njihovo arhiviranje v tajnih datotekah, ne da bi bile določene omejitve za izvajanje teh pooblastil, kar 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 zaradi teh pomanjkljivosti ugotovilo, da nacionalni zakon ne izpolnjuje zahteve glede predvidljivosti na podlagi člena 8 EKČP in da je ta člen kršen.

Primer: V zadevi *Taylor-Sabori proti Združenemu kraljestvu*[112] 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

108 Sodba ESČP z dne 16. februarja 2000 v zadevi *Amann proti Švici* [veliki senat], pritožba št. 27798/95, točka 50; glej tudi sodbi ESČP z dne 25. marca 1998 v zadevi *Kopp proti Švici*, pritožba št. 23224/94, točka 55, in z dne 10. februarja 2009 v zadevi *Iordachi in drugi proti Moldaviji*, pritožba št. 25198/02, točka 50.

109 Sodba ESČP z dne 16. februarja 2000 v zadevi *Amann proti Švici* [veliki senat], pritožba št. 27798/95, točka 56; glej tudi sodbi ESČP z dne 2. avgusta 1984 v zadevi *Malone proti Združenemu kraljestvu*, pritožba št. 8691/79, točka 66; in z dne 25. marca 1983 v zadevi *Silver in drugi proti Združenemu kraljestvu*, pritožbe št. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, točka 88.

110 Sodbe ESČP z dne 26. aprila 1979 v zadevi *The Sunday Times proti Združenemu kraljestvu*, pritožba št. 6538/74, točka 49; glej tudi sodbo ESČP z dne 25. marca 1983 v zadevi *Silver in drugi proti Združenemu kraljestvu*, pritožbe št. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, točka 88.

111 Sodba ESČP z dne 4. maja 2000 v zadevi *Rotaru proti Romuniji* [veliki senat], pritožba št. 28341/95, točka 57; glej tudi sodbe ESČP z dne 28. junija 2007 v zadevi *Association for European Integration and Human Rights in Ekimdzhiev proti Bolgariji*, pritožba št. 62540/00; z dne 21. junija 2011 v zadevi *Shimovolos proti Rusiji*, pritožba št. 30194/09, in z dne 31. maja 2005 v zadevi *Vetter proti Franciji*, pritožba št. 59842/00.

112 Sodba ESČP z dne 22. oktobra 2002 v zadevi *Taylor-Sabori proti Združenemu kraljestvu*, pritožba št. 47114/99.

in obdolžen zarote pri dobavi nadzorovane droge. Dokazi tožilstva zoper njega so deloma temeljili na zapisih sporočil pozivnika, ki jih je policija takrat prepisala. Vendar britanska zakonodaja v času sojenja pritožniku ni vsebovala določb, s katerimi bi bilo urejeno prestrezanje sporočil, poslanih prek zasebnih telekomunikacijskih sistemov. Poseganje v to pravico torej ni bilo „v skladu z zakonom". ESČP je ugotovilo, da je bil kršen člen 8 EKČP.

## Uresničevanje zakonitega cilja

Zakoniti cilj je lahko eden od navedenih javnih interesov ali ena od pravic in svoboščin drugih.

Primer: V zadevi *Peck proti Združenemu kraljestvu*[113] je pritožnik na ulici poskušal storiti samomor z rezanjem žil na zapestjih, pri čemer se ni zavedal, da ga je med poskusom posnela videonadzorna kamera . Rešila ga je policija, ki je spremljala nadzorne kamere, nato pa je policijski organ video posnetek predal 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.

## Nujno v demokratični družbi

Po navedbah ESČP „pojem nujnost pomeni, da poseganje temelji na pomembni socialni potrebi in zlasti da je sorazmerno z uresničevanjem zakonitega cilja".[114]

Primer: V zadevi *Khelili proti Švici*[115] je policija med policijsko kontrolo ugotovila, da ima pritožnica pri sebi vizitke, na katerih piše: „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, pri čemer je ta poklic vztrajno zanikala. Zahtevala je, naj se beseda „prostitutka" izbriše iz policijske računalniške evidence. ESČP je načeloma priznalo, da je lahko hramba osebnih podatkov

113 Sodba ESČP z dne 28. januarja 2003 v zadevi *Peck proti Združenemu kraljestvu*, pritožba št. 44647/98, zlasti točka 85.

114 Sodba ESČP z dne 26. marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81, točka 58.

115 Sodba ESČP z dne 18. oktobra 2011 v zadevi *Khelili proti Švici*, pritožba št. 16188/07.

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 socialne potrebe" v smislu člena 8 EKČP. Ker morajo organi dokazati točnost podatkov, shranjenih o pritožnici, in glede na resnost poseganja 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: ESČP je v zadevi *Leander proti Švedski*[116] 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 preverjanja, ki jih 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.

## 3.1.2. Pogoji za zakonito omejevanje na podlagi Listine EU

Zgradba in besedilo Listine sta drugačna kot pri EKČP. V Listini ni govora o poseganju v zagotovljene pravice, temveč vsebuje določbo o omejitvi(-ah) 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, na primer obdelave osebnih podatkov, dopustne samo, če:

- so določene z zakonom;
- spoštujejo bistvo pravice do varstva osebnih podatkov;
- so nujne in zanje velja načelo sorazmernosti ter

116 Sodba ESČP z dne 26. marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81, točki 59 in 67.

- izpolnjujejo cilje v splošnem interesu, ki jih priznava Unija, ali izhajajo iz potrebe po varstvu pravic in svoboščin drugih.

Primer: Sodišče EU je v zadevi *Volker und Markus Schecke*[117] ugotovilo, da sta Svet in Komisija z naložitvijo obveznosti objave osebnih podatkov vseh fizičnih oseb, ki so upravičene do pomoči iz [določenih kmetijskih skladov], ne da bi se ob 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.

Sodišče EU je zato ugotovilo, da je treba razveljaviti nekatere določbe Uredbe Sveta (ES) št. 1290/2005 in v celoti razveljaviti Uredbo št. 259/2008.[118]

Pogoji za zakonito obdelavo v členu 52(1) Listine kljub drugačnemu besedilu spominjajo na člen 8 (2) EKČP. Dejansko je treba šteti, da so pogoji iz člena 52(1) Listine v skladu s pogoji iz člena 8(2) EKČP, saj je v prvem stavku člena 52(3) Listine navedeno, da „[k]olikor 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 v skladu z zadnjim stavkom člena 52(3) „[t]a določba ne preprečuje širšega varstva po pravu Unije". S primerjavo člena 8(2) EKČP in prvega stavka člena 52(3) to lahko pomeni samo, da so pogoji za upravičeno vmešavanje v skladu s členom 8(2) EKČP minimalne zahteve za zakonito omejevanje pravice do varstva osebnih podatkov na podlagi Listine. Zato morajo biti za zakonito obdelavo osebnih podatkov na podlagi prava EU izpolnjeni vsaj pogoji iz člena 8(2) EKČP; vendar se lahko z zakonodajo EU določijo dodatne zahteve za posebne primere.

Ujemanje načela zakonite obdelave po pravu EU z zadevnimi določbami EKČP potrjuje tudi člen 6(3) PEU, ki določa, da so „[t]emeljne pravice, kakor jih zagotavlja

117 Sodba Sodišča EU z dne 9. novembra 2010 v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, C-92/09 in C-93/09, točki 89 in 86.

118 Uredba Sveta (ES) št. 1290/2005 z dne 21. junija 2005 o financiranju skupne kmetijske politike, UL 2005, L 209; 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 2008, L 76.

Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin[,] [...] kot splošna načela del prava Unije".

## 3.2. Načelo določenosti in omejitve namena

### Ključne točke

- Namen obdelave osebnih podatkov mora biti jasno določen pred začetkom obdelave.
- Po pravu EU mora biti namen obdelaveizrecno določen; po pravu Sveta Evrope je to vprašanje prepuščeno nacionalni zakonodaji.
- Obdelava za nedoločene namene ni v skladu s pravom o varstvu osebnih podatkov.
- Za nadaljnjo uporabo osebnih podatkov za drug namen je potrebna dodatna pravna podlaga, če novi namen obdelave ni v skladu s prvotnim.
- Posredovanje osebnih podatkov tretjim osebam je nov namen, ki potrebuje dodatno pravno podlago.

Načelo določenosti in omejitve namena ali načelo namembnosti (finality principle) v bistvu pomeni, da je zakonitost obdelave osebnih podatkov odvisna od namena obdelave.[119] Upravljavec mora namen določiti in izkazati pred začetkom obdelave podatkov.[120] **Po pravu EU** je treba to storiti s prijavo (notifikacijo), tj. z uradnim sporočilom ustreznemu nadzornemu organu, ali vsaj z notranjo dokumentacijo, ki jo mora upravljavec predložiti v pregled nadzornim organom in mora biti dostopna posameznику, na katerega se nanašajo osebni podatki.

Obdelava osebnih podatkov za nedoločene in/ali neomejene namene je nezakonita.

Vsak nov namen obdelave osebnih podatkov mora imeti svojo pravno podlago in se ne more zanašati na dejstvo, da so bili osebni podatki prvotno pridobljeni ali obdelani za drug zakonit namen. Zakonita obdelava je tako omejena na prvotno določen namen, za vsak nov namen obdelave pa je potrebna nova posebna pravna podlaga. Razkritje osebnih podatkov tretjim osebam je treba proučiti še posebno previdno,

119 Konvencija št. 108, člen 5(b), Direktiva o varstvu podatkov, člen 6(1)(b).

120 Glej tudi Mnenje 3/2013 delovne skupine iz člena 29 z dne 2. aprila 2013 o omejitvi namena, WP 203, Bruselj.

saj razkritje običajno pomeni nov namen, za kar je potrebna 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 hrana halal in 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 Konvenciji št. 108 in Direktivi o varstvu osebnih podatkov uporablja pojem združljivosti: uporaba podatkov za združljive namene je dovoljena na podlagi prvotne pravne podlage. Vendar pomen „združljivosti" ni opredeljen in je prepuščen razlagi za vsak primer posebej.

Primer: Prodaja osebnih podatkov o strankah družbe Sonček, ki jih je ta pridobila v okviru upravljanja odnosov s strankami, družbi za neposredno trženje, Mesečina, ki želi te podatke uporabiti pri trženjskih kampanjah tretjih družb, je nov namen, ki ni združljiv z upravljanjem odnosov s strankami, tj. s prvotnim namenom družbe Sonček za zbiranje podatkov o strankah. Za prodajo 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 Direktivi o varstvu osebnih podatkov je izrecno navedeno, da se „[n]adaljnja obdelava podatkov v zgodovinske, statistične ali znanstvene namene [...] ne šteje za nezdružljivo, če države članice zagotovijo ustrezne zaščitne ukrepe".[121]

121 Primer takih nacionalnih določb je avstrijski zakon o varstvu osebnih podatkov (*Datenschutzgesetz*), Fed. Law Gazette I, št. 165/1999, točka 46, ki je na voljo v angleščini na: www.dsk.gv.at/DocView.axd?CobId=41936.

Primera: 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.

Če naj bi se isti podatki posredovali tretji osebi, družbi Zvezdni sij, za izključno statistične namene, bi bilo posredovanje dovoljeno brez dodatne pravne podlage, vendar samo, če bi bili uvedeni ustrezni zaščitni ukrepi, na primer prikritje identitete posameznikov, na katere se nanašajo osebni podatki, saj identiteta za statistične namene običajno ni nujna.

## 3.3. Načela kakovosti osebnih podatkov

**Ključne točke**

- Upravljavec mora načela kakovosti osebnih podatkov izvajati v vseh postopkih obdelave.
- Na podlagi načela omejene hrambe osebnih podatkov je treba podatke izbrisati takoj, ko niso več potrebni za namene, za katere so bili zbrani.
- Izjeme od načela omejene hrambe morajo biti določene z zakonom, v zvezi z njimi pa so potrebni posebni zaščitni ukrepi za varstvo posameznikov, na katere se nanašajo osebni podatki.

### 3.3.1. Načelo sorazmernosti osebnih podatkov

Obdelujejo se samo osebni podatki, ki so „ustrezni in ne pretirani glede na namene, za katere se zbirajo in/ali daljenaprej obdelujejo“.[122] Kategorije podatkov, izbranih za obdelavo, morajo biti nujne za dosego izraženega skupnega cilja postopkov obdelave, upravljavec pa mora zbiranje podatkov strogo omejiti na informacije, ki so neposredno pomembne za izrecni namen obdelave.

V sodobni družbi je treba v zvezi z načelom sorazmernosti osebnih podatkov upoštevati še nekaj: z uporabo posebne tehnologije za boljše varovanje zasebnosti se je

122 Konvencija št. 108, člen 5(c), in Direktiva o varstvu osebnih podatkov, člen 6(1)(c).

mogoče včasih nasploh izogniti uporabi osebnih podatkov ali uporabiti psevdonimizirane podatke, s čimer se zagotovi spoštovanje zasebnosti. To je zlasti primerno v obsežnejših sistemih 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 potovalno kartico.

Načelo sorazmernosti 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. Osebni podatki se ne bi zbirali, kar je najboljša rešitev v smislu načela sorazmernosti, saj je treba v skladu z njim čim bolj zmanjšati zbiranje osebnih podatkov.

## 3.3.2. Načelo točnosti osebnih podatkov

Upravljavec, ki hrani osebne informacije, lahko te informacije uporabi samo, če z razumno gotovostjo poskrbi, da so podatki točni in posodobljeni.

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

Primer: Podjetje, ki prodaja pohištvo, je zbralo podatke o identiteti in naslovu strank, da bi jim izstavilo račun. Šest mesecev pozneje želi isto podjetje začeti trženjsko kampanjo in bi se rado obrnilo na nekdanje stranke. Da bi vzpostavilo stik z njimi, želi dobiti dostop do registra stalnega prebivalstva, ki najverjetneje vsebuje posodobljene naslove, saj morajo osebe s stalnim prebivališčem po zakonu registru sporočiti trenutni naslov. Dostop do podatkov v tem registru imajo samo osebe in subjekti, ki izkažejo upravičen razlog.

V teh okoliščinah se podjetje ne more sklicevati na to, da morajo biti podatki točni in posodobljeni, ter trditi, da ima pravico iz registra stalnega prebivalstva pridobiti podatke o novem naslovu vseh svojih nekdanjih strank. Podatki so bili zbrani ob izstavitvi računa; zato je pomemben naslov ob prodaji. Za zbiranje podatkov o novem naslovu ni nikakršne pravne podlage, saj trženje ni interes, ki bi prevladal nad pravico do varstva osebnih podatkov, zato ne more biti upravičen razlog za dostop do osebnih podatkov v registru.

Posodabljanje shranjenih osebnih podatkov je lahko celo zakonsko prepovedano, saj je glavni namen shranjevanja podatkov dokumentiranje dogodkov.

Primer: Zdravstvenega operacijskega protokola ni dovoljeno spreminjati, tj. „posodabljati", tudi če se ugotovitve, navedene v protokolu, pozneje izkažejo za napačne. V takih okoliščinah je dovoljeno samo dodajanje opomb k protokolu, če so jasno označene kot naknadni vnosi.

Nasprotno pa je lahko redno preverjanje točnosti podatkov, vključno s posodabljanjem, v nekaterih primerih nujno potrebno zaradi škode, ki bi jo lahko posameznik, na katerega se nanašajo osebni podatki, utrpel, če bi podatki ostali netočni.

Primer: Če nekdo želi skleniti pogodboz bančno ustanovo, bo banka običajno preverila kreditno sposobnost morebitne 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 ta oseba naleti na resne težave. Upravljavci takih podatkovnih zbirk si morajo zato še posebno prizadevati za upoštevanje načela točnosti.

Poleg tega se lahko podatki, ki se ne navezujejo na dejstva, ampak na sume, na primer v kazenskih preiskavah, zbirajo in hranijo tako dolgo, dokler ima upravljavec pravno podlago za zbiranje takih informacij in ima dovolj upravičenih razlogov za tak sum.

### 3.3.3. Načelo omejene hrambe osebnih podatkov

Države članice morajo na podlagi člena 6(1)(e) Direktive o varstvu osebnih podatkov in člena 5(e) Konvencije št. 108 zagotoviti, da so osebni podatki „shranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se osebni podatki nanašajo, le toliko

časa, kolikor je potrebno za namene, za katere so bili podatki zbrani ali za katere se naprej obdelujejo". Ko so ti nameni izpolnjeni, je treba torej osebne podatke izbrisati.

ESČP je v zadevi *S. in Marper* ugotovilo, da mora biti hramba osebnih podatkov glede na ključna načela iz zadevnih instrumentov Sveta Evrope ter zakonodajo in prakso drugih pogodbenic sorazmerna glede na namen zbiranja in časovno omejena, zlasti v policijskem sektorju.[123]

Vendar 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 anonimizacijo ali psevdonimizacijo podatkov.

Hramba osebnih podatkov za poznejšo znanstveno, zgodovinsko ali statistično uporabo je v Direktivi o varstvu osebnih podatkov izrecno izvzeta iz načela omejene hrambe podatkov.[124] Vendar morajo tako trajno hrambo in uporabo osebnih podatkov spremljati posebni zaščitni ukrepi na podlagi nacionalne zakonodaje.

## 3.4. Načelo poštene obdelave osebnih podatkov

### Ključne točke

- Poštena obdelava osebnih podatkov pomeni preglednost obdelave, zlasti za posameznike, na katere se nanašajo osebni podatki.
- Upravljavci morajo posameznike, na katere se nanašajo osebni podatki, obvestiti vsaj o namenu obdelave ter o identiteti in naslovu upravljavca.
- Obdelava osebnih podatkov ne sme biti tajna in prikrita, razen če to ni izrecno dovoljeno z zakonom.
- Posamezniki, na katere se nanašajo osebni podatki, imajo pravico do dostopa do svojih podatkov, ne glede na to, kje se ti podatki obdelujejo.

123 Sodba ESČP z dne 4. decembra 2008 v združenih zadevah *S. in Marper proti Združenemu kraljestvu*, pritožbi št. 30562/04 in 30566/04; glej tudi na primer sodbo ESČP z dne 13. novembra 2012 v zadevi *M. M. proti Združenemu kraljestvu*, pritožba št. 24029/07.

124 Direktiva o varstvu osebnih podatkov, člen 6(1)(e).

Načelo poštene obdelave osebnih podatkov se navezuje predvsem na razmerje med upravljavcem in posameznikom, na katerega se nanašajo osebni podatki.

## 3.4.1. Preglednost

To načelo določa obveznost upravljavca, da posameznike, na katere se nanašajo osebni podatki, obvešča o tem, kako se njihovi podatki uporabljajo.

> Primer: V zadevi *Haralambie proti Romuniji*[125] je pritožnik zaprosil za dostop do spisa, ki ga je v zvezi z njim hranila tajna služba, vendar je bilo njegovi prošnji ugodeno šele po petih letih. ESČP je opozorilo, da imajo posamezniki, o katerih imajo javni organi osebne spise, življenjski interes za to, da se jim omogoči dostop do teh spisov. Dolžnost organov je bila, da zagotovijo učinkovit postopek za pridobitev dostopa do takih informacij. ESČP je menilo, da niti količina poslanih spisov niti pomanjkljivosti sistema arhiviranja ne upravičujeta petletne zamude pri ugoditvi pritožnikovi prošnji za dostop do njegovih spisov. Organi pritožniku niso zagotovili učinkovitega in dostopnega postopka, ki bi mu v razumnem času zagotovil dostop do osebnih spisov. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Postopki obdelave morajo biti posameznikom, na katere se nanašajo osebni podatki, razloženi na lahko dostopen način, tako da razumejo, kaj se bo zgodilo z njihovimi podatki. Posameznik, na katerega se nanašajo osebni podatki, ima tudi pravico, da od upravljavca izve, ali se njegovi podatki obdelujejo, in če se, kateri.

## 3.4.2. Vzpostavitev zaupanja

Upravljavci morajo posameznikom, na katere se nanašajo osebni podatki, in splošni javnosti pisno zagotoviti, da bodo osebnih podatke obdelovali zakonito in pregledno. Postopki obdelave se ne smejo izvajati tajno in ne smejo imeti nepredvidljivih škodljivih učinkov. Upravljavci morajo zagotoviti, da so kupci, stranke ali državljani obveščeni o uporabi svojih osebnih podatkov. Poleg tega morajo upravljavci čim natančneje upoštevati želje posameznika, na katerega se nanašajo osebni podatki, zlasti če je njegova privolitev pravna podlaga za obdelavo osebnih podatkov.

125 Sodba ESČP z dne 27. oktobra 2009 v zadevi *Haralambie proti Romuniji*, pritožba št. 21737/03.

Primer: V zadevi *K. H. in drugi proti Slovaški*[126] je pritožbo vložilo osem Rominj, ki so se med nosečnostjo zdravile v dveh bolnišnicah na vzhodu Slovaške in so tam tudi rodile. Zatem 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 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 zdravstvenih kartotek utemeljila predvsem s potrebo po zaščiti zadevnih informacij pred zlorabo. Vendar ESČP ni razumelo, kako bi lahko pritožnice, ki jim je bil vsekakor 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.

Poštena obdelava osebnih podatkov pomeni tudi, da so upravljavci pripravljeni preseči obvezne minimalne zakonske zahteve v korist posameznikov, na katere se nanašajo osebni podatki, če je to potrebno glede na zakonite interese takih posameznikov.

126 Sodba ESČP z dne 6. novembra 2009 v zadevi *K. H. in drugi proti Slovaški*, pritožba št. 32881/04.

## 3.5. Načelo odgovorne obdelave osebnih podatkov

### Ključne točke

- Načelo odgovorne obdelave osebnih podatkov pomeni, da morajo upravljavci v okviru svojih dejavnosti obdelave dejavno izvajati ukrepe za spodbujanje in zagotavljanje varstva osebnih podatkov.
- Upravljavci so odgovorni za skladnost svojih dejavnosti obdelave z zakonodajo o varstvu osebnih podatkov.
- Upravljavci bi morali posameznikom, na katere se nanašajo osebni podatki, splošni javnosti in nadzornim organom kadar koli dokazati, da upoštevajo določbe o varstvu osebnih podatkov.

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 delovanja varstva osebnih podatkov v praksi. V smernicah je izoblikovano načelo odgovornosti, v skladu s katerim „mora biti upravljavec osebnih podatkov odgovoren za upoštevanje ukrepov, s katerimi se uresničujejo zgoraj navedena [vsebinska] načela".[127]

Medtem ko v Konvenciji št. 108 ni sklicevanja na odgovornost upravljavcev, tako da je to v bistvu prepuščeno nacionalni zakonodaji, pa je v členu 6(2) Direktive o varstvu osebnih podatkov navedeno, da mora upravljavec zagotoviti upoštevanje načel v zvezi s kakovostjo osebnih podatkov iz odstavka 1.

Primer: Načelo odgovorne obdelave osebnih podatkov je poudarjeno z zakonodajnim primerom spremembe Direktive o zasebnosti in elektronskih komunikacijah 2002/58/ES iz leta 2009.[128] Člen 4 navedene direktive v spremenjeni obliki določa obveznost izvajanja varnostne politike, in sicer da se „zagot[ovi] izvajanje varnostne politike pri obdelavi osebnih podatkov". Kar zadeva varno-

127 OECD (2013), Smernice o varstvu zasebnosti in čezmejnem prenosu osebnih podatkov, člen 14.

128 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 2009, L 337, str. 11.

stne določbe iz navedene direktive, se je zakonodajalec torej odločil, da je treba uvesti izrecno zahtevo po določitvi in izvajanju varnostne politike.

Po mnenju delovne skupine iz člena 29[129] je bistvo odgovornosti upravljavčeva obveznost, da:

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

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

Načelo odgovorne obdelave osebnih podatkov torej pomeni, da morajo upravljavci dejavno dokazati skladnost s predpisi in ne smejo samo čakati, da bodo posamezniki, na katere se nanašajo osebni podatki, in nadzorni organi opozorili na pomanjkljivosti.

129 Mnenje 3/2010 delovne skupine iz člena 29 z dne 13. julija 2010 o načelu odgovornosti, WP 173, Bruselj.

# 4

# Pravila evropskega prava o varstvu osebnih podatkov

| EU | Obravnavane teme | Svet Evrope |
|---|---|---|
| **Pravila o zakoniti obdelavi neobčutljivih osebnih podatkov** | | |
| Direktiva o varstvu osebnih podatkov, člen 7(a) | **Privolitev** | Priporočilo o profiliranju, člen 3(4)(b) in člen 3(6) |
| Direktiva o varstvu osebnih podatkov, člen 7(b) | **(Pred)pogodbeno razmerje** | Priporočilo o profiliranju, člen 3(4)(b) |
| Direktiva o varstvu osebnih podatkov, člen 7(c) | **Pravne obveznosti upravljavca** | Priporočilo o profiliranju, člen 3(4)(a) |
| Direktiva o varstvu osebnih podatkov, člen 7(d) | **Življenjski interesi posameznika, na katerega se nanašajo osebni podatki** | Priporočilo o profiliranju, člen 3(4)(b) |
| Direktiva o varstvu osebnih podatkov, člena 7(e) in 8(4)<br>Sodba Sodišča EU z dne 16. decembra 2008 v zadevi *Huber proti Bundesrepublik Deutschland*, C-524/06 | **Javni interes in izvrševanje javne oblasti** | Priporočilo o profiliranju, člen 3(4)(b) |
| Direktiva o varstvu osebnih podatkov, člen 7(f) ter člen 8(2) in 8(3)<br>Sodba Sodišča z dne 24. novembra 2011 v združenih zadevah *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, C-468/10 in C-469/10 | **Zakoniti interesi drugih** | Priporočilo o profiliranju, člen 3(4)(b) |

| | | |
|---|---|---|
| **Pravila o zakoniti obdelavi občutljivih osebnih podatkov** | | |
| Direktiva o varstvu osebnih podatkov, člen 8(1) | **Splošna prepoved obdelave** | Konvencija št. 108, člen 6 |
| Direktiva o varstvu osebnih podatkov, člen 8(2) do (4) | **Izjeme od splošne prepovedi** | Konvencija št. 108, člen 6 |
| Direktiva o varstvu osebnih podatkov, člen 8(5) | **Obdelava osebnih podatkov o (kazenskih) obsodbah** | Konvencija št. 108, člen 6 |
| Direktiva o varstvu osebnih podatkov, člen 8(7) | **Obdelava identifikacijskih številk** | |
| **Pravila o varni obdelavi osebnih podatkov** | | |
| Direktiva o varstvu podatkov, člen 17 | **Obveznost zagotovitve varne obdelave** | Konvencija št. 108, člen 7<br>Sodba ESČP z dne 17. julija 2008 v zadevi *I. proti Finski*, pritožba št. 20511/03 |
| Direktiva o zasebnosti in elektronskih komunikacijah, člen 4(2) | **Uradno obveščanje o kršitvah varnosti podatkov** | |
| Direktiva o varstvu osebnih podatkov, člen 16 | **Obveznost zaupnosti** | |
| **Pravila o preglednosti obdelave osebnih podatkov** | | |
| | **Preglednost na splošno** | Konvencija št. 108, člen 8(a) |
| Direktiva o varstvu osebnih podatkov, člena 10 in 11 | **Informacije** | Konvencija št. 108, člen 8(a) |
| Direktiva o varstvu osebnih podatkov, člena 10 in 11 | **Izjeme od obveznosti obveščanja** | Konvencija št. 108, člen 9 |
| Direktiva o varstvu osebnih podatkov, člena 18 in 19 | **Uradno obveščanje** | Priporočilo o profiliranju, člen 9(2)(a) |
| **Pravila o spodbujanju skladnosti** | | |
| Direktiva o varstvu osebnih podatkov, člen 20 | **Predhodno preverjanje** | |
| Direktiva o varstvu osebnih podatkov, člen 18(2) | **Odgovorne osebe za varstvo osebnih podatkov** | Priporočilo o profiliranju, člen 8(3) |
| Direktiva o varstvu osebnih podatkov, člen 27 | **Pravila ravnanja** | |

Načela so nujno splošna. Njihova uporaba v konkretnih primerih je deloma odvisna od razlage in izbire sredstev. Po **pravu Sveta Evrope** je pogodbenicam Konvencije št. 108 prepuščeno, da tako različno razlago pojasnijo v nacionalni zakonodaji. Položaj v **pravu EU** je drugačen: za uveljavitev varstva osebnih podatkov na notranjem trgu so se že na ravni EU zdela nujna podrobnejša pravila, da bi uskladili raven varstva osebnih podatkov v nacionalnih zakonodajah držav članic. Z Direktivo o varstvu osebnih podatkov se na podlagi načel iz njenega člena 6 uvajajo podrobna pravila, ki jih je treba dosledno uvesti v nacionalno zakonodajo. V naslednjih opombah k podrobnim pravilom o varstvu osebnih podatkov na evropski ravni je zato obravnavano predvsem pravo EU.

## 4.1. Pravila o zakoniti obdelavi osebnih podatkov

### Ključne točke

- Osebni podatki se lahko obdelujejo zakonito, če:
  - obdelava temelji na privolitvi posameznika, na katerega se nanašajo osebni podatki;
  - je obdelava osebnih podatkov posameznikov nujna zaradi njihovih življenjskih interesov ali
  - so razlog za obdelavo zakoniti interesi drugih, vendar samo, če nad njimi ne prevladajo interesi varstva temeljnih pravic posameznikov, na katere se nanašajo osebni podatki.
- Za zakonito obdelavo občutljivih osebnih podatkov velja posebna, strožja ureditev.

Direktiva o varstvu osebnih podatkov vsebuje dva različna sklopa pravil za zakonito obdelavo osebnih podatkov: enega za neobčutljive osebnih podatke v členu 7 in enega za občutljive osebnih podatke v členu 8.

### 4.1.1. Zakonita obdelava neobčutljivih osebnih podatkov

Poglavje II Direktive 95/46 z naslovom „Splošna pravila o zakonitosti obdelave osebnih podatkov“ določa, da je treba ob upoštevanju izjem, dovoljenih na podlagi

člena 13, pri vsaki obdelavi osebnih podatkov upoštevati, prvič, načela v zvezi s kakovostjo osebnih podatkov iz člena 6 Direktive o varstvu osebnih podatkov in, drugič, merila za zakonitost obdelave osebnih podatkov iz člena 7.[130] Tako so pojasnjeni primeri, v katerih je obdelava neobčutljivih osebnih podatkov zakonita.

## Privolitev

**V pravu Sveta Evrope** privolitev ni navedena v členu 8 EKČP ali Konvenciji št. 108, je pa navedena v sodni praksi ESČP in v več priporočilih Sveta Evrope. **V pravu EU** je privolitev kot podlaga za zakonito obdelavo osebnih podatkov dokončno uvedena s členom 7(a) Direktive o varstvu osebnih podatkov, izrecno pa je navedena tudi v členu 8 Listine.

## Pogodbeno razmerje

Podlaga za zakonito obdelavo osebnih podatkov **po pravu EU**, navedena v členu 7(b) Direktive o varstvu osebnih podatkov, je tudi, če je obdelava „potrebna za izvajanje pogodbe, katere stranka je posameznik, na katerega se nanašajo osebni podatki". S to določbo so zajeta tudi predpogodbena razmerja. Na primer: stranka namerava skleniti pogodbo, vendar tega še ni storila, ker verjetno 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 posameznika, na katerega se osebni podatki nanašajo, pred sklenitvijo pogodbe".

**Kar zadeva pravo Sveta Evrope**, je „varstvo pravic in svoboščin drugih" v členu 8(2) EKČP navedeno kot razlog za zakonito poseganje v pravico do varstva osebnih podatkov.

## Pravne obveznosti upravljavca

**V pravu EU** je nato izrecno navedeno še eno merilo za zakonito obdelavo osebnih podatkov, in sicer če „je obdelava potrebna za skladnost z zakonsko obveznostjo, ki velja za upravljavca" (člen 7(c) Direktive o varstvu osebnih podatkov). Ta določba se nanaša na upravljavce v zasebnem sektorju; pravne obveznosti upravljavcev

130 Sodbe Sodišča EU z dne 20. maja 2003 v združenih zadevah *Österreichischer Rundfunk in drugi*, C-465/00, C-138/01 in C-139/01, točka 65; z dne 16. decembra 2008 v zadevi *Huber proti Bundesrepublik Deutschland*, C-524/06, točka 48, in z dne 24. novembra 2011 v združenih zadevah *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, C-468/10 in C-469/10, točka 26.

osebnih podatkov v javnem sektorju so zajete s členom 7(e) navedene direktive. Upravljavci v zasebnem sektorju morajo v skladu z zakonom pogosto obdelovati osebne podatke o drugih; na primer zdravniki in bolnišnice imajo pravno obveznost, da podatke o zdravljenju bolnikov hranijo več let, delodajalci morajo podatke o svojih zaposlenih obdelovati zaradi socialne varnosti in obdavčitve, podjetja pa morajo zaradi obdavčitve obdelovati podatke o svojih strankah.

V okviru obveznega prenosa podatkov o potnikih z letalskih družb na tuje organe za nadzor nad priseljevanjem se je pojavilo vprašanje, ali so lahko pravne obveznosti na podlagi *tujega* prava zakonita podlaga za obdelavo osebnih podatkov na podlagi prava EU (to vprašanje je podrobneje obravnavano v razdelku 6.2).

Pravne obveznosti upravljavca so podlaga za zakonito obdelavo osebnih podatkov tudi **po pravu Sveta Evrope.** Kot je bilo že poudarjeno, so pravne obveznosti upravljavca v zasebnem sektorju samo en primer zakonitih interesov drugih, kot je navedeno v členu 8(2) EKČP. Zgornji primer je zato upošteven tudi za pravo Sveta Evrope.

## Življenjski interesi posameznika, na katerega se nanašajo osebni podatki

**V pravu EU** člen 7(d) Direktive o varstvu osebnih podatkov določa, da je obdelava osebnih podatkov zakonita, če je „potrebna za varstvo življenjskih interesov posameznikov, na katere se osebni podatki nanašajo“. Taki interesi, ki so tesno povezani s preživetjem posameznika, na katerega se nanašajo osebni podatki, bi lahko bili na primer podlaga za zakonito uporabo zdravstvenih podatkov ali podatkov o pogrešanih osebah.

**V pravu Sveta Evrope** življenjski interesi posameznika, na katerega se nanašajo osebni podatki, v členu 8 EKČP niso navedeni kot razlog za zakonito poseganje v pravico do varstva osebnih podatkov. Vendar so življenjski interesi posameznika, na katerega se nanašajo osebni podatki, v nekaterih priporočilih Sveta Evrope, ki na določenih področjih dopolnjujejo Konvencijo št. 108, izrecno navedeni kot podlaga za zakonito obdelavo osebnih podatkov.[131] Življenjski interesi posameznika, na katerega se nanašajo osebni podatki, naj bi bili seveda zajeti v upravičenih razlogih za obdelavo osebnih podatkov: varstvo temeljnih pravic ne bi smelo nikoli ogrožati življenjskih interesov osebe, ki je zaščitena.

131 Glej priporočilo o profiliranju, člen 3(4)(b).

## Javni interes in izvrševanje javne oblasti

Ker so lahko javne zadeve urejene različno, člen 7(e) Direktive o varstvu osebnih podatkov določa, da se lahko osebni podatki zakonito obdelujejo, če je obdelava „potrebna za izvajanje naloge, ki se opravlja v javnem interesu ali pri izvrševanju javne oblasti, dodeljene upravljavcu ali tretji stranki, ki so ji posredovani podatki […]".[132]

Primer: V zadevi *Huber proti Bundesrepublik Deutschland*[133] je g. 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 imajo stalno prebivališče 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 predložilo vprašanje, ali je obdelava osebnih podatkov v registru, na primer centralnem registru tujcev, do katerega imajo dostop tudi drugi javni organi, združljiva s pravom EU, ker za nemške državljane tak register ne obstaja.

Sodišče EU je najprej navedlo, da je lahko obdelava osebnih podatkov na podlagi člena 7(e) navedene direktive zakonita samo, 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 […] – ob upoštevanju cilja zagotovitve enakovredne ravni varstva v vseh državah članicah ne more spreminjati glede na posamezno 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)".[134]

Sodišče je opozorilo, 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 in določbami, ki so bile sprejete za njeno uporabo. Država članica lahko torej načeloma uporablja register, kot

132 Glej tudi Direktivo o varstvu osebnih podatkov, uvodna izjava 32.

133 Sodba Sodišča EU z dne 16 decembra 2008 v zadevi *Huber proti Bundesrepublik Deutschland*, C-524/06.

134 Prav tam, točka 52.

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) Direktive 95/46/ES.[135]

Nazadnje, Sodišče je v zvezi z vprašanjem uporabe podatkov iz registra za boj proti kriminalu razsodilo, 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. Ta določba, kot jo razlaga Sodišče, tako „onemogoča, da bi posamezna država članica zaradi preprečevanja kriminala vzpostavila sistem obdelave osebnih podatkov, ki so lastni državljanom Unije, ki niso državljani te države članice".[136]

Če osebne podatke uporabljajo osebe, ki delujejo v javnosti, morajo upoštevati tudi člen 8 EKČP.

## Zakoniti interesi, za katere si prizadeva upravljavec ali tretja oseba

Posameznik, na katerega se nanašajo osebni podatki, ni edina oseba z zakonitimi interesi. Člen 7(f) Direktive o varstvu osebnih podatkov določa, da se lahko osebni podatki obdelujejo zakonito, če je obdelava „potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani, razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo, ki se varujejo […]".

Sodišče EU je v naslednji sodbi razsodilo izključno na podlagi člena 7(f) navedene direktive:

135 Prav tam, točke 54, 58, 59, 66–68.

136 Prav tam, točki 78 in 81.

Primer: Sodišče EU je v zadevi *ASNEF in FECEMD*[137] pojasnilo, da z nacionalno zakonodajo ni dovoljeno določiti dodatnih pogojev, kot so za zakonito obdelavo osebnih podatkov navedeni v členu 7(f) navedene direktive. 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 zakoniti interes pri obdelavi osebnih podatkov sklicevale samo, če so informacije izhajale iz javno dostopnih virov.

Sodišče je najprej navedlo, da je namen Direktive 95/46, da v vseh državah članicah zagotovi enakovredno raven varstva pravic in svoboščin posameznikov glede obdelave 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.[138] Sodišče EU je zato odločilo, da „iz cilja zagotoviti enako raven varstva v vseh državah članicah izhaja, da je v členu 7 Direktive 95/46 določen izčrpen in taksativen seznam primerov, v katerih je mogoče šteti, 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 niti določiti dodatnih zahtev, ki bi spreminjale obseg enega od šestih načel, določenih v tem členu".[139] Sodišče je priznalo, da je „[k]ar zadeva tehtanje, ki je potrebno na podlagi člena 7(f) Direktive 95/46/ES, [...] mogoče upoštevati to, 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) te 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".

Sodišče je na podlagi tega ugotovilo, da „je treba člen 7(f) Direktive 95/46 razlagati tako, da nasprotuje nacionalni ureditvi, ki – kadar ni privolitve zadevne osebe – za dovolitev obdelave njenih osebnih podatkov, ki je potrebna zaradi

137 Sodba Sodišča EU z dne 24. novembra 2011 v združenih zadevah *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, C-468/10 in C-469/10.

138 Prav tam, točka 28. Glej Direktivo o varstvu podatkov, uvodni izjavi 8 in 10.

139 Sodba Sodišča EU z dne 24. novembra 2011 v združenih zadevah *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, C-468/10 in C-469/10, točki 30 in 32.

uresničitve zakonitega interesa upravljavca osebnih 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".[140]

Podobne navedbe je mogoče najti v priporočilih Sveta Evrope. V priporočilu o profiliranju se obdelava osebnih podatkov zaradi profiliranja priznava kot zakonita, če je nujna zaradi zakonitih interesov drugih, „razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki".[141]

## 4.1.2. Zakonita obdelava občutljivih osebnih podatkov

**V pravu Sveta Evrope** je določitev ustreznega varstva za uporabo občutljivih osebnih podatkov prepuščena nacionalni zakonodaji, medtem ko **pravo EU** v členu 8 Direktive o varstvu osebnih podatkov vsebuje podrobno ureditev za obdelavo kategorij podatkov, ki razkrivajo: rasni ali etnični izvor, politična stališča, verska ali filozofska prepričanja, pripadnost sindikatu ali informacije v zvezi z zdravjem ali spolnim življenjem. Obdelava osebnih podatkov je načeloma prepovedana.[142] Obstaja pa izčrpen seznam izjem od te prepovedi, ki ga je mogoče najti v členu 8(2) in (3) navedene direktive. Te izjeme vključujejo izrecno privolitev posameznika, na katerega se nanašajo osebni podatki, njegove življenjske interese, zakonite interese drugih in javni interes.

Pogodbeno razmerje s posameznikom, na katerega se nanašajo osebni podatki, se ne šteje za splošno podlago za zakonito obdelavo občutljivih osebnih podatkov, medtem ko je pri obdelavi neobčutljivih osebnih podatkov to drugače. Če naj bi se torej v okviru pogodbe s posameznikom, na katerega se nanašajo osebni podatki, obdelovali občutljivi osebnih podatki, se za uporabo teh podatkov poleg strinjanja s sklenitvijo pogodbe zahteva tudi posebna izrecna privolitev posameznika, na katerega se nanašajo osebni podatki. Vendar bi se morala izrecna prošnja posameznika, na katerega se nanašajo osebni podatki, za blago ali storitve, pri katerih se nujno razkrijejo občutljivi osebni podatki, šteti za enakovredno izrecno privolitev.

140 Prav tam, točke 40, 44, 48 in 49.

141 Glej priporočilo o profiliranju, člen 3(4)(b).

142 Direktiva o varstvu osebnih podatkov, člen 8(1).

Primer: Če letalski potnik ob rezervaciji leta zahteva, naj mu letalska družba priskrbi invalidski voziček in hrano košer, lahko letalska družba te podatke uporabi, tudi če potnik ni podpisal dodatne klavzule o soglasju, s katero bi potrdil, da se strinja z uporabo svojih podatkov, ki razkrivajo informacije o njegovem zdravju ali verskem prepričanju.

## Izrecna privolitev posameznika, na katerega se nanašajo osebni podatki

Prvi pogoj za zakonito obdelavo katerih koli osebnih podatkov, ne glede na to, ali so neobčutljivi ali občutljivi, je privolitev posameznika, na katerega se nanašajo osebni podatki. Če so osebni podatki občutljivi, mora biti taka privolitev izrecna. Vendar se lahko z nacionalno zakonodajo določi, da privolitev v uporabo občutljivih osebnih podatkov ni zadostna pravna podlaga, ki bi dovoljevala njihovo obdelavo,[143] na primer če obdelava izjemoma vključuje neobičajna tveganja za posameznika, na katerega se nanašajo osebni podatki.

V enem posebnem primeru pa se celo implicitna privolitev priznava kot pravna podlaga za obdelavo občutljivih podatkov: člen 8(2)(e) navedene direktive določa, da obdelava ni prepovedana, če se nanaša na podatke, ki jih posameznik, na katerega se nanašajo, javno objavi. S to določbo se jasno domneva, da je treba dejanje posameznika, na katerega se nanašajo osebni podatki in ki svoje podatke javno objavi, razlagati kot njegovo implicitno privolitev v uporabo takih podatkov.

## Življenjski interesi posameznika, na katerega se nanašajo osebni podatki

Občutljivi osebni podatki se lahko tako kot neobčutljivi obdelujejo zaradi življenjskih interesov posameznika, na katerega se nanašajo.[144]

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.

143 Prav tam, člen 8(2)(a).

144 Prav tam, člen 8(2)(c).

## Zakoniti interesi drugih

Tako kot pri neobčutljivih osebnih podatkih so lahko zakoniti interesi drugih tudi podlaga za obdelavo občutljivih osebnih podatkov. Vendar za občutljive osebne podatke v skladu s členom 8(2) Direktive o varstvu osebnih podatkov to velja samo v naslednjih primerih:

- če je obdelava potrebna zaradi življenjskih interesov druge osebe[145], kadar posameznik, na katerega se nanašajo osebni podatki, fizično ali pravno ni sposoben dati svoje privolitve;

- če so občutljivi osebnih podatki pomembni na področju prava zaposlovanja, kot so zdravstveni podatki, na primer v okviru posebej nevarnega delovnega mesta, ali podatki o verskem prepričanju, na primer v okviru praznikov;[146]

- če ustanove, združenja ali drugi nepridobitni organi s političnim, filozofskim, verskim ali sindikalnim ciljem obdelujejo osebne podatke o svojih članih, sponzorjih ali drugih zadevnih osebah (taki podatki so občutljivi, ker najverjetneje razkrivajo verska ali politična prepričanja zadevnih posameznikov);[147]

- če se občutljivi osebni podatki uporabljajo v pravnih postopkih pred sodiščem ali upravnim organom za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.[148]

- Poleg tega je v to izjemo v skladu s členom 8(3) Direktive o varstvu osebnih podatkov vključeno upravljanje zdravstvenih storitev, če izvajalci teh storitev zdravstvene podatke uporabljajo za zdravstvene preglede in zdravljenje. Kot poseben zaščitni ukrep velja, da so osebe kot „izvajalci zdravstvenih storitev“ priznane samo, če zanje veljajo posebne poklicne zahteve glede zaupnosti.

## Javni interes

Države članice lahko v skladu s členom 8(4) Direktive o varstvu osebnih podatkov uvedejo tudi dodatne namene, za katere se lahko osebni podatki obdelujejo, če:

145 Prav tam.

146 Prav tam, člen 8(2)(b).

147 Prav tam, člen 8(2)(d).

148 Prav tam, člen 8(2)(e).

- se osebni podatki obdelujejo zaradi javnega interesa bistvenega pomena;
- je to določeno z nacionalno zakonodajo ali odločitvijo nadzornega organa ter
- nacionalna zakonodaja ali odločitev nadzornega organa vsebuje potrebne zaščitne ukrepe za učinkovito zaščito interesov posameznikov, na katere se nanašajo osebni podatki.[149]

Dober primer so sistemi elektronskih zdravstvenih kartotek, ki naj bi bili kmalu uvedeni v številnih državah članicah. Taki sistemi omogočajo, da se zdravstveni podatki, ki jih izvajalci zdravstvenih storitev zberejo med zdravljenjem bolnika, v širšem obsegu (običajno na nacionalni ravni) dajo na voljo drugim izvajalcem storitev zdravljenja tega bolnika.

Delovna skupina iz člena 29 je ugotovila, da uvedba takih sistemov ni mogoča na podlagi veljavnih pravnih pravil za obdelavo osebnih podatkov o bolnikih, ki temeljijo na členu 8(3) Direktive o varstvu osebnih podatkov. Če pa bi se obstoj takih sistemov elektronskih zdravstvenih kartotek štel za javni interes bistvenega pomena, bi lahko temeljil na členu 8 (4) navedene direktive, s katerim se za njihovo uvedbo zahteva izrecna pravna podlaga, kar vključuje tudi potrebne zaščitne ukrepe za zagotovitev varnega delovanja sistema.[150]

## 4.2. Pravila o varnosti obdelave osebnih podatkov

### Ključne točke

- Pravila o varnosti obdelave podatkov vključujejo obveznost upravljavca in obdelovalca, da izvajata ustrezne tehnične in organizacijske ukrepe za preprečitev nepooblaščenega poseganja v postopke obdelave osebnih podatkov.
- Potrebna raven zavarovanja osebnih podatkov je odvisna od:
  - varnostnih značilnosti, ki so na trgu na voljo za posamezno vrsto obdelave,

149 Prav tam, člen 8(4).

150 Delovni dokument delovne skupine iz člena 29 z dne 15. februarja 2007 o obdelavi osebnih podatkov v zvezi z zdravjem v elektronskih zdravstvenih kartonih (EZK), WP 131, Bruselj.

  - stroškov in
  - občutljivosti osebnih podatkov, ki se obdelujejo.
- Varna obdelava osebnih podatkov je dodatno zagotovljena s splošno obveznostjo vseh oseb, upravljavcev ali obdelovalcev, da zagotovijo zaupnost osebnih podatkov.

Obveznost upravljavcev in obdelovalcev, da uvedejo ustrezne ukrepe za zagotovitev zavarovanja osebnih podatkov, je določena tako v **pravu Sveta Evrope** kot v **pravu EU o varstvu osebnih podatkov**.

## 4.2.1. Dejavniki zavarovanja osebnih podatkov

Zadevne določbe **prava EU** se glasijo:

> *„Države članice določijo, da mora upravljavec izvajati ustrezne tehnične in organizacijske ukrepe za zavarovanje osebnih podatkov pred slučajnim ali nezakonitim uničenjem ali slučajno izgubo, predelavo, nepooblaščenim posredovanjem ali dostopom, predvsem kadar obdelava vključuje prenos podatkov po omrežju, ter proti vsem drugim nezakonitim oblikam obdelave.“*[151]

Podobno določbo vsebuje **pravo Sveta Evrope**:

> *„Sprejmejo se ustrezni varnostni ukrepi za zavarovanje osebnih podatkov, shranjenih v avtomatiziranih podatkovnih datotekah, pred slučajnim ali nepooblaščenim uničenjem ali slučajno izgubo ter nepooblaščenim dostopom, predelavo ali razširjanjem.“*[152]

Za varno obdelavo osebnih podatkov pogosto obstajajo tudi industrijski, nacionalni in mednarodni standardi. Evropski pečat zaupnosti (EuroPriSe) je na primer projekt eTEN (vseevropska telekomunikacijska omrežja) EU, s katerim se raziskujejo možnosti potrjevanja izdelkov, zlasti programske opreme, kot skladnih z evropsko zakonodajo 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

151 Direktiva o varstvu osebnih podatkov, člen 17(1).

152 Konvencija št. 108, člen 7.

informacij, njihovo obravnavanje in odzivanje nanje.[153] Agencija ENISA redno objavlja analize varnostnih groženj in svetuje, kako jih odpraviti.

Zavarovanja 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 zavarovanjem osebnih podatkov in njihovih obveznostih na podlagi zakonodaje 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 posredovanje podatkov tretjim osebam;

- uporaba osebnih podatkov izključno v skladu z navodili pristojne osebe ali v skladu s splošno določenimi pravili;

- varovanje 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 dostop do osebnih podatkov z elektronskimi sredstvi in redno preverjanje takih protokolov, ki ga izvaja notranja nadzorna služba;

- 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 zagotovi ustrezno usposabljanje in izobraževanje o zavarovanju osebnih podatkov. Uvedeni morajo biti tudi postopki preverjanja za zagotovitev, da ustrezni ukrepi ne

153 Uredba (ES) št. 460/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij, UL 2004, L 77.

obstajajo samo na papirju, temveč da 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*[154] 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 podatkov. ESČP je ugotovilo, da je bil kršen člen 8 EKČP, ker je bil evidenčni sistem zdravstvenih kartotek bolnišnice „tak, da uporabe kartotek bolnikov ni bilo mogoče pojasniti za nazaj, saj je razkrival samo pet zadnjih vpogledov, in so se te informacije 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 nacionalne zakonodaje, temu dejstvu pa nacionalna sodišča niso pripisala ustreznega pomena.

## Uradno obveščanje o kršitvah varstva osebnih podatkov

V več evropskih državah je bil v zakonodajo o varstvu osebnih podatkov uveden nov instrument za obravnavanje kršitev varstva osebnih podatkov: obveznost ponudnikov telekomunikacijskih storitev, da verjetne žrtve in nadzorne organe obvestijo o kršitvah varstva osebnih podatkov. Za ponudnike telekomunikacijskih storitev je to po pravu EU obvezno.[155] Namen uradnega obveščanja posameznikov, na katere se nanašajo osebni podatki, o kršitvah varstva osebnih podatkov je preprečiti škodo: z obveščanjem o kršitvah in njihovih možnih posledicah se zmanjša tveganje škodljivih učinkov na posameznike, na katere se nanašajo osebni podatki. Ob hudi malomarnosti bi se lahko ponudnikom naložila tudi denarna kazen.

154 Sodba ESČP z dne 17. julija 2008 v zadevi *I. proti Finski*, pritožba št. 20511/03.

155 Glej Direktivo 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 2002, L 201, člen 4(3), 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 2009, L 337.

Nujna bo vzpostavitev predhodnih notranjih postopkov za učinkovito upravljanje kršitev varnosti in poročanje o njih, saj je rok za obvezno poročanje posameznikom, na katere se nanašajo osebni podatki, in/ali nadzornemu organu glede na nacionalno zakonodajo običajno precej kratek.

### 4.2.2. Zaupnost

**V pravu EU** je varna obdelava osebnih podatkov dodatno zagotovljena s splošno obveznostjo vseh oseb, upravljavcev ali obdelovalcev, da zagotovijo zaupnost osebnih podatkov.

> 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 ohranitve zaupnosti podatkov strank pred razkritjem osebnih podatkov izvesti vsaj minimalne varnostne ukrepe. Tako bi lahko na primer ponudila, da vrne klic na telefonsko številko, ki je navedena v spisu stranke.

Člen 16 Direktive o varstvu osebnih podatkov se nanaša na zaupnost samo v okviru razmerja med upravljavcem in obdelovalcem. Vprašanje, ali morajo upravljavci ohranjati zaupnost osebnih podatkov, tako da jih ne smejo razkriti tretjim osebam, je obravnavano v členih 7 in 8 navedene direktive.

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. Člen 16 Direktive o varstvu osebnih podatkov se v tem primeru ne uporablja, saj je uporaba osebnih podatkov s strani fizičnih oseb dejansko v celoti izvzeta s področja uporabe navedene direktive, če taka uporaba spada v okvir t. i. izjeme obdelave za domače potrebe.[156] Izjema obdelave za domače potrebe je uporaba osebnih podatkov „s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti“.[157] To izjemo je treba od sprejetja odločitve Sodišča EU v zadevi *Bodil Lindqvist*[158] kljub vsemu razlagati ozko, zlasti v zvezi z razkritjem osebnih podatkov. Izjema obdelave za domače potrebe zlasti ne velja za objavo osebnih podatkov neomejenemu številu prejemnikov na spletu (za več podrobnosti o tej zadevi glej razdelke 2.1.2, 2.2, 2.3.1 in 6.1).

156 Direktiva o varstvu osebnih podatkov, člen 3(2), druga alinea.

157 Prav tam.

158 Sodba Sodišča EU z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01.

**V pravu Sveta Evrope** je obveznost zaupnosti zajeta s pojmom zavarovanja osebnih podatkov v členu 7 Konvencije št. 108, v katerem je obravnavano zavarovanje osebnih podatkov.

Za pogodbene obdelovalce zaupnost pomeni, da lahko osebne podatke, ki jim jih zaupa upravljavec, uporabljajo samo v skladu z njegovimi navodili. Za zaposlene pri upravljavcu ali obdelovalcu pa 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 in za svoje zaposlene uvesti pravno obveznost zaupnosti, kar običajno dosežejo tako, da v njihovo pogodbo o zaposlitvi vključijo klavzule o zaupnosti.

Kršitev poklicnih dolžnosti zaupnosti se v številnih državah članicah EU in pogodbenicah Konvencije št. 108 kaznuje po kazenskem pravu.

## 4.3. Pravila o preglednosti obdelave osebnih podatkov

### Ključne točke

- Upravljavec mora pred začetkom obdelave osebnih podatkov posameznike, na katere se ti podatki nanašajo, obvestiti vsaj o svoji identiteti in namenu obdelave osebnih podatkov, razen če tak posameznik te informacije že ima.
- Če se osebni podatki zbirajo od tretjih oseb, obveznost zagotovitve informacij ne velja, če:
  - je obdelava osebnih podatkov določena z zakonom ali
  - se zagotavljanje informacij izkaže za nemogoče ali bi vključevalo nesorazmeren napor.
- Upravljavec mora pred začetkom obdelave osebnih podatkov poleg tega:
  - nadzorni organ obvestiti o nameravanih postopkih obdelave ali
  - poskrbeti, da neodvisna oseba, odgovorna za varstvo osebnih podatkov, notranje dokumentira obdelavo, če so taki postopki določeni z nacionalno zakonodajo.

Obdelava mora biti v skladu z načelom poštene obdelave pregledna. **Pravo Sveta Evrope** zato določa, da mora biti vsaki osebi omogočeno, da ugotovi obstoj zbirk, ki vsebujejo osebne podatke (o tej osebi), njihov namen in odgovornega upravljavca.[159] Kako je treba to doseči, je prepuščeno nacionalni zakonodaji. **Pravo EU** je bolj natančno, saj je preglednost za posameznika, na katerega se nanašajo osebni podatki, zagotovljena na podlagi obveznosti upravljavca, da ga obvešča, za splošno javnost pa je zagotovljena z uradnim obveščanjem.

V nacionalni zakonodaji je na podlagi obeh pravnih sistemov dovoljeno določiti izjeme in omejitve obveznosti upravljavca glede preglednosti, če taka omejitev pomeni nujen ukrep za zaščito nekaterih javnih interesov ali varstvo posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih, če je to nujno v demokratični družbi.[160] Take izjeme so lahko na primer nujne v okviru preiskovanja kaznivih dejanj, upravičene pa so lahko tudi v drugih okoliščinah.

## 4.3.1. Informacije

Upravljavci postopkov obdelave morajo **v skladu s pravom Sveta Evrope in prava EU** posameznika, na katerega se nanašajo osebni podatki, predhodno obvestiti o nameravani obdelavi.[161] Ta obveznost ni odvisna od zahteve posameznika, na katerega se nanašajo osebni podatki, temveč jo mora upravljavec upoštevati proaktivno, ne glede na to, ali tak posameznik pokaže zanimanje za take informacije ali ne.

### Vsebina informacij

Informacije morajo vključevati namen obdelave ter identiteto in kontaktne podatke upravljavca.[162] V Direktivi o varstvu osebnih podatkov se zahteva zagotovitev nadaljnjih informacij, če so te „potrebne, ob upoštevanju posebnih okoliščin, v katerih se podatki zbirajo“. V členih 10 in 11 navedene direktive so med drugim opisani kategorije podatkov, ki se obdelujejo, in njihovi prejemniki ter obstoj pravice do dostopa in pravice do popravka podatkov. Če se podatki zbirajo od posameznikov, na katere se nanašajo, je treba v informacijah pojasniti, ali so odgovori na vprašanja obvezni ali prostovoljni, pa tudi možne posledice, če se odgovori ne predložijo.[163]

159 Konvencija št. 108, člen 8(a).

160 Prav tam, člen 9(2), in Direktiva o varstvu osebnih podatkov, člen 13(1).

161 Konvencija št. 108, člen 8(a), in Direktiva o varstvu osebnih podatkov, člena 10 in 11.

162 Konvencija št. 108, člen 8(a), in Direktiva o varstvu osebnih podatkov, člen 10(a) in (b).

163 Direktiva o varstvu osebnih podatkov, člen 10(c).

Z vidika **prava Sveta Evrope** se lahko zagotovitev takih informacij šteje za dobro prakso na podlagi načela poštene obdelave osebnih podatkov in je v tem smislu tudi vključena v pravo Sveta Evrope.

Informacije morajo biti v skladu z načelom poštene obdelave 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 strokovnjaki akademiki.

Nekateri posamezniki, na katere se nanašajo osebni podatki, želijo biti samo na kratko obveščeni o tem, kako in zakaj se njihovi podatki obdelujejo, drugi pa zahtevajo podrobno pojasnilo. Kako uravnotežiti ta vidik poštenega obveščanja, je pojasnjeno v mnenju delovne skupine iz člena 29, v katerem se zagovarjajo t. i. večplastna obvestila[164], ki posamezniku, na katerega se nanašajo osebni podatki, omogočajo, da sam izbere raven podrobnosti.

## Čas zagotovitve informacij

Direktiva o varstvu osebnih podatkov vsebuje nekoliko različne določbe glede tega, kdaj je treba zagotoviti informacije, odvisno o tega, ali se podatki zbirajo od posameznika, na katerega se nanašajo, (člen 10) ali od tretje osebe (člen 11). Če se podatki zbirajo od posameznika, na katerega se nanašajo, je treba informacije zagotoviti najpozneje ob zbiranju. Če se podatki zbirajo od tretjih oseb, je treba informacije zagotoviti najpozneje, ko upravljavec podatke zbira, ali preden se podatki prvič posredujejo tretji osebi.

## Izjeme od obveznosti obveščanja

**Po pravu EU** splošna izjema od obveznosti obveščanja posameznika, na katerega se nanašajo osebni podatki, obstaja, če ta posameznik že ima informacije.[165] To se nanaša na primere, v katerih je posameznik, na katerega se nanašajo osebni podatki, glede na okoliščine primera že seznanjen s tem, da bo določen upravljavec njegove podatke obdeloval za določen namen.

164 Mnenje 10/2004 delovne skupine iz člena 29 z dne 25. novembra 2004 o bolj usklajenih določbah v zvezi z dajanjem informacij, WP 100, Bruselj.

165 Direktiva o varstvu osebnih podatkov, člen 10 in člen 11(1).

Člen 11 navedene direktive, ki se nanaša na obveznost, da je posameznik, na katerega se nanašajo osebni podatki, obveščen, če podatki niso bili pridobljeni od njega, prav tako določa, da taka obveznost ne velja, zlasti za obdelavo v statistične namene ali zaradi zgodovinskih ali znanstvenih raziskav, če:

- se zagotovitev takih informacij izkaže za nemogočo;
- bi vključevala nesorazmeren napor ali
- zakon izrecno določa zbiranje oziroma posredovanje.[166]

Samo v členu 11(2) Direktive o varstvu osebnih podatkov je navedeno, da posameznikov, na katere se nanašajo osebni podatki, ni treba obvestiti o postopkih obdelave, če so ti določeni z zakonom. Ker se v pravu na splošno domneva, da zadevne osebe poznajo pravo, bi bilo mogoče trditi, da posameznik, na katerega se nanašajo osebni podatki, že ima te informacije, če se podatki zbirajo od njega na podlagi člena 10 navedene direktive. Ker pa se poznavanje prava samo domneva, bi se v skladu z načelom poštene obdelave na podlagi člena 10 zahtevalo, da je treba posameznika, na katerega se nanašajo osebni podatki, obvestiti, tudi če je obdelava določena z zakonom, zlasti ker obveščanje takega posameznika ni posebno težka naloga, če se podatki zbirajo neposredno od njega.

**Kar zadeva pravo Sveta Evrope**, Konvencija št. 108 izrecno določa izjeme od člena 8. Izjeme, določene v členih 10 in 11 Direktive o varstvu osebnih podatkov, je mogoče razumeti tudi kot primere dobre prakse za izjeme na podlagi člena 9 Konvencije št. 108.

## Različni načini zagotavljanja informacij

Najboljši način zagotavljanja informacij bi bil, da bi se ustno ali pisno obrnili na vsakega posameznika, na katerega se nanašajo osebni podatki. Če se podatki zbirajo od takega posameznika, bi bilo treba informacije zagotoviti med zbiranjem. Zlasti če se podatki zbirajo od tretjih oseb, pa se lahko informacije zagotovijo tudi z ustrezno objavo, saj se je v praksi seveda težko osebno obrniti na posameznike, na katere se nanašajo osebni podatki.

166 Prav tam, uvodna izjava 40 in člen 11(2).

Eden od najučinkovitejših načinov za zagotovitev informacij so ustrezna obvestila na domači strani upravljavca, na primer politika varstva zasebnosti na spletišču. Kljub temu obstaja precejšen delež prebivalstva, ki ne uporablja interneta, pri čemer mora podjetje ali javni organ to upoštevati pri svoji politiki obveščanja.

## 4.3.2. Uradno obveščanje

Nacionalna zakonodaja lahko določa, da morajo upravljavci pristojni nadzorni organ uradno obveščati o svojih postopkih obdelave, da se lahko ti objavijo. Lahko pa nacionalna zakonodaja določa možnost, da upravljavci zaposlijo odgovorno osebo za varstvo osebnih podatkov, ki je odgovorna zlasti za vodenje registra postopkov obdelave, ki jih izvaja upravljavec.[167] Tak notranji register (katalog) je treba na zahtevo dati na voljo javnosti.

Primer: V uradnem obvestilu in dokumentaciji, ki jo vodi notranja oseba, odgovorna za varstvo osebnih podatkov, morajo biti opisane glavne značilnosti zadevne obdelave podatkov. To vključuje informacije o upravljavcu, namenu obdelave, pravni podlagi za obdelavo, kategorijah osebnih podatkov, ki se obdelujejo, tretjih osebah, ki bodo najverjetneje prejele osebne podatke, in podatek, ali je predviden čezmejni prenos (iznos) podatkov ali ne, in če je, kateri.

Nadzorni organ mora uradna obvestila objaviti v posebnem registru. Da bi tak register služil namenu, mora biti dostop do njega enostaven in brezplačen. Enako velja za dokumentacijo, ki jo vodi upravljavčeva oseba, odgovorna za varstvo osebnih podatkov.

Izjeme od obveznosti glede uradnega obveščanja pristojnega nadzornega organa ali zaposlitve notranje osebe, odgovorne za varstvo podatkov, se lahko z nacionalno zakonodajo določijo za postopke obdelave, ki najverjetneje ne bodo povzročili posebnega tveganja za posameznike, na katere se nanašajo osebni podatki, navedene pa so v členu 18(2) Direktive o varstvu podatkov.[168]

167 Prav tam, člen 18(2), druga alinea.

168 Prav tam, člen 18(2), prva alinea.

# 4.4. Pravila o spodbujanju skladnosti

**Ključne točke**

- V okviru izoblikovanja načela odgovorne obdelave osebnih podatkov je v Direktivi o varstvu osebnih podatkov navedenih več instrumentov za spodbujanje skladnosti:
  - predhodno preverjanje načrtovanih postopkov obdelave, ki ga izvede nacionalni nadzorni organ;
  - odgovorne osebe za varstvo osebnih podatkov, ki upravljavcu pomagajo s strokovnim znanjem na področju varstva osebnih podatkov;
  - pravila (kodeksi) ravnanja, v katerih so navedena sedanja pravila o varstvu osebnih podatkov, ki naj bi se uporabljala v določeni veji družbe, zlasti na poslovnem področju.
- V pravu Sveta Evrope so predlagani podobni instrumenti za spodbujanje skladnosti, in sicer v priporočilu o profiliranju.

## 4.4.1. Predhodno preverjanje

Nadzorni organ mora v skladu s členom 20 Direktive o varstvu osebnih podatkov pred začetkom obdelave preveriti postopke obdelave, ki bi lahko – zaradi namena ali okoliščin obdelave – povzročili posebno nevarnost za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Z nacionalno zakonodajo je treba določiti, pri katerih postopkih obdelave je potrebno predhodno preverjanje. Postopki obdelave se lahko na podlagi takega preverjanja prepovejo ali pa se odredi sprememba značilnosti predlagane zasnove teh postopkov. Namen člena 20 navedene direktive je zagotoviti, da se obdelava, ki je po nepotrebnem tvegana, sploh ne začne, saj lahko nadzorni organ take postopke prepove. Pogoj za učinkovitost takega mehanizma je, da je nadzorni organ o tem dejansko uradno obveščen. Nadzorni organi za zagotovitev, da upravljavci izpolnjujejo obveznost uradnega obveščanja, potrebujejo pooblastila za prisilne ukrepe, na primer možnost, da upravljavcem naložijo denarno kazen.

Primer: Če podjetje izvaja postopke obdelave, ki jih je treba v skladu z nacionalno zakonodajo predhodno preveriti, mora nadzornemu organu predložiti dokumentacijo o načrtovanih postopkih obdelave. Podjetje lahko začne postopke obdelave šele po prejetju pozitivnega odgovora nadzornega organa.

V nekaterih državah članicah pa lahko nacionalna zakonodaja tudi določa, da se lahko postopki obdelave začnejo, če se nadzorni organ ne odzove v določenem roku, na primer v treh mesecih.

## 4.4.2. Odgovorne osebe za varstvo osebnih podatkov

Direktiva o varstvu osebnih podatkov določa možnost, da se z nacionalno zakonodajo določi, da lahko upravljavci enega od uradnikovimenujejo za odgovorno osebo za varstvo osebnih podatkov.[169] Namen take funkcije je preprečiti, da bi postopki obdelave škodljivo vplivali na pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.[170]

Primer: V Nemčiji morajo podjetja v zasebni lasti v skladu s podpoglavjem 1 poglavja 4f nemškega zveznega zakona o varstvu podatkov (*Bundesdatenschutzgesetz*) imenovati notranjo odgovorno osebo za varstvo osebnih podatkov, če za avtomatizirano obdelavo osebnih podatkov stalno zaposlujejo deset ali več oseb.

Za dosego tega cilja je potrebna določena neodvisnost položaja odgovorne osebe v upravljavčevi organizaciji, kot je izrecno poudarjeno v navedeni direktivi. Za učinkovito delovanje te funkcije bi bile nujne tudi trdne zaposlitvene pravice kot varstvo v primerih, kot je neupravičena odpustitev.

Za spodbujanje skladnosti z nacionalno zakonodajo o varstvu podatkov je bil pojem notranjih odgovornih oseb za varstvo osebnih podatkov prevzet tudi v nekaterih priporočilih Sveta Evrope.[171]

## 4.4.3. Pravila (kodeksi) ravnanja

Da bi podjetja in drugi sektorji spodbudili skladnost, lahko pripravijo podrobna pravila, s katerimi se urejajo njihove značilne dejavnosti obdelave, in tako »uzakonijo« (kodificirajo) najboljše prakse. S strokovnim znanjem udeležencev sektorja se bo spodbudilo iskanje rešitev, ki so praktične in se bodo zato najverjetneje tudi uporabile. Države članice – in Evropsko komisijo – se v skladu s tem poziva, naj spodbujajo pripravo (kodificiranih) pravil ravnanja, ki bi pripomogla k pravilnemu izvajanju

169 Prav tam, člen 18(2), druga alinea.

170 Prav tam.

171 Glej na primer priporočilo o profiliranju, člen 8(3).

nacionalnih določb, ki jih države članice sprejmejo na podlagi navedene direktive, pri čemer je treba upoštevati posebnosti različnih sektorjev.[172]

Države članice morajo za zagotovitev, da so ta (kodificirana) pravila ravnanja v skladu z nacionalnimi določbami, sprejetimi na podlagi Direktive o varstvu osebnih podatkov, določiti postopek za ocenjevanje teh pravil. V ta postopek bi morali biti običajno vključeni nacionalni organi, trgovinska združenja in drugi organi, ki zastopajo preostale kategorije upravljavcev.[173]

Osnutki (kodificiranih) pravil ravnanja Skupnosti in spremembe ali razširitve sedanjih pravil (kodeksov) ravnanja Skupnosti se lahko predložijo v oceno delovni skupini iz člena 29. Ko jih ta odobri, lahko Evropska komisija zagotovi primerno objavo takih pravil.[174]

Primer: Evropska federacija združenj za direktni marketing (FEDMA) je pripravila evropski kodeks ravnanja za uporabo osebnih podatkov pri neposrednem trženju. Ta pravila so bila uspešno predložena delovni skupini iz člena 29. Leta 2010 je bila pravilom dodana priloga, ki se nanaša na komunikacije pri elektronskem trženju.[175]

172 Glej Direktivo o varstvu osebnih podatkov, člen 27(1).

173 Prav tam, člen 27(2).

174 Prav tam, člen 27(3).

175 Mnenje 4/2010 delovne skupine iz člena 29 z dne 13. julija 2010 o evropskem kodeksu ravnanja Evropske federacije združenj za direktni marketing (FEDMA) pri uporabi osebnih podatkov v neposrednem trženju, WP 174, Bruselj.

# 5

# Pravice posameznikov, na katere se nanašajo osebni podatki, in njihovo uveljavljanje

| EU | Obravnavane teme | Svet Evrope |
|---|---|---|
| **Pravica do dostopa** | | |
| Direktiva o varstvu osebnih podatkov, člen 12<br>Sodba Sodišča EU z dne 7. maja 2009 v zadevi *College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer*, C-553/07 | **Pravica do dostopa do lastnih osebnih podatkov** | Konvencija št. 108, člen 8(b) |
| | **Pravica do popravka, izbrisa (črtanja) ali blokiranja** | Konvencija št. 108, člen 8(c)<br>Sodba ESČP z dne 18. novembra 2008 v zadevi *Cemalettin Canli proti Turčiji*, pritožba št. 22427/04<br>Sodba ESČP z dne 6. junija 2006 v zadevi *Segerstedt-Wiberg in drugi proti Švedski*, pritožba št. 62332/00<br>Sodba ESČP z dne 27. aprila 2010 v zadevi *Ciubotaru proti Moldaviji*, pritožba št. 27138/04 |
| **Pravica do ugovora** | | |
| Direktiva o varstvu osebnih podatkov, člen 14(1)(a) | **Pravica do ugovora zaradi posebnega položaja posameznika, na katerega se nanašajo osebni podatki** | Priporočilo o profiliranju, člen 5(3) |

| | | |
|---|---|---|
| Direktiva o varstvu osebnih podatkov, člen 14(1)(b) | **Pravica do ugovora zoper nadaljnjo uporabo zaradi trženja** | Priporočilo o neposrednem trženju, člen 4(1) |
| Direktiva o varstvu osebnih podatkov, člen 15 | **Pravico do ugovora zoper avtomatizirane odločitve** | Priporočilo o profiliranju, člen 5(5) |
| **Neodvisen nadzor** | | |
| Listina, člen 8(3)<br>Direktiva o varstvu osebnih podatkov, člen 28<br>Uredba o varstvu osebnih podatkov v institucijah EU, poglavje V<br>Uredba o varstvu osebnih podatkov<br>Sodba Sodišča EU z dne 9. marca 2010 v zadevi *Evropska komisija proti Zvezni republiki Nemčiji*, C-518/07<br>Sodba Sodišča EU z dne 16. oktobra 2012 v zadevi *Evropska komisija proti Republiki Avstriji*, C-614/10<br>Tožba pred Sodiščem EU, vložena 8. aprila 2014, v zadevi *Evropska Komisija proti Madžarski*, C-288/12 | **Nacionalni nadzorni organi** | Konvencija št. 108, Dodatni protokol, člen 1 |
| **Pravna sredstva in sankcije** | | |
| Direktiva o varstvu osebnih podatkov, člen 12 | **Zahteva upravljavcu** | Konvencija št. 108, člen 8(b) |
| Direktiva o varstvu osebnih podatkov, člen 28(4)<br>Uredba o varstvu osebnih podatkov v institucijah EU, člen 32(2) | **Zahtevki, vloženi pri nadzornem organu** | Konvencija št. 108, Dodatni protokol, člen 1(2)(b) |
| Listina, člen 47 | **Sodišča (na splošno)** | EKČP, člen 13 |
| Direktiva o varstvu osebnih podatkov, člen 28(3) | **Nacionalna sodišča** | Konvencija št. 108, Dodatni protokol, člen 1(4) |
| PDEU, člen 263(4)<br>Uredba o varstvu osebnih podatkov v institucijah EU, člen 32(1)<br>PDEU, člen 267 | **Sodišče EU** | |
| | **ESČP** | EKČP, člen 34 |

| Pravna sredstva in sankcije | | |
|---|---|---|
| Listina, člen 47<br>Direktiva o varstvu osebnih podatkov, člena 22 in 23<br>Sodba Sodišča EU z dne 10. aprila 1984 v zadevi *Sabine von Colson ind Elisabeth Kamann proti Land Nordrhein-Westfalen*, C-14/83<br>Sodba Sodišča EU z dne 26. februarja 1986 v zadevi *M. H. Marshall proti Southampton and South-West Hampshire Area Health Authority*, C-152/84 | **Zaradi kršitev nacionalne zakonodaje o varstvu osebnih podatkov** | EKČP, člen 13 (samo za države članice Sveta Evrope)<br>Konvencija št. 108, člen 10<br>Sodba ESČP z dne 2. decembra 2008 v zadevi *K. U. proti Finski*, pritožba št. 2872/02<br>Sodba ESČP z dne 25. novembra 2008 v zadevi *Biriuk proti Litvi*, pritožba št. 23373/03 |
| Uredba o varstvu osebnih podatkov v institucijah EU, člena 34 in 49<br>Sodba Sodišča EU z dne 29. junija 2010 v zadevi *Evropska komisija proti The Bavarian Lager Co. Ltd.*, C-28/08 P | **Zaradi kršitev zakonodaje EU, ki so jih storili institucije in organi EU** | |

Učinkovitost pravnih pravil na splošno, zlasti pravic posameznikov, na katere se nanašajo osebni podatki, je zelo odvisna od obstoja ustreznih mehanizmov za njihovo uveljavljanje. V evropski zakonodaji o varstvu osebnih podatkov velja, da mora imeti posameznik, na katerega se nanašajo osebni podatki, na podlagi nacionalne zakonodaje pravico do varstva svojih podatkov. Z nacionalno zakonodajo morajo biti ustanovljeni tudi neodvisni nadzorni organi, ki posameznikom, na katere se nanašajo osebni podatki, pomagajo pri uveljavljanju njihovih pravic in nadzorujejo obdelavo osebnih podatkov. Pravica do učinkovitega pravnega sredstva, ki je zagotovljena na podlagi EKČP in Listine, prav tako pomeni, da mora imeti vsaka oseba na voljo pravna sredstva.

## 5.1. Pravice posameznikov, na katere se nanašajo osebni podatki

### Ključne točke

- Vsakdo ima na podlagi nacionalne zakonodaje pravico, da od katerega koli upravljavca zahteva informacije o tem, ali ta obdeluje njegove osebnih podatke.
- Posamezniki, na katere se nanašajo osebni podatki, imajo na podlagi nacionalne zakonodaje pravico:

  - dostopati do svojih podatkov pri katerem koli upravljavcu, ki obdeluje take podatke;
  - da upravljavec, ki obdeluje njihove osebne podatke, le-te popravi (ali po potrebi blokira), če so netočni;
  - da upravljavec njihove osebne podatke izbriše ali po potrebi blokira, če jih obdeluje nezakonito.
- Poleg tega imajo posamezniki, na katere se nanašajo osebni podatki, pravico, da pri upravljavcih vložijo ugovor glede:
  - avtomatiziranih odločitev (na podlagi osebnih podatkov, obdelanih izključno z avtomatskimi sredstvi);
  - obdelave osebnih podatkov, če le-ta povzroči nesorazmerne rezultate;
  - uporabe njihovih osebnih podatkov zaradi neposrednega trženja.

## 5.1.1. Pravica do dostopa

**V pravu EU** člen 12 Direktive o varstvu osebnih podatkov vsebuje elemente pravice posameznikov, na katere se nanašajo osebni podatki, do dostopa, vključno s pravico, da od upravljavca dobijo „potrditev tega, ali se podatki v zvezi z njim obdelujejo ali ne, in informacije vsaj glede namenov obdelave, vrste zadevnih podatkov in prejemnikov ali vrste prejemnikov, ki so jim podatki posredovani“, in „popravke, izbris ali blokiranje podatkov, katerih obdelava ni v skladu z določbami te direktive, predvsem zaradi nepopolnih ali netočnih podatkov“.

**V pravu Sveta Evrope** obstajajo enake pravice, ki morajo biti zagotovljene z nacionalno zakonodajo (člen 8 Konvencije št. 108). V več priporočilih Sveta Evrope je uporabljen pojem „dostop“, opisani pa so tudi različni vidiki pravice do dostopa, katerih izvajanje v nacionalni zakonodaji se predlaga enako, kot je poudarjeno v zgornjem odstavku.

V skladu s členom 9 Konvencije št. 108 in členom 13 Direktive o varstvu osebnih podatkov je mogoče obveznost upravljavcev, da odgovorijo na zahtevo za dostop, omejiti zaradi prevladujočih pravnih interesov drugih. Prevladujoči pravni interesi lahko vključujejo javne interese, kot so nacionalna varnost, javna varnost in pregon kaznivih dejanj, ter zasebne interese, ki so prepričljivejši od interesov varstva podatkov. Vsakršne izjeme ali omejitve morajo biti nujne v demokratični družbi in sorazmerne s ciljem. V zelo izjemnih primerih, na primer zaradi zdravstvenih indikacij, je lahko omejitev preglednosti nujna zaradi samega varstva osebnih podatkov; to se

nanaša zlasti na omejevanje pravice do dostopa vsakega posameznika, na katerega se nanašajo osebni podatki.

Če se osebni podatki obdelujejo samo za namen znanstvenih raziskav ali za statistične namene, je z Direktivo o varstvu osebnih podatkov dovoljeno, da se pravice do dostopa omejijo z nacionalno zakonodajo; vendar morajo biti uvedeni ustrezni zakonski zaščitni ukrepi. Zlasti je treba zagotoviti, da se v okviru take obdelave osebnih podatkov ne sprejmejo ukrepi ali odločitve v zvezi z določenim posameznikom in da „očitno ni nevarnosti za kršitev zasebnosti posameznika, na katerega se nanašajo osebni podatki".[176] Podobne določbe vsebuje člen 9(3) Konvencije št. 108.

## Pravica do dostopa do lastnih osebnih podatkov

**Po pravu Sveta Evrope** je pravica do dostopa do lastnih osebnih podatkov izrecno priznana s členom 8 Konvencije št. 108. ESČP je večkrat odločilo, da obstaja pravica do dostopa do informacij o osebnih podatkih, ki jih imajo ali uporabljajo drugi, in da ta pravica izhaja iz potrebe po spoštovanju zasebnega življenja.[177] V zadevi *Leander*[178] je ugotovilo, da je mogoče pravico do dostopa do osebnih podatkov, ki jih hranijo javni organi, v nekaterih okoliščinah kljub vsemu omejiti.

**V pravu EU** je pravica do dostopa do lastnih osebnih podatkov izrecno priznana s členom 12 Direktive o varstvu osebnih podatkov, kot temeljna pravica pa v členu 8(2) Listine.

Člen 12(a) navedene direktive določa, da morajo države članice vsakemu posamezniku, na katerega se nanašajo osebni podatki, zagotoviti pravico do dostopa do osebnih podatkov in informacij. Natančneje, vsak posameznik, na katerega se nanašajo osebni podatki, ima pravico, da od upravljavca dobi potrditev tega, ali se podatki v zvezi z njim obdelujejo ali ne, in informacije vsaj glede:

- namenov obdelave;
- vrste zadevnih osebnih podatkov;

176 Direktiva o varstvu osebnih podatkov, člen 13(2).

177 Sodbe ESČP z dne 7. julija 1989 v zadevi *Gaskin proti Združenemu kraljestvu*, pritožba št. 10454/83; z dne 13. februarja 2003 v zadevi *Odièvre proti Franciji* [veliki senat], pritožba št. 42326/98; z dne 28. aprila 2009 v zadevi *K. H. in drugi proti Slovaški*, pritožba št. 32881/04, in z dne 25. septembra 2012 v zadevi *Godelli proti Italiji*, pritožba št. 33783/09.

178 Sodba ESČP z dne 26. marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81.

- osebnih podatkov, ki so v obdelavi;
- prejemnikov ali vrste prejemnikov, ki so jim osebni podatki posredovani;
- razpoložljivih informacij o viru osebnih podatkov, ki se obdelujejo;
- logike, zajete v vse avtomatske obdelave osebnih podatkov, pri avtomatiziranih odločitvah.

Z nacionalno zakonodajo se lahko dodajo informacije, ki jih mora zagotoviti upravljavec, na primer navedba pravne podlage za obdelavo osebnih podatkov.

Primer: Posameznik lahko z dostopom do svojih osebnih podatkov ugotovi, ali so podatki točni ali ne. Zato je nujno, da je posameznik, na katerega se nanašajo osebni podatki, obveščen o kategorijah podatkov, ki se obdelujejo, in njihovi vsebini. Ni torej dovolj, da upravljavec posamezniku, na katerega se nanašajo osebni podatki, pove samo, da obdeluje njegovo ime, naslov, datum rojstva in področje zanimanja. Upravljavec mora takemu posamezniku tudi razkriti, da obdeluje „ime: N. N.; naslov: 1040 Dunaj, Schwarzenbergplatz 11, Avstrija; datum rojstva: 10. 10. 1974 in področje zanimanja (glede na izjavo posameznika, na katerega se nanašajo osebni podatki): klasična glasba“. Zadnja postavka poleg tega vsebuje informacije o viru podatkov.

Sporočilo posamezniku, na katerega se nanašajo osebni podatki, o podatkih, ki so v obdelavi, mora biti v razumljivi obliki, kar pomeni, da mora upravljavec temu posamezniku po potrebi podrobneje pojasniti, kaj obdeluje. Samo navajanje tehničnih okrajšav ali medicinskih izrazov v odgovor na zahtevo za dostop na primer običajno ni dovolj, tudi če so shranjeni samo take okrajšave in izrazi.

V odgovor na zahtevo za dostop v zvezi s temi informacijami je treba navesti informacije o viru osebnih podatkov, ki jih obdeluje upravljavec. To določbo je treba razumeti z vidika načel poštenosti in odgovornosti. Upravljavec ne sme uničiti informacij o viru podatkov, zato da mu jih ne bi bilo treba razkriti, niti ne sme prezreti običajnega standarda in ugotovljenih potreb po dokumentiranju svojih dejavnosti. Če upravljavec ne vodi dokumentacije o viru osebnih podatkov, ki se obdelujejo, običajno ne izpolnjuje svojih obveznosti v zvezi s pravico do dostopa.

Če se izvaja avtomatizirano ocenjevanje, je treba pojasniti splošno logiko ocenjevanja, vključno s posebnimi merili, ki se upoštevajo pri ocenjevanju posameznika, na katerega se nanašajo osebni podatki.

V navedeni direktivi ni pojasnjeno, ali se pravica do dostopa do informacij nanaša na preteklost, in če se, na katero obdobje v preteklosti. Pri tem, kot je poudarjeno v sodni praksi Sodišča EU, za pravico do dostopa do osebnih podatkov ne smejo neupravičeno veljati časovne omejitve. Posameznikom, na katere se nanašajo osebni podatki, je treba tudi razumno omogočiti, da dobijo informacije o preteklih postopkih obdelave podatkov.

Primer: Sodišče EU je bilo v zadevi *Rijkeboer*[179] pozvano, naj ugotovi, ali je lahko na podlagi člena 12(a) navedene direktive posameznikova pravica do dostopa do informacij glede prejemnikov ali vrste prejemnikov osebnih podatkov in glede vsebine posredovanih podatkov omejena na leto pred vložitvijo njegove zahteve za dostop.

Sodišče je odločilo, da je treba za določitev, ali je v skladu s členom 12(a) navedene direktive takšna časovna omejitev dovoljena, navedeni člen razlagati glede na namene direktive. 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 (člen 12(b)), ali da tretje osebe, ki so jim bili osebni podatki posredovani, uradno obvesti o teh popravkih, izbrisu ali blokiranju (člen 12(c)). Pravica do dostopa je potrebna tudi za to, da se posamezniku, na katerega se nanašajo osebni podatki, omogoči uveljavljanje pravice, da ugovarja obdelavi svojih osebnih podatkov (člen 14 navedene direktive), ali pravice do vložitve pravnega sredstva, če mu je nastala škoda (člena 22 in 23).

Da bi se zagotovil polni učinek določb, navedenih zgoraj, je Sodišče 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 osebnih podatkov, ki naj bi bili nezakoniti ali nepravilni, ter pravice vložiti pravno sredstvo pri sodišču in doseči povrnitev nastale škode“.

179 Sodba Sodišča EU z dne 7. maja 2009 v zadevi *College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer*, C-553/07.

## Pravica do popravka, izbrisa in blokiranja osebnih podatkov

„[V]saka oseba [mora biti] sposobna uresničiti pravico dostopa do podatkov v obdelavi, ki se nanašajo nanjo, da bi preverila zlasti njihovo točnost in zakonitost obdelave."[180] V skladu s temi načeli morajo imeti posamezniki, na katere se nanašajo osebni podatki, na podlagi nacionalne zakonodaje pravico, da od upravljavca pridobijo popravke, izbris ali blokiranje osebnih podatkov, če menijo, da njihova obdelava ni v skladu z določbami navedene direktive, predvsem zaradi nepopolnih ali netočnih podatkov.[181]

Primer: ESČP je v zadevi *Cemalettin Canli proti Turčiji*[182] ugotovilo kršitev člena 8 EKČP zaradi nepravilnega policijskega poročanja v kazenskem postopku.

Pritožnik je bil zaradi domnevnega članstva v nezakonitih organizacijah dvakrat udeležen v kazenskem postopku, vendar ni bil nikoli 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 informacije spadajo na področje „zasebnega življenja", če se sistematično zbirajo in shranjujejo v datotekah javnih organov. Poleg tega policijsko poročilo ni bilo pravilno, njegova priprava in predložitev kazenskemu sodišču pa nista bila v skladu z zakonom. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Primer: V zadevi *Segerstedt-Wiberg in drugi proti Švedski*[183] so bili pritožniki pripadniki določenih liberalnih in komunističnih političnih strank. Sumili so, da so bile informacije o njih vnesene v tajne policijske kartoteke. ESČP je bilo prepričano, da je imela hramba spornih podatkov pravno podlago in zakonit cilj. V zvezi z nekaterimi pritožniki je ugotovilo, da trajna hramba osebnih podatkov pomeni nesorazmerno vmešavanje v njihovo zasebno življenje. V primeru

180 Direktiva o varstvu osebnih podatkov, uvodna izjava 41.

181 Prav tam, člen 12(b).

182 Sodbi ESČP z dne 18. novembra 2008 v zadevi *Cemalettin Canli proti Turčiji*, pritožba št. 22427/04, točke 33, 42 in 43, ter z dne 2. februarja 2010 v zadevi *Dalea proti Franciji*, pritožba št. 964/07.

183 Sodba ESČP z dne 6. junija 2006 v zadevi *Segerstedt-Wiberg in drugi proti Švedski*, pritožba št. 62332/00, točki 89 in 90; glej tudi na primer sodbo ESČP z dne 18. aprila 2013 v zadevi *M. K. proti Franciji*, pritožba št. 19522/09.

g. Schmida so organi na primer hranili podatek, da se je leta 1969 domnevno zavzemal za nasilen upor proti policijskemu nadzoru med protesti. ESČP je ugotovilo, da te informacije ne morejo biti v nikakršnem zadevnem interesu nacionalne varnosti, zlasti ker se nanašajo na preteklost. Ugotovilo je, da je bil v zvezi s štirimi od petih pritožnikov kršen člen 8 EKČP.

Včasih na primer zadostuje, da posameznik, na katerega se nanašajo osebni podatki, preprosto zahteva popravek imena, spremembo naslova ali telefonske številke. Če pa so taki zahtevki povezani s pravnimi vprašanji, na primer pravnim statusom osebe, na katero se nanašajo osebni podatki, ali točnim krajem prebivanja za vročanje pravnih dokumentov, zahteve za popravek morda niso dovolj in upravljavec lahko ima 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.[184]

Primer: V zadevi *Ciubotaru proti Moldaviji*[185] pritožniku ni bilo omogočeno, da bi vpis svojega narodnostnega 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. Vendar je moral kljub temu v skladu 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.

184 Sodba ESČP z dne 4. maja 2000 v zadevi *Rotaru proti Romuniji*, pritožba št. 28341/95.

185 Sodba ESČP z dne 27. aprila 2010 v zadevi *Ciubotaru proti Moldaviji*, pritožba št. 27138/04, točki 51 in 59.

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. Upravljavec v tem obdobju osebnih podatkov ne sme predstavljati kot zanesljivih ali dokončnih, zlasti ne tretjim osebam.

Zahteva posameznika, na katerega se nanašajo osebni podatki, naj se podatki izbrišejo ali črtajo, pogosto temelji na trditvi, da obdelava osebnih podatkov nima pravne podlage. Take trditve se pogosto pojavijo, ko se privolitev umakne ali ko nekateri osebni podatki niso več skladni z namenom njihovega zbiranja. Dokazno breme glede zakonitosti obdelave nosi upravljavec osebnih podatkov, saj je odgovoren za zakonitost obdelave. Upravljavec mora biti v skladu z načelom odgovornosti kadar koli zmožen dokazati, da ima trdno pravno podlago za obdelavo osebnih podatkov, saj je treba z obdelavo v nasprotnem primeruprenehati.

Če se obdelavi osebnih podatkov nasprotuje, ker naj bi bili netočni ali nezakonito obdelani, lahko posameznik, na katerega se nanašajo osebni podatki, v skladu z načelom poštene obdelave zahteva, naj se sporni osebni podatki blokirajo. To pomeni, da se osebni podatki ne izbrišejo, vendar jih upravljavec v obdobju blokiranja ne sme uporabiti. To bi bilo nujno zlasti, če bi lahko nadaljnja uporaba netočnih ali nezakonito hranjenih osebnih podatkov škodovala posamezniku, na katerega se nanašajo ti podatki. Z nacionalno zakonodajo bi moralo biti podrobneje določeno, kdaj lahko velja obveznost blokiranja uporabe osebnih podatkov in kako jo je treba izvajati.

Posamezniki, na katere se nanašajo osebni podatki, imajo poleg tega pravico pri upravljavcu doseči uradno obvestilo tretjim osebam o vsakem blokiranju, popravku ali izbrisu, če so te osebe podatke prejele pred temi postopki obdelave. Ker je moral upravljavec dokumentirati posredovanje osebnih podatkov tretjim osebam, bi moralo biti mogoče opredeliti prejemnike osebnih podatkov in zahtevati izbris. Če pa so bili osebni podatki medtem že objavljeni, na primer na spletu, izbrisa morda ni mogoče doseči v vseh primerih, saj prejemnikov podatkov ni mogoče najti. V skladu z Direktivo o varstvu osebnih podatkov je treba za popravek, izbris ali blokiranje osebnih podatkov obvezno navezati stik s prejemniki podatkov, „razen če se to izkaže za nemogoče ali če vključuje nesorazmeren napor“.[186]

186 Direktiva o varstvu osebnih podatkov, člen 12(c), druga polovica stavka.

## 5.1.2. Pravica do ugovora

Pravica do ugovora vključuje pravico do ugovora zoper avtomatizirane posamezne odločitve, pravico do ugovora zaradi posebnega položaja posameznika, na katerega se nanašajo osebni podatki, in pravico do ugovora zoper nadaljnjo uporabo osebnih podatkov za namen neposrednega trženja.

### Pravica do ugovora zoper avtomatizirane posamezne odločitve

Avtomatizirane odločitve so odločitve, sprejete na podlagi osebnih podatkov, obdelanih izključno z avtomatskimi sredstvi. Če bi take odločitve najverjetneje precej vplivale na življenja posameznikov, ker se nanašajo na primer na kreditno sposobnost, delovno uspešnost, ravnanje ali zanesljivost, je potrebno posebno varstvo, da se preprečijo škodljive posledice. V Direktivi o varstvu osebnih podatkov je določeno, da se z avtomatiziranimi odločitvami ne bi smelo odločati o vprašanjih, ki so pomembna za posameznike, prav tako pa se v njej zahteva, da mora imeti posameznik pravico do ponovne proučitve avtomatizirane odločitve.[187]

Primer: Pomemben praktični primer avtomatiziranega odločanja je kreditno točkovanje. Za hitro odločitev o kreditni sposobnosti prihodnje stranke se od nje pridobijo nekateri podatki, kot sta poklic in družinske razmere, ki se povežejo s podatki o posamezniku, dobljenimi iz drugih virov, na primer iz bonitetnih informacijskih sistemov. Ti podatki se samodejno vnašajo v točkovalni algoritem, s katerim se izračuna skupna vrednost, ki pomeni kreditno sposobnost morebitne stranke. Uslužbenec podjetja se lahko tako v nekaj sekundah odloči, ali je posameznik, na katerega se nanašajo osebni podatki, sprejemljiv kot stranka ali ne.

Države članice v skladu z navedeno direktivo kljub temu določijo, da se lahko o osebi sprejme avtomatizirana posamezna odločitev, če interesi posameznika, na katerega se nanašajo osebni podatki, niso ogroženi, ker je bilo odločeno v njegovo korist, ali če so zaščiteni z drugimi ustreznimi sredstvi.[188] Pravica do ugovora zoper avtomatizirane odločitve je vključena tudi v **pravo Sveta Evrope**, kot je mogoče videti v priporočilu o profiliranju.[189]

187 Prav tam, člen 15(1).

188 Prav tam, člen 15(2).

189 Priporočilo o profiliranju, člen 5(5).

## Pravica do ugovora zaradi posebnega položaja posameznika, na katerega se nanašajo osebni podatki

Posamezniki nimajo splošne pravice do ugovora zoper obdelavo svojih osebnih podatkov.[190] Vendar ima posameznik, na katerega se nanašajo osebni podatki, na podlagi člena 14(a) Direktive o varstvu osebnih podatkov pravico vložiti ugovor na podlagi zakonitih in nujnih razlogov, povezanih z njegovim posebnim položajem. Podobna pravica je priznana v priporočilu o profiliranju Sveta Evrope.[191] S takimi določbami se poskuša najti primerno ravnotežje med pravicami posameznika, na katerega se nanašajo osebni podatki, do varstva osebnih podatkov in zakonitimi interesi drugih pri obdelavi osebnih podatkov tega posameznika.

Primer: Banka več let hrani osebnih podatke o svojih strankah, ki zamujajo s poplačilom posojila. Stranka, katere osebni podatki so shranjeni v tej podatkovni zbirki, zaprosi še za eno posojilo. Preveri se podatkovna zbirka, poda se ocena finančnega stanja in stranki se zavrne odobritev posojila. Vendar lahko stranka ugovarja hrambi osebnih podatkov v podatkovni zbirki in zahteva njihov izbris, če lahko dokaže, da je bila zamuda pri plačilu samo posledica napake, ki je bila odpravljena takoj, ko je stranka zanjo izvedela.

Posledica uspešnega ugovora je, da upravljavec zadevnih osebnih podatkov ne sme več obdelovati. Vendar postopki obdelave osebnih podatkov posameznika, na katerega se nanašajo, izvedeni pred vložitvijo ugovora, ostanejo še naprej zakoniti.

## Pravica do ugovora zoper nadaljnjo uporabo osebnih podatkov zaradi neposrednega trženja

Člen 14(b) Direktive o varstvu osebnih podatkov določa posebno pravico do ugovora zoper uporabo osebnih podatkov zaradi neposrednega trženja. Taka pravica je določena tudi v priporočilu Sveta Evrope o neposrednem trženju.[192] Tak ugovor je treba vložiti, še preden se osebni podatki zaradi neposrednega trženja posredujejo tretjim

190 Glej tudi sodbe ESČP z dne 27. avgusta 1997 v zadevi *M. S. proti Švedski*, pritožba št. 20837/92, pri kateri so bili zdravstveni podatki sporočeni brez soglasja ali možnosti nasprotovanja; z dne 26. marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81, in z dne 10. maja 2011 v zadevi *Mosley proti Združenemu kraljestvu*, pritožba št. 48009/08.

191 Priporočilo o profiliranju, člen 5(3).

192 Svet Evrope, Odbor ministrov (1985), Priporočilo Rec(85)20 z dne 25. oktobra 1985 državam članicam o varstvu osebnih podatkov, ki se uporabljajo za neposredno trženje, člen 4(1).

osebam. Posamezniku, na katerega se nanašajo osebni podatki, je treba zato pred prenosom podatkov omogočiti, da poda ugovor.

## 5.2. Neodvisen nadzor

### Ključne točke

- Za zagotovitev učinkovitega varstva osebnih podatkov je treba na podlagi nacionalne zakonodaje ustanoviti neodvisne nadzorne organe.
- Nacionalni nadzorni organi morajo delovati popolnoma neodvisno, kar je treba zagotoviti z ustanovitvenim zakonom in kar se mora kazati v posebni organizacijski zgradbi nadzornega organa.
- Nadzorni organi imajo posebne naloge, da med drugim:
  - spremljajo in spodbujajo varstvo osebnih podatkov na nacionalni ravni;
  - svetujejo posameznikom, na katere se nanašajo osebni podatki, ter vladi in javnosti na splošno;
  - obravnavajo pritožbe in posameznikom, na katere se nanašajo osebni podatki, pomagajo pri domnevnih kršitvah pravic do varstva osebnih podatkov;
  - nadzorujejo upravljavce in obdelovalce;
  - po potrebi posredujejo z:
    - opozorilom, opominom ali celo denarno kaznijo upravljavcem in obdelovalcem,
    - odreditvijo popravka, blokiranja ali izbrisa osebnih podatkov,
    - odreditvijo prepovedi obdelave;
  - predložijo zadeve sodišču.

Z Direktivo o varstvu osebnih podatkov se kot pomemben mehanizem za zagotovitev učinkovitega varstva osebnih podatkov zahteva neodvisen nadzor. Z navedeno direktivo je bil uveden instrument za izvajanje varstva osebnih podatkov, ki ga v Konvenciji št. 108 ali smernicah OECD o zasebnosti sprva ni bilo.

Ker se je izkazalo, da je neodvisen nadzor nepogrešljiv za razvoj učinkovitega varstva osebnih podatkov, se države članice z novo določbo spremenjenih smernic

OECD o zasebnosti, sprejetih leta 2013, poziva, naj „ustanovijo organe za uveljavljanje zasebnosti in jim zagotovijo potrebno upravo, vire in tehnično strokovno znanje, da bodo lahko učinkovito izvajali svoje pristojnosti ter odločali objektivno, nepristransko in dosledno".[193]

**V pravu Sveta Evrope** je ustanovitev nadzornih organov postala obvezna z Dodatnim protokolom h Konvenciji št. 108. Ta instrument v členu 1 vsebuje pravni okvir za neodvisne nadzorne organe, ki ga morajo pogodbenice uvesti v nacionalno zakonodajo. Naloge in pristojnosti teh organov so opisane podobno kot v Direktivi o varstvu osebnih podatkov. Nadzorni organi bi morali torej načeloma delovati enako po pravu EU in pravu Sveta Evrope.

**V pravu EU** so bile pristojnosti in organizacijska zgradba nadzornih organov najprej opisani v členu 28(1) Direktive o varstvu osebnih podatkov. Z Uredbo o varstvu osebnih podatkov v institucijah EU[194] je ENVP določen kot nadzorni organ za obdelavo osebnih podatkov v organih in institucijah EU. Ta uredba pri opisu vlog in odgovornosti nadzornega organa izhaja iz izkušenj, pridobljenih po razglasitvi Direktive o varstvu osebnih podatkov.

Neodvisnost organov za varstvo osebnih podatkov je zagotovljena na podlagi člena 16(2) PDEU in člena 8(3) Listine, pri čemer se nadzor, ki ga izvaja neodvisni organ, v zadnji določbi izrecno šteje za bistveni del temeljne pravice do varstva osebnih podatkov. Poleg tega se z Direktivo o varstvu osebnih podatkov zahteva, da države članice za spremljanje njenega izvajanja ustanovijo nadzorne organe, ki bodo delovali popolnoma neodvisno.[195] Zakon, ki je podlaga za ustanovitev nadzornega organa, mora vsebovati določbe, s katerimi se izrecno zagotavlja neodvisnost, pri čemer mora ta izhajati iz posebne organizacijske zgradbe organa.

Sodišče EU je leta 2010 prvič obravnavalo vprašanje obsega zahteve po neodvisnosti nadzornih organov za varstvo osebnih podatkov.[196] Njegovo razmišljanje ponazarjajo naslednji primeri.

193 OECD (2013), Smernice o varstvu zasebnosti in čezmejnem prenosu osebnih podatkov, odstavek 19(c).

194 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 2001, L 8, členi 41 do 48.

195 Direktiva o varstvu osebnih podatkov, člen 28(1), zadnji stavek, Konvencija št. 108, Dodatni protokol, člen 1(3).

196 Glej letno poročilo agencije FRA (2010), Temeljne pravice: izzivi in dosežki v letu 2010, str. 59. Agencija je to vprašanje podrobneje obdelala v poročilu z naslovom Varstvo osebnih podatkov v Evropski uniji: vloga nacionalnih organov za varstvo osebnih podatkov, objavljenem maja 2010.

Primer: Evropska komisija je v zadevi *Komisija proti Nemčiji*[197] od Sodišča EU zahtevala, naj razglasi, da Nemčija ni pravilno prenesla zahteve po „popolni neodvisnosti" nadzornih organov, odgovornih za zagotovitev varstva osebnih podatkov, in tako ni izpolnila svoje obveznosti na podlagi člena 28(1) Direktive o varstvu osebnih podatkov. Po mnenju Komisije je bila težava v tem, da je Nemčija v različnih zveznih državah (*Länder*) uvedla državni nadzor nad organi, odgovornimi za spremljanje obdelave osebnih podatkov, v zasebnem sektorju.

Preizkus utemeljenosti tožbe je bil po mnenju Sodišča odvisen od obsega zahteve po neodvisnosti, vsebovane v navedeni določbi, torej od njene razlage.

Sodišče je opozorilo, da je treba navedbo „s popolno neodvisnostjo" v členu 28(1) Direktive o varstvu osebnih podatkov razlagati na podlagi dejanskega besedila navedene določbe ter ob upoštevanju ciljev in sistematike navedene direktive o varstvu osebnih podatkov.[198] Poudarilo je, da so nadzorni organi „varuhi" pravic v zvezi z obdelavo osebnih podatkov, ki so zagotovljene v navedeni direktivi, njihova ustanovitev v državah članicah pa se zato šteje „za bistven element varstva oseb pri obdelavi osebnih podatkov".[199] Sodišče je ugotovilo, da „morajo nadzorni organi pri izvajanju nalog ravnati objektivno in nepristransko. Zato ne smejo podleči nobenemu zunanjemu vplivu – niti neposrednim ali posrednim vplivom države ali dežel –, ne le vplivu nadzorovanih organov."[200]

Sodišče EU je še ugotovilo, da je treba pomen „popolne neodvisnosti" razlagati ob upoštevanju neodvisnosti ENVP, kot je opredeljena v Uredbi o varstvu osebnih podatkov v institucijah EU. Kot je poudarilo Sodišče, je v členu 44(2) navedene uredbe „v zvezi s pojmom neodvisnosti dodatno pojasnjeno, da ENVP pri izvajanju svojih nalog pri nikomer ne išče in od nikogar ne prevzema navodil". Tako se prepreči državni nadzor nad neodvisnim nadzornim organom za varstvo osebnih podatkov.[201]

Sodišče EU je v skladu s tem ugotovilo, da nemške institucije za varstvo osebnih podatkov, ki so na ravni zvezne države odgovorne za spremljanje obdelave

197 Sodba Sodišča EU z dne 9. marca 2010 v zadevi *Evropska komisija proti Zvezni republiki Nemčiji*, C-518/07, točka 27.

198 Prav tam, točki 17 in 29.

199 Prav tam, točka 23.

200 Prav tam, točka 25.

201 Prav tam, točka 27.

osebnih podatkov zasebnihteles, niso dovolj neodvisne, saj so podvržene državnemu nadzoru.

Primer: Sodišče EU je v zadevi *Komisija proti Avstriji*[202] opozorilo na podobne težave v zvezi s položajem nekaterih članov in osebja avstrijskega organa za varstvo osebnih podatkov (komisija za varstvo osebnih podatkov, DSK). Sodišče je v tej zadevi ugotovilo, da avstrijska zakonodaja avstrijskemu organu za varstvo osebnih podatkov ne omogoča, da bi bil pri izvajanju svojih nalog popolnoma neodvisen v smislu Direktive o varstvu osebnih podatkov. Neodvisnost avstrijske DSK ni bila zadostna, saj urad zveznega kanclerja DSK zagotavlja delovno silo, jo nadzoruje in ima pravico, da je kadar koli obveščen o njenem delu.

Primer: V zadevi *Evropska Komisija proti Madžarski*[203] je Sodišče EU poudarilo, da »zahteva (...) po popolni neodvisnosti nadzornega organa pri izvajanju zaupanih nalog, vključuje tudi obveznost države članice, da dopusti takemu organu delovati do zaključka mandataOb tem je sodišče tudi ugotovilo, »da Madžarska zaradi predčasnega odvzema mandata nadzornemu organu za varstvo osebnih podatkov ni izpolnila svojih obveznosti iz Direktive 95/46/ES (...)«

Nadzorni organi imajo na podlagi nacionalne zakonodaje med drugim pristojnosti in zmogljivosti, da:[204]

- upravljavcem in posameznikom, na katere se nanašajo osebni podatki, svetujejo o vseh zadevah v zvezi z varstvom osebnih podatkov;
- preiskujejo postopke obdelave in ustrezno posredujejo;
- opozarjajo ali opominjajo upravljavce;
- odredijo popravke, blokiranje, izbris ali uničenje osebnih podatkov;
- naložijo začasno ali dokončno prepoved obdelave;

202 Sodba Sodišča EU z dne 16. oktobra 2012 v zadevi *Evropska komisija proti Republiki Avstriji*, C-614/10, točki 59 in 63.

203 Sodba SEU št. C-288/12 z dne 8. aprila 2014, *Evropska Komisija proti Madžarski*, členi 50 in 67.

204 Direktiva o varstvu osebnih podatkov, člen 28; glej tudi Konvencijo št. 108, Dodatni protokol, člen 1.

- zadevo predložijo sodišču.

Da lahko nadzorni organ izvaja svoje funkcije, mora imeti dostop do vseh osebnih podatkov in informacij, ki so nujne za preiskavo, ter dostop do vseh prostorov, v katerih upravljavec hrani zadevne informacije.

Med nacionalnimi pristojnostmi v postopkih in pravnim učinkom ugotovitev nadzornega organa so precejšnje razlike. Te lahko vključujejo vse od priporočil, podobnih tistim, ki jih izdaja varuh človekovih pravic, do neposredno izvršljivih sklepov. Zato je treba instrumente pravnih sredstev pri analizi učinkovitosti tovrstnih sredstev, ki so na voljo v okviru določene pristojnosti, presojati v lastnem okviru.

## 5.3. Pravna sredstva in sankcije

### Ključne točke

- V skladu s Konvencijo št. 108 in Direktivo o varstvu osebnih podatkov je treba v nacionalni zakonodaji določiti ustrezna pravna sredstva in sankcije zoper kršitve pravice do varstva osebnih podatkov.
  - Pravica do učinkovitega pravnega sredstva v skladu z zakonodajo EU pomeni, da je treba z nacionalno zakonodajo določiti pravna sredstva zoper kršitve pravic do varstva osebnih podatkov, ne glede na to, da se je mogoče obrniti na nadzorni organ.
  - Nacionalna zakonodaja mora določati sankcije, ki so učinkovite, enakovredne, sorazmerne in odvračilne.
- Preden se posameznik zateče na sodišče, se mora najprej obrniti na upravljavca. Ali se je pred iskanjem pravice na sodišču obvezno obrniti tudi na nadzorni organ, je prepuščeno nacionalni zakonodaji.
- Posamezniki, na katere se nanašajo osebni podatki, lahko kot zadnje sredstvo in pod določenimi pogoji pri ESČP vložijo pritožbo zaradi kršitev zakonodaje o varstvu osebnih podatkov.
- Posamezniki, na katere se nanašajo osebni podatki, se lahko obrnejo tudi na Sodišče EU, vendar samo v zelo omejenem obsegu.

Pravice na podlagi zakonodaje o varstvu osebnih podatkov lahko uveljavlja samo oseba, katere pravice so ogrožene; ta oseba je (ali tako vsaj trdi) posameznik, na katerega se nanašajo osebni podatki. Take osebe lahko pri uveljavljanju pravic

zastopajo osebe, ki na podlagi nacionalne zakonodaje izpolnjujejo nujne zahteve. Mladoletne osebe morajo zastopati njihovi starši ali skrbniki. Pred nadzornimi organi lahko osebo zastopajo tudi združenja, katerih zakoniti cilj je spodbujati pravice do varstva osebnih podatkov.

### 5.3.1. Zahteve upravljavcu

Pravice, navedene v razdelku 3.2, je treba najprej uveljavljati pri upravljavcu. Neposredno uveljavljanje pravice pri nacionalnem nadzornem organu ali sodišču ne bi pomagalo, saj bi lahko organ zgolj svetoval, da se je treba najprej obrniti na upravljavca, sodišče pa bi ugotovilo, da je vloga nedopustna. Formalne zahteve za pravno ustrezno zahtevo upravljavcu, zlasti ali mora biti zahteva pisna, morajo biti urejene z nacionalno zakonodajo.

Subjekt, ki mu je bila zahteva predložena kot upravljavcu, mora na zahtevo odgovoriti, tudi če ni upravljavec. Odgovor je treba posamezniku, na katerega se nanašajo osebni podatki, vedno zagotoviti v roku, določenem z nacionalno zakonodajo, tudi če se navede samo, da se osebni podatki o vložniku ne obdelujejo. V skladu z določbami člena 12(a) Direktive o varstvu osebnih podatkov in člena 8(b) Konvencije št. 108 je treba navedeno zahtevo obravnavati „brez večjih zamud“. Z nacionalno zakonodajo je treba zato določiti rok za odgovor, ki je dovolj kratek, vendar upravljavcu kljub temu omogoča, da ustrezno obravnava zahtevo.

Subjekt, ki mu je zahteva predložena kot upravljavcu, mora pred odgovorom na zahtevo preveriti identiteto vložnika, da ugotovi, ali je dejansko oseba, za katero se izdaja, in se tako izogne resni kršitvi zaupnosti. Če zahteve za preverjanje identitete niso posebej urejene z nacionalno zakonodajo, jih mora določiti upravljavec. Vendar upravljavci v skladu z načelom poštene obdelave ne smejo predpisati preveč obremenjujočih pogojev za potrditev identitete (in pristnosti zahteve, kot je obravnavana v razdelku 2.1.1).

Z nacionalno zakonodajo mora biti rešeno tudi vprašanje, ali lahko upravljavci, preden odgovorijo na zahteve, od vložnika zahtevajo plačilo takse ali ne: člen 12(a) Direktive in člen 8(b) Konvencije št. 108 določata, da je treba na zahteve za dostop dogovoriti „brez večjih [...] stroškov“. V številnih evropskih državah je z nacionalno zakonodajo določeno, da je treba na zahteve na podlagi zakonodaje o varstvu osebnih podatkov odgovoriti brezplačno, če za odgovor ni potreben prevelik ali neobičajen napor; upravljavci so tako z nacionalno zakonodajo običajno zaščiteni pred zlorabo pravice do odgovora na zahteve.

Če oseba, institucija ali organ, ki mu je zahteva predložena kot upravljavcu, ne zanika, da je upravljavec, mora v roku, določenem z nacionalno zakonodajo:

- zahtevi ugoditi in osebo, ki jo je vložila, uradno obvestiti, kako je bila zahteva izpolnjena, ali

- osebo, ki je vložila zahtevo, obvestiti, zakaj njena zahteva ne bo izpolnjena.

## 5.3.2. Zahtevki, vloženi pri nadzornem organu

Če oseba, ki je pri upravljavcu vložila zahtevo za dostop ali ugovor, ne prejme pravočasnega in zadovoljivega odgovora, lahko pri nacionalnem nadzornem organu za varstvo osebnih podatkov zaprosi za pomoč. V postopku pred nadzornim organom je treba pojasniti, ali se je od osebe, institucije ali organa, na katerega se je vložnik obrnil, dejansko zahtevalo, da odgovori na zahtevo ter ali je bil odgovor pravilen in zadosten. Nadzorni organ mora zadevno osebo obvestiti o izidu postopka obravnave zahtevka.[205] Pravni učinki izidov postopka pred nacionalnimi nadzornimi organi so odvisni od nacionalne zakonodaje: ali so odločitve organa pravno izvršljive, to pomeni, da jih lahko izvrši uradni organ, oziroma ali je treba pri sodišču vložiti pritožbo, če upravljavec ne upošteva odločitev (mnenja, opomina itd.) nadzornega organa.

Če institucije ali organi EU domnevno kršijo pravice do varstva osebnih podatkov, zagotovljene na podlagi člena 16 PDEU, lahko posameznik, na katerega se nanašajo osebni podatki, vloži pritožbo pri ENVP,[206] neodvisnem nadzornem organu za varstvo osebnih podatkov v skladu z Uredbo o varstvu osebnih podatkov v institucijah EU, v kateri so določene dolžnosti in pristojnosti ENVP. Če ENVP ne odgovori v šestih mesecih, se šteje, da je bila pritožba zavrnjena.

Zoper odločitve nacionalnega nadzornega organa mora biti dovoljeno vložiti pritožbo pri sodiščih. To velja za posameznike, na katere se nanašajo osebni podatki, in upravljavce, ki so stranka v postopku pred nadzornim organom.

205 Direktiva o varstvu osebnih podatkov, člen 28(4).

206 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 2001, L 8.

Primer: Informacijski pooblaščenec Združenega kraljestva je 24. julija 2013 izdal odločbo, v kateri je hertfordshirsko policijo pozval, naj preneha uporabljati sistem sledenja registrskih tablic vozil, ki se šteje za protipraven. Podatki, zbrani s kamerami, so bili shranjeni v podatkovnih zbirkah lokalne policijske enote in centralizirani podatkovni zbirki. Fotografije registrskih tablic so se hranile dve leti, fotografije vozil pa 90 dni. Ugotovljeno je bilo, da tako obširna uporaba kamer in drugih oblik nadzora ni sorazmerna s problematiko, ki naj bi se je lotila.

## 5.3.3. Zahtevek, vložen pri sodišču

Oseba, ki upravljavcu predloži zahtevo na podlagi zakonodaje o varstvu osebnih podatkov in ni zadovoljna z njegovim odgovorom, mora imeti v skladu z Direktivo o varstvu osebnih podatkov pravico vložiti pritožbo pri nacionalnem sodišču.[207]

Ali se je pred iskanjem pravice na sodišču obvezno najprej obrniti na nadzorni organ, je prepuščeno nacionalni zakonodaji. Kljub temu je za osebe, ki uveljavljajo pravice do varstva osebnih podatkov, večinoma koristno, da se najprej obrnejo na nadzorni organ, saj bi morali biti postopki na podlagi zaprosil za njihovo pomoč nebirokratski in brezplačni. Posameznik, na katerega se nanašajo osebni podatki, si lahko pri uveljavljanju pravic pred sodišči pomaga tudi s strokovnim mnenjem, dokumentiranim v odločitvi nadzornega organa (mnenju, opominu itd.).

**Po pravu Sveta Evrope** se lahko kršitve pravic do varstva osebnih podatkov, ki so domnevno storjene na nacionalni ravni pogodbenice EKČP in hkrati pomenijo kršitev člena 8 EKČP, 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 (členi 34 do 37 EKČP).[208]

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 nacionalni zakonodaji ni zagotovila zadostnega varstva pred kršitvami pravic do varstva osebnih podatkov.

207 Direktiva o varstvu osebnih podatkov, člen 22.

208 Sodba ESČP, členi 34 do 37 so na voljo na: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

Primer: V zadevi *K. U. proti Finski*[209] je pritožnik, mladoletna oseba, zatrjeval, da je bil na spletni strani za zmenke o njem objavljen oglas spolne narave. Ponudnik storitve zaradi obveznosti zaupnosti na podlagi finske zakonodaje ni 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 razsodilo, da se morajo države ne samo vzdržati samovoljnega poseganja v zasebno življenje posameznikov, ampak lahko zanje veljajo tudi pozitivne obveznosti, ki vključujejo „sprejetje ukrepov za zagotovitev spoštovanja zasebnega življenja celo v okviru medosebnih odnosov med posamezniki". V pritožnikovem primeru je bilo treba zaradi njegovega dejanskega in učinkovitega varstva sprejeti 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*[210] 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 država pogodbenica kršila katero od pravic, ki so zavarovane z EKČP, mora država pogodbenica izvršiti sodbo ESČP. Z ukrepi izvršbe 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.

**Po pravu EU**[211] lahko žrtve kršitev nacionalne zakonodaje o varstvu osebnih podatkov, s katero se izvaja zakonodaja EU o varstvu osebnih podatkov, v nekaterih pri-

209 Sodba ESČP z dne 2. decembra 2009 v zadevi *K. U. proti Finski*, pritožba št. 2872/02.

210 Sodba ESČP z dne 5. oktobra 2010 v zadevi *Köpke proti Nemčiji (dec.)*, pritožba št. 420/07.

211 EU (2007), Lizbonska pogodba, ki spreminja Pogodbo o Evropski uniji in Pogodbo o ustanovitvi Evropske skupnosti, podpisana v Lizboni 13. decembra 2007, UL 2007, C 306. Glej tudi prečiščeno različico Pogodbe o Evropski uniji, UL 2012, C 326, in Pogodbe o delovanju Evropske unije, UL 2012, C 326.

merih sprožijo postopek pred Sodiščem EU. Obstajata dva scenarija, po katerih lahko posameznik, na katerega se nanašajo osebni podatki, s sklicevanjem na kršitev pravic do varstva osebnih podatkov sproži postopek pred Sodiščem EU.

V prvem scenariju bi moral biti posameznik, na katerega se nanašajo osebni podatki, neposredna žrtev upravnega akta ali predpisa EU, s katerim se kršijo posameznikove pravice do varstva osebnih podatkov. Člen 263(4) PDEU določa:

> *„Fizične ali pravne osebe lahko [...] vložijo tožbe zoper nanje naslovljene akte ali zoper akte, ki se nanje neposredno in posamično nanašajo, in zoper predpise, ki se nanje neposredno nanašajo, a ne potrebujejo izvedbenih ukrepov."*

Žrtve nezakonite obdelave osebnih podatkov s strani organa EU lahko zato vložijo neposredno tožbo pri Splošnem sodišču EU, ki je pristojno za razsojanje v zadevah iz Uredbe o varstvu osebnih podatkov v institucijah EU. Obrniti se je mogoče tudi neposredno na Sodišče EU, če pravna določba EU neposredno vpliva na posameznikov pravni položaj.

Drugi scenarij se nanaša na pristojnost Sodišča EU za odločanje o predlogih za sprejetje predhodne odločbe v skladu s členom 267 PDEU.

Posamezniki, na katere se nanašajo osebni podatki, lahko nacionalno sodišče v postopku pred njim zaprosijo, naj od Sodišča EU zahteva pojasnilo glede razlage Pogodb EU ter glede razlage in veljavnosti aktov institucij, organov, uradov ali agencij EU. Taka pojasnila so poznana kot predhodno odločanje. Za pritožnika to ni neposredno pravno sredstvo, vendar nacionalnim sodiščem omogoča, da uporabijo pravilno razlago prava EU.

Če stranka v postopku pred nacionalnimi sodišči zahteva predložitev vprašanja Sodišču EU, morajo to storiti samo tista nacionalna sodišča, ki odločajo na zadnji stopnji in zoper odločitve katerih ni pravnih sredstev.

Primer: Avstrijsko ustavno sodišče je v zadevi *Kärntner Landesregierung in drugi*[212] Sodišču EU predložilo vprašanja glede veljavnosti členov 3 do 9 Direktive 2006/24/ES (*Direktive o hrambi podatkov*) z vidika členov 7, 9 in 11 Listine in vprašanje, ali so nekatere določbe avstrijskega zveznega zakona o

212 SEU, združeni zadevi C-293/12 and C-594/12, *Digital Rights Ireland and Seitling in drugi*, 8. april 2014.

telekomunikacijah, s katerim je bila prenesena Direktiva o hrambi podatkov, nezdružljive z vidiki Direktive o varstvu osebnih podatkov in Uredbe o varstvu osebnih podatkov v institucijah EU ali ne.

G. Seitlinger, eden od pritožnikov v postopku pred ustavnim sodiščem, je trdil, da telefon, internet in e-pošto uporablja na delovnem mestu in v zasebnem življenju. Informacije, ki jih pošilja in prejema, se zato prenašajo prek javnih telekomunikacijskih omrežij. Njegov ponudnik telekomunikacijskih storitev mora na podlagi avstrijskega zakona o telekomunikacijah iz leta 2003 po zakonu zbirati in shranjevati podatke o njegovi uporabi omrežja. G. Seitlinger je sprevidel, da tako zbiranje in shranjevanje njegovih osebnih podatkov nikakor ni nujno za tehnični vidik prenosa informacij od točke A do točke B v omrežju. Prav tako zbiranje in shranjevanje navedenih podatkov nista bila niti najmanj potrebna za obračunavanje. G. Seitlinger vsekakor ni nasprotoval tej uporabi osebnih podatkov. Edini razlog za zbiranje in shranjevanje vseh teh dodatnih podatkov je bil avstrijski zakon o telekomunikacijah iz leta 2003.

G. 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.

Sodišče EU odloča samo o sestavnih elementih predloga za sprejetje predhodne odločbe, ki mu je predložen. Za odločanje o prvotni zadevi ostane pristojno nacionalno sodišče.

Sodišče EU mora načeloma odgovoriti na vprašanja, ki so mu predložena. 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.

Nazadnje, če institucija ali organ EU med obdelavo osebnih podatkov domnevno krši pravice do varstva osebnih podatkov, zagotovljene s členom 16 PDEU, lahko posameznik, na katerega se nanašajo osebni podatki, sproži postopek pred Splošnim sodiščem EU (člen 32(1) in (4) Uredbe o varstvu osebnih podatkov v institucijah EU). Enako velja za odločbe ENVP, ki se nanašajo na take kršitve (člen 32(3) Uredbe o varstvu osebnih podatkov v institucijah EU).

Splošno sodišče EU je pristojno za odločanje v zadevah iz Uredbe o varstvu osebnih podatkov v institucijah EU, če pa oseba zahteva pravno varstvo kot član osebja institucije ali organa EU, se mora pritožiti pri Sodišču za uslužbence EU.

Primer: V sodbi v zadevi *Evropska komisija proti The Bavarian Lager Co. Ltd.*[213] so ponazorjena pravna sredstva zoper dejavnosti ali odločitve institucij in organov EU v zvezi z varstvom podatkov.

Družba Bavarian Lager je 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.[214] Družba Bavarian Lager je na podlagi člena 32 Uredbe o varstvu osebnih podatkov v institucijah EU zoper to odločitev vložila pritožbo pri Sodišču EU; natančneje pri Sodišču prve stopnje (predhodnik Splošnega sodišča). Sodišče prve stopnje je z odločitvijo v zadevi *Bavarian Lager proti Komisiji*, T-194/04, odločitev Komisije, da zavrne prošnjo za dostop, razglasilo za nično. Evropska komisija se je zoper to odločitev pritožila pri Sodišču EU. Sodišče (veliki senat) je razveljavilo sodbo Sodišča prve stopnje in potrdilo odločitev Evropske komisije, da zavrne prošnjo za dostop.

## 5.3.4. Sankcije

**V pravu Sveta Evrope** člen 10 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.[215] **V pravu EU** člen 24 Direktive o varstvu osebnih podatkov določa, da države članice „sprejmejo ustrezne ukrepe za zagotovitev popolne izvedbe določb te direktive in predvsem določijo sankcije, ki se naložijo ob kršitvi določb […]".

213 Sodba Sodišča EU z dne 29. junija 2010 v zadevi *Evropska komisija proti The Bavarian Lager Co. Ltd.*, C-28/08 P.

214 Za analizo utemeljitve glej ENVP (2011), Dostop javnosti do dokumentov, ki vsebujejo osebne podatke po odločitvi Sodišča v zadevi Bavarian Lager, Bruselj, na voljo na naslovu: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

215 Sodbi ESČP z dne 17. julija 2008 v zadevi *I. proti Finski*, pritožba št. 20511/03, in z dne 2. decembra 2008 v zadevi *K. U. proti Finski*, pritožba št. 2872/02.

Na podlagi obeh instrumentov imajo države članice širok manevrski prostor pri izbiri ustreznih sankcij in pravih sredstev. Noben pravni instrument ne vsebuje niti posebnih smernic o naravi ali vrsti primernih sankcij niti primerov sankcij.

Vendar:

> *„čeprav imajo države članice EU polje proste presoje pri določitvi, kateri ukrepi so najustreznejši za zavarovanje pravic, ki za posameznike izhajajo iz prava EU, je treba v skladu z načelom lojalnega sodelovanja iz člena 4(3) PEU spoštovati vsaj minimalne zahteve glede učinkovitosti, enakovrednosti, sorazmernosti in odvračilnosti."*[216]

Sodišče EU je večkrat navedlo, da nacionalna zakonodaja nima popolne svobode pri določitvi sankcij.

Primer: Sodišče EU je v zadevi *Von Colson in Kamann proti Land Nordrhein-Westfalen*[217] poudarilo, da morajo vse države članice, ki so naslovnice direktive, v nacionalnem pravnem sistemu sprejeti vse potrebne ukrepe za zagotovitev polnega učinka direktive v skladu z njenim ciljem. Razsodilo je, da lahko države članice sicer same izberejo način in sredstva za zagotovitev izvajanja direktive, vendar to ne vpliva na obveznost, ki jim je naložena. Zlasti je treba z učinkovitim pravnim sredstvom omogočiti, da posameznik zadevno pravico uporablja in uveljavlja v polnem materialnem obsegu. Za dosego dejanskega in učinkovitega varstva je treba s pravnimi sredstvi sprožiti kazenske in/ali odškodninske postopke, v katerih se naložijo sankcije z odvračilnim učinkom.

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 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 […]".

216 Mnenje 2/2012 Agencije Evropske unije za temeljne pravice z dne 1. oktobra 2012 o svežnju reform na področju varstva osebnih podatkov, Dunaj, str. 27.

217 SEU, C-14/83, *Sabine von Kolson and Elisabeth Kamann v. Land Nordrhein-Westfalen*, 10. april 1984.

# 6

# Čezmejni prenos osebnih podatkov

| EU | Obravnavane teme | Svet Evrope |
|---|---|---|
| **Čezmejni prenos podatkov** | | |
| Direktiva o varstvu osebnih podatkov, člen 25(1)<br>Sodba Sodišča EU z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01 | Opredelitev | Konvencija št. 108, Dodatni protokol, člen 2(1) |
| **Prosti prenos podatkov** | | |
| Direktiva o varstvu osebnih podatkov, člen 1(2) | Med državami članicami EU | |
| | Med pogodbenicami Konvencije št. 108 | Konvencija št. 108, člen 12(2) |
| Direktiva o varstvu osebnih podatkov, člen 25 | Tretjim državam z ustrezno ravnjo varstva | Konvencija št. 108, Dodatni protokol, člen 2(1) |
| Direktiva o varstvu osebnih podatkov, člen 26(1) | Tretjim državam v posebnih primerih | Konvencija št. 108, Dodatni protokol, člen 2(2)(a) |
| **Omejen prenos osebnih podatkov v tretje države** | | |
| Direktiva o varstvu osebnih podatkov, člen 26(2)<br>Direktiva o varstvu osebnih podatkov, člen 26(4) | Pogodbena določila | Konvencija št. 108, Dodatni protokol, člen 2(2)(b)<br>Priročnik za pripravo pogodbenih določil |
| Direktiva o varstvu osebnih podatkov, člen 26(2) | Zavezujoča poslovna pravila | |
| Primera:<br>Sporazum PNR med EU in ZDA<br>Sporazum SWIFT med EU in ZDA | Posebni mednarodni sporazumi | |

Direktiva o varstvu osebnih podatkov določa prosti prenos osebnih podatkov med državami članicami, vsebuje pa tudi določbe o zahtevah za prenos osebnih podatkov v tretje države zunaj EU. Pomen izvedbenih pravil za čezmejni prenos osebnih podatkov v tretje države je priznal tudi Svet Evrope, ki je leta 2001 sprejel Dodatni protokol h Konvenciji št. 108. S tem protokolom so prevzete glavne regulativne značilnosti čezmejnega prenosa osebnih podatkov iz držav podpisnic Konvencije in držav članic EU.

## 6.1. Narava čezmejnega prenosa osebnih podatkov

### Ključne točke

- Čezmejni prenos osebnih podatkov je prenos osebnih podatkov prejemniku, ki je pod pristojnostjo druge države.

V členu 2(1) Dodatnega protokola h Konvenciji št. 108 je čezmejni prenos osebnih podatkov opisan kot prenos osebnih podatkov prejemniku, ki je pod pristojnostjo druge države. S členom 25(1) Direktive o varstvu osebnih podatkov je urejen „prenos osebnih podatkov, ki so v obdelavi ali so namenjeni obdelavi po dovoljenem prenosu, v tretjo državo […]“. Tak prenos osebnih podatkov je dovoljen samo ob upoštevanju pravil iz člena 2 Dodatnega protokola h Konvenciji št. 108, za države članice EU pa tudi iz členov 25 in 26 Direktive o varstvu osebnih podatkov.

Primer: Sodišče EU je v zadevi *Bodil Lindqvist*[218] navedlo, 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“.

Sodišče je nato poudarilo, da navedena direktiva določa tudi posebna pravila, katerih namen je državam članicam omogočiti nadzor nad prenosi osebnih podatkov v tretje države.

218 Sodba Sodišča EU z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01, točke 27, 68 in 69.

Vendar ob upoštevanju stanja razvoja spleta ob nastanku navedene direktive na eni strani in nevključitve meril v zvezi z uporabo spleta vanjo na drugi strani „ni mogoče predpostaviti, da je nameraval zakonodajalec Skupnosti v pojem ‚prenos [osebnih podatkov] v tretjo državo' vnaprej vključiti vnos osebnih podatkov na spletno stran […], tudi če ti podatki s tem postanejo dostopni osebam iz tretjih držav, ki imajo tehnična sredstva za dostop do njih".

Če pa bi se direktiva razlagala tako, „da obstaja prenos osebnih podatkov v tretjo državo vsakič, ko se osebni podatki naložijo na spletno stran, bi bil ta prenos nujno prenos v vse tretje države, v katerih obstajajo tehnična sredstva, potrebna za dostop do spleta. Posebna ureditev iz [direktive] bi torej, kar zadeva postopke na spletu, nujno postala splošna ureditev. Ko bi namreč Komisija […] ugotovila, da ena sama tretja država ne zagotavlja ustrezne ravni varstva, bi morale vse države članice preprečiti kakršno koli nalaganje osebnih podatkov na splet."

Načelo, da se zgolj objava (osebnih) podatkov ne sme šteti za čezmejni prenos podatkov, velja tudi za javne registre in sredstva javnega obveščanja na spletu, kot so (elektronski) časopisi in televizija. Pojem „čezmejni prenos osebnih podatkov" se lahko uporablja samo za komunikacijo, namenjeno točno določenim prejemnikom.

## 6.2. Prosti prenos osebnih podatkov med državami članicami ali pogodbenicami

### Ključne točke

- Prenos osebnih podatkov v drugo državo članico Evropskega gospodarskega prostora ali drugo pogodbenico Konvencije št. 108 ne sme biti omejen.

V skladu s členom 12(2) Konvencije št. 108 je treba **po pravu Sveta Evrope** med pogodbenicami Konvencije zagotoviti prosti prenos osebnih podatkov. Z nacionalno zakonodajo ni dovoljeno omejiti prenosa osebnih podatkov v državo pogodbenico, razen če:

- je to potrebno zaradi posebne narave osebnih podatkov[219] ali

219 Konvencija št. 108, člen 12(3)(a).

- je omejitev potrebna, da se prepreči izogibanje nacionalnim zakonskim določbam o čezmejnem prenosu osebnih podatkov v tretje države.[220]

**Po pravu EU** so omejitve ali prepovedi prostega prenosa osebnih podatkov med državami članicami zaradi varstva osebnih podatkov prepovedane s členom 1(2) Direktive o varstvu osebnih podatkov. Območje prostega prenosa osebnih podatkov je bilo razširjeno s Sporazumom o Evropskem gospodarskem prostoru (EGP) [221], s katerim so se na notranji trg vključili Islandija, Lihtenštajn in Norveška.

Primer: Če odvisna družba mednarodne skupine družb, ki ima sedež v več državah članicah EU, med drugim v Sloveniji in Franciji, iz Slovenije v Francijo posreduje osebne podatke, tak prenos podatkov ne sme biti omejen ali prepovedan s slovensko nacionalno zakonodajo.

Če pa želi ista slovenska odvisna družba iste osebne podatke prenesti matični družbi v Združenih državah, mora slovenski izvoznik osebnih podatkov izvesti postopke, ki so v slovenski zakonodaji določeni za čezmejni prenos (iznos) osebnih podatkov v tretje države, ki nimajo ustreznega varstva osebnih podatkov, razen če je matična družba prevzela načela zasebnosti varnega pristana, neobvezna pravila ravnanja v zvezi z zagotavljanjem ustrezne ravni varstva osebnih podatkov (glej razdelek 6.3.1).

Ker pa se določbe Direktive o varstvu osebnih podatkov ne uporabljajo za čezmejni prenos osebnih podatkov v države članice EGP za namene, ki niso povezani z notranjim trgom, na primer preiskovanje kaznivih dejanj, zanj ne velja načelo prostega prenosa osebnih podatkov. Kar zadeva pravo Sveta Evrope, vsa področja spadajo na področje uporabe Konvencije št. 108 in Dodatnega protokola h Konvenciji št. 108, čeprav lahko pogodbenice določijo izjeme. Vse države članice EGP so tudi pogodbenice Konvencije št. 108.

220 Prav tam, člen 12(3)(b).

221 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, UL 1994, L 1.

## 6.3. Prosti prenos osebnih podatkov v tretje države

**Ključne točke**

- Prenos osebnih podatkov v tretje države je brez omejitev na podlagi nacionalne zakonodaje o varstvu osebnih podatkov, če:
  - je ugotovljeno ustrezno varstvo osebnih podatkov pri prejemniku ali
  - je nujen zaradi posebnih interesov posameznika, na katerega se nanašajo osebni podatki, ali zakonitih prevladujočih interesov drugih, zlasti pomembnih javnih interesov.
- Ustreznost varstva osebnih podatkov v tretji državi pomeni, da so bila v nacionalno zakonodajo te države učinkovito uvedena glavna načela varstva osebnih podatkov.
- Po pravu EU ustreznost varstva osebnih podatkov v tretji državi presoja Evropska komisija. Po pravu Sveta Evrope je ureditev presoje ustreznosti prepuščena nacionalni zakonodaji.

### 6.3.1. Prosti prenos osebnih podatkov zaradi ustrezne ravni varstva

**Pravo Sveta Evrope** dovoljuje, da se z nacionalno zakonodajo omogoči prosti prenos osebnih podatkov v države, ki niso pogodbenice, če država ali organizacija prejemnica za nameravani prenos osebnih podatkov zagotavlja ustrezno raven varstva.[222] Kako naj se oceni raven varstva v tuji državi in kdo naj jo oceni, je določeno z nacionalno zakonodajo.

**Po pravu EU** je prosti prenos osebnih podatkov v tretje države z ustrezno ravnjo varstva osebnih podatkov določen v členu 25(1) Direktive o varstvu osebnih podatkov. Ker se zahteva ustreznost in ne enakovrednost, je mogoče uporabiti različne načine izvajanja varstva osebnih podatkov. Evropska komisija je v skladu s členom 25(6) navedene direktive pristojna, da oceni raven varstva osebnih podatkov

222 Konvencija št. 108, Dodatni protokol, člen 2(1).

v tujih državah na podlagi ugotovitev o ustreznosti in posvetovanj o oceni z delovno skupino iz člena 29, kar je bistveno pripomoglo k razlagi členov 25 in 26.[223]

Ugotovitev Evropske komisije o ustreznosti ima zavezujoč učinek. Če Evropska komisija za določeno državo v *Uradnem listu Evropske unije* objavi ugotovitev o ustreznosti, morajo to odločitev upoštevati vse države članice EGP in njihovi organi, kar pomeni, da se lahko osebni podatki v te države prenašajo brez postopkov preverjanja ali potrjevanja pred nacionalnimi organi.[224]

Evropska komisija lahko tudi oceni dele pravnega sistema države ali se omeji na posamezne teme. Ugotovitev o ustreznosti je na primer podala samo v zvezi z zasebno trgovinsko zakonodajo Kanade.[225] Več ugotovitev o ustreznosti je tudi za prenose na podlagi sporazumov med EU in tujimi državami. Te odločitve se nanašajo izključno na eno vrsto prenosa osebnih podatkov, na primer prenos evidenc podatkov o potnikih z letalskih družb tujim organom za nadzor meje, če letalska družba leti iz EU v nekatere čezmorske destinacije (glej razdelek 6.4.3). Z novejšo prakso prenosa osebnih podatkov, ki temelji na posebnih sporazumih med EU in tretjimi državami, se na splošno odpravlja potreba po ugotovitvah o ustreznosti, saj se domneva, da je ustrezna raven varstva osebnih podatkov zagotovljena s samim sporazumom.[226]

Ena od najpomembnejših odločb o ustrezni ravni varstva osebnih podatkov se dejansko ne nanaša na sklop zakonskih določb.[227] Nasprotno, nanaša se na pravila,

223 Glej na primer Delovni dokument delovne skupine iz člena 29 z dne 3. junija 2003 o prenosu osebnih podatkov v tretje države: uporaba člena 26(2) Direktive EU o varstvu osebnih podatkov pri zavezujočih poslovnih pravilih za mednarodne prenose podatkov, WP 74, Bruselj, in Delovni dokument delovne skupine iz člena 29 z dne 25. novembra 2005 o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995, WP 114, Bruselj.

224 Za nenehno posodobljen seznam držav, ki so prejele odločbo o ustreznosti, glej domačo stran Evropske komisije, Generalni direktorat za pravosodje, ki je na voljo na naslovu: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 Evropska komisija (2002), 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 2002, L 2.

226 Na primer Sporazum med Združenimi državami Amerike in Evropsko unijo o uporabi in prenosu evidenc podatkov o potnikih ministrstvu Združenih držav za domovinsko varnost, UL 2012, L 215, str. 5–14, ali Sporazum med Evropsko unijo in Združenimi državami Amerike o obdelavi in posredovanju podatkov o sporočilih glede finančnih plačil iz Evropske unije Združenim državam Amerike za sledenje financiranja terorističnih dejavnosti, UL 2010, L 8, str. 11–16.

227 Evropska komisija (2000), 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 2000, L 215.

nekakšen kodeks ravnanja, ki so znana kot načela zasebnosti Varnega pristana. Ta načela so za podjetja v ZDA skupaj določile EU in ZDA. Članstvo v Varnem pristanu se doseže s prostovoljno zavezo, sprejeto pred ameriškim ministrstvom za trgovino in dokumentirano na seznamu, ki ga objavlja navedeno ministrstvo. Ker je učinkovitost izvajanja varstva osebnih podatkov eden od pomembnih dejavnikov ustreznosti, ureditev Varnega pristana določa tudi določen obseg državnega nadzora: Varnemu pristanu se lahko pridružijo samo podjetja, ki so pod nadzorom zvezne komisije za trgovino ZDA.

### 6.3.2. Prosti prenos osebnih podatkov v posebnih primerih

**V pravu Sveta Evrope** člen 2(2) Dodatnega protokola h Konvenciji št. 108 dovoljuje prenos osebnih podatkov v tretje države, ki nimajo ustreznega varstva osebnih podatkov, če je prenos določen z nacionalno zakonodajo in je nujen zaradi:

- posebnih interesov posameznika, na katerega se nanašajo osebni podatki, ali
- prevladujočih zakonitih interesov drugih, zlasti pomembnih javnih interesov.

**V pravu EU** člen 26(1) Direktive o varstvu osebnih podatkov vsebuje podobne določbe kot Dodatni protokol h Konvenciji št. 108.

V skladu z navedeno direktivo je lahko prosti prenos osebnih podatkov v tretjo državo upravičen zaradi interesov posameznika, na katerega se nanašajo osebni podatki, če:

- posameznik, na katerega se nanašajo osebni podatki, nedvoumno privoli v iznos podatkov;
- posameznik, na katerega se nanašajo osebni podatki, sklene pogodbeno razmerje, oziroma se pripravlja na njegovo sklenitev , v zvezi s katerim se jasno zahteva prenos podatkov prejemniku v tujini;
- sta upravljavec osebnih podatkov in tretja oseba sklenila pogodbo v interesu posameznika, na katerega se nanašajo osebni podatki;

- je prenos nujen za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki;

- gre za prenos podatkov iz javnih registrov; to je primer prevladujočih interesov splošne javnosti, da lahko dostopa do informacij, shranjenih v javnih registrih.

Prosti čezmejni prenos osebnih podatkov lahko upravičijo zakoniti interesi drugih:[228]

- zaradi pomembnega javnega interesa, ki ni povezan z zadevami nacionalne ali javne varnosti, saj te niso zajete z Direktivo o varstvu osebnih podatkov, ali

- za vlaganje, uveljavljanje ali obrambo pravnih zahtevkov.

Zgoraj navedene primere je treba razumeti kot izjeme od pravila, da je za neoviran prenos osebnih podatkov v druge države potrebna ustrezna raven varstva osebnih podatkov v državi prejemnici. Izjeme je treba vedno razlagati ozko. Delovna skupina iz člena 29 je to že večkrat poudarila v okviru člena 26(1) Direktive o varstvu osebnih podatkov, zlasti če je privolitev domnevna podlaga za prenos podatkov.[229] Ugotovila je, da splošna pravila glede pravnega pomena privolitve veljajo tudi za člen 26(1) navedene direktive. Če na primer v okviru odnosov med delodajalci in delojemalci ni jasno, ali je bila privolitev, ki so jo dali zaposleni, dejansko prostovoljna, potem prenos osebnih podatkov ne more temeljiti na členu 26(1)(a) navedene direktive. V takih primerih se uporabi člen 26(2), ki določa, da morajo nacionalni organi za varstvo osebnih podatkov izdati dovoljenje za prenos osebnih podatkov.

## 6.4. Omejen prenos osebnih podatkov v tretje države

### Ključne točke

- Od upravljavca se lahko zahteva, da pred iznosom osebnih podatkov v tretje države, ki ne zagotavljajo ustrezne ravni varstva osebnih podatkov, nameravani prenos podatkov predloži v pregled nadzornemu organu.

228 Direktiva o varstvu osebnih podatkov, člen 26(1)(d).

229 Glej zlasti Delovni dokument delovne skupine iz člena 29 z dne 25. novembra 2005 o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995, WP 114, Bruselj.

- Upravljavec, ki želi iznesti osebne podatke, mora med takim pregledom dokazati dvoje:
  - da obstaja pravna podlaga za prenos osebnih podatkov prejemniku in
  - da so uvedeni ukrepi za zagotovitev ustreznega varstva osebnih podatkov pri prejemniku.
- Ukrepi za izvajanje ustreznega varstva osebnih podatkov pri prejemniku lahko vključujejo:
  - pogodbene klavzule med upravljavcem, ki iznaša osebne podatke, in tujim prejemnikom podatkov ali
  - zavezujoča poslovna pravila, ki se običajno uporabljajo za prenos osebnih podatkov v mednarodni skupini družb.
- Prenos osebnih podatkov tujim organom je lahko urejen tudi s posebnim mednarodnim sporazumom.

Direktiva o varstvu osebnih podatkov in Dodatni protokol h Konvenciji št. 108 dovoljujeta, da se z nacionalno zakonodajo določijo ureditve za čezmejni prenos osebnih podatkov v tretje države, ki ne zagotavljajo ustrezne ravni varstva osebnih podatkov, če je upravljavec posebej poskrbel za zagotovitev ustreznih zaščitnih ukrepov za varstvo podatkov pri prejemniku in če lahko upravljavec to dokaže pristojnemu organu. Ta zahteva je izrecno navedena samo v Dodatnem protokolu h Konvenciji št. 108; vendar se šteje za standardni postopek tudi na podlagi Direktive o varstvu osebnih podatkov.

## 6.4.1. Pogodbena določila

**V pravu Sveta Evrope** in **pravu EU** so pogodbena določila (klavzule) med upravljavcem, ki iznaša osebne podatke, in prejemnikom v tretji državi navedena kot možni način za zagotovitev zadostne ravni varstva osebnih podatkov pri prejemniku.

Na **ravni EU** je Evropska komisija ob pomoči delovne skupine iz člena 29 razvila standardne pogodbene klavzule, ki so bile z odločbo Komisije uradno potrjene kot dokaz o ustrezni ravni varstva osebnih podatkov.[230] Ker so odločbe Komisije v državah članicah zavezujoče v celoti, morajo nacionalni organi, pristojni za nadzor nad čezmejnim prenosom osebnih podatkov, te standardne pogodbene klavzule priznati tudi v

230 Direktiva o varstvu osebnih podatkov, člen 26(4).

svojih postopkih.[231] Če se torej upravljavec, ki iznaša osebne podatke, in prejemnik v tretji državi dogovorita o teh določilih in jih podpišeta, mora biti to za nadzorni organ zadosten dokaz, da so uvedeni ustrezni zaščitni ukrepi.

Obstoj standardnih pogodbenih klavzul v pravnem okviru EU pa ne pomeni, da upravljavci ne smejo izoblikovati drugih začasnih pogodbenih določil. Vendar morajo poskrbeti za enako raven varstva, kot je zagotovljena s standardnimi pogodbenimi določili. 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;

- prejemnik osebnih podatkov ali uvoznik se strinja, da se zanj ob sporu uporabi postopek nadzornega organa in/ali sodišč upravljavca, ki izvaža podatke.

Upravljavec, ki iznaša osebne podatke, lahko zdaj izbira med dvema sklopoma standardnih klavzul, ki sta na voljo za prenose med upravljavci.[232] Za prenose med upravljavcem in obdelovalcem obstaja samo en sklop standardnih pogodbenih klavzul.[233]

V okviru **prava Sveta Evrope** je posvetovalni odbor iz Konvencije št. 108 pripravil navodila za pripravo pogodbenih klavzul.[234]

231 PDEU, člen 288.

232 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 2001, L 181; 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 2004, L 385.

233 Evropska komisija (2010), Odločba Komisije 2010/87 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 2010, L 39.

234 Svet Evrope, posvetovalni odbor iz Konvencije št. 108 (2002), *Smernice za pripravo pogodbenih določil o varstvu podatkov med prenosom osebnih podatkov tretjim strankam, ki jih ne zavezuje ustrezna raven varstva osebnih podatkov*.

## 6.4.2. Zavezujoča poslovna pravila

Pri večstranskih zavezujočih poslovnih pravilih zelo pogosto hkrati sodeluje več evropskih organov za varstvo osebnih podatkov.[235] Da bi se zavezujoča poslovna pravila odobrila, je treba njihov osnutek in standardne prijavne obrazce poslati vodilnemu organu.[236] Vodilni organ je razviden iz standardnega prijavnega obrazca. Ta organ nato obvesti vse nadzorne organe v državah članicah EGP, v katerih imajo sedež odvisne družbe skupine, čeprav njihovo sodelovanje pri ocenjevanju zavezujočih pravnih pravil ni obvezno. Čeprav to ni zavezujoče, bi morali vsi zadevni organi za varstvo osebnih podatkov rezultate ocenjevanja vključiti v svoje uradne postopke potrjevanja.

## 6.4.3. Posebni mednarodni sporazumi

EU je sklenila posebne sporazume za dve vrsti prenosa osebnih podatkov:

### Evidence podatkov o potnikih

Letalski prevozniki podatke iz evidenc podatkov o potnikih (PNR) zbirajo med rezervacijo, vključujejo pa imena, naslove, podatke o kreditni kartici in številke sedežev letalskih potnikov. Po pravu ZDA morajo letalske družbe te podatke pred odhodom potnika dati na voljo ministrstvu za domovinsko varnost. To velja za lete v ZDA in iz njih.

Za zagotovitev ustrezne zaščite osebnih podatkov o potnikih in uskladitev z določbami Direktive 95/46/SE, je bil v letu 2004 sprejet »paket PNR«[237], ki naj bi ZDA zavezoval k zagotavljanju ustrezne ravni varstva osebnih podatkov, ki jih je obdelovalo Ministrstvo Združenih držav za domovinsko varnost (DHS). Potem, ko je Sodišče

235 Vsebina in zgradba ustreznih zavezujočih poslovnih pravil sta pojasnjeni v Delovnem dokumentu delovne skupine iz člena 29 z dne 24. junija 2008 o vzpostavitvi okvira zgradbe zavezujočih poslovnih pravil, WP 154, Bruselj, in Delovnem dokumentu delovne skupine iz člena 29 z dne 24. junija 2008 o vzpostavitvi preglednice s sestavnimi deli in načeli za zavezujoča poslovna pravila, WP 153, Bruselj.

236 Priporočilo 1/2007 delovne skupine iz člena 29 z dne 10. januarja 2007 o standardni uporabi zavezujočih poslovnih pravi pri prenosu osebnih podatkov, WP 133, Bruselj.

237 Sklep Sveta 2004/496 /ES z dne 17. maja 2004 o sklenitvi sporazuma med Evropsko skupnostjo in Združenimi državami Amerike o obdelavi in prenosu podatkov iz PNR s strani letalskih prevoznikov Ministrstvu Združenih držav za domovinsko varnost, Uradu ZDA za carine in zaščito meja, UL 2004, L 183, str. 83, in Odločbo Komisije 2004/535 /ES z dne 14. maja 2004 o ustreznem varstvu in prenosu osebnih podatkov, vsebovanih v evidenci podatkov o potnikih (PNR) s strani letalskih prevoznikov, Uradu ZDA za carine in zaščito meja, UL 2004, L 235, str. 11-22.

EU[238] razveljavilo navedeni paket PNR, sta bila sprejeta dva ločena sporazuma z namenom: prvič, da se zagotovi pravno podlago za razkritje osebnih podatkov iz evidenc podatkov o potnikih organom ZDA in, drugič, določi ustrezno raven varstva osebnih podatkov v državi prejemnici.

Prvi sporazum o tem, kako se osebni podatki med državami EU in ZDA izmenjujejo in upravljajo, sklenjen v letu 2007, je imel več pomanjkljivosti in je bil nadomeščen v let 2012 z novim sporazumom, ki bolje zagotavlja pravno varnost.[239] Novi sporazum ponuja bistvene izboljšave. Z njim se omejujejo in pojasnjujejo nameni, za katere se lahko informacije uporabijo, na primer huda mednarodna kazniva dejanja in terorizem, ter določa dobo hrambe osebnih podatkov: po šestih mesecih morajo biti osebni podatki anonimizirani in prikriti. Na podlagi sporazuma imajo posamezniki tudi pravico dostopati do svojih osebnih podatkov iz evidenc podatkov o potnikih, ki se hranijo v ZDA. Če informacije niso točne, jih je treba spremeniti ali izbrisati, kar prej ni bilo zagotovljeno. Če se njihovi osebni podatki zlorabijo, imajo posamezniki pravico do pravnih sredstev v upravnih in sodnih postopkih v skladu s pravom ZDA. Ob tem imajo pravico dostopati do svojih osebnih podatkov iz evidenc podatkov o potnikih in od ministrstva za domovinsko varnost zahtevati njihov popravek, vključno z možnostjo izbrisa, če informacije niso točne.

Sporazum, ki je začel veljati 1. julija 2012, bo veljal sedem let, do leta 2019.

Svet Evropske unije je decembra 2011 odobril sprejetje posodobljenega Sporazuma med EU in Avstralijo o obdelavi in prenosu osebnih podatkov iz evidence podatkov o potnikih (PNR).[240] Sporazum med EU in Avstralijo o osebnih podatkih iz evidence podatkov o potnikih (PNR) je še en korak v programu EU, ki vključuje svetovne

238 Glej sklep Sodišča Evropske unije (C-317/04 in C-318/04), *Evropski parlament v. Svet Evropske unije*, 30. maja 2006, členi 57, 58 in 59, v katerem je Sodišče odločilo, da sta ustreznost in sporazumnost v procesu obdelave podatkov izključeni iz področja Direktive.

239 Sklep Sveta 2012/472/EU z dne 26. aprila 2012 o sklenitvi Sporazuma med Združenimi državami Amerike in Evropsko unijo o uporabi in prenosu evidenc podatkov o potnikih ministrstvu Združenih držav za domovinsko varnost, UL 2012, L 215/4. Besedilo sporazuma, ki je nadomestil prejšnji sporazum iz leta 2007, je priloženo k temu sklepu, UL 2012, L 215, str. 5–14.

240 Sklep Sveta 2012/381/EU z dne 13. decembra 2011 o sklenitvi sporazuma med Evropsko unijo in Avstralijo o obdelavi in prenosu podatkov iz evidence podatkov o potnikih (PNR) s strani letalskih prevoznikov avstralski carinski in mejni službi, UL 2012, L 186/3. Besedilo Sporazuma je priloženo k temu sklepu, UL 2012, L 186, str. 4–16.

smernice v zvezi z evidencami podatkov o potnikih[241], vzpostavitev programa za evidenco podatkov o potnikih EU[242] in sklepanje sporazumov s tretjimi državami.[243]

## Podatki o sporočilih glede finančnih poročil

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 ministrstvu za finance ZDA razkrije podatke zaradi preiskovanja terorizma.[244]

Z vidika EU ni bilo zadostne pravne podlage za razkritje teh večinoma evropskih podatkov, ki so bili v Združenih državah dostopni samo zato, ker je imel eden od centrov združenja SWIFT za obdelavo storitev sedež v Združenih državah.

Leta 2010 je bil sklenjen poseben sporazum med EU in Združenimi državami, poznan kot Sporazum SWIFT, da bi zagotovili potrebno pravno podlago in ustrezno varstvo osebnih podatkov.[245]

Na podlagi tega sporazuma se finančni podatki, ki jih shranjuje SWIFT, ministrstvu za finance ZDA posredujejo zaradi preprečevanja, preiskovanja, odkrivanja ali pregona terorizma ali njegovega financiranja. Ministrstvo za finance ZDA lahko združenje SWIFT zaprosi za finančne podatke, če zaprosilo:

241 Glej zlasti Sporočilo Komisije z dne 21. septembra 2010 o globalnem pristopu k prenosu podatkov iz evidence imen letalskih potnikov (PNR) tretjim državam, COM(2010) 492 final, Bruselj. Glej tudi Mnenje št. 7/2010 Delovne skupine iz člena 29, WP 178 z dne 12. Novembra 2010, o tem Sporočilu Komisije.

242 Predlog Direktive Evropskega parlamenta in Sveta z dne 2. februarja 2011 o uporabi podatkov iz evidence podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj, COM(2011) 32 final, Bruselj. Evropski parlament je agencijo FRA aprila 2011 zaprosil za mnenje o tem predlogu in njegovi skladnosti z Listino Evropske unije o temeljnih pravicah. Glej Mnenje 1/2011 agencije FRA (2011) z dne 14. junija 2011 – Evidenca podatkov o potnikih, Dunaj.

243 EU se trenutno s Kanado pogaja o novem sporazumu o evidenci podatkov o potnikih, ki bo nadomestil trenutno veljavni sporazum iz leta 2006.

244 Glej v zvezi s tem Mnenje 14/2011 delovne skupine iz člena 29 z dne 13. junija 2011 o vprašanjih varstva podatkov, povezanih s preprečevanjem pranja denarja in financiranja terorizma, WP 186, Bruselj, in Mnenje 10/2006 delovne skupine iz člena 29 z dne 22. novembra 2006 o obdelavi osebnih podatkov Družbe za svetovne medbančne finančne telekomunikacije (SWIFT), WP 128, Bruselj; Sklep belgijske komisije za varstvo zasebnosti (Commission de la protection de la vie privée) z dne 9. decembra 2008, „Postopek nadzora in priporočil, sprožen v zvezi z družbo SWIFT scrl".

245 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 sledenje financiranja terorističnih dejavnosti, UL 2010, L 195, str. 3 in 4. Besedilo Sporazuma je priloženo temu sklepu, UL 2010, L 195, str. 5–14.

- čim jasneje navede finančne podatke;
- jasno utemelji, zakaj so podatki potrebni;
- je zasnovano čim ožje, da se zahtevani osebnih podatki omejijo na najmanjši možni obseg;
- ne poizveduje po podatkih v zvezi z enotnim območjem plačil v eurih (SEPA).

Europol mora prejeti kopijo vsakega zaprosila ministrstva za finance ZDA in preveriti, ali se upoštevajo načela iz sporazuma SWIFT ali ne.[246] Če se potrdi, da se upoštevajo, mora združenje SWIFT finančne podatke posredovati neposredno ministrstvu za finance ZDA. 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 medsebojno povezani z nobeno drugo podatkovno zbirko. Na splošno se finančni podatki, ki jih pošlje združenja SWIFT, izbrišejo najpozneje pet let po prejemu. Finančni podatki, ki so pomembni za določene preiskave ali pregon, se lahko hranijo, dokler so potrebni za te preiskave ali pregon.

Ministrstvo za finance ZDA lahko informacije iz podatkov, ki jih prejme združenje SWIFT, pošlje 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.

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. Prav tako imajo pravico do popravka, izbrisa ali blokiranja svojih osebnih podatkov, ki jih ministrstvo za finance ZDA zbira

246 Nadzorni organ Europola je izvedel revizijo dejavnosti Europola na tem področju, rezultati so na voljo prek: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang= en.

in shranjuje na podlagi sporazuma SWIFT. Vendar lahko za pravice posameznikov, na katere se nanašajo osebni podatki, do dostopa 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 Združenih državah.

Sporazum SWIFT velja pet let, do avgusta 2015. Nato se samodejno podaljšuje za nadaljnja enoletna obdobja, razen če ena od strank drugih vsaj šest mesecev vnaprej ne obvesti, da ga ne namerava podaljšati.

# 7

# Varstvo osebnihosebnih podatkov v okviru policije in kazenskega pravosodja

| EU | Obravnavane teme | Svet Evrope |
|---|---|---|
| | Splošno | Konvencija št. 108 |
| | Policija | Priporočilo o policiji |
| | | Sodba ESČP z dne 17. decembra 2009 v zadevi *B. B. proti Franciji*, pritožba št. 5335/06 |
| | | Sodba ESČP z dne 4. decembra 2008 v združenih zadevah *S. in Marper proti Združenemu kraljestvu*, pritožbi št. 30562/04 in 30566/04 |
| | | Sodba ESČP z dne 31. maja 2005 v zadevi *Vetter proti Franciji*, pritožba št. 59842/00 |
| | Kibernetska kriminaliteta | Konvencija o kibernetski kriminaliteti |
| **Varstvo osebnih podatkov v okviru čezmejnega sodelovanja policijskih in pravosodnih organov** | | |
| Okvirni sklep o varstvu osebnih podatkov | Splošno | Konvencija št. 108<br>Priporočilo o policiji |
| Sklep k Prümski pogodbi | Za posebne osebne podatke: prstne odtise, DNK, huliganstvo itd. | Konvencija št. 108<br>Priporočilo o policiji |
| Sklep o ustanovitvi Europola<br>Sklep o Eurojustu<br>Uredba o Frontexu | Po posebnih agencijah | Konvencija št. 108<br>Priporočilo o policijskih podatkih |

| | | |
|---|---|---|
| Sklep Schengen II<br>Uredba VIS<br>Uredba Eurodac<br>Sklep CIS | **Po posebnih skupnih informacijskih sistemih** | Konvencija št. 108<br>Priporočilo o policiji<br>Sodba ESČP z dne 2. februarja 2010 v zadevi *Dalea proti Franciji*, pritožba št. 964/07 |

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.

## 7.1. Pravo Sveta Evrope o varstvu osebnih podatkov v policijskih in pravosodnih kazenskih zadevah

### Ključne točke

- V Konvenciji št. 108 in Priporočilu Sveta Evrope o policijskih osebnih podatkih je obravnavano varstvo osebnih podatkov na vseh področjih policijskega dela.
- Konvencija o kibernetski kriminaliteti (*Konvencija iz Budimpešte*) je zavezujoči mednarodni pravni instrument, v katerem so obravnavana kazniva dejanja, storjena zoper elektronska omrežja in prek njih.

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, čeprav lahko pogodbenice njeno uporabo tudi omejijo.

Pri zakonskih nalogah policijskih in kazenskih pravosodnih organov je pogosto potrebna obdelava osebnih podatkov, ki lahko ima resne posledice za zadevne posameznike. Priporočilo o policijskih osebnih podatkih, ki ga je Svet Evrope sprejel leta 1987, pogodbenicam zagotavlja smernice, kako naj uveljavijo načela iz Konvencije št. 108 v okviru obdelave osebnih podatkov, ki jo izvajajo policijski organi.[247]

247 Svet Evrope, Odbor ministrov (1987), Priporočilo Rec(87)15 z dne 17. septembra 1987 državam članicam, ki ureja uporabo osebnih podatkov v policijskem sektorju.

### 7.1.1. Priporočilo o policijskih osebnih podatkih

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 obravnavano v številnih sodbah ESČP.[248]

Primer: ESČP je v zadevi *B. B. proti Franciji*[249] odločilo, 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 ni bil kršen člen 8 EKČP.

Primer: V zadevi *S. in Marper proti Združenemu kraljestvu*[250] sta bila oba pritožnika obdolžena kaznivih dejanj, vendar nista bila spoznana za kriva. Policija je kljub temu imela in hranila njune prstne odtise, profil DNK in celične vzorce. 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.

V številnih drugih sodbah ESČP je obravnavana utemeljenost poseganja v pravico do varstva osebnih podatkov z nadzorom.

Primer: Organi so v zadevi *Allan proti Združenemu kraljestvu*[251] na skrivaj snemali zasebne pogovore zapornika s prijateljem v zaporniškem prostoru za obiske in s soobtoženim v zaporniški celici. ESČP je razsodilo, da uporaba naprav

248 Glej na primer sodbe ESČP z dne 26. marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81/; z dne 13. novembra 2012 v zadevi *M. M. proti Združenemu kraljestvu*, pritožba št. 24029/07, in z dne 18. aprila 2013 v zadevi *M. K. proti Franciji*, pritožba št. 19522/09.

249 Sodba ESČP z dne 17. decembra 2009 v zadevi *B. B. proti Franciji*, pritožba št. 5335/06.

250 Sodba ESČP z dne 4. decembra 2008 v združenih zadevah *S. in Marper proti Združenemu kraljestvu*, pritožbi št. 30562/04 in 30566/04, točki 119 in 125.

251 Sodba ESČP z dne 5. novembra 2002 v zadevi *Allan proti Združenemu kraljestvu*, pritožba št. 48539/99.

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, navedeno poseganje ni bilo v skladu z zakonom. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Primer: V zadevi *Klass in drugi proti Nemčiji*[252] so pritožniki trdili, da več nemških zakonodajnih aktov, ki dovoljujejo tajno spremljanje elektronske pošte, pošte in telekomunikacij, krši člen 8 EKČP, zlasti ker zadevna oseba o ukrepih spremljanja ni bila obveščena in se ni mogla obrniti na sodišče, ko so se ti ukrepi končali. ESČP je ugotovilo, da grožnja z nadzorom nujno pomeni poseganje v svobodo komuniciranja med uporabniki poštnih in telekomunikacijskih storitev. Vendar je ugotovilo, da so bili zoper zlorabo uvedeni zadostni zaščitni ukrepi. Nemški zakonodajalec je take ukrepe zaradi nacionalne varnosti in za preprečevanje nereda ali kriminala upravičeno štel za nujne v demokratični družbi. Sodišče je ugotovilo, da člen 8 EKČP ni bil kršen.

Ker lahko ima obdelava osebnih podatkov s strani policijskih organov precejšnje posledice za zadevne osebe, so podrobna pravila v zvezi z varstvom osebnih podatkov za vodenje podatkovnih zbirk na tem področju še posebno nujna. To vprašanje naj bi bilo obravnavano v Priporočilu Sveta Evrope o policijskih osebnih podatkih, 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 lahko ima dostop do tehzbirk, vključno s pogoji za prenos osebnih podatkov tujim policijskim organom, kako je treba posameznikom, na katere se nanašajo osebni podatki, omogočiti uveljavljanje pravic do varstva osebnih podatkov in kako je treba izvajati nadzor, ki ga zagotavljajo neodvisni organi. Obravnavana je tudi obveznost zagotavljanja ustreznega zavarovanja osebnih podatkov.

Priporočilo ne predvideva časovno neomejenega, neselektivnega zbiranja osebnih podatkov s strani policijskih organov. Zbiranje osebnih podatkov v okviru policijskih organov je omejeno na to, kar je nujno za preprečevanje resne nevarnosti ali zatiranje določenih kaznivih dejanj. Vsako dodatno zbiranje osebnih podatkov bi moralo temeljiti na posebni nacionalni zakonodaji. Obdelava osebnih podatkov bi morala biti omejena na to, kar je v okviru določene preiskave nujno potrebno.

252 Sodba ESČP z dne 6. septembra 1978 v zadevi *Klass in drugi proti Nemčiji*, pritožba št. 5029/71.

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 ovira preiskave. Zbiranje osebnih podatkov s tehničnim nadzorom ali drugimi avtomatskimi sredstvi bi moralo prav tako temeljiti na posebnih zakonskih določbah.

Primer: V zadevi *Vetter proti Franciji*[253] so anonimne priče pritožnika obtožile umora. Ker je pritožnik redno zahajal na prijateljev dom, je policija tam z dovoljenjem preiskovalnega sodnika namestila prisluškovalne naprave. Zaradi prepričljivosti pogovorov, ki so bili posneti, je bil pritožnik aretiran in obtožen umora. Zahteval je, naj se posnetek ne upošteva kot dokaz, pri čemer je zlasti trdil, da to ni določeno z zakonom. Za ESČP je bilo ključno vprašanje, ali je uporaba prisluškovalnih naprav „v skladu z zakonom" ali ne. Nameščanje prisluškovalnih naprav v zasebnih prostorih očitno ni spadalo na področje uporabe člena 100 in naslednjih zakonika o kazenskem postopku, saj so se navedene določbe nanašale na prestrezanje telefonskih povezav. V členu 81 zakonika ni bil dovolj jasno naveden obseg ali način izvajanja diskrecijske pravice organov pri odobritvi spremljanja zasebnih pogovorov. V skladu s tem pritožniku ni bilo zagotovljeno minimalno varstvo, do katerega so državljani upravičeni v pravni državi in demokratični družbi. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

Priporočilo se konča z ugotovitvijo, da je treba pri shranjevanju osebnih podatkov jasno razlikovati med: upravnimi in policijskimi podatki, različnimi vrstami posameznikov, na katere se nanašajo osebni podatki, kot so osumljenci, obsojenci, žrtve in priče, ter podatki, ki se štejejo za zanesljiva dejstva, in tistimi, ki temeljijo na sumih in domnevah.

Policijski podatki bi morali imeti strogo omejen namen. To vpliva na sporočanje policijskih podatkov tretjim osebam: prenos ali sporočanje takih podatkov v policijskem sektorju bi morala biti urejena ne glede na to, ali obstaja zakoniti interes za izmenjavo informacij. Prenos ali sporočanje takih informacij zunaj policijskega sektorja bi morala biti dovoljena samo, če obstaja jasna pravna obveznost ali odobritev. Mednarodni prenos ali sporočanje 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.

253 Sodba ESČP z dne 31. maja 2005 v zadevi *Vetter proti Franciji*, pritožba št. 59842/00.

Obdelava osebnih podatkov s strani policije 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 Konvencija št. 108. Če so pravice posameznikov, na katere se nanašajo osebni podatki, do dostopa v skladu s členom 9 navedene konvencije omejene v interesu učinkovitih policijskih preiskav, mora imeti tak posameznik na podlagi nacionalne zakonodaje pravico, da se pritoži pri nacionalnem nadzornem organu za varstvo osebnih podatkov ali drugem neodvisnem organu.

## 7.1.2. Konvencija iz Budimpešte o kibernetski kriminaliteti

Ker pri kriminalnih dejavnostih narašča uporaba elektronskih sistemov za obdelavo osebnih podatkov, ki so tudi vse bolj kritično obravnavani, 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 Konvencija iz Budimpešte, da bi obravnaval vprašanje kaznivih dejanj, storjenih zoper elektronska omrežja in prek njih.[254] K tej konvenciji lahko pristopijo tudi države, ki niso članice Sveta Evrope, pri čemer so bile do sredine leta 2013 njene pogodbenice štiri take države (Avstralija, Dominikanska republika, Japonska in ZDA), še 12 drugih držav nečlanic pa je konvencijo podpisalo ali pa so bile povabljene, da pristopijo k njej.

Konvencija o kibernetski kriminaliteti ostaja najvplivnejša mednarodna pogodba, v kateri se obravnavajo kršitve zakona prek spleta ali drugih informacijskih omrežij. Od pogodbenic se zahteva, naj posodobijo in uskladijo svojo kazenskopravno zakonodajo proti vdorom v računalniške sisteme in drugim varnostnim kršitvam, vključno s kršitvami avtorskih pravic, računalniško podprtimi goljufijami, otroško pornografijo in drugimi nezakonitimi kibernetskimi dejavnostmi. Konvencija določa tudi procesna pooblastila, s katerimi sta zajeti preiskovanje računalniških omrežij in prestrezanje komunikacij v okviru boja proti kibernetski kriminaliteti. Nazadnje omogoča tudi učinkovito mednarodno sodelovanje. V Dodatnem protokolu h Konvenciji je obravnavana kriminalizacija rasistične in ksenofobične propagande v računalniških omrežjih.

254 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.

Čeprav Konvencija dejansko ni instrument za spodbujanje varstva osebnih podatkov, pa kriminalizira dejavnosti, s katerimi bi se lahko kršila pravica posameznikado varstva osebnih podatkov. Določa še, da morajo pogodbenice pri izvajanju Konvencije predvideti ustrezno varstvo človekovih pravic in svoboščin, vključno s pravicami, zagotovljenimi z EKČP, na primer pravico do varstva osebnih podatkov.[255]

## 7.2. Pravo EU o varstvu osebnih podatkov v policijskih in pravosodnih kazenskih zadevah

**Ključne točke**

- Na ravni EU je varstvo osebnih podatkov v policijskih in kazenskopravnih zadevah urejeno samo v okviru čezmejnega sodelovanja policijskih in pravosodnih organov.
- Posebni ureditvi varstva osebnih podatkov sta uvedeni za Evropski policijski urad (Europol) in Urad za evropsko pravosodno sodelovanje (Eurojust), ki sta organa EU za pomoč in spodbujanje čezmejnega sodelovanja organov odkrivanja in pregona .
- Posebne ureditve varstva 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 Schengen II, vizumski informacijski sistem (VIS) in Eurodac, centraliziran sistem, ki vsebuje prstne odtise državljanov tretjih držav, ki zaprosijo za azil v eni od držav članic EU.

Direktiva o varstvu osebnih podatkov se na področju policije in kazenskega pravosodja ne uporablja. Najpomembnejši pravni instrumenti na tem področju so opisani v razdelku 7.2.1.

### 7.2.1. Okvirni sklep o varstvu osebnih podatkov

Namen Okvirnega sklepa Sveta 2008/977/PNZ o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (*Okvirni sklep o varstvu osebnih podatkov*)[256] je zagotoviti varstvo osebnih podatkov fizičnih oseb, če se njihovi podatki obdelujejo zaradi preprečevanja, preiskovanja,

255 Prav tam, člen 15(1).

256 Svet Evropske unije (2008), Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (*Okvirni sklep o varstvu osebnih podatkov*), UL 2008, L 350.

odkrivanja ali pregona kaznivega dejanja ali izvrševanja kazni za tako dejanje. V imenu držav članic ali EU delujejo pristojni organi na področju policije in kazenskega pravosodja. Ti organi so agencije ali organi EU ter organi držav članic.[257] Uporaba okvirnega sklepa je omejena na zagotavljanje varstva osebnih podatkov pri čezmejnem sodelovanju med temi organi in ni razširjena na nacionalno varnost.

Okvirni sklep o varstvu osebnih podatkov večinoma temelji na načelih in opredelitvah, ki jih vsebujeta Konvencija št. 108 in Direktiva o varstvu osebnih podatkov.

Osebne podatke mora uporabljati samo pristojni organ, in sicer samo za namen, za katerega so bili posredovani ali dani na voljo. Država članica, ki prejme osebne podatke, mora upoštevati morebitne omejitve v zvezi z izmenjavo osebnih podatkov, določene v zakonodaji države članice, ki je posredovala podatke. Vendar lahko država prejemnica podatke pod določenimi pogoji uporabi tudi za drug namen. Posebna naloga pristojnih organov je prijava in dokumentiranje posredovanja, da se ob pritožbah lažje razjasnijo pristojnosti. Za nadaljnji prenos osebnih podatkov, prejetih v okviru čezmejnega sodelovanja, tretjim osebam je potrebna privolitev države članice, iz katere izvirajo podatki, čeprav so v nujnih primerih mogoče tudi izjeme.

Pristojni organi morajo sprejeti potrebne varnostne ukrepe za varstvo osebnih podatkov pred nezakonitimi oblikami obdelave.

Vsaka država članica mora določiti enega ali več neodvisnih nadzornih organov, odgovornih za svetovanje in spremljanje uporabe predpisov, sprejetih na podlagi Okvirnega sklepa o varstvu osebnih podatkov. Ti organi obravnavajo tudi zahtevke, ki jih vloži katera koli oseba v zvezi z varstvom njenih pravic in svoboščin, povezanim z obdelavo osebnih podatkov s strani pristojnih organov.

Posameznik, na katerega se nanašajo osebni podatki, ima pravico biti obveščen o obdelavi svojih osebnih podatkov ter pravico do dostopa, popravka, izbrisa in blokiranja teh podatkov. Če se uveljavljanje teh pravic zavrne iz nujnih razlogov, mora imeti posameznik, na katerega se nanašajo osebni podatki, pravico vložiti pritožbo pri pristojnem nacionalnem nadzornem organu in/ali sodišču. Če oseba utrpi škodo zaradi kršitev nacionalne zakonodaje o izvajanju Okvirnega sklepa o varstvu osebnih podatkov, je upravičena do odškodnine od upravljavca.[258] Na splošno morajo imeti posamezniki, na katere se nanašajo osebni podatki, ob kršitvi pravic, zagotovljenih

257 Prav tam, člen 2(h).

258 Prav tam, člen 19.

z nacionalno zakonodajo o izvajanju Okvirnega sklepa o varstvu osebnih podatkov, pravico do sodnega varstva.[259]

Evropska komisija je predlagala reformo, ki vključuje Splošno uredbo o varstvu osebnih podatkov[260] in Splošno direktivo o varstvu osebnih podatkov.[261] Nova direktiva bo nadomestila trenutno veljavni Okvirni sklep o varstvu osebnih podatkov, hkrati pa se bodo v policijsko in pravosodno sodelovanje v kazenskih zadevah uvedla splošna načela in pravila.

## 7.2.2. Podrobnejši pravni instrumenti o varstvu osebnih podatkov pri čezmejnem sodelovanju med policijo in organi kazenskega pregona

Poleg Okvirnega sklepa o varstvu osebnih podatkov je izmenjava informacij, ki jih imajo države članice, na določenih področjih urejena z več pravnimi instrumenti, kot sta Okvirni sklep Sveta 2009/315/PNZ o organizaciji in vsebini izmenjave informacij iz kazenske evidence med državami članicami in Sklep Sveta o dogovoru glede sodelovanja med enotami za finančni nadzor (FIU-ji) držav članic pri izmenjavi informacij.[262]

Pomembno je, da čezmejno sodelovanje[263] 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 nadzora na notranjih mejah v EU se je povečalo tveganje

259 Prav tam, člen 20.

260 Evropska komisija (2012), predlog Uredbe Evropskega parlamenta in Sveta z dne 25. januarja 2012 o varstvu posameznikov v zvezi z obdelavo osebnih podatkov in prostem pretoku takih podatkov (*Splošna uredba o varstvu podatkov*), COM(2012) 11 final, Bruselj.

261 Evropska komisija (2012), predlog Direktive Evropskega parlamenta in Sveta z dne 25. januarja 2012 o varstvu posameznikov v zvezi z obdelavo osebnih podatkov, ki jo pristojni organi izvajajo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazni, in prostim pretokom takih podatkov (*Splošna direktiva o varstvu podatkov*), COM(2012) 10 final, Bruselj.

262 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 2009, L 93; Svet Evropske unije (2000), Sklep Sveta 2000/642/PNZ z dne 17. oktobra 2000 o dogovoru glede sodelovanja med enotami za finančni nadzor držav članic pri izmenjavi informacij, UL 2000, L 271.

263 Evropska komisija (2012), Sporočilo Komisije Evropskemu parlamentu in Svetu z dne 7. decembra 2012 – Krepitev sodelovanja na področju kazenskega pregona v EU: evropski model za izmenjavo informacij (EIXM), COM(2012) 735 final, Bruselj.

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.

## Sklep k Prümski pogodbi

Pomemben primer institucionaliziranega čezmejnega sodelovanja z izmenjavo osebnih podatkov, shranjenih na nacionalni ravni, je Sklep Sveta 2008/615/PNZ o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu (*Sklep k Prümski pogodbi*), s katerim je bila Prümska pogodba leta 2008 vključena v pravo EU.[264] Prümska pogodba je bila mednarodni sporazum o policijskem sodelovanju, ki so ga leta 2005 podpisali Avstrija, Belgija, Francija, Nemčija, Luksemburg, Nizozemska in Španija.[265]

Sklep k Prümski pogodbi naj bi državam članicam pomagal izboljšati izmenjavo informacij za preprečevanje in boj proti kriminalu na treh področjih: terorizem, čezmejni kriminal in nezakonito priseljevanje. 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 Sklepa k Prümski pogodbi, so v celoti urejene z nacionalno zakonodajo, izmenjava osebnih podatkov pa je dodatno urejena s sklepom in po novem tudi z Okvirnim sklepom o varstvu osebnih podatkov. Organi, pristojni za nadzor nad prenosom takih osebnih podatkov, so nacionalni nadzorni organi za varstvo osebnih podatkov.

264 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 2008, L 210.

265 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 je na voljo na: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

## 7.2.3. Varstvo osebnih podatkov v okviru Europola in Eurojusta

### Europol

Europol, agencija EU za odkrivanje, preprečevanje in pregon kaznivih dejanj, ima sedež v Haagu, nacionalne enote Europola pa so v vsaki državi članici. Europol je bil ustanovljen leta 1998; njegov sedanji pravni status agencije EU temelji na Sklepu Sveta o ustanovitvi Evropskega policijskega urada (*Sklep o ustanovitvi Europola*).[266] Cilj Europola je pomagati pri preprečevanju in preiskovanju organiziranega kriminala, terorizma in drugih hujših oblik kriminala, navedenih v Prilogi k Sklepu o ustanovitvi Europola, ki prizadenejo dve ali več držav članic.

Da bi Europol dosegel svoje cilje, je vzpostavil Europolov informacijski sistem, ki državam članicam zagotavlja podatkovno zbirko za izmenjavo obveščevalnih podatkov o kaznivih dejanjih in informacij 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 osebnih podatke vnašajo neposredno v Europolov informacijski sistem in jih tam tudi poiščejo. Podatke lahko spreminja, popravlja ali izbriše samo oseba, ki jih je vnesla v sistem.

Europol lahko, kadar je to potrebno za izvajanje njegovih nalog, v analitičnih delovnih datotekah hrani, spreminja in uporablja podatke o kaznivih dejanjih. Analitične delovne datoteke se odprejo zaradi zbiranja, obdelave ali uporabe osebnih podatkov v pomoč pri konkretnih preiskavah kaznivih dejanj, ki jih Europol vodi v sodelovanju z državami članicami EU.

Kot odziv na nova dogajanja je bil 1. januarja 2013 pri Europolu ustanovljen Evropski center za boj proti kibernetski kriminaliteti.[267] Center deluje kot informacijsko vozlišče

266 Svet Evropske unije (2009), Sklep Sveta z dne 6. aprila 2009 o ustanovitvi Evropskega policijskega urada (Europol), UL 2009, L 121. Glej tudi predlog Uredbe Komisije, ki zagotavlja pravni okvir za nov Europol, ki nasledi in nadomesti Europol, kot je bil ustanovljen s Sklepom Sveta 2009/371/PNZ z dne 6. aprila 2009 o ustanovitvi Evropskega policijskega urada (Europol), in akademijo Cepol, kot je bila ustanovljena s Sklepom Sveta 2005/681/PNZ o ustanovitvi Evropske policijske akademije (Cepol), COM(2013) 173 final.

267 Glej tudi mnenje Evropskega nadzornika za varstvo osebnih podatkov z dne 29. junija 2012 o Sporočilu Evropske komisije Svetu in Evropskemu parlamentu o ustanovitvi Evropskega centra za boj proti kibernetski kriminaliteti, Bruselj.

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 ogromne nezakonite dobičke, kot so spletne goljufije;
- žrtvi povzročijo resno škodo, kot so spolno izkoriščanje otrok na spletu;
- vplivajo na ključno infrastrukturo in informacijske sisteme v EU.

Sistem varstva osebnih podatkov, s katerim so urejene dejavnosti Europola, je okrepljen. V členu 27 Sklepa o ustanovitvi Europola je navedeno, da se uporabljajo načela iz Konvencije št. 108 in iz Priporočila o policijskem sodelovanju, ki se nanašajo na avtomatizirano in neavtomatizirano obdelavo osebnih podatkov. Pri prenosu osebnih podatkov med Europolom in državami članicami je treba upoštevati tudi pravila iz Okvirnega sklepa o varstvu osebnih podatkov.

Za zagotovitev upoštevanja veljavne zakonodaje o varstvu osebnih podatkov, zlasti za zagotovitev, da z obdelavo osebnih podatkov niso kršene pravice posameznikov, dejavnosti Europola preverja in nadzoruje neodvisen skupni nadzorni organ Europola.[268] Vsak posameznik ima pravico dostopati do vseh osebnih podatkov, ki jih Europol morda hrani o njem, poleg tega pa ima tudi pravico zahtevati, naj se njegovi osebni podatki preverijo, popravijo ali izbrišejo. Če oseba ni zadovoljna z Europolovo odločitvijo v zvezi z uveljavljanjem teh pravic, se lahko pritoži pri odboru za pritožbe skupnega nadzornega organa.

V primeru škode, ki je posledica pravnih ali dejanskih napak v osebnih podatkih, shranjenih ali obdelanih v Europolu, lahko oškodovanec vloži pravno sredstvo samo pri pristojnem sodišču države članice, v kateri se je zgodil škodni dogodek.[269] Če je škoda nastala, ker Europol ni izpolnil svojih zakonskih obveznosti, ta državi članici plača odškodnino.

268 Sklep o Europolu, člen 34.

269 Prav tam, člen 52.

## Eurojust

Eurojust, ustanovljen leta 2002, je organ EU s sedežem v Haagu, ki spodbuja pravosodno sodelovanje pri preiskavah in pregonu hudih kaznivih dejanj, povezanih vsaj z dvema državama članicama.[270] 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, katerega status je urejen z nacionalno zakonodajo in ki ima potrebna pooblastila za izvajanje nalog, potrebnih za spodbujanje in izboljšanje 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.[271] 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 Konvencije Sveta Evrope št. 108 in njenih poznejših

270 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 2002, L 63; 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 2003, L 44; Svet Evropske unije (2009), Sklep Sveta 2009/426/PNZ z dne 16. decembra 2008 o krepitvi Eurojusta in o spremembi Sklepa 2002/187/PNZ o ustanovitvi Eurojusta za okrepitev boja proti težjim oblikam kriminala, UL 2009, L 138 (*sklepi o Eurojustu*).

271 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).

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.[272]

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 Eurojustovim odgovorom na zaprosilo za dostop do osebnih podatkov ali 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.

### 7.2.4. 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 je bilo na ravni EU vzpostavljenih več skupnih informacijskih sistemov, ki delujejo kot platforma za izmenjavo osebnih podatkov med pristojnimi nacionalnimi organi in organi EU za določene namene kazenskega pregona, vključno z zakonodajo o priseljevanju in carinsko zakonodajo. Nekateri od teh sistemov so se razvili iz večstranskih sporazumov, ki so bili pozneje dopolnjeni s pravnimi instrumenti in sistemi EU, kot je na primer schengenski informacijski sistem, vizumski informacijski sistem, Eurodac, Eurosur ali carinski informacijski sistem.

Evropska agencija za obsežne informacijske sisteme (eu-LISA)[273], ustanovljena leta 2012, je odgovorna za dolgoročno operativno upravljanje druge generacije schengenskega informacijskega sistema (SIS II), vizumskega informacijskega sistema (VIS) in sistema 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.

272 Poslovnik o obdelavi in varstvu osebnih podatkov v Eurojustu z dne 19. marca 2005, UL 2005, C 68/01, str. 1.

273 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 2011, L 286.

## Schengenski informacijski sistem

Leta 1985 je več držav članic nekdanjih Evropskih 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 na schengenskem območju.[274] 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.

Schengenski sistem je na podlagi pristopa novih držav k Schengenskemu sporazumu dokončno postal del pravnega okvira EU z Amsterdamsko pogodbo.[275] Ta sklep se je začel izvajati leta 1999. Najnovejša različica schengenskega informacijskega sistema, t. i. SIS II, je začela delovati 9. aprila 2013. Zdaj ga uporabljajo vse države članice EU ter Islandija, Lihtenštajn, Norveška in Švica.[276] 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 določenepodatke, ki jih države članice vnesejo o osebah in stvareh. Uporabljajo ga nacionalni organi za nadzor meja ter carinski, vizumski in pravosodni organi na celotnem schengenskem območju. Vsaka država članica upravlja nacionalno kopijo sistema C-SIS, znano kot nacionalni schengenski informacijski sistem (N-SIS), ki se nenehno posodablja, s tem pa se posodablja tudi sistem C-SIS. V sistemu N-SIS se opravijo poizvedbe in izda opozorilo, če:

- oseba nima pravice vstopiti na schengensko območje ali na njem prebivati;
- osebo ali stvar iščejo pravosodni organi ali organi pregona;
- je bila oseba prijavljena kot pogrešana ali

274 Sporazum med vladami držav Gospodarske unije Beneluksa, Zvezne republike Nemčije in Francoske republike o postopni odpravi kontrol na njihovih skupnih mejah, UL 2000, L 239.

275 Evropske skupnosti (1997), Amsterdamska pogodba, ki spreminja Pogodbo o Evropski uniji, pogodbi o ustanovitvi Evropskih skupnosti in nekaj z njima povezanih aktov, UL 1997, C 340.

276 Uredba (ES) št. 1987/2006 Evropskega parlamenta in Sveta z dne 20. decembra 2006 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema, UL 2006, L 381, (*SIS II*), 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 2007, L 205.

- je blago, na primer bankovci, avtomobili, kombiji, orožje ali osebni dokumenti, prijavljeno kot ukradena ali izgubljena lastnina.

Ob opozorilu je treba nadaljnje dejavnosti začeti prek nacionalnih schengenskih informacijskih sistemov.

Sistem SIS II ima nove funkcije, na primer možnost vnosa: biometričnih osebnih podatkov, kot so na primer prstni odtisi in fotografije, novih kategorij opozoril, kot so na primer ukradena plovila, zrakoplovi, zabojniki ali plačilna sredstva, izboljšanih opozoril o osebah in stvareh ter kopij evropskih nalogov za prijetje oseb, za katere se zahteva prijetje, predaja ali izročitev.

Sklep Sveta 2007/533/PNZ o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (Sklep Schengen II) vključuje Konvencijo št. 108: „Osebni podatki, obdelani v okviru uporabe tega sklepa, so zaščiteni v skladu s Konvencijo št. 108“.[277] Če nacionalni policijski organi osebne podatke uporabljajo na podlagi Sklepa Schengen II, je treba v nacionalno zakonodajo prenesti določbe Konvencije št. 108 in Priporočila o policijskih osebnih podatkih.

Pristojni nacionalni nadzorni organ v vsaki državi članici nadzoruje nacionalni sistem N-SIS. Natančneje, preveriti mora kakovost osebnih podatkov, ki jih država članica v sistem C-SIS vnaša prek sistema N-SIS. Nacionalni nadzorni organ mora zagotoviti, da se vsaj vsaka štiri leta izvede revizija postopkov obdelave osebnih podatkov v nacionalnem sistemu N-SIS. Nacionalni nadzorni organi in ENVP sodelujejo in zagotavljajo usklajen nadzor nad sistemom SIS, ENVP pa je odgovoren za nadzor nad C-SIS. Zaradi preglednosti se Evropskemu parlamentu, Svetu in agenciji eu-LISA vsaki dve leti pošlje skupno poročilo o dejavnostih.

Pravice posameznikov do dostopa v zvezi s sistemom SIS II se lahko uveljavljajo v vseh državah članicah, saj je vsak sistem N-SIS natančna kopija sistema C-SIS.

Primer: V zadevi *Dalea proti Franciji*[278] 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 vladnim svetom neuspešno zahte-

277 Svet Evropske unije (2007), Sklep Sveta 2007/533/PNZ z dne 12. junija 2007 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema, UL 2007, L 205, člen 57.

278 Sodba ESČP z dne 2. februarja 2010 v zadevi *Dalea proti Franciji (dec.)*, pritožba št. 964/07.

val 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, je bila zato razglašena za nedopustno.

## 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.[279] Sistem VIS državam schengenskega območja omogoča izmenjavo vizumskih podatkov prek sistema, ki konzulate 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 za izdajo vizumov za kratkoročno prebivanje zaradi obiska ali tranzita prek schengenskega območja. Sistem VIS mejnim organom omogoča, da na podlagi biometričnih osebnih podatkov preverijo, ali je oseba, ki predloži vizum, zakoniti imetnik dokumenta ali ne, in ugotovijo istovetnost oseb, ki nimajo dokumentov ali katerih dokumenti so ponarejeni.

V skladu z Uredbo (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*) se lahko v sistem VIS vnašajo samo osebni podatki o prosilcu, njegovi vizumi, fotografije, prstni odtisi, povezave do prejšnjih vlog in dosjeji oseb, ki ga spremljajo.[280] Dostop do sistema VIS za vnos, spremembo ali izbris podatkov je omejen izključno na vizumske organe držav članic, medtem ko je dostop za vpogled v podatke zagotovljen vizumskim organom in organom, pristojnim za preverjanje na zunanjih mejnih prehodih,

279 Svet Evropske unije (2004), Sklep Sveta z dne 8. junija 2004 o vzpostavitvi vizumskega informacijskega sistema (VIS), UL 2004, L 213; 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, UL 2008, L 218 (*Uredba VIS*); 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 2008, L 218.

280 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 2008, L 218.

kontrolo nad priseljevanjem in azil. Pod določenimi pogoji lahko nacionalni pristojni policijski organi in Europol zaprosijo za dostop do podatkov, vnesenih v sistem VIS, da bi lahko preprečevali, odkrivali in preiskovali teroristična in druga kazniva dejanja.[281]

## Eurodac

Ime Eurodac se nanaša na daktilograme ali prstne odtise. Gre za centraliziran sistem podatkov o prstnih odtisih državljanov tretjih držav, ki zaprosijo za azil v eni od držav članic EU.[282] Sistem je začel delovati leta 2003, pomagal pa naj bi pri določanju, katera država članica je odgovorna za obravnavanje prošnje za mednarodno zaščito na podlagi Uredbe Sveta (ES) št. 343/2003 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za azil, ki jo v eni od držav članic vloži državljan tretje države (*Uredba Dublin II*).[283] Osebni podatki v sistemu Eurodac se lahko uporabljajo le za lažje izvajanje Uredbe Dublin II; vsakršna druga uporaba je kazniva.

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 najmanj 14 let, ki ni državljan EU ali je brez državljanstva in zaprosi za azil na njihovem ozemlju oziroma je prijeta zaradi nezakonitega prečkanja njihove zunanje meje. Države članice lahko odvzamejo in posredujejo tudi prstne odtise oseb, ki niso državljani EU ali so brez državljanstva in v zvezi s katerimi se izkaže, da na ozemlju teh držav članic prebivajo brez dovoljenja.

Osebni podatki o prstnih odtisih se v podatkovni zbirki Eurodac shranjujejo samo v psevdonimizirani obliki. Ob ujemanju se psevdonim in ime prve države članice, ki je posredovala podatke o prstnih odtisih, razkrijeta drugi državi članici. Druga država

281 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 2008, L 218.

282 Uredba Sveta (ES) št. 2725/2000 z dne 11. decembra 2000 o vzpostavitvi sistema „Eurodac" za primerjavo prstnih odtisov zaradi učinkovite uporabe Dublinske konvencije, UL 2000, L 316; 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 2002, L 62 (*uredbe Eurodac*).

283 Uredba Sveta (ES) št. 343/2003 z dne 18. februarja 2003 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za azil, ki jo v eni od držav članic vloži državljan tretje države, UL 2003, L 50 (*Uredba Dublin II*).

članica se nato obrne na prvo državo članico, saj je v skladu z Uredbo Dublin II za obravnavanje prošnje za azil odgovorna prva država članica.

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 dve leti. 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.

Poleg vseh držav članic EU sistem Eurodac na podlagi mednarodnih sporazumov uporabljajo tudi Islandija, Norveška, Lihtenštajn in Švica.

## Eurosur

Evropski sistem varovanja meja (*Eurosur*)[284] je namenjen okrepitvi 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 skladnega upravljanja meja.[285] Njegovi splošni cilji so:

- zmanjšati število nezakonitih priseljencev, ki neopaženo vstopijo v EU;
- zmanjšati število smrtnih primerov med nezakonitimi priseljenci z rešitvijo večjega števila življenj na morju;
- povečati notranjo varnost EU kot celote s prizadevanji za preprečevanje čezmejnega kriminala.[286]

284 Uredba (EU) št. 1052/2013 Evropskega parlamenta in Sveta z dne 22. oktobra 2013 o vzpostavitvi Evropskega sistema varovanja meja (Eurosur), UL 2013, L 295.

285 Uredba (EU) št. 1168/2011 Evropskega parlamenta in Sveta z dne 25. oktobra 2011 o spremembah Uredbe Sveta (ES) št. 2007/2004 o ustanovitvi Evropske agencije za upravljanje in operativno sodelovanje na zunanjih mejah držav članic Evropske unije (*Uredba Frontex*), UL 2011, L 394.

286 Glej tudi Evropska komisija (2008), Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij z dne 13. februarja 2008 z naslovom Proučitev vzpostavitve evropskega sistema nadzorovanja meja (Eurosur), COM(2008) 68 final, Bruselj; Evropska komisija (2011), Ocena učinka, priložena k predlogu Uredbe Evropskega parlamenta in Sveta z dne 12. decembra 2011 o vzpostavitvi Evropskega sistema varovanja meja (Eurosur), delovni dokument, SEC(2011) 1536 final, Bruselj, str. 18.

Sistem je v vseh državah članicah z zunanjimi mejami začel delovati 2. decembra 2013, 1. decembra 2014 pa bo začel delovati še v vseh drugih. Ureditev se bo uporabljala za varovanje kopnega, morskih zunanjih meja in zračnih meja držav članic.

## Carinski informacijski sistem

Še en pomemben skupni informacijski sistem, vzpostavljen na ravni EU, je carinski informacijski sistem (CIS).[287] Med vzpostavitvijo 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.

Informacije, ki jih vsebuje sistem CIS, obsegajo osebne podatke glede proizvodov, prevoznih sredstev, podjetij, oseb ter zadržanega, zaseženega ali zarubljenega blaga in denarja. Te informacije se lahko uporabljajo le za opažanje, poročanje ali izvajanje posebnega nadzora ali za strateške ali operativne analize v zvezi z osebami, osumljenimi kršitev 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 št. 515/97 in Konvencije CIS[288] ter določbami Direktive o varstvu osebnih podatkov, Uredbe o varstvu osebnih podatkov v institucijah EU, Konvencije št. 108 in priporočila o policijskih osebnih podatkih. ENVP je odgovoren za nadzor nad skladnostjo CIS z Uredbo (ES) št. 45/2001 in sklicuje najmanj enkrat letno sestanek z vsemi nadzornimi nacionalnimi organi, pristojnimi za nadzor nad zadevami v zvezi s CIS.

287 Svet Evropske unije (1995), akt Sveta z dne 26. julija 1995 o sestavi Konvencije o uporabi informacijske tehnologije za carinske namene, UL 1995, C 316, spremenjen s Sklepom Sveta 2009/917/PNZ z dne 30. novembra 2009 o uporabi informacijske tehnologije za carinske namene (*Sklep CIS*), UL 2009, L 323, dopolnjena 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 s Komisijo zaradi zagotavljanja pravilnega izvajanja carinske in kmetijske zakonodaje.

288 Prav tam.

# 8

# Druga posebna evropska zakonodaja o varstvu osebnih podatkov

| EU | Obravnavane teme | Svet Evrope |
|---|---|---|
| Direktiva o varstvu osebnih podatkov<br>Direktiva o zasebnosti in elektronskih komunikacijah | **Elektronske komunikacije** | Konvencija št. 108<br>Priporočilo o telekomunikacijskih storitvah |
| Direktiva o varstvu osebnih podatkov, člen 8(2)(b) | **Odnosi med delodajalci in delojemalci** | Konvencija št. 108<br>Priporočilo o zaposlovanju |
| | | Sodba z dne 3. aprila 2007 v zadevi *Copland proti Združenemu kraljestvu*, pritožba št. 62617/00 |
| Direktiva o varstvu osebnih podatkov, člen 8(3) | **Zdravstveni podatki** | Konvencija št. 108<br>Priporočilo o zdravstvenih podatkih |
| | | Sodba z dne 25. februarja 1997 v zadevi *Z. proti Finski*, pritožba št. 22009/93 |
| Direktiva o kliničnih preskušanjih | **Klinična preskušanja** | |
| Direktiva o varstvu osebnih podatkov, člen 6(1)(b) in (e) ter člen 13(2) | **Statistika** | Konvencija št. 108<br>Priporočilo o statističnih podatkih |
| Uredba (ES) št. 223/2009 o evropski statistiki<br>Sodba Sodišča EU z dne 16. decembra 2008 v zadevi *Huber proti Bundesrepublik Deutschland*, C-524/06 | **Uradna statistika** | Konvencija št. 108<br>Priporočilo o statističnih podatkih |

| | | |
|---|---|---|
| Direktiva 2004/39/ES o trgih finančnih instrumentov<br>Uredba (EU) št. 648/2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov<br>Uredba (ES) št. 1060/2009 o bonitetnih agencijah<br>Direktiva 2007/64/EC o plačilnih storitvah na notranjem trgu | **Finančni podatki** | Konvencija št. 108<br>Priporočilo 90(19), ki se uporablja za plačila in druge s tem povezane transakcije<br>Sodba z dne 6. decembra 2012 v zadevi *Michaud proti Franciji*, pritožba št. 12323/11 |

V več primerih so bili na evropski ravni sprejeti posebni pravni instrumenti, s katerimi se splošna pravila iz Konvencije št. 108 ali Direktive o varstvu osebnih podatkov izvajajo podrobneje za posebne primere.

## 8.1. Elektronske komunikacije

### Ključne točke

- Posebna pravila o varstvu osebnih podatkov na področju telekomunikacij, s posebnim sklicevanjem na telefonske storitve, 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 samo na vsebino komunikacije, ampak tudi na podatke o prometu, na primer informacije o tem, kdo je komuniciral s kom, kdaj in kako dolgo, in podatke o lokaciji, 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, s posebnim sklicevanjem na telefonske storitve.[289] V skladu s

289 Svet Evrope, Odbor ministrov (1995), Priporočilo Rec(95)4 z dne 7. februarja 1995 državam članicam o varstvu osebnih podatkov na področju telekomunikacijskih storitev, zlasti telefonskih storitev.

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 prejemanje oglaševalskih sporočil. 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 je treba določiti z nacionalno zakonodajo.

Kar zadeva **pravni okvir EU**, je bila Direktiva o zasebnosti in elektronskih komunikacijah po prvem poskusu leta 1997 sprejeta leta 2002 in spremenjena leta 2009, da bi dopolnili in podrobneje opredelili določbe Direktive o varstvu osebnih podatkov za telekomunikacijski sektor.[290] 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;
- podatki, ki so potrebni za vzpostavitev in ohranjanje komunikacije, t. i. podatki o prometu, kot so informacije o partnerjih komunikacije ter njenem času in trajanju;
- med podatki o prometu so podatki, ki se posebej nanašajo na lokacijo komunikacijske naprave, t. i. lokacijski podatki; to so hkrati tudi podatki o lokaciji

290 Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, UL 2002, L 201, (*Direktiva o zasebnosti in elektronskih komunikacijah*), 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 2009, L 337.

*uporabnikov* komunikacijskih naprav in so zlasti pomembni v zvezi z uporabniki 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 v zvezi z lokacijo uporabnika na naslednji postaji podzemne železnice ali v lekarni ali v zvezi z vremensko napovedjo za to lokacijo.

Drug dostop do podatkov o komunikacijah v elektronskih omrežjih, na primer dostop za preiskovanje kaznivih dejanj, mora v skladu s členom 15 Direktive o zasebnosti in elektronskih komunikacijah izpolnjevati 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.

S spremembami iz leta 2009 je bilo v Direktivo o zasebnosti in elektronskih komunikacijah[291] 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 komunikacij;[292]

- nameščanje piškotkov, programske opreme, ki spremlja in beleži dejanja računalniškega uporabnika, ni več dovoljeno brez njegove privolitve. Z nacionalno

291 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 2009, L 337.

292 Glej spremenjeno direktivo, člen 13.

zakonodajo je treba podrobneje določiti, kako mora biti privolitev izražena in pridobljena, da se zagotovi zadostno varstvo.[293]

Če je kršitev varstva osebnih podatkov posledica 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 varstva osebnih podatkov.[294]

Ponudniki komunikacijskih storitev so morali na podlagi Direktive o hrambi podatkov[295], ki je bila razveljavljena 8. Aprila 2014, dati na voljo podatke o prometu zlasti za boj proti hudim oblikam kriminala, in sicer vsaj za šest- in največ štiriindvajsetmesečno obdobje, ne glede na to, ali ponudnik te podatke še potrebuje za obračunavanje ali tehnično zagotavljanje storitve ali ne.

Države članice EU določijo neodvisne javne organe, ki so odgovorni za nadzor in varnost hranjenih osebnih podatkov.

Hramba telekomunikacijskih podatkov jasno posega v pravico do varstva osebnih podatkov.[296] Ali je tako poseganje upravičeno ali ne, je bilo izpodbijano v več sodnih postopkih v državah članicah EU.[297]

Primer: V zadevi *Digital Rights Ireland in Seitlinger in drugi*[298] je SEU odločilo, da je Direktiva o hrambi podatkov neveljavna. Po odločitvi sodišča *"je direktiva v pomembnem nasprotju s temeljnimi pravicami v tej zadevi, njeno učinkovanje*

293 Glej prav tam, člen 5, glej tudi Mnenje 04/2012 delovne skupine iz člena 29 z dne 7. junija 2012 o piškotkih, ki so izvzeti iz zahteve po soglasju, WP 194, Bruselj.

294 Glej tudi Delovni dokument 01/2011 delovne skupine iz člena 29 z dne 5. aprila 2011 o sedanjem okviru EU za kršitve osebnih podatkov in priporočilih o prihodnjem razvoju politike, WP 184, Bruselj.

295 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 2006, L 105.

296 ENVP (2011), Mnenje z dne 31. maja 2011 o poročilu Komisije Svetu in Evropskemu parlamentu o oceni direktive o hrambi podatkov (Direktiva 2006/24/ES).

297 Nemčija, Zvezno ustavno sodišče (*Bundesverfassungsgericht*), št. 1 BvR 256/08, z dne 2. marca 2010; Romunija, Zvezno ustavno sodišče (*Curtea Constituțională a României*), št. 1258, z dne 8. oktobra 2009; Češka republika, Zvezno ustavno sodišče (*Ústavní soud České republiky*), št. 94/2011 Coll., z dne 22. marca 2011.

298 Sodba sodišča SEU, združeni zadevi C-293/12 in C-594/12, *Digital Rights Ireland in Seitlinger in drugi*, 8. april 2014, čl. 65.

*pa ni dovolj omejeno, da bi zagotavljalo najmanjšo še sprejemljivo mero posegov vanje.“*

Ključno vprašanje v okviru elektronskih komunikacij je vmešavanje javnih organov. Sredstva nadzora ali prestrezanja komunikacij, kot so na primer prisluškovalne naprave, so dovoljena samo, če je to določeno z zakonom in če se v demokratični družbi šteje za nujen ukrep zaradi: zaščite državne varnosti, javne varnosti, denarnih interesov države ali zatiranja kaznivih dejanj oziroma zaščite posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih.

Primer: V zadevi *Malone proti Združenemu kraljestvu*[299] je bil pritožnik obdolžen več kaznivih dejanj v zvezi z nepoštenim ravnanjem z ukradenim blagom. Med sojenjem se je izkazalo, da je bil na podlagi naloga, ki ga je izdal minister za notranje zadeve, prestrežen telefonski pogovor pritožnika. Čeprav je bil način prestrezanja pritožnikove komunikacije zakonit v smislu nacionalne zakonodaje, je ESČP ugotovilo, da ni pravnih predpisov v zvezi z obsegom in načinom izvajanja diskrecijske pravice, ki jo imajo javni organi na tem področju, zato prestrezanje, ki je izhajalo iz obstoja spornega ravnanja, ni bilo „v skladu z zakonom“. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

## 8.2. Osebni podatki o zaposlitvi

### Ključne točke

- Posebna pravila za varstvo osebnih podatkov pri odnosih med delodajalci in delojemalci vsebuje priporočilo Sveta Evrope o osebnih podatkih o zaposlitvi.
- V Direktivi o varstvu osebnih podatkov 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 vprašljiva glede na ekonomsko neravnovesje med delodajalcem in delojemalcem. Okoliščine privolitve je treba presojati previdno.

V EU ni posebnega pravnega okvira, s katerim bi bila urejena obdelava podatkov v okviru zaposlitve. V Direktivi o varstvu osebnih podatkov so odnosi med delodajalci in delojemalci izrecno navedeni samo v členu 8(2), ki se nanaša na obdelavo

299 Sodba ESČP z dne 2. avgusta 1984 v zadevi *Malone proti Združenemu kraljestvu*, pritožba št. 8691/79.

občutljivih osebnih podatkov. Kar zadeva Svet Evrope, je bilo leta 1989 izdano priporočilo o osebnih podatkih o zaposlitvi, ki se trenutno posodablja.[300]

Pregled najpogostejših težav v zvezi z varstvom osebnih podatkov zlasti v okviru zaposlovanja vsebuje delovni dokument delovne skupine iz člena 29.[301] Delovna skupina je analizirala pomen privolitve kot pravne podlage za obdelavo osebnih podatkov o zaposlitvi.[302] 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 se zahteva privolitev.

Pogosta težava v zvezi z varstvom osebnih podatkov v današnjem značilnem delovnem okolju je zakonitost spremljanja elektronskih komunikacij zaposlenega na delovnem mestu. 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. Pri tem je zlasti pomembna naslednja sodba ESČP:

Primer: V zadevi *Copland proti Združenemu kraljestvu*[303] 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 ugotovilo, 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 pritožničini zadevi ni bilo predpisano, v kakšnih okoliščinah lahko delodajalci nadzorujejo uporabo telefona, elektronske pošte in interneta svojih

300 Svet Evrope, Odbor ministrov (1989), Priporočilo Rec(89)2 z dne 18. januarja 1989 državam članicam o varstvu osebnih podatkov, ki se uporabljajo za poslovne namene. Glej poleg tega tudi posvetovalni odbor iz Konvencije št. 108, študija priporočila št. R(89)2 o varstvu osebnih podatkov, ki se uporabljajo za poslovne namene, in predložitev predlogov za revizijo zgoraj navedenega priporočila z dne 9. septembra 2011.

301 Mnenje 8/2001 delovne skupine iz člena 29 z dne 13. septembra 2001 o obdelavi osebnih podatkov v okviru zaposlovanja, WP 48, Bruselj.

302 Delovni dokument delovne skupine iz člena 29 z dne 25. novembra 2005 o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995, WP 114, Bruselj.

303 Sodba ESČP z dne 3. aprila 2007 v zadevi *Copland proti Združenemu kraljestvu*, pritožba št. 62617/00.

zaposlenih. Tako vmešavanje zato ni bilo v skladu z zakonom. Sodišče je ugotovilo, da je bil kršen člen 8 EKČP.

V skladu s priporočilom Sveta Evrope o osebnih podatkih o zaposlitvi je 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 možnosti.

V priporočilu so tudi posebej navedene subjektivne informacije v zvezi z uspešnostjo ali možnostmi 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 zakonodaje o varstvu osebnih podatkov v odnosu med delodajalcem in zaposlenim je vloga predstavnikov zaposlenih. Ti lahko osebne podatke o zaposlenih prejmejo samo, če je to nujno za zastopanje njihovih interesov.

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 jih lahko zdravstveno pregledajo samo, če je to nujno za: ugotovitev njihove primernosti za zaposlitev, izpolnitev zahtev preventivne medicine ali odobritev socialnih prejemkov. Zdravstveni osebni podatki se lahko pridobijo samo 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 shranjenih osebnih podatkov, subjektih, ki se jim podatki redno pošiljajo, ter namenu in pravni podlagi za tako pošiljanje. Delodajalci morajo zaposlene tudi predhodno obvestiti o uvedbi ali prilagoditvi avtomatiziranih sistemov za obdelavo osebnih podatkov zaposlenih oziroma za spremljanje gibanja ali produktivnosti zaposlenih.

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 ugovora. 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 nacionalno zakonodajo določeni ustrezni postopki za ugovarjanje taki zavrnitvi.

## 8.3. Zdravstveni osebni podatki

### Ključne točke

- Zdravstveni podatki so občutljivi osebnih podatki, zato zanje velja posebno varstvo.

Osebni podatki o zdravstvenem stanju posameznika, na katerega se nanašajo, se štejejo za občutljive na podlagi člena 8(1) Direktive o varstvu podatkov in člena 6 Konvencije št. 108. Za zdravstvene osebne podatke zato velja strožja ureditev obdelave osebnih podatkov kot za neobčutljive osebne podatke.

Primer: V zadevi *Z. proti Finski*[304] je pritožničin nekdanji mož, ki je bil okužen z virusom HIV, storil več kaznivih dejanj zoper spolno nedotakljivost. Pozneje je bil obsojen umora, 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. Sodišče je zato ugotovilo, da bi odobritev vpogleda v identiteto in zdravstveno stanje pritožnice, kot je opisano v sodbi pritožbenega sodišča, po zgolj desetih letih po izdaji sodbe pomenila kršitev člena 8 EKČP.

Člen 8(3) Direktive o varstvu osebnih podatkov dovoljuje obdelavo zdravstvenih osebnih podatkov, kadar se podatki obdelujejo za potrebe preventivne medicine,

304 Sodba ESČP z dne 25. februarja 1997 v zadevi *Z. proti Finski*, pritožba št. 22009/93, točki 94 in 112; glej tudi sodbe ESČP z dne 27. avgusta 1997 v zadevi *M. S. proti Švedski*, pritožba št. 20837/92; z dne 10. oktobra 2006 v zadevi *L. L. proti Franciji*, pritožba št. 7508/02; z dne 17. julija 2008 v zadevi *I. proti Finski*, pritožba št. 20511/03; z dne 28. aprila 2009 v zadevi *K. H. in drugi proti Slovaški*, pritožba št. 32881/04, in z dne 2. junija 2009 v zadevi *Szuluk proti Združenemu kraljestvu*, pritožba št. 36936/05.

zdravstvene diagnoze, za zagotovitev oskrbe ali zdravljenja ali vodenje zdravstvenih služb. Vendar je obdelava dovoljena samo, če podatke obdeluje zdravstveni delavec na podlagi dolžnosti poklicne molčečnosti ali druga oseba, ki je prav tako zavezana enaki dolžnosti.[305]

V Priporočilu Sveta Evrope o zdravstvenih podatkih iz leta 1997 so načela iz Konvencije št. 108 pri obdelavi osebnih podatkov na zdravstvenem področju podrobneje upoštevana.[306] Predlagana pravila so v skladu s pravili iz Direktive o varstvu osebnih podatkov glede zakonitih namenov obdelave zdravstvenih osebnih podatkov, nujne dolžnosti poklicne molčečnosti oseb, ki uporabljajo zdravstvene osebne podatke, ter pravice 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".[307]

Priporočilo o zdravstvenih podatkih vsebuje tudi posebne določbe o zdravstvenih podatkih nerojenih otrok in oseb, ki niso sposobne odločati o sebi, ter obdelavi genetskih 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 anomizirani podatki ne zadostujejo.

Psevdonimizacija je lahko ustrezen način za izpolnitev znanstvenih zahtev in hkrati zaščito interesov zadevnih bolnikov. Pojem psevdonimizacije v okviru varstva osebnih podatkov je podrobneje pojasnjen v razdelku 2.1.3.

Na nacionalni in evropski ravni poteka poglobljena razprava o pobudah za shranjevanje podatkov o zdravljenju bolnika v elektronski zdravstveni kartoteki.[308] Posebnost vsedržavnih sistemov elektronskih zdravstvenih kartotek je, da so na voljo v tujini: ta tema je v EU zlasti zanimiva v okviru čezmejnega zdravstvenega varstva.[309]

305 Glej tudi sodbo ESČP z dne 25. novembra 2008 v zadevi *Biriuk proti Litvi*, pritožba št. 23373/03.

306 Svet Evrope, Odbor ministrov (1997), Priporočilo Rec(97)5 državam članicam o varstvu zdravstvenih podatkov z dne 13. februarja 1997.

307 Sodba ESČP z dne 6. junija 2013 v zadevi *Avilkina in drugi proti Rusiji*, pritožba št. 1585/09, točka 53 (še v teku).

308 Delovni dokument delovne skupine iz člena 29 z dne 15. februarja 2007 o obdelavi osebnih podatkov v zvezi z zdravjem v elektronskih zdravstvenih kartonih (EZK), WP 131, Bruselj.

309 Direktiva 2011/24/EU Evropskega parlamenta in Sveta z dne 9. marca 2011 o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu, UL 2011, L 88.

Še eno področje, o katerem se razpravlja v zvezi z novimi določbami, je klinično preskušanje, tj. preskušanje novih zdravil na bolnikih v dokumentiranem raziskovalnem okolju; tudi ta tema je precej povezana z varstvom osebnih podatkov. Klinično preskušanje zdravil za ljudi je urejeno z Direktivo 2001/20/ES Evropskega parlamenta in Sveta z dne 4. aprila 2001 o približevanju zakonov in drugih predpisov držav članic v zvezi z izvajanjem dobre klinične prakse pri kliničnem preskušanju zdravil za ljudi (*Direktiva o kliničnem preskušanju*).[310] Evropska komisija je decembra 2012 predlagala uredbo, ki naj bi nadomestila Direktivo o kliničnem preskušanju ter s katero naj bi postopki preskušanja postali enotnejši in učinkovitejši.[311]

Na ravni EU poteka še veliko drugih zakonodajnih in ostalih pobud v zvezi z osebnimi podatki v zdravstvu.[312]

## 8.4. Obdelava osebnih podatkov za statistične namene

### Ključne točke

- Osebni podatki, zbrani za statistične 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 namene, če so z nacionalno zakonodajo predpisani ustrezni zaščitni ukrepi, ki jih izvajajo uporabniki. Zato je treba pred pošiljanjem tretjim osebam predvideti zlasti anonimizacijo in psevdonimizacijo.

V Direktivi o varstvu osebnih podatkov je obdelava osebnih podatkov za statistične namene navedena v okviru možnih izjem od načel varstva osebnih podatkov. V členu 6(1)(b) navedene direktive se je mogoče načelu omejitve namena odreči zaradi nadaljnje uporabe za statistične namene, čeprav morajo biti z nacionalno

310 Direktiva 2001/20/ES Evropskega parlamenta in Sveta z dne 4. aprila 2001 o približevanju zakonov in drugih predpisov držav članic v zvezi z izvajanjem dobre klinične prakse pri kliničnem preskušanju zdravil za ljudi, UL 2001, L 121.

311 Evropska komisija (2012), predlog Uredbe Evropskega parlamenta in Sveta z dne 17. julija 2012 o kliničnih preskušanjih zdravil za uporabo v humani medicini in razveljavitvi Direktive 2001/20/ES, COM(2012) 369 final, Bruselj.

312 ENVP (2013), mnenje evropskega nadzornika za varstvo osebnih podatkov z dne 27. marca 2013 o sporočilu Komisije o „Akcijskem načrtu za e-zdravje za obdobje 2012–2020 – Inovativno zdravstveno varstvo za 21. stoletje", Bruselj.

zakonodajo določeni tudi vsi nujni zaščitni ukrepi. Člen 13(2) navedene direktive dovoljuje, da se pravice do dostopa omejijo z nacionalno zakonodajo, če se osebni podatki obdelujejo izključno za statistične namene; tudi v tem primeru morajo biti z nacionalno zakonodajo uvedeni zaščitni ukrepi. Direktiva o varstvu osebnih podatkov v zvezi s tem določa posebno zahtevo, da se noben podatek, pridobljen ali ustvarjen s statističnimi raziskavami, ne sme uporabiti za konkretne odločitve o posameznikih, na katere se nanašajo osebni podatki.

Čeprav lahko upravljavec osebne podatke, ki jih je zakonito zbral za kateri koli namen, znova uporabi za lastne statistične namene (t. i. sekundarna statistika), bi jih bilo treba pred pošiljanjem tretji osebi, ki bi jih prav tako uporabila za statistične namene, anonimizirati ali psevdonimizirati, glede na kontekst, razen če posameznik, na katerega se nanašajo osebni podatki, v to privoli ali če je to izrecno določeno z nacionalno zakonodajo. To izhaja iz zahteve po ustreznih zaščitnih ukrepih na podlagi člena 6(1)(b) Direktive o varstvu osebnih podatkov.

Najpomembnejši primeri uporabe osebnih podatkov za statistične namene so uradne statistike, ki jih nacionalni statistični uradi in statistični urad EU izvajajo na podlagi nacionalnih zakonov in zakonov EU o uradni statistiki. Državljani in podjetja morajo v skladu s temi zakoni podatke običajno razkriti statističnim organom. Uradnike, zaposlene v statističnih uradih, zavezujejo posebne dolžnosti poklicne molčečnosti, ki se skrbno upoštevajo, saj so bistvenega pomena za visoko raven zaupanja državljanov, ki je nujna, če naj bi se osebni podatki posredovali statističnim organom.

Uredba (ES) št. 223/2009 o evropski statistiki (*Uredba o evropski statistiki*) vsebuje bistvena pravila za varstvo osebnih podatkov v uradni statistiki, zato je lahko pomembna tudi za določbe o uradni statistiki na nacionalni ravni.[313] V uredbi se zagovarja načelo, da je za postopke uradne statistike potrebna dovolj natančna pravna podlaga.[314]

313 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 2009, L 87.

314 To načelo naj bi bilo nadalje opredeljeno v kodeksu ravnanja Eurostata, ki bo v skladu s členom 11 Uredbe o evropski statistiki zagotovila etične smernice o vodenju uradnih statistik, vključno s premišljeno uporabo osebnih podatkov, ki je na voljo na: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

Primer: Sodišče EU je v zadevi *Huber proti Bundesrepublik Deutschland*[315] ugotovilo, da zbiranje in shranjevanje osebnih podatkov, ki ju organ izvaja za statistične namene, sama po sebi nista zadosten razlog za zakonitost obdelave. Zakon, ki določa obdelavo osebnih podatkov, mora izpolnjevati tudi zahtevo po nujnosti obdelave, ki v danem primeru ni bila izpolnjena.

V okviru Sveta Evrope je bilo leta 1997 izdano Priporočilo o statističnih podatkih, ki zajema izvajanje statistike v javnem in zasebnem sektorju.[316] S tem priporočilom so bila uvedena načela, ki sovpadajo z glavnimi pravili iz Direktive o varstvu osebnih podatkov, opisanimi zgoraj. Podrobnejša pravila so navedena v zvezi z naslednjimi vprašanji.

Medtem ko se osebni podatki, ki jih je upravljavec zbral za statistične namene, ne smejo uporabiti za noben drug namen, se osebni podatki, ki so bili zbrani za nestatistične namene, dajo na voljo za nadaljnjo statistično uporabo. Na podlagi Priporočila o statističnih podatkih je dovoljeno celo 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, je treba predpostavljati, da morajo biti z nacionalno zakonodajo uvedeni ustrezni zaščitni ukrepi, da se zmanjšajo tveganja zlorabe osebnih podatkov, na primer obveznost, da se osebni podatki pred pošiljanjem anonimizirajo ali psevdonimizirajo.

Za osebe, ki se poklicno ukvarjajo s statističnimi raziskavami, bi morale na podlagi nacionalne zakonodaje veljati posebne dolžnosti poklicne molčečnosti – kot je značilno za uradno statistiko. Enako bi moralo veljati za anketarje, če zbirajo osebne podatke od posameznikov, na katere se nanašajo osebni podatki, ali drugih oseb.

Da bi bila statistična raziskava, pri kateri se uporabijo osebni podatki in ki ni določena z zakonom, zakonita, bi morali posamezniki, na katere se nanašajo osebni podatki, privoliti v uporabo svojih podatkov ali imeti vsaj možnost, da ji ugovarjajo. Če se osebni podatki za statistične namene zbirajo na podlagi razgovorov z osebami, je treba tem osebam jasno sporočiti, ali je razkritje osebnih podatkov na podlagi nacionalnega zakona obvezno ali ne. Občutljivi osebni podatki se nikoli ne bi smeli zbirati

315 Sodba Sodišča EU z dne 16. decembra 2008 v zadevi *Huber proti Bundesrepublik Deutschland*, C-524/06, glej zlasti točko 68.

316 Svet Evrope, Odbor ministrov (1997), Priporočilo Rec(97)18 z dne 30. septembra 1997 državam članicam o varstvu osebnih podatkov, zbranih in obdelanih v statistične namene.

tako, da je mogoče ugotoviti istovetnost posameznika, razen če je to izrecno dovoljeno z nacionalnim zakonom.

Če statistične raziskave ni mogoče izvesti brez anonimnih podatkov in so dejansko potrebni osebni podatki, je treba osebne podatke, zbrane za ta namen, čim prej anonimizirati. Iz rezultatov statistične raziskave bi morala biti izvzeta vsaj istovetnost vseh posameznikov, na katere se nanašajo osebni podatki, razen če to očitno ne bi povzročilo nikakršnega tveganja.

Uporabljene osebne podatke je treba po koncu statistične analize izbrisati ali jih anonimizirati. V takem primeru se v Priporočilu o statističnih podatkih predlaga, naj se identifikacijski podatki hranijo ločeno od drugih osebnih podatkov. To pomeni, da je treba na primer podatke psevdonimizirati, šifrirni ključ ali seznam identifikacijskih sinonimov pa hraniti ločeno od psevdonimiziranih podatkov.

## 8.5. Finančni osebni podatki

### Ključne točke

- Čeprav finančni osebni podatki niso občutljivi osebni podatki v smislu Konvencije št. 108 ali Direktive o varstvu osebnih podatkov, pa so za njihovo obdelavo nujni posebni zaščitni ukrepi za zagotovitev točnosti in varnosti osebnih podatkov.
- Elektronski plačilni sistemi morajo imeti vgrajeno varstvo osebnih podatkov, t. i. vgrajeno zasebnost.
- Posebne težave v zvezi z varstvom osebnih podatkov na tem področju izhajajo iz potrebe po uvedbi ustreznih mehanizmov za avtentikacijo.

Primer: V zadevi *Michaud proti Franciji*[317] je pritožnik, francoski odvetnik, izpodbijal obveznost, ki jo je imel po francoskem pravu, da prijavi sum pranja denarja svojih strank. ESČP je opozorilo, da zahteva, da morajo odvetniki upravnim organom sporočiti informacije o drugi osebi, ki so jih dobili na podlagi izmenjav s to osebo, pomeni poseganje v pravico odvetnikov do spoštovanja njihovega dopisovanja in zasebnega življenja na podlagi člena 8 EKČP, saj so s tem poj-

317 Sodba ESČP z dne 6. decembra 2012 v zadevi *Michaud proti Franciji*, pritožba št. 12323/11; glej tudi sodbi ESČP z dne 16. decembra 1992 v zadevi *Niemietz proti Nemčiji*, pritožba št. 13710/88, točka 29, in z dne 25. junija 1997 v zadevi *Halford proti Združenemu kraljestvu*, pritožba št. 20605/92, točka 42.

mom zajete poklicne ali poslovne dejavnosti. Vendar je bilo poseganje v skladu z zakonom in je imelo zakonit cilj, tj. preprečevanje nereda in kriminala. Ker je obveznost prijave suma za odvetnike veljala samo v zelo omejenih okoliščinah, je ESČP razsodilo, da je ta obveznost sorazmerna, in ugotovilo, da člen 8 EKČP ni bil kršen.

Uporaba splošnega pravnega okvira za varstvo osebnih podatkov, ki ga vsebuje Konvencija št. 108, je bila v okviru plačil izoblikovana v Priporočilu Sveta Evrope Rec(90)19 iz leta 1990.[318] V tem Priporočilu je pojasnjen obseg zakonitega zbiranja in uporabe osebnih podatkov v okviru plačil, zlasti s plačilnimi karticami. Poleg tega Priporočilo nacionalnim zakonodajalcem predlaga podrobno ureditev glede omejitve pošiljanja podatkov o plačilih tretjim osebam, časovnih rokov hrambe osebnih podatkov, preglednosti, varnosti osebnih podatkov in čezmejnega prenosa podatkov ter, nazadnje, glede nadzora in pravnih sredstev. Predlagane rešitve ustrezajo temu, kar je bilo pozneje kot splošni okvir za varstvo osebnih podatkov v EU določeno v Direktivi o varstvu osebnih podatkov.

Pripravlja se veliko pravnih instrumentov za ureditev trgov finančnih instrumentov ter dejavnosti kreditnih institucij in investicijskih podjetij.[319] Drugi pravni instrumenti pomagajo v boju proti trgovanju z notranjimi informacijami in tržni manipulaciji.[320] Najbolj kritična vprašanja na teh področjih, ki vplivajo na varstvo osebnih podatkov, so:

- hramba evidenc o finančnih transakcijah;

318 Svet Evrope, Odbor ministrov (1990), Priporočilo št. R(90)19 z dne 13. septembra 1990 o varstvu osebnih podatkov, ki se uporabljajo za plačila in druge povezane finančne transakcije.

319 Evropska komisija (2011), predlog Direktive Evropskega parlamenta in Sveta z dne 20. oktobra 2011 o trgih finančnih instrumentov in razveljavitvi Direktive 2004/39/ES Evropskega parlamenta in Sveta, COM(2011) 656 final, Bruselj; Evropska komisija (2011), predlog Uredbe Evropskega parlamenta in Sveta z dne 20. oktobra 2011 o trgih finančnih instrumentov in spremembi uredbe o infrastrukturi evropskega trga o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov, COM(2011) 652 final, Bruselj; Evropska komisija (2011), predlog Direktive Evropskega parlamenta in Sveta z dne 20. julija 2011 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij in spremembi Direktive 2002/87/ES Evropskega parlamenta in Sveta o dopolnilnem nadzoru kreditnih institucij, zavarovalnic in investicijskih družb v finančnem konglomeratu, COM(2011) 453 final, Bruselj.

320 Evropska komisija (2011), predlog Uredbe Evropskega parlamenta in Sveta z dne 20. oktobra 2011 o trgovanju z notranjimi informacijami in tržni manipulaciji (zloraba trga), COM(2011) 651 final, Bruselj; Evropska komisija (2011), predlog Direktive Evropskega parlamenta in Sveta z dne 20. oktobra 2011 o kazenskih sankcijah za trgovanje z notranjimi informacijami in tržni manipulaciji, COM(2011) 654 final, Bruselj.

- 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, npr. sistemi za razkrivanje 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,[321] ali čezmejnimi plačili z bančnimi nakazili, ki nujno vključujejo prenos osebnih podatkov.[322]

321 Uredba (ES) št. 1060/2009 Evropskega parlamenta in Sveta z dne 16. septembra 2009 o bonitetnih agencijah, UL 2009, L 302; Evropska komisija, predlog Uredbe Evropskega parlamenta in Sveta z dne 2. junija 2010 o spremembi Uredbe (ES) št. 1060/2009 o bonitetnih agencijah, COM(2010) 289 final, Bruselj.

322 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 2007, L 319.

# 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.

EDRi, *An introduction to data protection*, Bruselj, na voljo na: www.edri.org/files/paper06_datap.pdf.

Frowein, J., in Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C., in Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C., in Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

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*, št. 5, str. 281–288.

Warren, S., in Brandeis, L. (1890), „The right to privacy", *Harvard Law Review,* zv. 4, št. 5, str. 193–220, na voljo na: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R., in Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

## Poglavje 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

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.

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.

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*, na voljo na: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

## Poglavja od 3 do 5

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.

Dammann, U., in Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Agencija Evropske unije za temeljne pravice) (2010), *Data Protection in the European Union: the role of National Data Protection 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.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, na voljo na: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

## Poglavje 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C., in Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

## Poglavje 7

Europol (2012), *Data Protection at Europol*, Luxembourg, Urad za publikacije, na voljo na: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

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.

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, na voljo na: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

# Poglavje 8

Büllesbach, A., Gijrath, S., Poullet, Y., in Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P., in Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, 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.

Rosemary, J., in Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

# Sodna praksa

## Izbrana sodna praksa Evropskega sodišča za človekove pravice

**Dostop do osebnih podatkov**

Sodba z dne 7. julija 1989 v zadevi *Gaskin proti Združenemu kraljestvu*, pritožba št. 10454/83
Sodba z dne 25. septembra 2012 v zadevi *Godelli proti Italiji*, pritožba št. 33783/09
Sodba z dne 28. aprila 2009 v zadevi *K. H. in drugi proti Slovaški*, pritožba št. 32881/04
Sodba z dne 26. marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81
Sodba z dne 13. februarja 2003 v zadevi *Odièvre proti Franciji* [veliki senat], pritožba št. 42326/98

**Uravnoteženje varstva osebnih podatkov s svobodo izražanja**

Sodba z dne 7. februarja 2012 v zadevi *Axel Springer AG proti Nemčiji* [veliki senat], pritožba št. 39954/08
Sodba z dne 24. junija 2004 v zadevi *Von Hannover proti Nemčiji*, pritožba št. 59320/00
Sodba z dne 7. februarja 2012 v združenih zadevah *Von Hannover proti Nemčiji (št. 2)* [veliki senat], pritožbi št. 40660/08 in 60641/08

**Izzivi varstva osebnih podatkov na spletu**

Sodba z dne 2. decembra 2008 v zadevi *K. U. proti Finski,* pritožba št. 2872/02

**Dopisovanje**

Sodba z dne 16. februarja 2000 v zadevi *Amann proti Švici* [veliki senat], pritožba št. 27798/95
Sodba z dne 14. marca 2013 v zadevi *Bernh Larsen Holding AS in drugi proti Norveški*, pritožba št. 24117/08
Sodba z dne 18. novembra 2008 v zadevi *Cemalettin Canli proti Turčiji*, pritožba št. 22427/04
Sodba z dne 2. februarja 2010 v zadevi *Dalea proti Franciji,* pritožba št. 964/07
Sodba z dne 7. julija 1989 v zadevi *Gaskin proti Združenemu kraljestvu*, pritožba št. 10454/83
Sodba z dne 27. oktobra 2009 v zadevi *Haralambie proti Romuniji*, pritožba št. 21737/03
Sodba z dne 18. oktobra 2011 v zadevi *Khelili proti Švici*, pritožba št. 16188/07
Sodba z dne 26. marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81
Sodba z dne 2. avgusta 1984 v zadevi *Malone proti Združenemu kraljestvu*, pritožba št. 8691/79
Sodba z dne 24. februarja 1995 v zadevi *McMichael proti Združenemu kraljestvu*, pritožba št. 16424/90
Sodba z dne 24. septembra 2002 v zadevi *M. G. proti Združenemu kraljestvu*, pritožba št. 39393/98
Sodba z dne 4. maja 2000 v zadevi *Rotaru proti Romuniji* [veliki senat], pritožba št. 28341/95
Sodba z dne 4. decembra 2008 v združenih zadevah *S. in Marper proti Združenemu kraljestvu*, pritožbi št. 30562/04 in 30566/04
Sodba z dne 21. junija 2011 v zadevi *Shimovolos proti Rusiji*, pritožba št. 30194/09
Sodba z dne 14. februarja 2006 v zadevi *Turek proti Slovaški*, pritožba št. 57986/00

**Podatkovne zbirke kazenskih evidenc**

Sodba z dne 17. decembra 2009 v zadevi *B. B. proti Franciji*, pritožba št. 5335/06
Sodba z dne 13. novembra 2012 v zadevi *M. M. proti Združenemu kraljestvu*, pritožba št. 24029/07

**Podatkovne zbirke DNK**

Sodba z dne 4. decembra 2008 v združenih zadevah *S. in Marper proti Združenemu kraljestvu*, pritožbi št. 30562/04 in 30566/04

**Podatki GPS**

Sodba z dne 2. septembra 2010 v zadevi *Uzun proti Nemčiji*, pritožba št. 35623/05

**Zdravstveni podatki**

Sodba z dne 25. novembra 2008 v zadevi *Biriuk proti Litvi*, pritožba št. 23373/03
Sodba z dne 17. julija 2008 v zadevi *I. proti Finski*, pritožba št. 20511/03
Sodba z dne 10. oktobra 2006 v zadevi *L. L. proti Franciji*, pritožba št. 7508/02
Sodba z dne 2. julija 2002 v zadevi *M. S. proti Švedski*, pritožba št. 34209/96
Sodba z dne 2. junija 2009 v zadevi *Szuluk proti Združenemu kraljestvu*, pritožba št. 36936/05
Sodba z dne 25. februarja 1997 v zadevi *Z. proti Finski*, pritožba št. 22009/93

**Identiteta**

Sodba z dne 27. aprila 2010 v zadevi *Ciubotaru proti Moldaviji*, pritožba št. 27138/04
Sodba z dne 25. septembra 2012 v zadevi *Godelli proti Italiji*, pritožba št. 33783/09
Sodba z dne 13. februarja 2003 v zadevi *Odièvre proti Franciji* [veliki senat], pritožba št. 42326/98

**Informacije o poklicnih dejavnostih**

Sodba z dne 6. decembra 2012 v zadevi *Michaud proti Franciji*, pritožba št. 12323/11
Sodba z dne 16. decembra 1992 v zadevi *Niemietz proti Nemčiji*, pritožba št. 13710/88

**Prestrezanje informacij**

Sodba z dne 16. februarja 2000 v zadevi *Amann proti Švici* [veliki senat], pritožba št. 27798/95
Sodba z dne 3. aprila 2007 v zadevi *Copland proti Združenemu kraljestvu*, pritožba št. 62617/00
Sodba z dne 3. junija 2003 v zadevi *Cotlet proti Romuniji*, pritožba št. 38565/97
Sodba z dne 24. aprila 1990 v zadevi *Kruslin proti Franciji*, pritožba št. 11801/85
Sodba z dne 24. avgusta 1998 v zadevi *Lambert proti Franciji*, pritožba št. 23618/94
Sodba z dne 1. julija 2008 v zadevi *Liberty in drugi proti Združenemu kraljestvu*, pritožba št. 58243/00
Sodba z dne 2. avgusta 1984 v zadevi *Malone proti Združenemu kraljestvu*, pritožba št. 8691/79

Sodba z dne 25. junija 1997 v zadevi *Halford proti Združenemu kraljestvu*, pritožba št. 20605/92
Sodba z dne 2. junija 2009 v zadevi *Szuluk proti Združenemu kraljestvu*, pritožba št. 36936/05

**Obveznosti nosilcev dolžnosti**

Sodba z dne 17. decembra 2009 v zadevi *B. B. proti Franciji*, pritožba št. 5335/06
Sodba z dne 17. julija 2008 v zadevi *I. proti Finski*, pritožba št. 20511/03
Sodba z dne 10. maja 2011 v zadevi *Mosley proti Združenemu kraljestvu*, pritožba št. 48009/08

**Fotografije**

Sodba z dne 11. januarja 2005 v zadevi *Sciacca proti Italiji*, pritožba št. 50774/99
Sodba z dne 24. junija 2004 v zadevi *Von Hannover proti Nemčiji*, pritožba št. 59320/00

**Pravica biti pozabljen**

Sodba z dne 6. junija 2006 v zadevi *Segerstedt-Wiberg in drugi proti Švedski*, pritožba št. 62332/00

**Pravica do ugovora**

Sodba z dne 26. marca 1987 v zadevi *Leander proti Švedski*, pritožba št. 9248/81
Sodba z dne 10. maja 2011 v zadevi *Mosley proti Združenemu kraljestvu*, pritožba št. 48009/08
Sodba z dne 2. julija 2002 v zadevi *M. S. proti Švedski*, pritožba št. 34209/96
Sodba z dne 4. maja 2000 v zadevi *Rotaru proti Romuniji* [veliki senat], pritožba št. 28341/95

**Občutljivi osebni podatki**

Sodba z dne 17. julija 2008 v zadevi *I. proti Finski*, pritožba št. 20511/03
Sodba z dne 6. decembra 2012 v zadevi *Michaud proti Franciji*, pritožba št. 12323/11
Sodba z dne 4. decembra 2008 v združenih zadevah *S. in Marper proti Združenemu kraljestvu*, pritožbi št. 30562/04 in 30566/04

**Nadzor in pregon (vloga različnih akterjev, vključno z organi za varstvo podatkov)**

Sodba z dne 17. julija 2008 v zadevi *I. proti Finski*, pritožba št. 20511/03

Sodba z dne 2. decembra 2008 v zadevi *K. U. proti Finski*, pritožba št. 2872/02
Sodba z dne 24. junija 2004 v zadevi *Von Hannover proti Nemčiji*, pritožba št. 59320/00
Sodba z dne 7. februarja 2012 v združenih zadevah *Von Hannover proti Nemčiji (št. 2)* [veliki senat], pritožbi št. 40660/08 in 60641/08

**Metode nadzora**

Sodba z dne 5. novembra 2002 v zadevi *Allan proti Združenemu kraljestvu*, pritožba št. 48539/99
Sodba z dne 24. maja 2011 v združenih zadevah *Association „21 Décembre 1989" in drugi proti Romuniji,* pritožbi št. 33810/07 in 18817/08
Sodba z dne 10. marca 2009 v zadevi *Bykov proti Rusiji* [veliki senat], pritožba št. 4378/02
Sodba z dne 18. maja 2010 v zadevi *Kennedy proti Združenemu kraljestvu*, pritožba št. 26839/05
Sodba z dne 6. septembra 1978 v zadevi *Klass in drugi proti Nemčiji*, pritožba št. 5029/71
Sodba z dne 4. maja 2000 v zadevi *Rotaru proti Romuniji* [veliki senat], pritožba št. 28341/95
Sodba z dne 22. oktobra 2002 v zadevi *Taylor-Sabori proti Združenemu kraljestvu*, pritožba št. 47114/99
Sodba z dne 2. septembra 2010 v zadevi *Uzun proti Nemčiji*, pritožba št. 35623/05
Sodba z dne 31. maja 2005 v zadevi *Vetter proti Franciji*, pritožba št. 59842/00

**Videonadzor**

Sodba z dne 5. oktobra 2010 v zadevi *Köpke proti Nemčiji,* pritožba št. 420/07
Sodba z dne 28. januarja 2003 v zadevi *Peck proti Združenemu kraljestvu*, pritožba št. 44647/98

**Glasovni vzorci**

Sodba z dne 25. septembra 2001 v zadevi *P. G. in J. H. proti Združenemu kraljestvu*, pritožba št. 44787/98
Sodba z dne 20. decembra 2005 v zadevi *Wisse proti Franciji*, pritožba št. 71611/01

# Izbrana sodna praksa Sodišča Evropske unije

**Sodna praksa v zvezi z Direktivo o varstvu podatkov**

Sodba z dne 16. decembra 2008 v zadevi *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy in Satamedia Oy*, C-73/07
[Pojem „novinarske dejavnosti" v smislu člena 9 Direktive o varstvu podatkov]

Sodba z dne 9. novembra 2010 v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti Land Hessen*, C-92/09 in C-93/09
[Sorazmernost pravne obveznosti objave osebnih podatkov o upravičencih do sredstev iz nekaterih kmetijskih skladov EU]

Sodba z dne 6. novembra 2003 v zadevi *Bodil Lindqvist*, C-101/01
[Zakonitost objave, ki jo fizična oseba izvede v zvezi z zasebnim življenjem drugih na spletu]

Predlog za sprejetje predhodne odločbe, ki ga je Audiencia Nacional (Španija) vložilo 9. marca 2012, 25. maja 2012, še v teku. *Google Inc. proti Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12
[Obveznost ponudnikov spletnih iskalnikov, da na zahtevo posameznika, na katerega se nanašajo osebni podatki, v rezultatih iskanja prikrijejo njegove osebne podatke]

Sodba z dne 30. maja 2013 v zadevi *Evropska komisija proti Kraljevini Švedski*, C-270/11
[Denarna kazen zaradi neizvajanja Direktive]

Sodba z dne 29. januarja 2008 v zadevi *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, C-275/06
[Obveznost ponudnikov internetnega dostopa, da združenju za varstvo intelektualne lastnine razkrijejo identiteto uporabnikov programov za izmenjavo datotek KaZaA]

Tožba, vložena 8. aprila 2014, v zadevi *Evropska komisija proti Madžarski*, C-288/12
[Zakonitost ukinitve urada nacionalnega nadzornika za varstvo podatkov]

Mnenje generalnega pravobranilca z dne 13. junija 2013 v zadevi *Michael Schwarz proti Stadt Bochum*, C-291/12

[Kršitev primarne zakonodaje EU z Uredbo (ES) št. 2252/2004, ki določa, da morajo biti v potnih listih shranjeni prstni odtisi]

Sodba z dne 8. aprila 2014 v združeni zadevi C-293/12 and C-594/12, *Digital Rights Ireland in Seitling in drugi*

[Kršitev primarnega prava EU z Direktivo o hrambi podatkov]

Sodba z dne 16. februarja 2012 v zadevi *SABAM proti Netlog N. V.*, C-360/10

[Obveznost ponudnikov družbenih omrežij, da uporabnikom omrežja preprečijo nezakonito uporabo glasbenih in avdio-vizualnih del]

Sodba z dne 20. maja 2003 v združenih zadevah *Rechnungshof proti Österreichischer Rundfunk in drugim ter Neukomm in Lauermann proti Österreichischer Rundfunk*, C-465/00, C-138/01 in C-139/01

[Sorazmernost pravne obveznosti objave osebnih podatkov o plačah zaposlenih v nekaterih vrstah institucij, povezanih z javnim sektorjem]

Sodba z dne 24. novembra 2011 v združenih zadevah *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, C-468/10 in C-469/10

[Pravilno izvajanje člena 7(f) Direktive o varstvu podatkov – „zakoniti interesi drugih" – v nacionalnem pravu]

Sodba z dne 9. marca 2010 v zadevi *Evropska komisija proti Bundesrepublik Deutschland*, C-518/07

[Neodvisnost nacionalnega nadzornega organa]

Sodba z dne 16. decembra 2008 v zadevi *Huber proti Bundesrepublik Deutschland*, C-524/06

[Zakonitost hrambe podatkov o tujcih v statističnem registru]

Sodba z dne 5. maja 2011 v zadevi *Deutsche Telekom AG proti Nemčiji*, C-543/09

[Nujnost ponovne privolitve]

Sodba z dne 7. maja 2009 v zadevi *College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer*, C-553/07

[Pravica posameznika, na katerega se nanašajo osebni podatki, do dostopa]

Sodba z dne 16. oktobra 2012 v zadevi *Evropska komisija proti Republiki Avstriji*, C-614/10
[Neodvisnost nacionalnega nadzornega organa]

**Sodna praksa v zvezi z Direktivo o varstvu podatkov v institucijah EU**

Sodba z dne 29. junija 2010 v zadevi *Evropska komisija proti The Bavarian Lager Co. Ltd.*, C-28/08 P
[Dostop do dokumentov]

Sodba z dne 6. marca 2003 v zadevi *Interporc Im- und Export GmbH proti Komisiji Evropskih skupnosti*, C-41/00 P
[Dostop do dokumentov]

Sodba z dne 15. junija 2010 v zadevi *Pachtitis proti Komisiji in EPSO*, F-35/08
[Uporaba osebnih podatkov v okviru zaposlitve v institucijah EU]

Sodba z dne 5. julija 2011 v zadevi *V proti Parlamentu*, F-46/09
[Uporaba osebnih podatkov v okviru zaposlitve v institucijah EU]

# Seznam zadev

**Sodna praksa Sodišča Evropske unije**

**Sodna praksa Evropskega sodišča za človekove pravice**

**Sodna praksa nacionalnih sodišč**

Agencija Evropske unije za temeljne pravice
Svet Evrope – Evropsko sodišče za človekove pravice

**Priročnik o evropskem pravu varstva osebnih podatkov**

2014 — 198 str. — 14,8 × 21 cm

ISBN 978-92-871-9936-2 (Svet Evrope)
ISBN 978-92-9239-341-0 (FRA)
doi:10.2811/55931

Veliko informacij o Agenciji Evropske unije za temeljne pravice je na voljo na spletu. Do njih je mogoče dostopati preko spletne strani Agencije Evropske unije za temeljne pravice (http://fra.europa.eu).

Več informacij o Svetu Evrope je na voljo na spletni strani hub.coe.int.

Dodatne informacije v zvezi s sodno prakso Evropskega sodišča za človekove pravice so na voljo na spletni strani Sodišča: www.echr.coe.int. Iskalnik HUDOC nudi 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 Evropske unije

**Brezplačne publikacije:**
- en izvod:
  na spletni strani EU Bookshop (http://bookshop.europa.eu);
- več kot en izvod ter plakati in zemljevidi:
  pri predstavništvih Evropske unije (http://ec.europa.eu/represent_sl.htm),
  pri delegacijah v državah, ki niso članice EU (http://eeas.europa.eu/delegations/index_sl.htm),
  pri službi Europe Direct (http://europa.eu/europedirect/index_sl.htm) ali
  s klicem na telefonsko številko 00 800 6 7 8 9 10 11 (brezplačna številka za celotno EU) (*).

**Publikacije, ki so naprodaj:**
- na spletni strani EU Bookshop (http://bookshop.europa.eu).

**Plačljive naročnine:**
- pri prodajnih zastopnikih Urada za publikacije Evropske unije (http://publications.europa.eu/others/agents/index_sl.htm).

(*) Informacije so brezplačne, kakor tudi večina klicev (nekateri operaterji, telefonske govorilnice ali hoteli lahko klic zaračunajo).

## 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 omogoča uporabnikom dostop do odlomkov iz pravkar objavljenih glavnih publikacij ali do celotnih besedil nekaterih uradnih dokumentov brez plačila.

Informacije o konvencijah Sveta Evrope in njihovo polno besedilo je na voljo na spletni strani Urada za mednarodne pogodbe: http://conventions.coe.int/.

10.2811/55931 TK-01-13-772-SL-C

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

S hitrim razvojem informacijskih in komunikacijskih tehnologij še narašča potreba po zanesljivem varstvu osebnih podatkov – pravici, ki je varovana z instrumenti Evropske unije (EU) in Sveta Evrope. S tehnološkim napredkom se na primer širijo meje nadzora, prestrezanja komunikacij in shranjevanja podatkov, kar prinaša precejšnje izzive za pravico do varstva osebnih podatkov. Priročnik delavce v pravni stroki, ki niso specializirani na področju varstva osebnih podatkov, seznanja s tem pravnim področjem, saj vsebuje pregled veljavnih pravnih okvirov EU in Sveta Evrope. V njem je s povzetki glavnih sodb Evropskega sodišča za človekove pravice (ESČP) in Sodišča Evropske unije (SEU) pojasnjena ključna sodna praksa. Kadar take sodne prakse ni, so praktično ponazorjeni hipotetični scenariji. Skratka, priročnik naj bi pripomogel k zavzetemu in odločnemu zagovarjanju pravice do varstva osebnih podatkov.

**AGENCIJA EVROPSKE UNIJE ZA TEMELJNE PRAVICE**
Schwarzenbergplatz 11 – 1040 Dunaj – Avstrija
Tel. +43 (1) 580 30-60 – Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

**SVET EVROPE**
**EVROPSKO SODIŠČE ZA ČLOVEKOVE PRAVICE**
67075 Strasbourg Cedex – Francija
Tel. +33 (0) 3 88 41 20 00 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Urad za publikacije
ISBN 978-92-871-9936-2 (Svet Evrope)
ISBN 978-92-9239-341-0 (FRA)