KÉZIKÖNYV

Európai adatvédelmi jogi kézikönyv

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

© Az Európai Unió Alapjogi Ügynöksége, 2014
Európa Tanács, 2014

A kézikönyv kézirata 2014. áprilisban készült el.
Az aktualizált változatok a későbbiekben elérhetőek lesznek az FRA honlapján: fra.europa.eu, az Európa Tanács honlapján: coe.int/dataprotection és az Emberi Jogok Európai Bírósága honlapján az „Ítélkezési gyakorlat” (Case-Law) menüpont alatt: echr.coe.int.

A sokszorosítás engedélyezett, kivéve kereskedelmi célra, feltéve, a források feltüntetésével.

A Europe Direct szolgáltatás az Európai Unióval kapcsolatos kérdéseire segít Önnek választ találni.

Ingyenesen hívható telefonszám (*):

00 800 6 7 8 9 10 11

(*) A legtöbb hívás és a megadott információk ingyenesek (noha egyes mobiltelefon-szolgáltatókon keresztül, telefonfülkékből és hotelekből a számot csak díjfizetés ellenében lehet hívni).

Fotó (borító & belső): © iStockphoto

Bővebb tájékoztatást az Európai Unióról az interneten talál (http://europa.eu).

Katalógusadatok a kiadvány végén találhatóak.

Luxembourg: Az Európai Unió Kiadóhivatala, 2014

ISBN 978-92-871-9944-7 (Európa Tanács)
ISBN 978-92-9239-334-2 (FRA)
doi:10.2811/5399

Printed in Belgium

Fehér klórmentes papírra nyomtatva (ECF)

A kézikönyv angol nyelven készült. Az Európa Tanács és az Emberi Jogok Európai Bírósága (EJEB) a más nyelveken készült fordítások minőségéért semmilyen felelősséget nem vállalnak. A kézikönyvben kifejtett nézetek az Európa Tanácsot és az EJEB-et semmire nem kötelezik. A kézikönyv különféle észrevételekre és kézikönyvekre hivatkozik. Az Európa Tanács és az EJEB nem vállalnak felelősséget ezek tartalmáért, és az irodalomjegyzékben való feltüntetésük semmilyen értelemben nem minősül e kiadványok jóváhagyásának. Az EJEB könyvtárának internetes oldalain, a következő címen megtalálható a további kiadványok listája: 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

Európai adatvédelmi jogi kézikönyv

Előszó

Ezt az európai adatvédelmi jogról szóló kézikönyvet az Európai Unió Alapjogi Ügynöksége és az Európa Tanács – az Emberi Jogok Európai Bíróságának hivatalával együtt – közösen készítette. Ez a jogi kézikönyv a harmadik abban a sorban, amelyeket az FRA és az Európa Tanács közösen dolgozott ki. 2011 márciusában tették közzé az első kézikönyvet az európai antidiszkriminációs jogról, amit 2013. júniusában egy második kézikönyv követett a menekültüggyel, a határokkal és a bevándorlással kapcsolatos európai jogszabályokról.

Elhatároztuk, hogy folytatjuk együttműködésünket egy mindannyiunk mindennapi életét érintő, igen időszerű témával, a személyes adatok védelmével kapcsolatban. Ezen a területen Európa rendelkezik az egyik legnagyobb védelmet biztosító rendszerrel, amely az Európa Tanács 108. egyezményén, európai uniós (EU) jogi aktusokon, valamint az Emberi Jogok Európai Bírósága (EJEB) és az Európai Unió Bírósága (EUB) ítélkezési gyakorlatán alapszik.

A kézikönyv célja az Európai Unióban és az Európa Tanács tagállamaiban az adatvédelmi szabályokkal kapcsolatos tudatosság növelése és e szabályok jobb megismertetése azáltal, hogy az olvasók elsődleges hivatkozási alapként forgathatják a kiadványt. Az ismertető nem erre a területre szakosodott jogi szakemberek, bírák, nemzeti adatvédelmi hatóságok és az adatvédelem területén dolgozó más személyek részére készült.

A Lisszaboni Szerződés 2009. decemberi hatálybalépésével az Európai Unió Alapjogi Chartája jogilag kötelező erejűvé vált, és ezzel a személyes adatok védelméhez való jog az önálló alapvető jogok közé emelkedett. Az Európa Tanács 108. egyezménye és az Európai Unió jogi aktusainak mélyebb megértése, amelyek elősegítették Európában az adatvédelem fejlődését, továbbá az EUB és az EJEB ítélkezési gyakorlatának alaposabb megismerése elengedhetetlen ezen alapvető jog védelméhez.

Köszönetet szeretnénk mondani a Ludwig Boltzmann Emberi Jogi Intézetnek a kézikönyv megszövegezéséért, az Európai Adatvédelmi Biztos Hivatalának a megszövegezésben való közreműködésért, külön is az Európai Bizottság adatvédelmi osztályának a kézikönyv kidolgozása során nyújtott segítségéért. Végül szeretnénk

kifejezni köszönetünket a Nemzeti Adatvédelmi és Információszabadság Hatóságának (NAIH) a kézikönyv fordításának ellenőrzésében végzett tevékenységéért.

Philippe Boillat

Az Európa Tanács
Emberi Jogi és Jogi Ügyek
főigazgatója

Morten Kjaerum

Az Európai Unió Alapjogi
Ügynökségének igazgatója

Tartalomjegyzék

Rövidítések és betűszavak

108. egyezmény	Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (Európa Tanács)
BCR	Kötelező erejű vállalati szabályok
CCTV	Zárt láncú televíziós rendszer
CETS	Az Európa Tanács egyezményei
Charta	Az Európai Unió Alapjogi Chartája
CRM	Ügyfélkapcsolat-kezelés
C-SIS	Schengeni Információs Rendszer „Központi Rész”
EAW	Európai elfogatóparancs
EDPS	Európai Adatvédelmi Biztos
EFTA	Európai Szabadkereskedelmi Társulás
EGT	Európai Gazdasági Térség
EJEB	Az Emberi Jogok Európai Bírósága
EJEE	Az Emberi Jogok Európai Egyezménye
EK	Európai Közösség
ENISA	Európai Hálózat- és Információbiztonsági Ügynökség
ENSZ	Egyesült Nemzetek Szervezete
ENU	Europol nemzeti egység
ESMA	Európai Értékpapír-piaci Hatóság
eTEN	Transzeurópai távközlési hálózatok
EUB	Az Európai Unió Bírósága (2009. december előtt: Európai Bíróság, EB)
EU	Európai Unió
eu-LISA	Az EU Nagyméretű Informatikai Rendszerekkel Foglalkozó Ügynöksége
EUMSZ	Szerződés az Európai Unió működéséről

EuroPriSe	Európai adatvédelmi bizalompecsét
EUSZ	Szerződés az Európai Unióról
FRA	Az Európai Unió Alapjogi Ügynöksége
GPS	Globális helymeghatározó rendszer
JSB	Közös ellenőrző szerv
NGO	Nem kormányzati szervezet
N-SIS	Schengeni Információs Rendszer „Nemzeti Rész”
OECD	Gazdasági Együttműködési és Fejlesztési Szervezet
PIN	Személyi azonosítószám
PNR	Utas-nyilvántartási adatállomány
SEPA	Egységes eurófizetési térség
SIS	Schengeni Információs Rendszer
SWIFT	Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság
UDHR	Az Emberi Jogok Egyetemes Nyilatkozata
VIR	Váminformációs rendszer
VIS	Vízuminformációs Rendszer

Útmutató a kézikönyv használatához

Ez a kézikönyv az Európai Unió és az Európa Tanács tekintetében az adatvédelemre vonatkozó jogszabályokról nyújt áttekintést.

A kézikönyv olyan jogi szakembereknek nyújt segítséget, akik nem az adatvédelem területén dolgoznak; ügyvédeknek, bíráknak vagy más gyakorló szakembereknek, valamint egyéb – például nem kormányzati – szervezeteknél dolgozó munkatársaknak, akik adatvédelemmel kapcsolatos jogi kérdésekkel kerülhetnek szembe.

Az adatvédelem terén elsődleges hivatkozási alapul szolgál az uniós jogszabályok és az emberi jogok európai egyezménye (EJEE) tekintetében; kifejti, hogy az uniós jog és az EJEE, valamint az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménye (108. egyezmény) és az Európa Tanács más jogi eszközei hogyan szabályozzák ezt a területet. Minden fejezet egy táblázattal kezdődik, amely összefoglalja a két különálló európai jogrendszer szerint alkalmazandó jogi rendelkezéseket, és válogatott fontos jogeseteket is tartalmaz. Ezután egyesével bemutatja a két európai jogrend vonatkozó jogszabályait, ahogyan azok az egyes témákra érvényesek. Az olvasó ezáltal megismerheti a két jogrendszer hasonlóságait és különbségeit.

A fejezetek elején található táblázatok felsorolják az adott fejezetben tárgyalt témaköröket, és megnevezik a vonatkozó jogszabályokat és más releváns anyagokat, például ítéleteket. A témakörök sorrendje kissé eltérhet a fejezeten belül a szöveg struktúrájától, ha ez a fejezet tartalmának tömör bemutatása szempontjából kedvezőbb. A táblázatokban az Európa Tanács és az Európai Unió jogszabályai egyaránt szerepelnek. Ez segíti a felhasználókat a saját helyzetükre vonatkozó legfontosabb információk megtalálásában, különösen ha csak az Európa Tanács jogszabályainak hatálya alá tartoznak.

Azoknak a nem uniós tagállamoknak a gyakorló szakemberei, amelyek az Európa Tanácsnak tagállamai, és ezáltal az EJEE-nek és a 108. egyezménynek részes felei, a saját országukra vonatkozó információkat az Európa Tanácsra vonatkozó részekben találják meg. Az uniós tagállamok gyakorló szakembereinek mindkét részt tanulmányozniuk kell, mivel ezekre az államokra mind a két jogrend érvényes. Aki egy bizonyos kérdésről szeretne többet megtudni, annak a kézikönyv „Ajánlott szakirodalom" című részében szereplő, speciálisabb anyagokat is tartalmazó irodalomjegyzéket érdemes tanulmányoznia.

Az Európa Tanács jogszabályainak ismertetéséhez röviden bemutatjuk az Emberi Jogok Európai Bíróságának (EJEB) válogatott ügyeit. Ezeket az EJEB létező adatvédelmi kérdésekről szóló nagyszámú ítélete és határozata közül választottuk ki.

Az uniós jog az eddig elfogadott jogalkotási intézkedésekben, valamint a szerződések és az Európai Unió Alapjogi Chartája vonatkozó rendelkezéseiben található meg, az Európai Unió Bíróságának (EUB; a 2009 előtti megnevezés szerint az Európai Bíróság [EB]) ítélkezési gyakorlatából következő értelmezés szerint.

A kézikönyvben bemutatott vagy idézett ítélkezési gyakorlat az EJEB és az EUB fontos esetjogi corpusából hoz példákat. A kézikönyv végén szereplő iránymutatások az ítélkezési gyakorlat online keresésében kívánják segíteni az olvasót.

Ezenfelül, a keretes szövegekben gyakorlati példákat közlünk feltételezett esetekkel, amelyek az európai adatvédelmi szabályok gyakorlati alkalmazását szemléltetik, különösen ha az EJEB-nek vagy az EUB-nak nincs a témában konkrét ítélkezési gyakorlata.

A kézikönyv az EJEE és az európai uniós jog által létrehozott két jogrendszer szerepének rövid leírásával kezdődik (1. fejezet). A 2–8. fejezet a következő kérdéseket tárgyalja:

- adatvédelmi terminológia;
- az európai adatvédelmi jog alapelvei;
- az európai adatvédelmi jog szabályai;
- az érintettek jogai és e jogok érvényesítése;
- határokon átnyúló adatáramlás;
- adatvédelem a rendőrségi és büntető igazságügyi területen;
- egyéb egyedi európai adatvédelmi jogszabályok.

1

Az európai adatvédelmi jog kontextusa és háttere

EU	Tárgyalt kérdések	Európa Tanács
Az adatvédelemhez való jog		
95/46/EK irányelv a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (*adatvédelmi irányelv*), HL L 281., 1995		EJEE, 8. cikk (magán- és családi élet, lakás és levelezés tiszteletben tartásához való jog) Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (108. egyezmény)
A jogok közötti egyensúly		
EUB, C-92/09. és C-93/09. sz., *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* egyesített ügyek, 2010	Általánosságban	
EUB, C-73/07. sz. *Tietosuojavaltuutettu kontra Satakunnan Markkinapörssi Oy és Satamedia Oy ügy*, 2008	A véleménynyilvánítás szabadsága	EJEB, *Axel Springer AG kontra Németország*, 2012 EJEB, *Mosley kontra Egyesült Királyság*, 2011
	A művészet és a tudomány szabadsága	EJEB, *Vereinigung bildender Künstler kontra Ausztria*, 2007
EUB, C-275/06. sz. *Productores de Música de España (Promusicae) kontra Telefónica de España SAU ügy*, 2008	A tulajdon védelme	
EUB, C-28/08 P. sz. *Európai Bizottság kontra The Bavarian Lager Co. Ltd ügy*, 2010	Dokumentumokhoz való hozzáférés	EJEB, *Társaság a Szabadságjogokért kontra Magyarország*, 2009

1.1. Az adatvédelemhez való jog

Főbb pontok

- Az EJEE 8. cikke értelmében a személyes adatok gyűjtésével és felhasználásával szembeni védelemhez való jog a magán- és családi élet, a lakás és a levelezés tiszteletben tartásához való jog részét képezi.
- Az Európa Tanács 108. egyezménye az első nemzetközi, jogilag kötelező erejű eszköz, amely kifejezetten az adatvédelemmel foglalkozik.
- Az uniós jogban az adatvédelmet elsőként az adatvédelmi irányelv szabályozta.
- Az uniós jog alapvető jognak ismeri el az adatvédelmet.

Az egyén magánéletének mások – különösen az állam – beavatkozása elleni védelméhez való jogát nemzetközi jogi okiratban először az ENSZ 1948-as Emberi Jogok Egyetemes Nyilatkozatának (UDHR) a magán- és családi élet tiszteletben tartásáról szóló 12. cikkében mondták ki.[1] Az UDHR más emberi jogi okmányok fejlődésére is hatással volt Európában.

1.1.1. Az Emberi Jogok Európai Egyezménye

Az Európa Tanács a második világháború utóhatásaként alakult meg, hogy összefogja az európai államokat a jogállamiság, a demokrácia, az emberi jogok és a társadalmi fejlődés előmozdítása érdekében. E célból 1950-ben elfogadta Az Emberi Jogok Európai Egyezményét (EJEE), amely 1953-ban lépett hatályba.

Az államokat nemzetközi kötelezettség terheli az EJEE betartása tekintetében. Mára már az Európa Tanács minden tagállama beépítette nemzeti jogába vagy hatályba léptette az EJEE-t, így köteles az egyezmény rendelkezéseinek megfelelően eljárni.

Annak biztosítása céljából, hogy a Szerződő Felek eleget tegyenek az EJEE értelmében fennálló kötelezettségeiknek, 1959-ben Strasbourgban létrehozták az Emberi Jogok Európai Bíróságát (EJEB). Az EJEB azzal biztosítja az egyezmény alapján fennálló kötelezettségek betartását, hogy foglalkozik az egyezmény állítólagos megsértésére vonatkozó, magánszemélyektől, személyek csoportjaitól, civil szervezetektől vagy jogi személyektől érkező panaszokkal. 2013-ban az Európa Tanács 47

1 ENSZ Emberi Jogok Egyetemes Nyilatkozata (UDHR), 1948. december 10.

tagállamból állt, amelyek közül 28 egyben az Európai Uniónak is tagja. Az EJEB-hez folyamodó kérelmezőnek nem feltétlenül kell valamelyik tagállam állampolgárának lennie. Az EJEB az Európa Tanács egy vagy több tagállama által egy másik tagállam ellen indított államközi ügyeket is vizsgálhatja.

A személyes adatok védelméhez való jog az EJEE 8. cikke alapján oltalomban részesülő jogok közé tartozik, amely cikk garantálja a magán- és családi élet, a lakás és a levelezés tiszteletben tartását, és meghatározza azokat a feltételeket, amelyekkel e jog korlátozható.[2]

Az EJEB ítélkezési gyakorlata során számos olyan helyzetet vizsgált, amelyben az adatvédelem kérdése felmerült, ideértve többek között a kommunikáció megszakításával,[3] a megfigyeléssel[4] és a hatóságok által tárolt személyes adatok elleni védelemmel kapcsolatos eseteket.[5] pontosította, hogy az EJEE nemcsak arra kötelezte az államokat, hogy tartózkodjanak az olyan fellépéstől, amely sértheti az egyezményben foglalt jogot, hanem azt is rögzítette, hogy az államokat bizonyos körülmények fennállása esetén pozitív kötelezettség is terheli abban a vonatkozásban, hogy valóban biztosítsák a magán- és családi élet tényleges tiszteletben tartását.[6] A megfelelő fejezetekben több említett üggyel részletesen is foglalkozunk.

1.1.2. Az Európa Tanács 108. egyezménye

Az információs technológia 1960-as évekbeli fejlődésével egyre szükségesebbé vált az egyének (személyes) adatainak védelmére vonatkozó részletes szabályok megállapítása. Az 1970-es évek közepéig az Európa Tanács Miniszteri Bizottsága az EJEE 8. cikkére való hivatkozással számos határozatot fogadott el a személyes adatok védelmével kapcsolatban.[7] 1981-ben a személyes adatok gépi feldolgozása során

2 Európa Tanács, Emberi Jogok Európai Egyezménye, CETS 005., 1950.

3 Lásd például: EJEB, 8691/79. sz. *Malone kontra Egyesült Királyság* ügy, 1984. augusztus 2.; EJEB, 62617/00. sz. *Copland kontra Egyesült Királyság* ügy, 2007. április 3.

4 Lásd például: EJEB, 5029/71. sz. *Klass és társai kontra Németország* ügy, 1978. szeptember 6.; EJEB, 35623/05. sz. *Uzun kontra Németország* ügy, 2010. szeptember 2.

5 Lásd például: EJEB, 9248/81. sz. *Leander kontra Svédország* ügy, 1987. március 26.; EJEB, 30562/04. sz. és 30566/04. *S. és Marper kontra Egyesült Királyság* ügy, 2008. december 4.

6 Lásd például: EJEB, 20511/03. sz. *I. kontra Finnország* ügy, 2008. július 17.; EJEB, 2872/02. sz. *K.U. kontra Finnország* ügy, 2008. december 2.

7 Az Európa Tanács Miniszteri Bizottsága (1973) (73)22. sz. határozata a magánéletnek a magánszektorbeli elektronikus adatbankokkal szembeni védelméről, 1973. szeptember 26.; Az Európa Tanács Miniszteri Bizottsága (1974) (74)29. sz. határozata a magánéletnek a magánszektorbeli elektronikus adatbankokkal szembeni védelméről, 1974. szeptember 20.

az egyének védelméről szóló egyezmény (108. egyezmény)[8] nyílt meg aláírásra. A mai napig a 108. egyezmény az egyetlen jogilag kötelező erejű nemzetközi eszköz az adatvédelem területén.

A 108. egyezmény vonatkozik mind a magánszféra, mind a közszféra által végzett olyan adatkezelésre, mint például a bírósági és bűnüldözési hatóságok adatkezelése. A 108. egyezmény megvédi az egyént a személyes adatok gyűjtésével és feldolgozásával összefüggő visszaélésektől, ugyanakkor törekszik a határokon átnyúló személyesadat-áramlás szabályozására. A személyes adatok gyűjtésére és feldolgozására vonatkozóan az egyezményben meghatározott elvek a következők: az adatokat csak tisztességesen és törvényesen szabad gyűjteni és feldolgozni, az adatokat csak meghatározott és törvényes célra szabad tárolni, és attól eltérő módon nem szabad felhasználni, továbbá csak a tárolás céljához szükséges ideig szabad tárolni. Az elvek érintik ezenkívül az adatok minőségét, főleg azt, hogy az adatoknak megfelelőnek, relevánsnak kell lenniük, és nem haladhatják meg a feldolgozás célját (arányosság), továbbá pontosaknak is kell lenniük.

Azon kívül, hogy az egyezmény garanciákat nyújt a személyes adatok gyűjtésével és feldolgozásával kapcsolatban, megfelelő jogi biztosítékok hiányában tiltja a „különleges" adatok feldolgozását, azaz a faji eredetre, politikai véleményre, vallásos vagy más meggyőződésre és az egészségre, a szexuális életre vonatkozó, valamint a büntető ítéletekkel kapcsolatos személyes adatok feldolgozását.

Az egyezmény az egyén azon jogáról is rendelkezik, hogy tudomást szerezhessen a róla tárolt adatokról, továbbá szükség esetén helyesbíttethesse azokat. Az egyezményben megállapított jogok korlátozása csak magasabb rendű érdekek, például a biztonság vagy a védelem, fennállása esetén lehetséges.

Bár az egyezmény a személyes adatoknak az egyezmény részes államai közötti szabad áramlásáról rendelkezik, bizonyos korlátozásokat is előír az olyan államokba történő adatáramlás tekintetében, ahol a jogi szabályozás nem nyújt azonos védelmet.

A 108. egyezményben meghatározott általános elvek és szabályok továbbfejlesztése érdekében az Európa Tanács Miniszteri Bizottsága számos ajánlást elfogadott, amelyek jogilag nem kötelező erejű dokumentumok (lásd a 7. és 8. fejezetet).

8 Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során, Európa Tanács, CETS 108., 1981.

Valamennyi európai uniós tagállam ratifikálta a 108. egyezményt. 1999-ben a 108. egyezményt úgy módosították, hogy az EU is részes fele lehessen az egyezménynek.[9] 2001-ben elfogadtak egy kiegészítő jegyzőkönyvet a 108. egyezményhez, amely az egyezmény nem részes feleihez, az úgynevezett harmadik országokba történő, országhatárokat átlépő adatáramlásra és a nemzeti adatvédelmi hatóságok kötelező létrehozására vonatkozóan vezetett be rendelkezéseket.[10]

Kilátások

A 108. egyezmény modernizálására vonatkozó határozatot követően a 2011-ben folytatott nyilvános konzultáció folyományaként megerősítést nyerhetett a munka két fő célkitűzése: a magánélet védelme a digitális korszakban, valamint az egyezmény nyomon követési mechanizmusának megerősítése.

A 108. egyezmény azon országok számára is nyitva áll a csatlakozásra, amelyek nem tagjai az Európa Tanácsnak, az Európán kívüli országokat is beleértve. Az, hogy az egyezmény az egész világon érvényes normává válhat, és hogy nyílt jellegű, alapul szolgálhat az adatvédelem globális előmozdításához.

Eddig a 108. egyezmény 46 részes fele közül 45-en tagjai az Európa Tanácsnak. Uruguay az első Európán kívüli ország, amely 2013 augusztusában csatlakozott az egyezményhez, Marokkó esetében pedig, amelyet a Miniszteri Bizottság kért fel a 108. egyezményhez való csatlakozásra, a hivatalos csatlakozási eljárás folyamatban van.

1.1.3. Az Európai Unió adatvédelmi joga

Az uniós jog a szerződésekből és a másodlagos joganyagból áll. A szerződéseket, azaz az Európai Unióról szóló szerződést (EUSZ) és az Európai Unió működéséről szóló szerződést (EUMSZ) az EU valamennyi tagállama jóváhagyta. Ezeket nevezzük az „elsődleges joganyagnak". Az EU rendeleteit, irányelveit és határozatait a szerződések szerint erre felhatalmazott uniós intézmények fogadják el; ezek gyakori megnevezése a „másodlagos joganyag".

9 Európa Tanács, A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezmény (ETS 108.) módosítása, amely lehetővé teszi az Európai Közösségek csatlakozását – elfogadta a Miniszteri Bizottság Strasbourgban, 1999. június 15-én; a 108. egyezmény 23. cikkének (2) bekezdése módosított formában.

10 Európa Tanács, Kiegészítő jegyzőkönyv a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményhez, az adatvédelmi hatóságokra és az országhatárokat átlépő adatáramlásra vonatkozóan, CETS 181., 2011.

Az adatvédelemmel kapcsolatos legfőbb uniós jogi aktus a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv (*adatvédelmi irányelv*).[11] Az adatvédelmi irányelvet 1995-ben fogadták el – akkor, amikor már számos tagállam rendelkezett nemzeti adatvédelmi törvénnyel. A belső piacon az áruk, a tőke, a szolgáltatások és a személyek szabad mozgásához szabad adatáramlás szükséges, ami csak akkor valósítható meg, ha a tagállamok egységes, magas szintű adatvédelemre hagyatkozhatnak.

Mivel az adatvédelmi irányelv elfogadásának célja a nemzeti szintű adatvédelmi jogszabályok összehangolása volt[12], az irányelv a (korábbi) nemzeti adatvédelmi szabályokhoz viszonyítva bizonyos mértékig részletesebb. „A 95/46 irányelv célja, amint az többek között annak (8) preambulumbekezdéséből következik, hogy minden tagállamban azonossá tegye az egyének jogai és szabadságai védelmének szintjét az ilyen adatok kezelése terén. Az erre vonatkozó jogszabályok közelítése nem vezethet az általuk nyújtott védelem szintjének csökkenéséhez, sőt, magas védelmi szintet kell, hogy biztosítson az Unión belül. Ennek megfelelően az említett nemzeti jogszabályok harmonizációja nem korlátozódik minimális mértékű harmonizációra, hanem annak főszabály szerint teljes harmonizációt kell eredményeznie."[13] Ennek következtében, az irányelv végrehajtásakor a tagállamok csak korlátozott mozgásszabadsággal rendelkeznek.

Az adatvédelmi irányelvet azért dolgozták ki, hogy a 108. egyezményben már szereplő adatvédelemhez való jogból fakadó elveket konkrét jelleggel ruházzák fel és kiterjesszék. Az a tény, hogy 1995-ben mind a 15 uniós tagállam a 108. egyezménynek is részes fele volt, kizárja, hogy e két jogi eszközben egymásnak ellentmondó szabályokat fogadtak volna el. Az adatvédelmi irányelv mindazonáltal azzal a 108. egyezmény 11. cikkében foglalt lehetőséggel is számol, hogy a védelmet biztosító további jogi aktusokkal is kiegészülhet. Különösen a független felügyelet mint az adatvédelmi szabályok jobb betartatását szolgáló eszköz bevezetése bizonyult fontos hozzájárulásnak az európai adatvédelmi jog tényleges érvényesüléséhez. (Ezért ezt 2001-ben a 108. egyezményhez fűzött kiegészítő jegyzőkönyvvel át is vették az Európa Tanács jogába.)

11 Adatvédelmi irányelv, HL L 281., 1995., 31. o.

12 Lásd például az adatvédelmi irányelv (1), (4), (7) és (8) preambulumbekezdését.

13 EUB, C-468/10. és C-469/10. sz. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) kontra Administración del Estado egyesített ügyekben hozott ítélet* (2011. november 24.), 28-29. pont.

Az adatvédelmi irányelv területi hatálya túlmutat a 28 uniós tagállamon, hiszen az Európai Gazdasági Térséghez (EGT) tartozó nem uniós tagállamokra[14] – azaz Izlandra, Liechtensteinre és Norvégiára – is kiterjed.

Az EUB rendelkezik joghatósággal annak megállapítására, hogy egy tagállam teljesítette-e az adatvédelmi irányelv alapján fennálló kötelezettségeit, és előzetes döntéseket hozhat az irányelv érvényességével és értelmezésével kapcsolatban annak érdekében, hogy biztosítsa a tagállamokban az irányelv hatékony és egységes alkalmazását. Fontos kivétel az adatvédelmi irányelv alkalmazhatósága alól az úgynevezett háztartási kivétel, azaz a személyes adatok magánszemélyek általi, pusztán személyes vagy háztartási célokra történő feldolgozása.[15] Az ilyen adatfeldolgozás általában az egyén szabadságai közé tartozik.

Az EU-nak az adatvédelmi irányelv elfogadásakor hatályos elsődleges joganyagával összhangban az irányelv tárgyi hatálya a belső piaci kérdésekre korlátozódik. Elsősorban a rendőrségi és büntető igazságszolgáltatási együttműködés körébe tartozó kérdések esnek az irányelv hatályán kívül. Ezekben a kérdésekben az adatvédelem különböző jogi aktusokból származik, amelyek részletes ismertetése a 7. fejezetben található.

Mivel az adatvédelmi irányelvnek csak uniós tagállamok lehetnek a címzettjei, további jogi eszközre volt szükség az uniós intézmények és szervek általi személyesadat-feldolgozásra vonatkozó adatvédelem kiépítéséhez. A személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló 45/2001/EK rendelet (*uniós intézmények adatvédelmi rendelete*) tölti be ezt a funkciót.[16]

Ezenkívül a többi jogos érdekkel való egyensúly megteremtése érdekében gyakran részletesebb adatvédelmi rendelkezésekre is szükség van – akár az adatvédelmi irányelv hatálya alá tartozó területeken is. Két példa erre: az elektronikus hírközlési ágazatban a személyes adatok feldolgozásáról és a magánélet védelméről szóló

14 Megállapodás az Európai Gazdasági Térségről, *HL L 1., 1994.,* amely 1994. január 1-jén lépett hatályba.

15 Adatvédelmi irányelv, 3. cikk, (2) bekezdés, második francia bekezdés.

16 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, HL 2001 L 8.

2002/58/EK irányelv (*elektronikus hírközlési adatvédelmi irányelv*)[17] és a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról szóló 2006/24/EK irányelv (*adatmegőrzési irányelv, érvénytelenítve 2014. április 8-án)*.[18] A 8. fejezetben más példákat is bemutatunk. Az ilyen rendelkezéseknek összhangban kell állniuk az adatvédelmi irányelvvel.

Az Európai Unió Alapjogi Chartája

Az Európai Közösségek eredeti szerződései nem tartalmaztak semmilyen utalást az emberi jogokra vagy azok védelmére. Mivel azonban az akkori Európai Bíróság (EB) elé – az uniós jog hatálya alá tartozó területeken – állítólagos emberi jogsértésekkel kapcsolatos ügyek kerültek, a Bíróság új megközelítést dolgozott ki. Ahhoz, hogy az egyének részére védelmet biztosítson, az EB az alapvető jogokat az európai jog úgynevezett általános elvei közé sorolta. Az EUB szerint ezek az általános elvek tükrözik a nemzeti alkotmányokban és az emberi jogi szerződésekben, különösen az EJEE-ben foglalt emberi jogvédelmi tartalmat. Az EUB kijelentette, hogy gondoskodik arról, hogy az uniós jog megfeleljen ezeknek az elveknek.

Az EU 2000-ben kihirdette az Európai Unió Alapjogi Chartáját (a „Charta"), miután felismerte, hogy szakpolitikái hatással lehetnek az emberi jogokra, és törekedett arra, hogy a polgárok „közelebb" kerüljenek az EU-hoz. A Charta azzal, hogy szintetizálja a közös tagállami alkotmányos hagyományokat és nemzetközi kötelezettségeket, az európai polgárok polgári, politikai, gazdasági és szociális jogainak teljes skáláját felöleli. A Chartában leírt jogok hat fejezetre oszlanak: méltóság, szabadságok, egyenlőség, szolidaritás, a polgárok jogai és igazságszolgáltatás.

17 Az Európai Parlament és a Tanács 2002. július 12-i 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (*elektronikus hírközlési adatvédelmi irányelv*), HL L 201., 2002.

18 Az Európai Parlament és a Tanács 2006. március 15-i 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (*adatmegőrzési irányelv, érvénytelenítve 2014. április 8-án)*, HL L 105., 2006.

Bár eredetileg a Charta csupán politikai dokumentum volt,[19] a Lisszaboni Szerződés 2009. december 1-jei hatálybalépésével elsődleges uniós joganyagként (lásd az EUSZ 6. cikkének (1) bekezdését) jogilag kötelező erejűvé vált.[20]

Az EU elsődleges joganyaga szintén az EU általános hatásköréről rendelkezik adatvédelmi kérdésekben (az EUMSZ 16. cikke).

A Charta nemcsak garantálja a magán- és családi élet tiszteletben tartását (7. cikk), hanem megállapítja az adatvédelemhez való jogot (8. cikk), kifejezetten alapjogi szintre emelve e védelem szintjét az uniós jogban. Az uniós intézmények és a tagállamok kötelesek elismerni és szavatolni ezt a jogot, amely az uniós jogszabályok végrehajtása során a tagállamokra is vonatkozik (a Charta 51. cikke). A Charta 8. cikkét, amely sok évvel az adatvédelmi irányelv után keletkezett, úgy kell értelmezni, hogy az a korábban már létezett uniós adatvédelmi jogot is magában foglalja. A Charta ezért a 8. cikk (1) bekezdésében nemcsak kifejezetten megemlíti az adatvédelemhez való jogot, hanem a 8. cikk (2) bekezdésében a legfontosabb adatvédelmi elvekre is kitér. Végül a Charta 8. cikkének (3) bekezdése biztosítja, hogy a szóban forgó elvek végrehajtását független hatóság ellenőrizze.

Kilátások

2012 januárjában az Európai Bizottság adatvédelmi reformcsomagra tett javaslatot, egyúttal kijelentette, hogy – figyelemmel a gyors technológiai fejlődésre és a globalizációra – a hatályos adatvédelmi szabályokat korszerűsíteni kell. A reformcsomag a következő részekből áll: általános adatvédelmi rendeletre vonatkozó javaslat[21], amely az adatvédelmi irányelv helyébe lépne, valamint egy új adatvédelmi irányelv[22] , amely a rendőrségi és igazságügyi együttműködés terén rendelkezik az adatvédelemről. E kézikönyv közzétételekor folyamatban van a reformcsomag tárgyalása.

19 EU (2012), Az Európai Unió Alapjogi Chartája, HL C 326., 2012.

20 Lásd az Európai Közösségeknek (2012) az Európai Unióról szóló szerződése (HL C 326., 2012) és az Európai Közösségekről szóló szerződés (EUMSZ, HL C 326., 2012) egységes szerkezetbe foglalt változatát.

21 Európai Bizottság (2012), Javaslat, Az Európai Parlament és a Tanács rendelete a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet), COM(2012) 0011, Brüsszel, 2012. január 25.

22 Európai Bizottság (2012), Javaslat, Az Európai Parlament és a Tanács irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi irányelv), COM(2012) 0010, Brüsszel, 2012. január 25.

1.2. A jogok közötti egyensúly

Fő pont

- Az adatvédelemhez való jog nem abszolút jog; egyensúlyt kell teremteni e jog és más jogok között.

A Charta 8. cikke szerinti, a személyes adatok védelméhez való jog „nem abszolút jog, hanem a társadalomban betöltött szerepének függvényében kell figyelembe venni”.[23] A Charta 52. cikkének (1) bekezdése elfogadja tehát, hogy lehetséges a Charta 7. és 8. cikkében említett jogok gyakorlásának korlátozása, feltéve, hogy a korlátozásra a törvény által, a jogok és szabadságok lényeges tartalmának, valamint az arányosság elvének tiszteletben tartásával kerül sor, továbbá a korlátozás elengedhetetlen és ténylegesen az Európai Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.[24]

Az EJEE rendszerében az adatvédelmet a 8. cikk (a magán- és családi élet tiszteletben tartásához való jog) biztosítja, és a Charta rendszeréhez hasonlóan e jogot más versengő jogok hatályának tiszteletben tartásával kell alkalmazni. Az EJEE 8. cikkének (2) bekezdése szerint „e jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban [...] mások jogainak és szabadságainak védelme érdekében szükséges”.

Mind az EJEB, mind az EUB tehát ismételten kijelentette, hogy az EJEE 8. cikkének és a Charta 8. cikkének alkalmazása és értelmezése során egyensúlyt kell teremteni e jog és más jogok között.[25] Számos fontos példával szemléltetjük, hogyan teremthető meg ez az egyensúly.

---

23 Lásd például az EUB, C-92/09. és C-93/09. sz., *Volker és Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* egyesített ügyekben hozott 2010. november 9-i ítélet 48. pontját.

24 *Uo.*, 50. pont.

25 EJEB, 40660/0. és 60641/08. sz. *Von Hannover kontra Németország* ügy [GC], 2012. február 7.; EUB, C-468/10. és C-469/10. sz. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado* egyesített ügyekben hozott ítélet (2011. november 24.), 48. pont; EUB, C-275/06. sz. *Productores de Música de España (Promusicae) kontra Telefónica de España SAU* ügyben hozott ítélet (2008. január 29.), 68. pont. Lásd még Európa Tanács (2013), Az Emberi Jogok Európai Bíróságának a személyes adatok védelmével kapcsolatos ítélkezési gyakorlata (DP 2013 ítélkezési gyakorlat), elérhető a következő címen: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP%202013%20Case%20Law_Eng%20%28final%2018%2007%202013%29.pdf.

1.2.1. A véleménynyilvánítás szabadsága

Az adatvédelemhez való joggal valószínűsíthetően ütköző egyik jog a véleménynyilvánításhoz való jog.

A véleménynyilvánítás szabadságát a Charta 11. cikke (A véleménynyilvánítás és a tájékozódás szabadsága) védi. Ez a jog magában foglalja a véleményalkotás szabadságát és az információk, illetve eszmék megismerésének és közlésének szabadságát országhatárokra való tekintet nélkül és anélkül, hogy ebbe hatósági szerv beavatkozhasson. A 11. cikk megfelel az EJEE 10. cikkének. A Charta 52. cikkének (3) bekezdése szerint: amennyiben e Charta olyan jogokat tartalmaz, amelyek megfelelnek az EJEE-ben biztosított jogoknak, akkor „e jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az említett egyezményben szerepelnek". A Charta 11. cikkében biztosított jog jogszerű korlátozása tehát nem terjedhet túl az EJEE 10. cikkének (2) bekezdésében említett korlátozásokon, azaz a korlátozást törvényben kell meghatározni, és „mások jó hírneve vagy jogai védelme [...] céljából" szükséges intézkedésnek kell minősülnie. Ez a koncepció érvényes az adatvédelemhez való jogra.

A személyes adatok védelme és a véleménynyilvánítás szabadsága közötti kapcsolatra az adatvédelmi irányelvnek „A személyes adatok feldolgozása és a szólásszabadság" című 9. cikke az irányadó.[26] E cikk szerint a tagállamok kötelesek előírni ezen irányelv II., IV. és VI. fejezetében foglalt, az adatok védelmétől és így a magánélet tiszteletben tartásához való alapvető jog védelmétől való bizonyos kivételeket vagy korlátozásokat. E kivételekről a szólásszabadság alapvető jogába tartozó újságírás vagy művészi, illetve irodalmi kifejezés céljából lehet rendelkezni, amennyiben azok szükségesnek bizonyulnak a magánélet tiszteletben tartásához való jognak a szólásszabadságra vonatkozó szabályokkal való összeegyeztetéséhez.

Példa: A *Tietosuojavaltuutettu kontra Satakunnan Markkinapörssi Oy és Satamedia Oy* ügyben[27] az EUB-ot arra kérték, hogy értelmezze az adatvédelmi irányelv 9. cikkét, és határozza meg az adatvédelem és a sajtószabadság közötti viszonyt. A Bíróságnak a finn adóhatóságtól jogszerűen kapott, mintegy 1,2 millió természetes személyre vonatkozó adófizetési adatoknak a Markkinapörssi és a Satamedia általi terjesztését kellett vizsgálnia. A Bíróságnak azt

26 Adatvédelmi irányelv, 9. cikk.

27 EUB, a C-73/07. sz. *Tietosuojavaltuutettu kontra Satakunnan Markkinapörssi Oy és Satamedia Oy* ügyben 2008. december 16-án hozott ítélet, 56., 61. és 62. pont.

kellett értékelnie, hogy a személyesadat-feldolgozás, amit az adóhatóság azért tett lehetővé, hogy a mobiltelefon-használók más természetes személyekre vonatkozó adózási adatokat kaphassanak, kizárólag újságírás céljából végzett tevékenységnek minősül-e. Miután a Bíróság megállapította, hogy a Satakunnan tevékenysége az adatvédelmi irányelv 3. cikke (1) bekezdése szerinti értelemben vett „személyesadat-feldolgozás" volt, a Bíróság az irányelv 9. cikkének értelmezésével haladt tovább. Először megjegyezte a véleménynyilvánítás szabadságához való jog fontosságát minden demokratikus társadalomban, és kijelentette, hogy az e szabadsággal kapcsolatos fogalmakat, például az újságírás fogalmát, tágan kell értelmezni. Ezután megállapította, hogy a két alapvető jog közötti egyensúly megteremtéséhez az adatvédelemhez való jog alóli kivételeket és korlátozásokat kizárólag a feltétlenül szükséges mértékben kell alkalmazni. Ilyen körülmények között a Bíróság megítélése szerint a Markkinapörssi és a Satamedia által a nemzeti jogszabályok szerint nyilvánosan hozzáférhető dokumentumokból származó adatokkal kapcsolatban végzett tevékenységek „újságírás céljából végzett tevékenységnek" minősíthetők, ha információk, vélemények vagy gondolatok nagyközönséggel való közlésére irányulnak – függetlenül a továbbításukhoz használt médiumtól. A Bíróság azt is megállapította, hogy e tevékenységek nem korlátozódnak csupán a médiavállalkozásokra, és jövedelemszerzés céljából is végezhetők. Az EUB annak eldöntését azonban a nemzeti bíróságra hagyta, hogy a konkrét esetben erről volt-e szó.

Az adatvédelemhez való jognak a véleménynyilvánítás szabadságával való összeegyeztetése tekintetében az EJEB számos iránymutató ítéletet kiadott.

Példa: Az *Axel Springer AG kontra Németország* ügyben[28] az EJEB megállapította, hogy egy hazai bíróság azzal, hogy egy újság tulajdonosát, aki egy ismert színész letartóztatásáról és elítéléséről akart cikket közölni, eltiltotta a cikk közlésétől, megsértette az EJEE 10. cikkét. Az EJEB ismételten rámutatott a véleménynyilvánítás szabadsága és a magánélet tiszteletben tartása közötti egyensúly megteremtése tekintetében az ítélkezési gyakorlatában általa megállapított kritériumokra:

- először is arra, hogy a szóban forgó cikk általános érdeket szolgált: egy személy letartóztatása és elítélése nyilvános igazságügyi tény, ennélfogva közérdekű esemény;

28 Az EJEB Nagytanácsának az 39954/7. sz., *Axel Springer AG kontra Németország* ügyben 2012. február 7-én hozott ítélete, 90. és 91. pont.

- másodszor, hogy az érintett személy közismert volt: eléggé ismert színész ahhoz, hogy közszereplőnek minősüljön; és

- harmadszor, az információszerzés módja és megbízhatósága tekintetében: az információt az államügyészi hivatal szolgáltatta, és a felek nem vitatták a közleményekben szereplő információk pontosságát.

Ezért az EJEB úgy határozott, hogy a társasággal szemben megállapított közzétételi korlátozások nem álltak megfelelően arányban a felperes magánélethez való joga védelmének törvényes céljával. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 10. cikkét.

Példa: A *Von Hannover kontra Németország 2. sz. ügyben*[29] az EJEB azt állapította meg, hogy nem sértették meg az EJEE 8. cikkében foglalt, a magánélet tiszteletben tartásához való jogot, amikor elutasították Caroline monacói hercegnő jogsértés megszüntetésére irányuló keresetét, amit egy őt és a férjét síelés közben ábrázoló fénykép közlésének megakadályozására indított. A fényképhez egy cikk is tartozott, amely egyebek mellett Rainier herceg gyenge egészségi állapotáról tudósított. Az EJEB arra a következtetésre jutott, hogy a hazai bíróságok gondosan egyensúlyt teremtettek a kiadóvállalat véleménynyilvánításhoz való joga és a felperesnek a magánélet tiszteletben tartásához való joga között. A hazai bíróságok megállapítása, miszerint Rainier herceg betegsége foglalkoztatja a társadalmat, nem tekinthető ésszerűtlennek, és az EJEB el tudta fogadni, hogy a fénykép – a cikkre is figyelemmel – legalábbis bizonyos mértékig hozzájárult a közérdekű vitához.

Az EJEB ítélkezési gyakorlatában a szóban forgó jogok kiegyensúlyozásával kapcsolatos egyik legfontosabb kritérium az, hogy az adott kifejezés hozzájárul-e közérdekű vitához.

Példa: A *Mosley kontra Egyesült Királyság* ügyben[30] egy országos hetilap intim fényképeket közölt a felperesről. Ezután a felperes az EJEE 8. cikkének megsértése miatt keresetet indított, mert a kérdéses fotók közlése előtt nem tudott jogsértés megszüntetésére irányuló végzést kérni, hiszen nem tudott eleget tenni az újság előzetes figyelmeztetésére vonatkozó követelménynek, ami

29 Az EJEB Nagytanácsának az 40660/08. és 60641/08. sz., *Von Hannover kontra Németország 2. sz.* ügyben 2012. február 7-én hozott ítélete, 118. és 124. pont.

30 EJEB, *Mosley kontra Egyesült Királyság (48009/08)*, 2001. május 10., 129. és 130. pont.

a magánélethez való jog megsértésére alkalmas anyag közzététele esetén előírás. Bár a szóban forgó anyag terjesztése általánosságban szórakoztatási, nem pedig oktatási célt szolgált, kétségtelenül részesült az EJEE 10. cikke szerinti védelemben, ami elvezethet az EJEE 8. cikkében foglalt követelményekhez, amennyiben magán- vagy intim jellegű információkról volt szó, és a terjesztéshez nem fűződött közérdek. Különös gondossággal kellett azonban vizsgálni azokat a korlátozásokat, amelyek a közzététel előtti cenzúraként működhettek. Az előzetes értesítési követelménynek a kedélyeket lehűtő hatásával, az e követelmény hatékonyságával kapcsolatos kételyekkel és az e téren fennálló széles mérlegelési mozgástérrel kapcsolatban az EJEB arra a következtetésre jutott, hogy a 8. cikk nem ír elő jogilag kötelező előzetes értesítést. Ennek megfelelően a Bíróság arra a következtetésre jutott, hogy nem sértették meg a 8. cikket.

Példa: A *Biriuk kontra Litvánia* ügyben[31] a felperes kártérítést követelt egy napilaptól, mert a lap olyan cikket közölt, amely arról tudósított, hogy a felperes HIV-pozitív beteg. Ezt az információt a helyi kórház orvosai állítólag megerősítették. Az EJEB vélekedése szerint a szóban forgó cikk nem járult hozzá közérdekű vitához, és az EJEB ismételten rámutatott, hogy a személyes adatok – nem csupán az egészségügyi adatok –védelme alapvető jelentőségű a személy magán- és családi élete tiszteletben tartásához való joga szempontjából, amit az EJEE 8. cikke biztosít. A Bíróság különös jelentőséget tulajdonít annak, hogy az újságban szereplő tudósítás szerint a kórházi személyzet tájékoztatást nyújtott a felperes HIV-fertőzéséről, ami nyilvánvalóan sérti az orvosi titoktartási kötelezettséget. Az állam tehát nem biztosította a felperes magánélete tiszteletben tartásához való jogát. A Bíróság arra a következtetésre jutott, hogy megsértették a 8. cikket.

1.2.2. Dokumentumokhoz való hozzáférés

A Charta 11. cikke és az EJEE 10. cikke szerinti tájékozódási szabadság nem csak az információk átadásához, hanem *átvételéhez* való jogot is oltalomban részesíti. A demokratikus társadalom működése szempontjából egyre inkább felismerik a kormányzat átláthatóságának fontosságát. Az elmúlt két évtizedben a hatóságoknál lévő okiratokhoz való hozzáférést minden uniós polgár, valamint a tagállamokban tartózkodó vagy székhellyel rendelkező bármely természetes vagy jogi személy fontos jogának ismerték el.

31 EJEB, *Biriuk kontra Litvánia* ügy: 23373/03, 2008. november 25.

Az Európa Tanács joga szerint a hivatalos dokumentumokhoz való hozzáférésre vonatkozó ajánlásban szereplő elvekre is hivatkozni lehet, amely ajánlás a hivatalos dokumentumokhoz való hozzáférésről szóló egyezmény (*205. egyezmény*) szövegezőire is hatással volt.[32] **Az uniós jog szerint** a dokumentumokhoz való hozzáférés jogát az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló 1049/2001/EK rendelet *(a dokumentumokhoz való hozzáférésről szóló rendelet)* garantálja.[33] A Charta 42. cikke és az EUMSZ 15. cikkének (3) bekezdése „az Unió intézményeinek, szerveinek és hivatalainak dokumentumaira" is kiterjesztette ezt a hozzáférési jogot, „függetlenül azok megjelenési formájától". A Charta 52. cikke (2) bekezdésével összhangban a dokumentumokhoz való hozzáférési jogot olyan körülmények és határok között is gyakorolják, amelyeket az EUMSZ 15. cikkének (3) bekezdése előír. E jog ütközhet az adatvédelmi joggal, ha egy dokumentumhoz való hozzáférés mások személyes adatait felfedné. Ezért a hatóságok által kezelt dokumentumokhoz vagy információkhoz való hozzáférés iránti kérelmek elbírálásakor meg kell teremteni az egyensúlyt a hozzáférési jog és azon személyek adatvédelemhez való joga között, akiknek adatait a kért dokumentumok tartalmazzák.

Példa: A *Bizottság kontra Bavarian Lager* ügyben[34] az EUB az uniós intézmények dokumentumaihoz való hozzáféréssel összefüggésben meghatározta a személyes adatok védelmének terjedelmét, továbbá az 1049/2001/EK rendelet (*dokumentumokhoz való hozzáférésről szóló rendelet*) és a 45/2001/EK rendelet (*adatvédelmi rendelet*) közötti viszonyt. Az 1992-ben alapított Bavarian Lager üveges német sört importál az Egyesült Királyságba, elsősorban vendéglőkbe és bárokba. A cég azonban nehézségekkel találta szemben magát, mert a brit jogszabályok ténylegesen előnyben részesítették a nemzeti termelőket. A Bavarian Lager panaszára válaszul az Európai Bizottság úgy döntött, hogy eljárást indít az Egyesült Királyság ellen kötelezettségszegés miatt, aminek eredményeként az Egyesült Királyság módosította és az uniós joghoz igazította a vitatott rendelkezéseket. Ezt követően a Bavarian Lager – más dokumentumok mellett – a Bizottság, a brit hatóságok és a *Confédération des Brasseurs*

32 Az Európa Tanács Miniszteri Bizottsága (2002), 2002/2. sz. ajánlás a tagállamoknak a hivatalos dokumentumokhoz való hozzáférésről, 2002. február 21.; Európa Tanács, Egyezmény a hivatalos dokumentumokhoz való hozzáférésről, CETS 205., 2009. június 18. Az egyezmény még nem lépett hatályba.

33 Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. május 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről, HL L 145., 2001.

34 EUB, C-28/08 P. sz. *Európai Bizottság kontra The Bavarian Lager Co. Ltd ügy*, 2010. június 29., 60., 63., 76., 78. és 79. pont.

du Marché Commun (CBMC) képviselői részvételével tartott ülés jegyzőkönyvének másolatát kérte a Bizottságtól. A Bizottság beleegyezett az üléssel kapcsolatos egyes dokumentumok közzétételébe, de a jegyzőkönyvben szereplő öt nevet kitakarta – ketten közülük kifejezetten tiltakoztak személyazonosságuk felfedése ellen, három másik személyt pedig a Bizottság nem tudott elérni. A Bizottság 2004. március 18-i döntésével elutasította a Bavarian Lager újabb, az ülés teljes jegyzőkönyvének kiadására vonatkozó kérelmét, konkrét hivatkozással a szóban forgó személyeknek az adatvédelmi rendeletben biztosított, a magánélet védelméhez való jogára. Mivel a Bavarian Lager nem volt elégedett ezzel az állásponttal, keresetet indított az Elsőfokú Bíróságon, amely hatályon kívül helyezte a Bizottság 2007. november 8-i határozatát (T-194/04. sz. *Bavarian Lager kontra Bizottság* ügy), figyelemmel különösen arra, hogy a szóban forgó személyek nevének azon személyek listáján való puszta feltüntetése, akik az általuk képviselt szervezet nevében vettek részt az ülésen, nem tette tönkre a magánéletet, és semmiféle veszélyt nem jelentett az érintett személyek magánéletére.

A Bizottság fellebbezése nyomán az EUB hatályon kívül helyezte az Elsőfokú Bíróság ítéletét. Az EUB megállapította, hogy a dokumentumokhoz való hozzáférésről szóló rendelet „egyedi és megerősített védelmi rendszert hoz létre azon személyek vonatkozásában, akiknek a személyes adatai adott esetben nyilvánosan hozzáférhetővé tehetők". Az EUB szerint, amennyiben a dokumentumokhoz való hozzáférésről szóló rendeleten alapuló kérelem célja személyes adatokat tartalmazó dokumentumokhoz való hozzáférés, az adatvédelmi rendelet rendelkezései teljes mértékben alkalmazandóvá válnak. Az EUB ezt követően arra a következtetésre jutott, hogy a Bizottság helyesen utasította el az 1996. októberi ülés teljes jegyzőkönyvéhez való hozzáférés iránti kérelmet. Az ülésen részt vevő öt személy hozzájárulásának hiányában a Bizottság kellően eleget tett a nyíltságra vonatkozó kötelezettségének azáltal, hogy a dokumentum szóban forgó változatában áthúzta az öt nevet.

Ezenfelül az EUB szerint „mivel a Bavarian Lager nem terjesztett elő semmilyen kifejezett és törvényes célt, illetve meggyőző érvet e személyes adatok továbbításának szükségességét alátámasztandó, a Bizottság nem tudta az érintett felek különböző érdekeit mérlegelni. Nem tudta azt ellenőrizni, hogy nincs semmilyen ok annak feltételezésére, hogy e továbbítás sértené az érintettek jogos érdekeit", amint azt az adatvédelmi rendelet előírja.

Ezen ítélet szerint a dokumentumokhoz való hozzáférés vonatkozásában az adatvédelmi jogba való beavatkozáshoz konkrét és alapos indok szükséges. A dokumentumokhoz való hozzáférés joga nem részesülhet automatikusan előnyben az adatvédelemhez való joggal szemben.[35]

Az EJEB alábbi ítélete a hozzáférés iránti kérelem egy konkrét szempontjával foglalkozott:

Példa: A *Társaság a Szabadságjogokért kontra Magyarország* ügyben[36] a felperes, egy emberi jogi civil szervezet, egy folyamatban lévő üggyel kapcsolatos információkhoz kért hozzáférést az Alkotmánybíróságtól. Az Alkotmánybíróság – anélkül, hogy konzultált volna az ügyet az Alkotmánybíróság elé terjesztő országgyűlési képviselővel – elutasította a hozzáférés iránti kérelmet azon a címen, hogy előtte fekvő beadványokat külső személyek részére kizárólag a panaszos jóváhagyásával tehet hozzáférhetővé. A nemzeti bíróságok helybenhagyták az elutasítást azzal az indoklással, hogy a szóban forgó személyes adatok védelmét más jogos érdek, köztük a nyilvános információkhoz való hozzáférés, nem írhatja felül. A felperes „társadalmi megfigyelőként" járt el, akinek tevékenysége a sajtónak kijáró védelemhez hasonló védelmet indokol. A sajtószabadsággal kapcsolatban az EJEB következetesen azt az álláspontot képviselte, hogy a nagyközönségnek joga van megtudni a közérdeklődésre számot tartó információkat. A felperes által kért információk „készen álltak és elérhetők voltak", semmiféle adatgyűjtést nem igényeltek. Ilyen körülmények között az állam nem akadályozhatja a felperes által kért információáramlást. Összegezve az EJEB úgy vélte, hogy a közérdekű információkhoz való hozzáférés akadályozása gátolhatja a médiában vagy az ehhez kapcsolódó területeken dolgozókat abban, hogy ellássák a „nyilvános megfigyelő" létfontosságú szerepét. A Bíróság arra a következtetésre jutott, hogy megsértették a 10. cikket.

Az uniós jog határozottan megállapítja az átláthatóság fontosságát. Az átláthatóság elve szerepel az EUSZ 1. és 10. cikkében, valamint az EUMSZ 15. cikke (1)

35 Lásd azonban az európai adatvédelmi biztos *„Nyilvános hozzáférés személyes adatokat tartalmazó dokumentumokhoz a Bavarian Lager ügyben hozott ítélet után"* című, 2011-es tanulmányában (Brüsszel, 2011. március 24.) található részletes megfontolásokat, amely a következő címen érhető el: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 EJEB, *Társaság a Szabadságjogokért kontra Magyarország* (37374/05), 2009. április 14., 27., 36–38. pont.

bekezdésében.[37] Az 1049/2001/EK rendelet (2) preambulumbekezdése szerint az átláthatóság lehetővé teszi a polgárok számára, hogy még inkább részt vegyenek a döntéshozatali eljárásban, és biztosítja a polgárok irányában a közigazgatás nagyobb legitimációját, hatékonyságát és felelősségét a demokratikus rendszerben.[38]

Ezen indokolást követve a közös agrárpolitika finanszírozásáról szóló 1290/2005/EK tanácsi rendelet és az e rendelet alkalmazása részletes szabályainak megállapításáról szóló 259/2008/EK bizottsági rendelet kötelezővé teszi a mezőgazdasági ágazatban egyes uniós alapok kedvezményezettjeire vonatkozó információk és kedvezményezettként a kapott összegek közzétételét.[39] A közzétételnek hozzá kell járulnia a közpénzek közigazgatás általi megfelelő felhasználásának nyilvános ellenőrzéséhez. A közzététel arányosságát számos kedvezményezett vitatta.

Példa: A *Volker és Markus Schecke és Hartmut Eifert kontra Land Hessen* ügyben[40] az EUB-nak azt kellett megítélnie, hogy az uniós mezőgazdasági támogatások kedvezményezettjei nevének és az általuk kapott összegeknek – az uniós jogszabályok által előírt – közzététele arányos-e.

A Bíróság – azzal a megjegyzéssel, hogy az adatvédelemhez való jog nem abszolút – úgy érvelt, hogy két uniós mezőgazdasági támogatási alap kedvezményezettjei nevének és az általuk kapott pontos összegeknek egy internetes oldalon való közzététele általánosságban beavatkozást jelent e személyek magánéletébe, konkrétan pedig sérti személyes adataik védelmét.

A Bíróság megítélése szerint a Charta 7. és 8. cikkének szóban forgó megsértését jogszabály írta elő, a rendelkezés pedig az EU által elismert közérdekű célt szolgálta, azaz többek között a közösségi alapok felhasználása átláthatóságának

37 EU (2012), Az Európai Unióról szóló szerződés és az EUMSZ egységes szerkezetbe foglalt változata, HL C 326., 2012.

38 EUB, C-41/00 P. sz. *Interporc Im- und Export GmbH kontra az Európai Közösségek Bizottsága ügy*, 2003. március 6., 39. pont; valamint EUB, C-28/08 P. sz. *Európai Bizottság kontra The Bavarian Lager Co. Ltd.*, 2010. június 29., 54. pont.

39 A Tanács 1290/2005/EK rendelete (2005. június 21.) a közös agrárpolitika finanszírozásáról, HL L 209., 2005; valamint A Bizottság 259/2008/EK rendelete (2008. március 18.) az 1290/2005/EK tanácsi rendeletnek az Európai Mezőgazdasági Garanciaalapból (EMGA) és az Európai Mezőgazdasági Vidékfejlesztési Alapból (EMVA) származó pénzeszközök kedvezményezettjeire vonatkozó információk nyilvánosságra hozatalának tekintetében történő alkalmazása részletes szabályainak megállapításáról, HL L 76., 2008.

40 EUB, C-92/09. és C-93/09. sz., *Volker és Markus Schecke GbR (C-92/09) és Hartmut Eifert (C-93/09) kontra Land Hessen* egyesített ügyek, 2010. november 9., 47–52., 58., 66–67., 75., 86. és 92. pont.

fokozását. Az EUB mindazonáltal megállapította, hogy a szóban forgó két alapból uniós mezőgazdasági támogatásban részesült kedvezményezett természetes személyek nevének és az általuk kapott pontos összegeknek a közzététele aránytalan intézkedés volt, ami – figyelemmel a Charta 52. cikkének (1) bekezdésére – nem volt indokolt. Ezért a Bíróság az európai mezőgazdasági alapok kedvezményezettjeire vonatkozó információk nyilvánosságra hozataláról szóló uniós jogszabályt részlegesen érvénytelennek nyilvánította.

1.2.3. A művészet és a tudomány szabadsága

Egy másik jog, amelynek esetében meg kell teremteni az egyensúlyt a magánélet tiszteletben tartásához és az adatvédelemhez való joggal szemben, a művészet és a tudomány szabadsága, amelyet a Charta 13. cikke kifejezetten oltalomban részesít. E jog elsősorban a gondolatszabadságból, valamint a véleménynyilvánítás szabadságából származik, és a Charta 1. cikkének (Az emberi méltóság) tiszteletben tartásával gyakorolható. Az EJEB úgy véli, a művészet szabadságát az EJEE 10. cikke oltalomban részesíti.[41] A Charta 13. cikkében biztosított jog az EJEE 10. cikke által megengedett korlátozásoknak vethető alá.[42]

Példa: A *Vereinigung bildender Künstler kontra Ausztria* ügyben[43] az osztrák bíróságok eltiltották a felperes szervezetet egy festmény további kiállításától, amely szexuális helyzetben ábrázol alakokat, akiknek az arcát különböző közszereplőkről készült fotókkal helyettesítették. Egy osztrák parlamenti képviselő, akinek a fényképét felhasználták a festményen, eljárást indított a felperes szervezet ellen, és a festmény kiállítását megtiltó végzés kiadását kérte. A hazai bíróság a kérelemnek helyt adó végzést bocsátott ki. Az EJEB ismételten rámutatott, hogy az EJEE 10. cikke olyan gondolatok közlésére is alkalmazható, amelyek az államot vagy a lakosság bármely csoportját sértik, megbotránkoztatják vagy zavarják. Az alkotást létrehozó, előadó, terjesztő vagy kiállító személyek hozzájárultak a gondolatok és vélemények cseréjéhez, és az államot az a kötelesség terhelte, hogy indokolatlanul ne csorbítsa a véleménynyilvánítás szabadságát. Figyelemmel arra, hogy a festmény kollázs volt, amely csupán személyek portréját ábrázoló fényképeket használt fel, a testeket pedig irreális, túlzó módon festették meg, amely nyilván nem a valóságra utalt, illetve nyilván nem

41 EJEB, *Müller és társai kontra Svájc* (10737/84), 1988. május 24.

42 Magyarázatok az EU Alapjogi Chartájához, HL C 303., 2007.

43 EJEB, *Vereinigung bildender Künstler kontra Ausztria* (68345/01), 2007. január 25., lásd különösen a 26. és 34. pontot.

azt kívánta sugallni, az EJEB azt is megállapította, hogy „a festmény aligha értelmezhető úgy, hogy a megfestett személyek magánéletének részleteivel foglalkozik, inkább nyilvános politikusi szerepükre utal", és „[az ábrázolt személynek] e minőségében nagyobb türelmet kell tanúsítania a kritikával szemben". A szóban forgó különböző érdekeket mérlegelve az EJEB megállapította, hogy a festmény további kiállításának korlátlan betiltása aránytalan. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 10. cikkét.

Ami a tudományt illeti, az európai adatvédelmi jog tisztában van a tudomány társadalomban betöltött különleges értékével. Ezért a személyes adatok felhasználásának általános korlátozásait mérsékeli. Mind az adatvédelmi irányelv, mind a 108. egyezmény akkor is engedélyezi az adatok tudományos kutatás céljából való megőrzését, ha az adatok az adatgyűjtés eredeti céljára már nem szükségesek. Ezen kívül a személyes adatok tudományos kutatás céljára való későbbi felhasználása nem minősül összeférhetetlen célnak. A részletesebb rendelkezések, többek között a szükséges biztosítékok kidolgozása a nemzeti jog feladata; a cél a tudományos kutatáshoz fűződő érdek összeegyeztetése az adatvédelemhez való joggal (lásd még a 3.3.3 és a 8.4 szakaszt).

1.2.4. A tulajdon védelme

A tulajdon védelméhez fűződő jogot az EJEE első kiegészítő jegyzőkönyvének 1. cikke, valamint a Charta 17. cikkének (1) bekezdése is tartalmazza. A tulajdon védelméhez fűződő jog egyik fontos vonatkozása a szellemi tulajdon védelme, amelyet a Charta 17. cikkének (2) bekezdése kifejezetten megemlít. Az EU jogrendje számos olyan irányelvet tartalmaz, amely a szellemi tulajdon, különösen a szerzői jog hatékony védelmére irányul. A szellemi tulajdon körébe nemcsak az irodalmi és művészeti tulajdon, hanem a szabadalom, a védjegy és a szomszédos jogok is beletartoznak.

Ahogyan az EUB ítélkezési gyakorlata *már* világossá tette, egyensúlyt kell teremteni különösen a tulajdonhoz való alapvető jog védelme és az adatvédelemhez való jog között.[44] Voltak olyan ügyek, amelyekben szerzői jogvédő szervezetek azt követelték, hogy internetszolgáltatók fedjék fel az internetes fájlmegosztó platformok felhasználóinak személyazonosságát. Az ilyen platformok gyakran lehetővé teszik, hogy internethasználók zenei fájlokat töltsenek le ingyenesen annak ellenére, hogy ezek a címek szerzői jogilag védettek.

44 EJEB, *Ashby Donald és mások kontra Franciaország* (36769/08), 2013. január 10.

Példa: A *Promusicae kontra Telefónica de España* ügy[45] tárgya szerint a Telefónica spanyol internetszolgáltató megtagadta, hogy kiadja a zenei producereket, valamint zenei és audiofelvételek kiadóit tömörítő, Promusicae nonprofit szervezetnek bizonyos olyan személyek személyes adatait, akik számára internethozzáférést biztosított. A Promusicae azért kérte az információk átadását, hogy polgári jogi eljárást indíthasson a szóban forgó személyek ellen, mert állítása szerint fájlcsereprogramot használtak, amely olyan hangfelvételekhez biztosít hozzáférést, amelyek hasznosítási jogai a Promusicae-tagokat illetik.

A spanyol bíróság az EUB elé utalta az ügyet, azt a kérdést felvetve, hogy a hatékony szerzői jogi védelem biztosítása érdekében a szóban forgó személyes adatokat a közösségi jog szerint – a polgári jogi eljárással összefüggésben – közölni kell-e. Hivatkozott a 2000/31/EK, a 2001/29/EK és a 2004/48/EK irányelvre – a Charta 17. és 47. cikkének figyelembevételével is értelmezve. A Bíróság arra a következtetésre jutott, hogy e három irányelv – az elektronikus hírközlési adatvédelmi irányelvvel (2002/58/EK irányelv) kiegészítve – nem zárja ki, hogy a tagállamok polgári jogi eljárással összefüggésben – a hatékony szerzői jogi védelem biztosítása céljából – személyes adatok közlésére vonatkozó kötelezettséget írjanak elő.

Az EUB rámutatott, hogy az ügy tehát azt a kérdést veti fel, hogy egyeztetni kell-e a különböző alapvető jogok – azaz a magánélet tiszteletben tartásához való jog, illetve a tulajdon védelméhez és a hatékony jogorvoslathoz való jog – védelmére vonatkozó követelményeket.

A Bíróság arra a következtetésre jutott, hogy „a tagállamoknak a fent említett irányelvek átültetése során ezek olyan értelmezésére kell támaszkodniuk, mely lehetővé teszi a közösségi jogrend által védett különböző alapvető jogok megfelelő egyensúlyának a biztosítását. Továbbá az említett irányelvek átültetésére vonatkozó intézkedések végrehajtása során a tagállami hatóságoknak és bíróságoknak nemcsak az a kötelessége, hogy nemzeti jogukat az utóbbiakkal összhangban értelmezzék, hanem az is, hogy ne támaszkodjanak ezen irányelvek olyan értelmezésére, amely sérti az alapvető jogokat vagy a közösségi jog egyéb általános elveit, úgymint az arányosság elvét.”[46]

45 EUB, C-275/06. sz. *Productores de Música de España (Promusicae) kontra Telefónica de España SAU ügy*, 2008. január 29., 54. és 60. pont.

46 *Uo.*, 65. és 68. pont; lásd még: EUB, C-360/10. sz. *SABAM kontra Netlog N.V.*, 2012. február 16.

2 Adatvédelmi terminológia

EU	Tárgyalt kérdések	Európa Tanács
Személyes adatok		
Adatvédelmi irányelv, 2. cikk, a) pont EUB, C-92/09. és C-93/09. sz., *Volker és Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* egyesített ügyek, 2010. november 9. EUB, C-275/06. sz., *Productores de Música de España (Promusicae) kontra Telefónica de España SAU ügy*, 2008. január 29.	Jogi fogalommeghatározás	108. egyezmény, 2. cikk, a) pont EJEB, *Bernh Larsen Holding AS és társai kontra Norvégia* (24117/08), 2013. március 14.
Adatvédelmi irányelv, 8. cikk, (1) bekezdés EUB, C-101/01. sz. *Bodil Lindqvist ügy*, 2003. november 6.	Személyes adatok különleges kategóriái (érzékeny adatok)	108. egyezmény, 6. cikk
Adatvédelmi irányelv, 6. cikk, (1) bekezdés, e) pont	Névtelenné tett és álnéven kezelt adatok	108. egyezmény, 5. cikk, e) pont 108. egyezmény, Magyarázó jelentés, 42. cikk
Adatok feldolgozása		
Adatvédelmi irányelv, 2. cikk, b) pont EUB, C-101/01. sz. *Bodil Lindqvist ügy*, 2003. november 6.	Fogalommeghatározások	108. egyezmény, 2. cikk, c) pont
Az adatok felhasználói		
Adatvédelmi irányelv, 2. cikk, d) pont	Adatkezelő	108. egyezmény, 2. cikk, d) pont A profilalkotásra vonatkozó ajánlás, 1. cikk, g) pont*

EU	Tárgyalt kérdések	Európa Tanács
Adatvédelmi irányelv, 2. cikk, e) pont EUB, C-101/01. sz. *Bodil Lindqvist ügy*, 2003. november 6.	**Adatfeldolgozó**	Profilalkotási ajánlás, 1. cikk, h) pont
Adatvédelmi irányelv, 2. cikk, g) pont	**Címzett**	108. egyezmény, Kiegészítő jegyzőkönyv, 2. cikk, (1) bekezdés
Adatvédelmi irányelv, 2. cikk, f) pont	**Harmadik fél**	
Hozzájárulás		
Adatvédelmi irányelv, 2. cikk, h) pont EUB, C-543/09. sz., *Deutsche Telekom AG kontra Bundesrepublik Deutschland* ügy, 2011. május 5.	**Az érvényes hozzájárulás fogalmának meghatározása és a rá vonatkozó követelmények**	Orvosi adatokra vonatkozó ajánlás, 6. cikk, valamint különböző későbbi ajánlások

*Megjegyzés: *Az Európa Tanács Miniszteri Bizottságának Rec(2010)13. sz., 2010. november 23-i ajánlása a tagállamok részére az egyéneknek a profilalkotás összefüggésében a személyes adatok automatikus feldolgozásával kapcsolatos védelméről (Profilalkotási ajánlás)*

2.1. Személyes adatok

Főbb pontok

- Az adatok akkor minősülnek személyes adatnak, ha azonosított vagy legalább azonosítható természetes személyre, az érintettre vonatkoznak.
- A személy akkor azonosítható, ha túlzott erőfeszítés nélkül olyan kiegészítő információk nyerhetők róla, amelyek lehetővé teszik azonosítását.
- A hitelesítés annak bizonyítását jelenti, hogy egy bizonyos személy egy bizonyos személyazonossággal és/vagy bizonyos tevékenységek folytatására vonatkozó engedéllyel rendelkezik.
- Vannak olyan, a 108. egyezményben és az adatvédelmi irányelvben felsorolt különleges adatkategóriák, az úgynevezett érzékeny adatok, amelyek fokozott védelmet igényelnek, ezért különleges jogi szabályozás vonatkozik rájuk.
- Az adatok akkor minősülnek anonimizált adatnak, ha már semmiféle azonosítót nem tartalmaznak; akkor minősülnek pszeudoanonimizált kezeltnek, ha az azonosítókat kódolják.
- A pszeudoanonimizált adatok – az anonimizált adatokkal ellentétben – személyes adatnak minősülnek.

2.1.1. A személyes adat fogalmának főbb vonatkozásai

A „személyes adat” fogalmát az **uniós jog** és az **Európa Tanács joga** egyaránt úgy határozza meg, mint azonosított vagy azonosítható természetes személyre vonatkozó információt,[47] azaz olyan személyre vonatkozó információt, akinek személyazonossága vagy nyilvánvalóan egyértelmű, vagy legalább kiegészítő információk beszerzésével megállapítható.

Ha ilyen személlyel kapcsolatos adatok feldolgozására kerül sor, ezt a személyt „érintettnek” nevezik.

A személy

Az adatvédelemhez való jog a magánélet tiszteletben tartásához való jogból fejlődött ki. A magánélet fogalma az emberhez kötődik. Az adatvédelem elsődleges kedvezményezettjei tehát természetes személyek. Ezenfelül a 29. cikk szerinti munkacsoport szerint az európai adatvédelmi jog csupán az *élő személyeket* részesíti oltalomban.[48]

Az EJEB az EJEE 8. cikkével kapcsolatos ítélkezési gyakorlatának tanúsága szerint előfordulhat, hogy a magán- és a szakmai élet kérdései nehezen különíthetők el egymástól.[49]

> Példa: Az *Amann kontra Svájc* ügyben[50] a hatóságok lehallgattak egy, a felpereshez beérkezett üzleti telefonhívást. E telefonhívás alapján a hatóságok nyomoztak a felperes után, és a nemzetbiztonsági személyi nyilvántartásban kitöltöttek egy rá vonatkozó lapot. Bár a lehallgatás üzleti telefonhívást érintett, az EJEB a szóban forgó hívással kapcsolatos adatok tárolását a felperes magánéletével összefüggőnek minősítette. Rámutatott, hogy a „magánélet” fogalma nem értelmezhető korlátozóan, különösen mivel a magánélet tiszteletben tartása a más személyekkel és a külvilággal való kapcsolatok kialakításához és

47 Adatvédelmi irányelv, 2. cikk, a) pont; 108. egyezmény, 2. cikk, a) pont.

48 A 29. cikk szerinti munkacsoport (2007) *4/2007. sz. véleménye a személyes adat fogalmáról*, WP 136, 2007. június 20., 22. o.

49 Lásd például EJEB, *Rotaru kontra Románia* [nagytanács] (28341/95), 2000. május 4., 43. pont; EJEB, *Niemietz kontra Németország (13710/88)*, 1992. december 16., 29. pont.

50 EJEB, *Amann kontra Svájc* [nagytanács] (27798/95), 2000. február 16., 65. pont.

fenntartásához való jogot is magában foglalja. Ezen kívül nem volt olyan elvi ok, amely indokolta volna a szakmai vagy üzleti jellegű tevékenységeknek a „magánélet" fogalmából való kizárását. Ez a tág értelmezés megfelel a 108. egyezmény szerinti értelmezésnek. Az EJEB ezen felül megállapította, hogy a felperes ügyében szereplő beavatkozás nem a jogszabályokkal összhangban történt, mivel a hazai jog nem ír elő konkrét, részletes rendelkezéseket az információk gyűjtésére, rögzítésére és tárolására vonatkozóan. Ezért a bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Továbbá, ha a szakmai élet kérdései is az adatvédelem hatálya alá tartoznak, megkérdőjelezhető, hogy kizárólag természetes személyeket kell-e oltalomban részesíteni. Az EJEE-ben foglalt jogok nem csupán természetes személyek, hanem mindenki számára garantáltak.

Az EJEB-nek van jogi személyek kereseti kérelme ügyében hozott ítélete, amelyet jogi személy adatainak felhasználásával szembeni, az EJEE 8. cikke szerinti védelemhez való jog állítólagos megsértésével kapcsolatban fogadott el. A Bíróság azonban nem a magánélet, hanem a lakás és levelezés tiszteletben tartásához való jog alapján vizsgálta az ügyet.

Példa: A *Bernh Larsen Holding AS és mások kontra Norvégia* ügy[51] három norvég társaság által egy adóhatósági határozattal kapcsolatos panasszal foglalkozott, amely határozat előírta, hogy a nevezett társaságok az általuk közösen használt számítógépes szerveren található összes adatról készítsenek másolatot, és adják át az adóellenőröknek.

Az EJEB megállapította, hogy a felperesi társaságok erre való kötelezése beavatkozás az EJEE 8. cikke értelmében vett „lakás" és „levelezés" tiszteletben tartásához való jogba. A Bíróság megítélése szerint azonban az adóhatóságoknak tényleges és megfelelő biztosítékai voltak a visszaélés elkerülésére: a felperesi társaságokat jó előre értesítették; e társaságok jelen voltak a helyszíni beavatkozás során, és indítványokat tehettek; az adóügyi vizsgálat befejezését követően az anyagot meg akarták semmisíteni. Ilyen körülmények között méltányos egyensúlyt teremtettek egyrészről a felperesi társaságok „lakás" és „levelezés" tiszteletben tartásához való joga és a náluk dolgozó személyek adatainak védelméhez fűződő jog, másrészről az adóellenőrzés céljából végzett

51 EJEB, *Bernh Larsen Holding AS és mások kontra Norvégia* (24117/08), 2013. március 14. Lásd még azonban: EJEB, *Liberty és mások kontra Egyesült Királyság* (58243/00), 2008. július 1.

hatékony szemléhez fűződő közérdek között. A Bíróság arra a következtetésre jutott, hogy nem sértették meg a 8. cikket.

A 108. egyezmény szerint az adatvédelem elsősorban természetes személyek védelmével foglalkozik; a szerződő felek azonban – saját hazai joguk szerint – jogi személyekre, például vállalkozásokra és szervezetekre is kiterjeszthetik az adatvédelem hatályát. Az **európai uniós adatvédelmi jog** általában nem terjed ki jogi személyek védelmére a rájuk vonatkozó adatfeldolgozás tekintetében. A nemzeti jogalkotók szabadon szabályozhatják ezt a kérdést.[52]

Példa: A *Volker és Markus Schecke és Hartmut Eifert kontra Land Hessen* ügyben[53] az EUB a mezőgazdasági támogatás kedvezményezettjeire vonatkozó személyes adatok közzétételére hivatkozva megállapította, hogy „a jogi személyek csak annyiban részesülhetnek az ilyen nevesítéssel szembeni, a Charta 7. és 8. cikke szerinti védelemben, amennyiben a jogi személy hivatalos neve alapján azonosítható egy vagy több természetes személy. ...A magánélethez való jognak a személyes adatok védelméhez való jog tekintetében történő tiszteletben tartása – amelyet a Charta 7. és 8. cikke elismer – az azonosított vagy azonosítható természetes személyre vonatkozó valamennyi információra kiterjed...".[54]

A személy azonosíthatósága

Az **uniós jog** és az **Európa Tanács joga** szerint az információ akkor tartalmaz személyre vonatkozó adatokat, ha:

- az információban a személyt azonosítják; vagy
- ha a személyt, bár nem azonosították, az információ olyan módon írja le, ami további kutatással lehetővé teszi az érintett személyazonosságának megállapítását.

Az európai adatvédelmi jog mindkét típusú információt azonos módon védi. Az EJEB ismételten kimondta, hogy a „személyes adat" EJEE szerinti fogalma azonos a 108.

52 Adatvédelmi irányelv, (24) preambulumbekezdés.

53 EUB, C-92/09. és C-93/09. sz. *Volker és Markus Schecke GbR (C-92/09) és Hartmut Eifert kontra Land Hessen (C-93/09)* egyesített ügyek, 2010. november 9., 53. pont.

54 *Uo.*, 52. pont.

egyezményben szereplő fogalommal, különösen ami az azonosított vagy azonosítható személyekre vonatkozó feltételt illeti.[55]

A személyes adat jogi fogalommeghatározásai nem pontosítják, hogy egy személy mikor minősül azonosítottnak.[56] Az azonosításhoz kétségtelenül olyan elemek szükségesek, amelyek úgy írnak le egy személyt, hogy a személy minden más személytől megkülönböztethető és egyénként felismerhető legyen. Az ilyen leíró elemre a legjobb példa a személy neve. Kivételes esetekben más azonosítók a személy nevével azonos hatásúak lehetnek. Közszereplők esetében elegendő lehet a személy által betöltött tisztség – pl. az Európai Bizottság elnöke – említése.

Példa: A *Promusicae* ügyben[57] az EUB megállapította, hogy „nem vitatott, hogy [egy bizonyos internetes fájlmegosztó platform] meghatározott használói nevének és címének Promusicae által kért közlése személyes adatok, vagyis – a 95/46 irányelv 2. cikke a) pontja fogalom meghatározásának megfelelően – azonosított vagy azonosítható természetes személyre vonatkozó információk rendelkezésre bocsátásának minősül[…]. A Promusicae szerint a Telefónica által tárolt – amelyet ez utóbbi nem vitatott – információk e közlése személyes adatok feldolgozásának minősül a 95/46 irányelv 2. cikkének b) pontjával összefüggésben olvasott 2002/58 irányelv 2. cikkének első albekezdése értelmében."

Mivel sok név nem egyedi, a személyazonosság megállapításához további azonosító adatokra is szükség lehet annak biztosításához hogy a személyt nem tévesztik össze más személlyel. A születési időt és helyet gyakran használják erre a célra. Ezenfelül egyes országokban – a polgárok jobb megkülönböztethetősége érdekében – személyi azonosítószámokat is bevezettek. A biometrikus adatok, köztük az ujjlenyomatok, a digitális fényképek vagy az íriszfelismerés a technológia korában egyre nagyobb szerepet kapnak a személyek azonosítása terén.

Az európai adatvédelmi jog alkalmazhatóságához azonban nincs szükség az érintett kiváló minőségű azonosítására; elegendő, ha az érintett személy azonosítható. A személy akkor minősül azonosíthatónak, ha egy információ olyan azonosító elemeket tartalmaz, amelyeken keresztül a személy közvetlen vagy közvetett módon

55 Lásd EJEB, *Amann kontra Svájc* [nagytanács] (27798/95), 2000. február 16., 65. és további pontok.

56 Lásd még EJEB, *Odièvre kontra Franciaország* [nagytanács] (42326/98), 2003. február 13.; valamint EJEB, *Godelli kontra Olaszország (33783/09)*, 2012. szeptember 25.

57 EUB, C-275/06. sz., *Productores de Música de España (Promusicae) kontra Telefónica de España SAU ügy*, 2008. január 29., 45. pont.

azonosítható.[58] Az adatvédelmi irányelv (26) preambulumbekezdése szerint az a döntő, hogy az információ felhasználói számára rendelkezésre állnak-e hasznos eszközök az azonosításhoz, és ezen eszközöket a szóban forgó felhasználók valószínűleg felhasználják-e e célra; a címzett harmadik felek is ebbe a körbe tartoznak (lásd a 2.3.2 szakaszt).

Példa: Egy helyi hatóság elhatározta, hogy adatokat gyűjt a helyi utcákon gyorshajtást elkövető autókról. Lefényképezi a gépkocsikat, automatikusan rögzítve az időt és a helyet annak érdekében, hogy az adatokat az illetékes hatóságnak továbbítsa, hogy ez utóbbi hatóság megbüntethesse a sebességhatárt túllépő személyeket. Egy érintett panaszt nyújt be azzal, hogy a helyi hatóságnak az adatvédelmi törvény értelmében nem volt jogalapja az ilyen adatgyűjtésre. A helyi hatóság fenntartja, hogy nem gyűjt személyes adatokat. Álláspontja szerint a rendszámtáblák anonim személyekre vonatkozó adatok. A helyi hatóságnak nincs hozzáférési engedélye az általános gépjármű-nyilvántartáshoz, amelyből kideríthetné a gépjármű tulajdonosának vagy vezetőjének kilétét.

Ez az indokolás nem áll összhangban az adatvédelmi irányelv (26) preambulumbekezdésével. Figyelemmel arra, hogy az adatgyűjtés célja egyértelműen a gyorshajtók azonosítása, várható, hogy megkísérlik az azonosítást. Bár a helyi hatóságok nem rendelkeznek az azonosításra alkalmas közvetlen eszközökkel, továbbítják az adatokat az illetékes hatóságnak, a rendőrségnek, amelynek viszont vannak ilyen eszközei. A (26) preambulumbekezdés is kifejezetten tartalmaz olyan forgatókönyvet, mely szerint valószínű, hogy az adatok közvetlen felhasználójától eltérő további címzettek megkísérlik a személy azonosítását. A (26) preambulumbekezdés figyelembevételével a helyi hatóság intézkedése kimeríti az azonosítható személyekről való adatgyűjtés fogalmát, ezért az adatvédelmi törvény szerint jogalap szükséges hozzá.

Az **Európa Tanács joga** szerint az azonosíthatóságot is ehhez hasonlóan kell értelmezni. A fizetési adatokra vonatkozó ajánlás[59] 1. cikkének (2) bekezdése például kimondja, hogy a személy nem minősül „azonosíthatónak”, ha az azonosítás túl hosszú időt vesz igénybe, illetve túlságosan nagy költséggel vagy munkával jár.

58 Adatvédelmi irányelv, 2. cikk, a) pont.

59 Európa Tanács Miniszteri Bizottsága (1990) (90)19. sz. ajánlása a fizetéshez és más kapcsolódó műveletekhez használt személyes adatok védelméről, 1990. szeptember 13.

Hitelesítés

A hitelesítés olyan eljárás, amellyel a személy bizonyítani tudja személyazonosságát és/vagy azt, hogy engedéllyel rendelkezik bizonyos dolgokra, pl. egy biztonsági területre való belépésre vagy egy bankszámláról pénz kivételére. A hitelesítés történhet biometrikus adatoknak – pl. az útlevélben található fényképnek vagy ujjlenyomatnak – a személy által például idegenrendészeti ellenőrzés során önmagáról állított adatokkal való összevetésével; vagy olyan információkra való rákérdezéssel, amelyeket csak egy bizonyos személy vagy egy bizonyos engedéllyel rendelkező személy tudhat, például személyi azonosítószám (PIN) vagy jelszó; vagy egy bizonyos jelzés bemutatásának kérésével, amely kizárólag egy bizonyos személyazonosságú személy vagy egy bizonyos engedéllyel rendelkező személy birtokában lehet – ilyen például a speciális chipkártya vagy banki széfkulcs. A jelszón és a chipkártyán kívül – egyes esetekben a PIN-kóddal együtt – az elektronikus aláírás is a személy azonosítására és hitelesítésére alkalmas eszköz lehet az elektronikus kommunikáció során.

Az adatok jellege

Mindenfajta információ személyes adat lehet, amennyiben személyre vonatkozik.

> Példa: A felettesnek a munkavállaló munkateljesítményéről leírt, a munkavállaló személyzeti dossziéjában tárolt értékelése a munkavállalóra vonatkozó személyes adat akkor is, ha adott esetben teljes egészében vagy részben a felettes személyes véleményét tükrözi, mint például: „a munkavállaló nem végzi odaadással a munkáját", és nem tartalmaz konkrétumokat, mint például: „a munkavállaló az elmúlt hat hónapban öt hetet hiányzott".

A személyes adatok körébe a személy magánéletére, valamint szakmai vagy közéleti tevékenységére vonatkozó információk tartoznak.

Az *Amann* ügyben[60] az EJEB a „személyes adat" fogalmát úgy értelmezte, hogy az nem korlátozódik csupán az egyén magánszférájába tartozó dolgokra (lásd a 2.1.1 szakaszt). A „személyes adat" fogalmának ilyen értelmezése az adatvédelmi irányelv esetében is igaz:

60 Lásd EJEB, *Amann kontra Svájc* (27798/95), 2000. február 16., 65. pont.

Példa: A *Volker és Markus Schecke és Hartmut Eifert kontra Land Hessen* ügyben[61] az EUB megállapította, hogy „e tekintetben nincs jelentősége annak a ténynek, hogy a közzétett adatok szakmai tevékenységre vonatkoznak[...]. E tekintetben az Emberi Jogok Európai Bírósága az EJEE 8. cikkének értelmezésére vonatkozóan kimondta, hogy a „magánélet" fogalmát nem lehet megszorítóan értelmezni, és semmiféle elv nem teszi lehetővé a szakmai [...] tevékenységek »magánélet« fogalmából való kizárását".

Az adatok akkor is személyekre vonatkoznak, ha az információ tartalma közvetve fed fel adatokat egy személyről. Egyes esetekben, amikor szoros kapcsolat áll fenn egy tárgy vagy esemény – pl. egyfelől egy mobiltelefon, autó, baleset –, másfelől pedig egy személy (pl. az előbbiek tulajdonosa, használója vagy áldozata) között, a tárgyra vagy eseményre vonatkozó információt is személyes adatnak kell tekinteni.

Példa: Az *Uzun kontra Németország* ügyben[62] a felperest és egy másik férfit egy globális helymeghatározó rendszerhez (GPS) kapcsolódó, a másik férfi gépkocsijába szerelt eszközön keresztül megfigyelés alá helyezték, mert bombatámadásban való részvétellel gyanúsították őket. Ebben az ügyben az EJEB megállapította, hogy a felperes GPS-en keresztül történt megfigyelése kimeríti az EJEE 8. cikke által védett, a magánélethez való jog megsértését. A GPS-megfigyelés azonban a jogszabályokkal összhangban történt, továbbá arányos volt a jogszerű céllal – többrendbeli emberölési kísérletekkel kapcsolatos nyomozással –, ennélfogva szükséges intézkedés volt a demokratikus társadalomban. A bíróság arra a következtetésre jutott, hogy nem sértették meg az EJEE 8. cikkét.

Az adatok megjelenési formája

A személyes adatok tárolásának vagy felhasználásának formája az adatvédelmi jogszabályok alkalmazhatósága szempontjából nem releváns. Személyes adatokat és képeket írásbeli vagy szóbeli kommunikáció egyaránt tartalmazhat,[63] a zártláncú

61 C-92/09. és C-93/09. sz. *Volker és Markus Schecke GbR (C-92/09) és Hartmut Eifert kontra Land Hessen (C-93/09)* egyesített ügyek, 2010. november 9., 59. pont.

62 EJEB, *Uzun kontra Németország* (35623/05), 2010. szeptember 2.

63 EJEB, *Von Hannover kontra Németország* (59320/00), 2004. június 24.; EJEB, *Sciacca kontra Olaszország* (50774/99), 2005. január 11.

televíziós (CCTV) felvételeket[64] vagy hangfelvételeket is beleértve.[65] Az elektronikusan rögzített információ és a nyomtatott formátumú információ is lehet személyes adat; még emberi szövetből származó sejtminták is lehetnek személyes adatok, mivel egy adott személy DNS-ét rögzítik.

2.1.2. Személyes adatok különleges kategóriái

Az **uniós jogban** és az **Európa Tanács jogában** is vannak olyan különleges személyesadat-kategóriák, amelyek feldolgozásuk esetén – jellegüknél fogva – veszélyt jelenthetnek az érintettre nézve, ezért fokozott védelmet igényelnek. Ezért e különleges adatkategóriák („érzékeny adatok") feldolgozását kizárólag egyedi biztosítékokkal szabad engedélyezni.

Az érzékeny adatok fogalmának meghatározásával kapcsolatban a 108. egyezmény (6. cikk) és az adatvédelmi irányelv (8. cikk) egyaránt a következő kategóriákat nevezi meg:

- faji vagy etnikai hovatartozásra vonatkozó személyes adatok;
- politikai véleményre, vallási vagy világnézeti meggyőződésre vonatkozó személyes adatok; és
- az egészségi állapotra vagy a szexuális életre vonatkozó személyes adatok.

Példa: A *Bodil Lindqvist* ügyben[66] az EUB megállapította, hogy „annak feltüntetése, hogy valamely személy lába megsérült, és ezért részleges betegszabadságon van, a 95/46 irányelv 8. cikkének (1) bekezdése értelmében vett, egészségi állapotra vonatkozó személyes adatnak minősül".

Az adatvédelmi irányelv ezenkívül a „szakszervezeti tagságot" is felsorolja az érzékeny adatok között, mivel ez az információ erőteljes jelzés lehet a politikai vélemény vagy hovatartozás tekintetében.

64 EJEB, *Peck kontra Egyesült Királyság* (44647/98), 2003. január 28.; EJEB, *Köpke kontra Németország* (420/07), 2010. október 5.

65 Adatvédelmi irányelv, (16) és (17) preambulumbekezdés; EJEB, *P.G. és J.H. kontra Egyesült Királyság* (44787/98), 2001. szeptember 25., 59. és 60. pont; EJEB, *Wisse kontra Franciaország* (71611/01), 2005. december 20.

66 EUB, C-101/01. sz. *Bodil Lindqvist ügy*, 2003. november 6., 51. pont.

A 108. egyezmény a büntetőítéletekkel kapcsolatos személyes adatokat is érzékeny adatnak minősíti.

Az adatvédelmi irányelv 8. cikkének (7) bekezdése megbízza az uniós tagállamokat, hogy „határozzák meg a nemzeti azonosító számok és egyéb általános jellegű azonosító jelek feldolgozásának feltételeit".

2.1.3. Anonimizált és pszeudoanonimizált adatok

Az adatvédelmi irányelvben és a 108. egyezményben egyaránt szereplő, korlátozott adatmegőrzés elve szerint (részletesebb kifejtését lásd a 3. fejezetben) az adatokat „olyan formában kell megőrizni, amely az adatalanyok azonosítását csak addig teszi lehetővé, ameddig az adatgyűjtés eredeti célja, illetve a továbbfeldolgozás célja indokolja".[67] Ebből következően az adatokat anonimizálni kellene, ha az adatkezelő azután is tárolni akarná őket, hogy aktualitásukat vesztették, és már nem szolgálják eredeti céljukat.

Névtelenné tett adatok

Az adatok akkor minősülnek névtelenítettnek, ha egy személyesadat-állományból valamennyi azonosító elemet eltávolítottak. Nem maradhat olyan elem az információban, amely a továbbiakban – ésszerű erőfeszítés mellett – lehetővé tehetné az érintett személy(ek) azonosítását.[68] Ha az adatokat sikeresen anonimizálták, már nem minősülnek személyes adatnak.

Ha a személyes adat már nem tölti be eredeti célját, de történelmi, statisztikai vagy tudományos célból személyhez kötött formában kell tárolni, az adatvédelmi irányelv és a 108. egyezmény is lehetővé teszi ezt a tárolást azzal a feltétellel, hogy a visszaélések ellen megfelelő garanciákat kell alkalmazni.[69]

Pszeudoanonimizált adatok

A személyes adat azonosítókat – pl. nevet, születési időpontot, nemet és címet – tartalmaz. Amikor a személyes adatot álnéven kezelik, az azonosítókat álnévvel

67 Adatvédelmi irányelv, 6. cikk, (1) bekezdés, e) pont; valamint 108. egyezmény, 5. cikk, e) pont.

68 *Uo.,* (26) preambulumbekezdés.

69 *Uo.,* Adatvédelmi irányelv, 6. cikk, (1) bekezdés, e) pont; valamint 108. egyezmény, 5. cikk, e) pont.

helyettesítik. Az anonimizálást például a személyes adatban előforduló azonosítók titkosításával érik el.

Az álnéven kezelt adatokat sem a 108. egyezmény, sem az adatvédelmi irányelv nem említi kifejezetten a jogi fogalom meghatározások között. A 108. egyezményhez fűzött magyarázó jelentés 42. cikkében azonban szerepel, hogy „az adatok névhez kötött formában való tárolására vonatkozó határidőkkel kapcsolatos követelmény [...] nem azt jelenti, hogy az adatokat bizonyos idő elteltével visszavonhatatlanul külön kell választani a személy nevétől, akire vonatkoznak, hanem csupán azt, hogy az adatok és az azonosítók nem lehetnek azonnal összekapcsolhatók». Ez a hatás az adatok álnéven való kezelésével elérhető. Az álnéven kezelt adatok minden olyan személy számára nehezen azonosíthatóak, aki nincs birtokában a dekódoló kulcsnak. A személyazonossággal való kapcsolat azonban az álnév és a dekódoló kulcs együttes megléte esetén áll fenn. A dekódoló kulcs használatára jogosult személyek számára könnyen lehetséges az újbóli azonosítás. A dekódoló kulcsok jogosulatlan személyek általi használata ellen különösen védekezni kell.

Mivel az adatok álnéven való kezelése a tömeges adatvédelem egyik legfontosabb módja olyan esetekben, amikor a személyes adatok használata teljes mértékben nem küszöbölhető ki, az ilyen intézkedés mögöttes logikáját és hatását részletesebben is ki kell fejteni.

Példa: Az a mondat például, hogy „az 1967. április 3-án született Charles Spencer négy gyermek, két fiú és két lány apja”, a következőképpen anonimizálható:

„C. S. (1967) négy gyermek, két fiú és két lány apja”; vagy:

„324 négy gyermek, két fiú és két lány apja”; vagy:

„YESz3201 négy gyermek, két fiú és két lány apja”.

A felhasználók, akik hozzáférnek ezekhez az anonimizált adatokhoz, a „324”-ből vagy a „YESz3201”-ből rendszerint nem tudják azonosítani „az 1967. április 3-án született Charles Spencert”. Ezért az anonimizált adatok valószínűsíthetően védenek a visszaéléssel szemben.

Az első példa azonban kevésbé biztonságos. Ha a „C. S. (1967) négy gyermek, két fiú és két lány apja” mondatot a kis faluban használják, ahol Charles Spencer él,

Spencer úr könnyen felismerhető. Az anonimizálás módszere befolyásolja az adatvédelem hatékonyságát.

A kódolt azonosítókkal ellátott személyes adatokat számos összefüggésben használják a személyazonosság titkosítására. Ez különösen akkor hasznos, ha az adatkezelőnek biztosítania kell, hogy ugyanazon érintettekkel foglalkozik, de nem szükséges – vagy nem feltétlenül kell – ismernie az érintettek valódi személyazonosságát. Ez a helyzet például akkor, ha egy kutató olyan betegekkel tanulmányozza egy betegség lefolyását, akiknek személyazonosságát csak az a kórház ismeri, ahol kezelik őket, és ahonnan a kutató az anonimizált kórtörténeteket kapja. Az anonimizálás tehát erős elem a magánélet védelmét erősítő technológia fegyvertárában. Fontos lehet a beépített adatvédelem megvalósítása során. A beépített adatvédelem azt jelenti, hogy a fejlett adatfeldolgozó rendszerek szerkezetébe eleve beépítik az adatvédelmet.

2.2. Adatfeldolgozás

Főbb pontok

- Az „adatfeldolgozás” kifejezés elsősorban az automatikus adatfeldolgozást jelenti.
- Az uniós jogban az „adatfeldolgozás” fogalmába a strukturált nyilvántartó rendszerekben való kézi adatfeldolgozás is beletartozik.
- Az Európa Tanács joga értelmében az „adatfeldolgozás” fogalmát a hazai jog a kézi adatfeldolgozásra is kiterjesztheti.

A 108. egyezményben és az adatvédelmi irányelvben szereplő adatvédelmi szabályozás elsősorban az automatizált adatfeldolgozásra összpontosít.

Az **Európa Tanács joga** szerint azonban az automatizált adatfeldolgozás fogalom meghatározása elismeri, hogy az automatizált műveletek között bizonyos manuális személyesadat-felhasználási lépésekre is szükség lehet. Az **uniós jog –** ehhez hasonlóan – a következőképpen határozza meg az automatizált adatfeldolgozás fogalmát: „személyes adatokon automatikus vagy nem automatikus módon végzett [...] műveletek összessége”.[70]

70 108. egyezmény, 2. cikk, c) pont; és adatvédelmi irányelv, 2. cikk, b) pont és 3. cikk, (1) bekezdés.

Példa: A *Bodil Lindqvist* ügyben[71] az EUB megállapította, hogy:

„internetes oldalon több személyre történő hivatkozás, és azoknak akár nevükkel, akár más módon – például telefonszámukkal vagy munkakörülményeikre és időtöltésükre vonatkozó információkkal – történő azonosítása a 95/46 irányelv 3. cikkének (1) bekezdése értelmében „személyes adatok részben vagy egészben automatizált módon való feldolgozásá[nak]" minősül".

A manuális adatfeldolgozás szintén adatvédelmet igényel.

Az **uniós jog** szerinti adatvédelem semmiképpen sem korlátozódik az automatizált adatfeldolgozásra. Ennek megfelelően az uniós jog értelmében az adatvédelem a manuális nyilvántartási rendszerben, azaz speciális rendszerű papíralapú nyilvántartásban történő személyesadat-feldolgozásra is vonatkozik.[72] Az adatvédelem ilyen kiterjesztésének okai a következők:

- a papíralapú nyilvántartások szerkezete kialakítható olyan módon, ami lehetővé teszi az információk gyors és könnyű megtalálását; és

- személyes adatok strukturált papíralapú nyilvántartásban történő tárolása esetén az automatizált adatfeldolgozásra vonatkozó jogszabályi korlátozások könnyen megkerülhetők.[73]

Az **Európa Tanács joga** értelmében a 108. egyezmény elsősorban a számítógépes adatfájlokban történő adatfeldolgozást szabályozza.[74] Emellett arról a lehetőségről is rendelkezik azonban, hogy a hazai jogban a védelmet a manuális feldolgozásra is kiterjesszék. A 108. egyezmény részes felei közül többen is kihasználták ezt a lehetőséget, és nyilatkoztak erről az Európa Tanács főtitkárának.[75] Az adatvédelem ilyen nyilatkozat alapján való kiterjesztésének minden manuális adatfeldolgozásra vonatkoznia kell, nem korlátozódhat csupán a manuális nyilvántartó rendszerekben történő adatfeldolgozásra.[76]

71 EUB, C-101/01. sz. *Bodil Lindqvist ügy*, 2003. november 6., 27. pont.

72 Adatvédelmi irányelv, 3. cikk (1) bekezdés.

73 *Uo.,* (27) preambulumbekezdés.

74 108. egyezmény, 2. cikk, b) pont.

75 Lásd a 108. egyezmény 3. cikke (2) bekezdésének c) pontja szerint tett nyilatkozatokat.

76 Lásd a 108. egyezmény 3. cikke (2) bekezdésének szövegét.

Ami az ide tartozó adatfeldolgozási műveletek jellegét illeti, az „adatfkezelés” az **uniós jog** és az **Európa Tanács joga** szerint is átfogó jelentésű fogalom: „személyes adatok kezelése „ […]: a személyes adatokkal […] végzett bármely művelet […], azaz gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, közlés továbbítás útján, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés”.[77] A „kezelés” fogalmába beletartoznak azok a cselekmények is, amelyek révén az adatok az egyik adatkezelő felelősségi köréből átkerülnek egy másik adatkezelőhöz.

Példa: Munkáltatók adatokat gyűjtenek és kezelnek munkavállalóikról, a munkavállalók fizetésére vonatkozó információkat is beleértve. Erre a munkaszerződés biztosít törvényes jogcímet.

A munkáltatóknak a személyzet fizetési adatait továbbítaniuk kell az adóhatósághoz. Ez az adattovábbítás a 108. egyezmény és az irányelv szerinti értelemben véve szintén „adatkezelésnek” minősül. Az adatok közlésére a jogalapot azonban nem a munkaszerződés biztosítja. Az adatfeldolgozási műveletekre vonatkozóan további jogalapnak is kell lennie, amelynek eredményeként a fizetési adatokat a munkáltatótól az adóhatósághoz továbbítják. Ezt a jogalapot általában a nemzeti adójogszabályok rendelkezései tartalmazzák. Ilyen rendelkezés nélkül az adatok továbbítása jogellenes adatkezelés lenne.

2.3. A személyes adatok felhasználói

Főbb pontok

- Aki úgy dönt, hogy mások személyes adatait feldolgozza, az adatvédelmi jog szerint „adatkezelőnek” minősül; ha többen döntenek így közösen, „közös adatkezelőnek” minősülnek.
- Az „adatfeldolgozó” jogilag különálló jogalany, aki az adatkezelő nevében személyes adatokat dolgoz fel.
- Az adatfeldolgozó akkor válik adatkezelővé, ha az adatokat a saját céljaira – azaz nem csupán az adatkezelő utasításait követve – felhasználja.

77 Adatvédelmi irányelv, 2. cikk b) pont. Lásd még a 108. egyezmény 2. cikkének c) pontját.

- Bárki, aki adatkezelőtől adatokat kap, „címzettnek” minősül.
- A „harmadik fél” olyan természetes vagy jogi személy, aki nem az adatkezelő utasításai szerint jár el (és nem az érintett).
- A „harmadik fél címzett” olyan személy vagy jogalany, aki/amely jogilag elkülönül az adatkezelőtől, de személyes adatokat kap tőle.

2.3.1. Adatkezelők és adatfeldolgozók

Annak, hogy valaki adatkezelőnek vagy adatfeldolgozónak minősül, az a legfontosabb következménye, hogy jogilag felel az adatvédelmi jog értelmében fennálló kötelezettségek betartásáért. Ennélfogva kizárólag a vonatkozó jogszabályok szerint felelős személyek tölthetik be ezeket a szerepeket. A magánszektorban az adatkezelő, illetve az adatfeldolgozó általában természetes vagy jogi személy, a közszférában pedig rendszerint hatóság. Más jogalanyok, például jogi személyiség nélküli szervezetek vagy intézmények csak akkor lehetnek adatkezelők vagy adatfeldolgozók, ha külön jogi előírás rendelkezik erről.

Példa: Ha a Sunshine vállalat marketing részlege piackutatáshoz adatok feldolgozását tervezi, a szóban forgó feldolgozás tekintetében nem a marketing részleg, hanem a Sunshine vállalat lesz az adatkezelő. A marketing részleg nem lehet adatkezelő, mivel nem önálló jogi személy.

Vállalatcsoport esetén az anyavállalat és minden egyes leányvállalat – mivel önálló jogi személyek – külön adatkezelőnek, illetve adatfeldolgozónak minősülnek. Az önálló jogállás miatt az egyazon vállalatcsoport tagjai közötti adattovábbításhoz speciális jogalap szükséges. Nincsen olyan előjog, amely lehetővé tenné a személyes adatok cseréjét a vállalatcsoporton belüli önálló jogalanyok között.

Ezzel összefüggésben meg kell említeni a magánszemélyek szerepét. Az **uniós jog szerint** a magánszemélyek, amikor kizárólag személyes célra vagy háztartási tevékenység keretében végzik más személyek adatainak kezelését, nem tartoznak az adatvédelmi irányelv hatálya alá; nem minősülnek adatkezelőnek.[78]

A joggyakorlat azonban azt mutatja, hogy az adatvédelmi jog ennek ellenére alkalmazandó, amikor egy magánszemély az internethasználat során adatokat tesz közzé másokról.

78 Adatvédelmi irányelv, (12) preambulumbekezdés és 3. cikk, (2) bekezdés, utolsó francia bekezdés.

Példa: Az EUB a *Bodil Lindqvist* ügyben[79] úgy érvelt, hogy:

„internetes oldalon több személyre történő hivatkozás, és azoknak akár nevükkel, akár más módon [...] történő azonosítása a 95/46 irányelv 3. cikkének (1) bekezdése értelmében „személyes adatok részben vagy egészben automatizált módon való adatkezelésnek" minősül".[80]

Az ilyen személyesadat-kezelés nem tartozik a kizárólag személyes célra végzett vagy a háztartási tevékenységek közé, amelyek kívül esnek az adatvédelmi irányelv hatályán, mivel ezt a kivételt „úgy kell [...] értelmezni, hogy az kizárólag a magánszemélyek magán- vagy családi élete keretébe tartozó tevékenységekre vonatkozik, nyilvánvalóan nem erről van azonban szó a személyes adatok interneten való közzétételét jelentő olyan adatkezelés esetében, amely során ezen adatok meghatározatlan számú személy számára válnak hozzáférhetővé". [81]

Adatkezelő

Az **uniós jogban** az adatkezelő az a személy, amely „önállóan vagy másokkal együtt meghatározza a személyes adatok kezelésének céljait és módját".[82] Az adatkezelő döntése határozza meg, miért és hogyan történjen az adatok feldolgozása. Az **Európa Tanács joga szerint** az „adatkezelő" fogalom meghatározásában ezen felül az is szerepel, hogy az adatkezelő határozza meg a tárolható személyes adatok kategóriáit.[83]

A 108. egyezmény az adatkezelő fogalom meghatározásában az adatkezelés egy másik vonatkozására is utal, amely megfontolást érdemel. Ez a fogalom meghatározás arról a kérdésről is említést tesz, hogy ki dolgozhat fel jogszerűen bizonyos adatokat egy bizonyos célra. Ha azonban állítólagos jogellenes adatfeldolgozás történik és meg kell találni az adatkezelőt, az a természetes vagy jogi személy – vállalat vagy hatóság – lesz az adatkezelő, aki/amely döntött az adatok feldolgozásáról,

79 EUB, C-101/01. sz. *Bodil Lindqvist ügy*, 2003. november 6.

80 *Uo.*, 27. pont.

81 *Uo.*, 47. pont.

82 Adatvédelmi irányelv, 2. cikk, d) pont.

83 108. egyezmény, 2. cikk, d) pont.

függetlenül attól, hogy erre jogszerűen fel volt-e hatalmazva.[84] Ezért a törlés iránti kérelmet mindig a „tényleges" adatkezelőhöz kell címezni.

Közös adatkezelés

Az „adatkezelőnek" az adatvédelmi irányelvben található fogalom meghatározása úgy rendelkezik, hogy több, jogilag különálló szervezet is eljárhat – közösen vagy másokkal együtt – adatkezelőként. Ez azt jelenti, hogy ők együtt döntenek adatoknak egy bizonyos közös célra történő feldolgozásáról.[85] Jogilag ez azonban csak olyan esetben lehetséges, amikor különleges jogalap rendelkezik adatoknak egy közös célra közösen történő kezeléséről.

Példa: Egy több hitelintézet által közösen működtetett, a késedelmes ügyfeleik adatait tartalmazó adatbázis jó példa a közös adatkezelésre. Amikor valaki hitelkérelmet nyújt be egy bankhoz, amely a közös adatkezelők egyike, a bankok az adatbázis segítségével hozhatnak tájékozott döntést az igénylő hitelképességéről.

Az előírások kifejezetten nem mondják ki, hogy a közös adatkezeléshez az is szükséges, hogy mindegyik adatkezelő célja azonos legyen, vagy elég az is, ha céljaik csupán részben átfedik egymást. Nincs azonban még erre vonatkozó európai szintű joggyakorlat, és a felelősséggel kapcsolatos következmények sem egyértelműek. A 29. cikk szerinti munkacsoport a közös adatkezelés fogalmának kiterjesztő értelmezése mellett foglal állást annak érdekében, hogy – figyelemmel a jelenlegi adatfeldolgozási realitás egyre növekvő bonyolultságára – némi rugalmasságot tegyen lehetővé.[86] A Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaságot (SWIFT) érintő egyik ügy jól szemlélteti a munkacsoport álláspontját.

Példa: Az úgynevezett SWIFT-ügyben európai bankok banki tranzakciók során történő adattovábbítás elvégzésével bízták meg a SWIFT-et – kezdetben mint adatfeldolgozót. A SWIFT a szóban forgó, egy egyesült államokbeli számítógépközpontban tárolt banki tranzakciós adatokat felfedte az USA Pénzügyminisztériuma felé anélkül, hogy az őt megbízó európai bankok kifejezetten utasították

84 Lásd a 29. cikk szerinti munkacsoport véleményét (2010): *1/2010. sz. véleménye (2010) az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 15. o.

85 Adatvédelmi irányelv, 2. cikk, d) pont.

86 A 29. cikk szerinti munkacsoport *1/2010. sz. véleménye (2010) az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 19. o.

volna erre. A helyzet jogszerűségének értékelése során a 29. cikk szerinti munkacsoport arra a következtetésre jutott, hogy a SWIFT-et megbízó európai bankok és maga a SWIFT is mint közös adatkezelők felelősek az európai ügyfelek felé az utóbbiak adatainak az amerikai hatóságok felé történt felfedéséért.[87] A SWIFT azzal, hogy az adatok felfedéséről döntött, felvette – jogellenesen – az adatkezelő szerepét; a pénzintézetek nyilvánvalóan nem teljesítették az adatfeldolgozójuk felügyeletére vonatkozó kötelezettségüket, ezért nem mentesülhettek teljesen az adatkezelői felelősségük alól. A helyzet eredményeként közös adatkezelés jön létre.

Adatfeldolgozó

Az **uniós jog** úgy határozza meg az adatfeldolgozót, mint olyan személyt, aki/amely személyes adatokat dolgoz fel az adatkezelő nevében.[88] Az adatfeldolgozóra bízott tevékenységek valamely igen konkrét feladatra vagy összefüggésre is korlátozódhatnak, de általánosak és átfogóak is lehetnek.

Az **Európa Tanács jogában** az adatfeldolgozó fogalma azonos az uniós jog szerinti fogalommal.

Az adatfeldolgozók – a mások számára történő adatfeldolgozáson kívül – a saját céljaikra történő adatfeldolgozás, pl. saját munkavállalóik, értékesítéseik és elszámolásaik nyilvántartása tekintetében egyben saját jogú adatkezelők is.

Példák: Az Everready vállalat humánerőforrás-adatok kezelése céljából más vállalatok részére végzett adatfeldolgozásra szakosodott. Ebben a minőségében az Everready adatfeldolgozó.

Ha azonban az Everready a saját munkavállalói adatait dolgozza fel, a munkáltatói kötelezettségeinek teljesítése céljából végzett adatfeldolgozási műveletek tekintetében adatkezelő.

87 A 29. cikk szerinti munkacsoport *10/2006. sz. véleménye (2006) a Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) általi személyesadat-feldolgozásról,* WP 128., Brüsszel, 2006. november 22.

88 Adatvédelmi irányelv, 2. cikk, e) pont.

Az adatkezelő és az adatfeldolgozó közötti jogviszony

Ahogy fentebb már láthattuk, az adatkezelő a fogalommeghatározás szerint az a személy, aki meghatározza az adatfeldolgozás céljait és módját.

> Példa: A Sunshine vállalat igazgatója úgy dönt, hogy a Moonlight nevű, piacelemzésre szakosodott vállalatnak piacelemzést kellene végeznie a Sunshine ügyféladatairól. Bár a feldolgozás módjának meghatározását a Moonlightra bízza, a Sunshine cég marad az adatkezelő, a Moonlight pedig csak a feldolgozó, mivel a szerződés szerint a Moonlight csak a Sunshine által meghatározott célokra használhatja fel a Sunshine ügyféladatait.

Ha az adatfeldolgozás módjának meghatározására vonatkozó jogkört az adatfeldolgozóra ruházzák, az adatkezelőnek ettől még bele kell tudnia szólni az adatkezelőnek a feldolgozás módjára vonatkozó döntéseibe. A végső felelősség továbbra is az adatkezelőé, akinek felügyelnie kell az adatfeldolgozókat annak biztosítása érdekében, hogy döntéseik megfeleljenek az adatvédelmi jognak. Az a szerződés tehát, amely megtiltja az adatkezelőnek, hogy beleszóljon az adatfeldolgozó döntéseibe, végső soron közös adatkezelésként értelmezendő, ahol mindkét fél osztozik az adatkezelő jogi felelősségében.

Ezenkívül, ha az adatfeldolgozó nem tartja tiszteletben az adatkezelő által az adatok felhasználására vonatkozóan előírt korlátozásokat, a feldolgozó legalábbis az adatkezelő utasításai megszegésének erejéig adatkezelővé válik. Ez minden valószínűség szerint adatkezelővé emeli a feldolgozót, aki jogellenesen jár el. Az eredeti adatkezelőnek viszont meg kell magyaráznia, hogyan volt lehetséges, hogy a feldolgozó megszegje megbízatását. A 29. cikk szerinti munkacsoport ilyen esetekben közös ellenőrzés feltételezésére hajlik, mivel az biztosítja az adatalanyok érdekeinek legmegfelelőbb védelmét.[89] A közös adatkezelés egyik fontos következménye az egyetemleges kártérítési felelősség, ami többféle jogorvoslati lehetőséget nyújt az érintetteknek.

A felelősség megosztásával kapcsolatban is lehetnek kérdések, ha az adatkezelő kisvállalkozás, a feldolgozó pedig egy nagyvállalat, amely elég erős ahhoz, hogy

89 A 29. cikk szerinti munkacsoport *1/2010. sz. véleménye (2010) az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 25. o.; és a 29. cikk szerinti munkacsoport *10/2006. sz. véleménye a Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) általi személyesadat-feldolgozásról*, WP 128., Brüsszel, 2006. november 22.

diktálja a szolgáltatására vonatkozó feltételeket. Ilyen körülmények között azonban a 29. cikk szerinti munkacsoport fenntartja, hogy a felelősség mértéke a gazdasági egyensúly hiánya miatt nem csökkenthető, és az adatkezelő fogalmának értelmét meg kell tartani.[90]

Az egyértelműség és átláthatóság kedvéért, az adatkezelő és az adatfeldolgozó közötti jogviszony részleteit írásbeli szerződésben kell szabályozni.[91] Ha nincs ilyen szerződés, azzal a felek megsértik az adatkezelő azon kötelezettségét, hogy írásos dokumentumba foglalja a kölcsönös kötelezettségeket, ami szankciókhoz vezethet.[92]

Előfordulhat, hogy az adatfeldolgozók bizonyos feladatokat további feldolgozókkal szeretnének elvégeztetni. Ez jogilag megengedett, részleteit tekintve az adatkezelő és az adatfeldolgozó közötti szerződéses kikötésektől függ, többek között attól, hogy az adatkezelő engedélye szükséges-e minden egyes esetben, vagy a puszta tájékoztatás is elegendő.

Az **Európa Tanács joga** szerint az adatkezelő és az adatfeldolgozó fogalmának fentebb kifejtett értelmezése teljes mértékben alkalmazható, amit a 108. egyezmény szerint kidolgozott ajánlások is mutatnak.[93]

2.3.2. Címzettek és harmadik felek

A személyek vagy szervezetek – az adatvédelmi irányelv által bevezetett – e két kategóriája közötti különbség elsősorban az adatkezelővel fennálló jogviszonyukban, valamint ebből következően az adatkezelő által kezelt személyes adatokhoz való hozzáférési jogosultságukban rejlik.

A „harmadik fél" az adatkezelőtől jogilag különböző személy. Ezért az adatok harmadik féllel való közléséhez mindig konkrét jogalap szükséges. Az adatvédelmi irányelv 2. cikkének f) pontja szerint a harmadik fél „az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely nem azonos az érintettel, az adatkezelővel, a feldolgozóval vagy azokkal a személyekkel, akik az adatkezelő

90 A 29. cikk szerinti munkacsoport *1/2010. sz. véleménye (2010) az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 26. o.

91 Adatvédelmi irányelv, 17. cikk, (3) és (4) bekezdés.

92 A 29. cikk szerinti munkacsoport *1/2010. sz. véleménye (2010) az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 27. o.

93 Lásd például a Profilalkotási ajánlás 1. cikkét.

vagy a feldolgozó közvetlen felügyelete alatt felhatalmazást kaptak az adatok feldolgozására". Ez azt jelenti, hogy az adatkezelőtől jogilag különböző szervezetnél dolgozó személyek – akkor is, ha a szervezet az adatkezelővel azonos vállalatcsoporthoz vagy holdinghoz tartozik – „harmadik félnek" minősülnek (vagy harmadik félhez tartoznak). Másrészről, az ügyfelek számláit vezető, a központ közvetlen irányítása alatt álló bankfiókok nem minősülnek „harmadik félnek".[94]

A „címzett" a „harmadik félnél" tágabb fogalom. Az adatvédelmi irányelv 2. cikkének g) pontja értelmében a címzett „az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, akinek vagy amelynek a részére az adatot továbbítják, függetlenül attól, hogy harmadik személy-e vagy sem". A címzett vagy az adatkezelőn és a feldolgozón kívüli személy (azaz harmadik fél), vagy az adatkezelőn vagy a feldolgozón belüli személy, például az adott vállalat vagy hatóság munkavállalója vagy egy másik részlege.

A címzettek és a harmadik felek megkülönböztetése kizárólag az adatok jogszerű közlésének feltételei szempontjából fontos. Az adatkezelő vagy -feldolgozó alkalmazottai minden további jogi követelmény nélkül személyes adatok címzetteinek minősülnek, ha részt vesznek az adatkezelő vagy -feldolgozó adatfeldolgozási műveleteiben. Másrészről, az adatkezelőtől vagy -feldolgozótól jogilag különálló harmadik fél nem jogosult az adatkezelő által feldolgozott személyes adatok felhasználására – kivéve, ha konkrét esetben konkrét jogalap áll fenn. Az adatok „harmadik fél címzetteinek" tehát mindig jogalappal kell rendelkezniük ahhoz, hogy jogszerűen kaphassanak személyes adatokat.

Példa: Egy adatfeldolgozó alkalmazottja, aki a munkáltatója által rábízott feladatok keretében személyes adatokat használ, az adatok címzettje, de nem harmadik fél, mivel az adatfeldolgozó nevében vagy utasításai alapján használja az adatokat.

Ha azonban ugyanez a munkavállaló úgy dönt, hogy a számára mint a feldolgozó alkalmazottja számára hozzáférhető adatokat a saját céljaira használja fel, és egy másik cégnek értékesíti, így már harmadik félként jár el. A továbbiakban már nem az adatfeldolgozó (a munkáltató) utasításait követi. Harmadik félként a munkavállalónak jogalappal kellene rendelkeznie az adatok megszerzéséhez

94 A 29. cikk szerinti munkacsoport *1/2010. sz. véleménye (2010) az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 31. o.

és értékesítéséhez. Ebben a példában a munkavállaló bizonyára nem rendelkezik ilyen jogalappal, tehát a szóban forgó cselekmények jogellenesek.

2.4. Hozzájárulás

Főbb pontok

- A hozzájárulásnak mint a személyes adatok kezelése jogalapjának szabadnak, tényszerűnek (a megfelelő információk birtokában megadottnak) és konkrétnak kell lennie.
- A hozzájárulás megadásának egyértelműnek kell lennie. A hozzájárulás kifejezetten vagy hallgatólagosan is megadható – olyan módon, hogy ne maradjon kétség afelől, hogy az érintett beleegyezik adatainak kezelésébe.
- Érzékeny adatok beleegyezés alapján történő kezeléséhez kifejezett hozzájárulás szükséges.
- A hozzájárulás bármikor visszavonható.

A hozzájárulás „az érintett kívánságának önkéntes, kifejezett és tájékozott kinyilvánítását" jelenti.[95] Számos esetben ez a jogszerű adatkezelés jogalapja (lásd a 4.1 szakaszt).

2.4.1. Az érvényes hozzájárulás elemei

Az **uniós jog** három elemet határoz meg ahhoz, hogy a hozzájárulás érvényes legyen; ezek célja annak garantálása, hogy az érintettek valóban bele akartak egyezni adataik felhasználásába:

- az érintett a hozzájárulás megadásakor nem lehetett nyomás alatt;
- az érintettet kellően tájékoztatták a hozzájárulás tárgyáról és következményeiről; és
- a hozzájárulás hatályának eléggé konkrétnak kell lennie.

Az adatvédelmi jog értelmében a hozzájárulás csak mindhárom követelmény együttes teljesülése esetén minősül érvényesnek.

95 Adatvédelmi irányelv, 2. cikk, h) pont.

A 108. egyezmény nem határozza meg a hozzájárulás fogalmát; ezt a hazai jogra hagyja. Az **Európa Tanács joga** szerint azonban az érvényes hozzájárulás elemei megfelelnek a fentebb leírtaknak, ahogyan a 108. egyezmény szerint kidolgozott ajánlásokban is szerepel.[96] A hozzájárulásra vonatkozó követelmények megegyeznek az európai polgári jog szerinti érvényes szándéknyilatkozatra vonatkozó feltételeknek.

Az érvényes hozzájárulásra vonatkozó polgári jogi kiegészítő követelmények, például a jogképesség, természetesen az adatvédelemmel kapcsolatban is alkalmazandók, mivel e követelmények alapvető jogi előfeltételek. A jogképességgel nem rendelkező személyek érvénytelen hozzájárulása esetén hiányzik a jogalap e személyek adatainak kezeléséhez.

A hozzájárulás kifejezetten[97] vagy nem kifejezetten is megadható. A kifejezett hozzájárulás nem hagy kétséget az érintett szándéka felől, és szóban vagy írásban is megtehető; a nem kifejezett hozzájárulás a körülményekből következik. A hozzájárulást minden esetben egyértelműen kell megadni.[98] Ez azt jelenti, hogy semmiféle ésszerű kétség nem maradhat azzal kapcsolatban, hogy az érintett beleegyezését kívánta közölni adatainak kezeléséhez. Ha a hozzájárulásra a cselekvés puszta hiányából következtetnek, az például nem alkalmas az egyértelmű hozzájárulás igazolására. Ha a feldolgozandó adatok érzékeny adatnak minősülnek, a kifejezett hozzájárulás kötelező, amelynek egyértelműnek kell lennie.

Szabad hozzájárulás

A szabad hozzájárulás csak akkor érvényes, „ha az érintettnek valódi választási lehetősége van, és nem áll fenn a megtévesztés, megfélemlítés, kényszerítés vagy jelentős negatív következmények kockázata, ha az érintett nem adja hozzájárulását”.[99]

Példa: Számos repülőtéren az utasoknak biztonsági szkenneren kell áthaladniuk ahhoz, hogy beléphessenek a beszállási területre.[100] Tekintettel arra, hogy

96 Lásd például a 108. egyezményhez fűzött Statisztikai adatokra vonatkozó ajánlás 6. pontját.

97 Adatvédelmi irányelv, 8. cikk (2) bekezdés.

98 *Uo.* 7. cikk, a) pont és 26. cikk, (1) bekezdés.

99 Lásd még a 29. cikk szerinti munkacsoportnak *a hozzájárulás fogalmáról szóló 15/2011. sz. véleményét (2011)*, WP 187, Brüsszel, 2011. július 13., 12. o.

100 Ez a példa a fentebb idézett műből származik (15. o.).

a szkennelés során utasok adatainak feldolgozása történik, a kezeléshez szükséges az adatvédelmi irányelv 7. cikke szerinti egyik jogalap megléte (lásd a 4.1.1 szakaszt). A biztonsági szkenneren való áthaladást olykor választási lehetőségként tüntetik fel az utasok előtt, azt a látszatot keltve, hogy hozzájárulásuk indokolhatja az adatkezelést. Az utasok azonban attól tarthatnak, hogy ha megtagadják a biztonsági szkenneren való áthaladást, azzal gyanút keltenek vagy újabb ellenőrzéseknek, például motozásnak teszik ki magukat. Sok utas azért egyezik bele a szkennerrel történő ellenőrzésbe, mert ezzel esetleges problémákat vagy késedelmet védhet ki. Az ilyen hozzájárulás feltehetően nem kellően szabad.

Ennélfogva megalapozott, törvényes jogalap – az adatvédelmi irányelv 7. cikkének e) pontja alapján – csupán jogalkotási aktusban található, amelynek értelmében az utasok azért kötelesek együttműködni, mert ehhez magasabb rendű közérdek fűződik. Az ilyen jogszabály még mindig kínálhat választási lehetőséget a szkenneres átvilágítás és a manuális vizsgálat között, de csakis bizonyos körülmények között szükséges határellenőrzési kiegészítő intézkedések részeként. 2011-ben az Európai Bizottság erről rendelkezett a biztonsági szkennerekről szóló két rendeletben.[101]

A szabad hozzájárulás olyan alárendelt helyzetekben is veszélybe kerülhet, amikor nincs gazdasági egyensúly a hozzájárulást biztosító adatkezelő és a hozzájárulást megadó érintett között.[102]

Példa: Egy nagyvállalat – kizárólag a vállalaton belüli kommunikáció javítása céljából – névjegyzék létrehozását tervezi, amely az összes munkavállaló nevét, beosztását és munkahelyi címét tartalmazza. A személyzeti vezető fényképet is szeretne közölni minden munkavállalóról a névjegyzékben, például azért, hogy a kollegákat könnyebb legyen felismerni az értekezleteken. A

101 A Bizottság 2011. november 10-i 1141/2011/EU rendelete a polgári légi közlekedés védelmére vonatkozó közös alapkövetelmények kiegészítéséről szóló 272/2009/EK rendeletnek a biztonsági szkennerek európai uniós repülőtereken való alkalmazása tekintetében történő módosításáról, HL L 293., 2011, valamint Bizottság 2011. november 11-i 1147/2011/EU végrehajtási rendelete a polgári légi közlekedés védelmére vonatkozó közös alapkövetelmények végrehajtásáról szóló 185/2010/EU rendeletnek a biztonsági szkennerek európai uniós repülőtereken való alkalmazása tekintetében történő módosításáról, HL L 294., 2011.

102 Lásd a 29. cikk szerinti munkacsoport, *személyes adatok foglalkoztatással összefüggő feldolgozásáról szóló véleményét (2001)*, WP 48, Brüsszel, 2001. szeptember 13.; valamint a 29. cikk szerinti munkacsoportnak az 1995. október 24-i 95/46/EK irányelv 26. cikke (1) bekezdésének egységes értelmezéséről szóló munkadokumentumát (2005), WP 114, Brüsszel, 2005. november 25.

munkavállalók képviselői szerint ezt kizárólag az egyes munkavállalók hozzájárulásával lehetne megtenni.

Ilyen helyzetben a munkavállaló hozzájárulását kellene jogalapnak elismerni a névjegyzékben szerepeltetendő fényképek feldolgozásához, mert egyértelmű, hogy a fénykép névjegyzékben való közzétételének önmagában nincs negatív következménye, ezenkívül a munkavállalót valószínűleg nem fogják negatív hatások érni a munkáltató részéről, ha nem egyezik bele fényképének a névjegyzékben való közlésébe.

Ez nem jelenti azonban azt, hogy a hozzájárulás sosem lehet érvényes olyan körülmények között, amikor a hozzájárulás megtagadása negatív következményekkel járna. Ha például egy áruházi törzsvásárlói kártya visszautasítása csupán azzal a következménnyel jár, hogy az adott személy nem kap engedményt bizonyos áruk árából, a hozzájárulás érvényes jogalap azon vásárlók személyes adatainak feldolgozására, akik beleegyeztek, hogy ilyen kártyát kapjanak. Nincs alárendelt helyzet a cég és a vásárló között, és a hozzájárulás megtagadásának következményei nem olyan súlyosak, hogy az érintett ne választhatna szabadon.

Másrészről viszont, ha kellően fontos áruk vagy szolgáltatások csak és kizárólag úgy szerezhetők be, ha bizonyos személyes adatokat harmadik felek tudomására hoznak, az érintett adatai közléséhez való hozzájárulása rendszerint nem tekinthető szabad döntésnek, ezért az adatvédelmi jog értelmében nem érvényes.

Példa: Az utasok hozzájárulása, amelyet egy légitársaságnak adtak arra vonatkozóan, hogy a légitársaság úgynevezett utas-nyilvántartási adatokat, azaz az utasok személyazonossági adatait, étkezési szokásaival vagy egészségi problémáival kapcsolatos adatokat egy meghatározott külföldi ország bevándorlási hatóságainak továbbítson, az adatvédelmi jog értelmében nem minősíthető érvényes hozzájárulásnak, mivel az utasoknak nincs választási lehetőségük, ha el szeretnének utazni a szóban forgó országba. Ha ezeket az adatokat jogszerűen szeretnék továbbítani, ahhoz a hozzájáruláson kívül más jogalap szükséges: leginkább egy speciális jogszabály.

A megfelelő információk birtokában történő hozzájárulás

Az érintettnek elegendő információval kell rendelkeznie, mielőtt döntését meghozza. Csak eseti alapon dönthető el, hogy a rendelkezésre álló információ

elegendő-e vagy sem. A megfelelő információk birtokában történő hozzájárulás rendszerint a következőkből áll: a tárgy, amihez a hozzájárulás szükséges, pontos és könnyen érthető leírása, és ezenfelül a hozzájárulás megadása vagy megtagadása következményeinek vázolása. A tájékoztatás nyelvét az információ várható címzettjeihez kell igazítani.

A tájékoztatásnak az érintett számára könnyen hozzáférhetőnek is kell lennie. A tájékoztatás hozzáférhetősége és átláthatósága fontos elemek. Online környezetben a többrétegű tájékoztató feljegyzések jó megoldást jelenthetnek, mivel az érintett a tömör információkon felül bővebb verzióhoz is hozzáférhet.

Konkrét hozzájárulás

Az érvényes hozzájárulásnak konkrétnak is kell lennie. Ez együtt jár a hozzájárulás tárgyáról adott tájékoztatás minőségével. Ebből a szempontból az átlagos érintett ésszerű elvárásai lesznek irányadók. Újra kérni kell az érintett hozzájárulását, ha a műveleteket olyan módon bővítik vagy megváltoztatják, ami az eredeti hozzájárulás megadásakor – elvárhatóan – nem volt előrelátható.

Példa: A *Deutsche Telekom AG* ügyben[103] az EUB azzal a kérdéssel foglalkozott, hogy egy távközlési szolgáltatónak, amely az *elektronikus hírközlési adatvédelmi irányelv* [104] 12. cikke alapján előfizetői személyes adatait köteles továbbítani, újabb hozzájárulást kell-e kérnie az érintettektől, mivel az eredeti hozzájárulás megadásakor a címzettek nem voltak megnevezne.

Az EUB megállapította, hogy a nevezett cikk alapján nem kell új hozzájárulást kérni az adatok továbbítása előtt, mert az érintetteknek a szóban forgó rendelkezés alapján csak arra volt lehetőségük, hogy a kezelés céljához – azaz adataik közzétételéhez – járuljanak hozzá, és nem választhattak több címjegyzék között, amelyekben az adatok közzétehetők.

A Bíróság kiemelte, hogy „az elektronikus hírközlési adatvédelmi irányelv 12. cikkének összefüggés szerinti és rendszertani értelmezéséből az következik,

103 EUB, C-543/09. sz. *Deutsche Telekom AG kontra Németország* ügy, 2011. május 5.; lásd különösen az 53. és 54. pontot.

104 Az Európai Parlament és a Tanács 2002. július 12-i 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (*elektronikus hírközlési adatvédelmi irányelv*), HL L 201., 2002.

hogy az e cikk (2) bekezdése alapján a hozzájárulás elsődlegesen a személyes adatok nyilvános telefonkönyvben való megjelentetésének céljára, nem pedig e telefonkönyv szolgáltatójára vonatkozik".[105] Ezenfelül, „önmagában a személyes adatoknak valamely sajátos rendeltetésű telefonkönyvben való megjelentetése az előfizető számára [nem pedig a kiadvány szerzője számára] hátrányosnak bizonyulhat".[106]

2.4.2. A hozzájárulás bármely időpontban való visszavonásának joga

Az adatvédelmi irányelv nem említi a hozzájárulás bármely időpontban történő visszavonásához való általános jogot. Széles körben vélelmezett azonban, hogy ez a jog létezik, és lehetővé kell tenni az érintett számára, hogy szabad mérlegelése szerint élhessen vele. Nem szabad olyan követelményt előírni, hogy a visszavonást indokolni kell, és a korábbi beleegyezéssel történő adathasználatból következő bármely előny megszűnésén túl semmiféle egyéb negatív következmény nem állhat be.

Példa: Egy vásárló hozzájárul, hogy az általa az adatkezelőnek megadott címre reklámlevelet kapjon. Ha a vásárló visszavonja hozzájárulását, az adatkezelőnek azonnal le kell állítania a reklámlevél küldését. A leállítás semmiféle büntető jellegű következménnyel, például díj kiszabásával nem járhat.

Ha a vásárló 5%-os árengedményt kapott egy szállodai szoba árából cserébe azért, mert beleegyezett, hogy adatait reklámlevélhez felhasználják, a beleegyezés későbbi visszavonása nem járhat azzal, hogy vissza kell fizetnie az engedményt.

105 EUB, C-543/09. sz. *Deutsche Telekom AG kontra Németország* ügy, 2011. május 5.; lásd különösen a 61. pontot.

106 Uo., lásd különösen a 62. pontot.

3

Az európai adatvédelmi jog alapelvei

EU	Tárgyalt kérdések	Európa Tanács
Adatvédelmi irányelv, 6. cikk, (1) bekezdés, a) és b) pont EUB, C-524/06. sz. *Huber kontra Németország* ügy, 2008. december 16. EUB, C-92/09. és C-93/09. sz., *Volker és Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* egyesített ügyek, 2010. november 9.	**A jogszerű adatkezelés elve**	108. egyezmény, 5. cikk, a) és b) pont EJEB, *Rotaru kontra Románia* [nagytanács] (28341/95), 2000. május 4. EJEB, *Taylor-Sabori kontra Egyesült Királyság* (47114/99), 2002. október 22. EJEB, *Peck kontra Egyesült Királyság* (44647/98), 2003. január 28. EJEB, *Khelili kontra Svájc* (16188/07), 2011. október 18. EJEB, *Leander kontra Svédország* (9248/81), 1987. március 26.
Adatvédelmi irányelv, 6. cikk, (1) bekezdés, b) pont	**A célmeghatározás és a célhoz kötöttség elve**	108. egyezmény, 5. cikk, b) pont
	Az adatminőségi elvek:	
Adatvédelmi irányelv, 6. cikk, (1) bekezdés, c) pont	**Az adatok relevanciája**	108. egyezmény, 5. cikk, c) pont
Adatvédelmi irányelv, 6. cikk, (1) bekezdés, d) pont	**Az adatok pontossága**	108. egyezmény, 5. cikk, d) pont

EU	Tárgyalt kérdések	Európa Tanács
Adatvédelmi irányelv, 6. cikk, (1) bekezdés, e) pont	Az adatok korlátozott ideig történő megőrzése	108. egyezmény, 5. cikk, e) pont
Adatvédelmi irányelv, 6. cikk, (1) bekezdés, e) pont	Mentesség tudományos kutatás és statisztika céljából	108. egyezmény, 9. cikk, (3) bekezdés
Adatvédelmi irányelv, 6. cikk (1) bekezdés a) pont	A tisztességes adatfeldolgozás elve	108. egyezmény, 5. cikk, a) pont EJEB, *Haralambie kontra Románia* (21737/03), 2009. október 27. EJEB, *K.H. és társai kontra Szlovákia* (32881/04), 2009. november 6.
Adatvédelmi irányelv, 6. cikk, (2) bekezdés	Az elszámoltathatóság elve	

A 108. egyezmény 5. cikkében szereplő elvek összegzik az európai adatvédelmi jog lényegét. Ezek az elvek az adatvédelmi irányelv 6. cikkében is megjelennek, és az irányelv további cikkeiben foglalt részletes rendelkezések alapját alkotják. Valamennyi európa tanácsi vagy uniós szintű adatvédelmi jogszabálynak meg kell felelnie ezeknek az elveknek, és a jogszabályok értelmezésénél is tekintetbe kell venni őket. Az ezen alapelvek alóli kivételekről és az alapelvek korlátozásáról nemzeti szintű szabályozás rendelkezhet;[107] a kivételeket és korlátozásokat jogszabályba kell foglalni, azoknak törvényes célt kell szolgálniuk, és szükségesnek kell lenniük egy demokratikus társadalomban. Mindhárom feltételnek egyaránt teljesülnie kell.

3.1. A jogszerű adatfeldolgozás elve

Főbb pontok

- A jogszerű adatkezelés elvének megértéséhez utalni kell az adatvédelemhez való jog jogszerű korlátozásának feltételeire a Charta 52. cikke (1) bekezdésének figyelembevételével, valamint az igazolható sérelemnek az EJEE 8. cikke szerinti követelményeire.
- Eszerint a személyes adatok feldolgozása csak akkor jogszerű, ha:

107 108. egyezmény, 9. cikk, c) pont; adatvédelmi irányelv, 13. cikk és 9. cikk, (2) bekezdés.

- megfelel a jogszabályoknak, és
- törvényes célt szolgál, és
- a törvényes cél eléréséhez szükséges egy demokratikus társadalomban.

Az **EU és az Európa Tanács adatvédelmi jogában** a jogszerű adatfeldolgozás elve az első megnevezett elv; a 108. egyezmény 5. cikkében és az adatvédelmi irányelv 6. cikkében csaknem ugyanazokkal a szavakkal szerepel.

Egyik fenti rendelkezés sem határozza meg, mi minősül „jogszerű adatfeldolgozásnak". E jogi fogalom megértéséhez említést kell tenni az EJEE szerinti igazolható sérelemről, amit az EJEB joggyakorlata értelmez, valamint a jogszerű korlátozásoknak a Charta 52. cikke szerinti feltételeiről.

3.1.1. Az igazolható sérelemnek az EJEE szerinti követelményei

A személyes adatok feldolgozása sértheti az érintettnek a magánélet tiszteletben tartásához való jogát. A magánélet tiszteletben tartásához való jog azonban nem abszolút jog, hanem egyensúlyt kell teremteni közte és más törvényes érdekek között, ezekkel össze kell egyeztetni – legyenek azok más személyek (magánérdek) vagy a társadalom érdekei (közérdek).

Az állami beavatkozás a következő feltételekkel indokolt:

A jogszabályokkal összhangban

Az EJEB joggyakorlata szerint a beavatkozás akkor áll összhangban a jogszabályokkal, ha bizonyos jellemzőkkel rendelkező hazai jogszabályi rendelkezésen alapszik. A jogszabálynak „hozzáférhetőnek kell lennie az érintett személyek számára, és hatásainak előre láthatónak kell lennie".[108] Egy szabály akkor előre látható, ha „kellő pontossággal van meghatározva ahhoz, hogy egy személy – szükség esetén a megfelelő tanácsokat követve – magatartását ennek megfelelően kiigazítsa".[109] „A

108 EJEB, *Amann kontra Svájc* [nagytanács] (27798/95), 2000. február 16., 50. pont; lásd még EJEB, *Kopp kontra Svájc* (23224/94), 1998. március 25., 55. pont; EJEB, *Iordachi és mások kontra Moldova* (25198/02), 2009. február 10., 50. pont.

109 EJEB, *Amann kontra Svájc* [nagytanács] (27798/95), 2000. február 16., 56. pont; lásd még EJEB, *Malone kontra Egyesült Királyság* (8691/79), 1984. augusztus 2., 66. pont; EJEB, *Silver és mások kontra Egyesült Királyság* (5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75), 1983. március 25., 88. pont.

„jogszabálytól" e tekintetben megkövetelt pontosság mértéke a konkrét tárgytól függ."[110]

Példa: A *Rotaru kontra Románia* ügyben[111] az EJEB megállapította az EJEE 8. cikkének megsértését, mert a román jog anélkül engedélyezte a nemzetbiztonságot érintő információk gyűjtését, rögzítését és titkos fájlokban való archiválását, hogy meghatározta volna e jogkörök gyakorlásának korlátait, amit így a hatóságok mérlegelésére bízott. A hazai jog nem határozta meg például a feldolgozható információk típusát, azon személyek kategóriáit, akikkel szemben megfigyelés foganatosítható, a körülményeket, amelyek fennállása esetén ezen intézkedések meghozhatók, illetve a követendő eljárást. E hiányosságok miatt a Bíróság megállapította, hogy a hazai jogszabály nem felel meg az EJEE 8. cikke szerinti előreláthatóság követelményének, és hogy e cikket megsértették.

Példa: A *Taylor-Sabori kontra Egyesült Királyság* ügyben[112] a felperes volt a rendőrségi megfigyelés célpontja. A felperes személyhívójának „klónozásával" a rendőrség el tudta fogni a neki küldött üzeneteket. A felperest ezt követően letartóztatták, és megvádolták ellenőrzött gyógyszer átadásában való közreműködéssel. Az ellene emelt vád részben a személyhívóra beérkezett írásos üzenetek rendőrség általi átiratán alapult. A felperes tárgyalásának idején azonban a brit jogban nem volt a magán távközlési rendszeren keresztül továbbított közlések lehallgatását szabályozó rendelkezés. Ezért a felperes jogainak sérelme nem állt „összhangban a jogszabályokkal". Az EJEB arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Törvényes cél előmozdítása

A törvényes cél lehet bármely nevesített közérdek, vagy mások jogai és szabadságai.

110 EJEB, *The Sunday Times kontra Egyesült Királyság* (6538/74), 1979. április 26., 49. pont; lásd még EJEB, *Silver és mások kontra Egyesült Királyság* (5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75), 1983. március 25., 88. pont.

111 EJEB, *Rotaru kontra Románia* [nagytanács] (28341/95), 2000. április 4., 57. pont; lásd még EJEB, *Association for European Integration and Human Rights és Ekimdzhiev kontra Bulgária* (62540/00), 2007. június 28.; EJEB, *Shimovolos kontra Oroszország* (30194/09), 2011. június 21.; és EJEB, *Vetter kontra Franciaország* (59842/00), 2005. május 31.

112 EJEB, *Taylor-Sabori kontra Egyesült Királyság* (47114/99), 2002. október 22.

Példa: A *Peck kontra Egyesült Királyság* ügyben[113] a felperes csuklójának elvágásával öngyilkosságot kísérelt meg az utcán, nem tudva arról, hogy egy zártláncú kamera filmre veszi őt ezalatt. A rendőrség, figyelve a zártláncú kamerát, letartóztatta őt és elküldte a zártláncú videofelvételt a médiának, amely a felperes arcának kitakarása nélkül közzétette azt. Az EJEB megállapította, hogy nincs olyan lényeges vagy elégséges ok, amely indokolná a felvétel hatóságok általi közvetlen nyilvánosságra hozatalát anélkül, hogy megszereznék a felperes hozzájárulását, vagy elfednék személyazonosságát. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Szükséges egy demokratikus társadalomban

Az EJEB kimondta, „a szükségesség fogalma magában foglalja, hogy a beavatkozás kényszerítő társadalmi igénynek felel meg, és azt is, hogy arányos a kitűzött jogszerű céllal".[114]

Példa: A *Khelili kontra Svájc* ügyben[115] a rendőrség egy rendőri ellenőrzés során a következő szövegű névjegyeket találta a felperesnél: „Kedves, csinos, harmincas évei második felében járó nő megismerkedne egy férfival rendszeres találkozás vagy szabadidős programok céljából. Telefonszám: [...]". A felperes állítása szerint ezt követően a rendőrség prostituáltként felvette őt a nyilvántartásába, mely tevékenység folytatását a felperes folyamatosan tagadta. A felperes a „prostituált" szó törlését kérte a számítógépes rendőrségi nyilvántartásból. Az EJEB főszabályként elismerte, hogy az egyén személyes adatainak azon a címen való őrzése, hogy a szóban forgó egyén más bűncselekményt is elkövethet, bizonyos körülmények között arányos lehet. A felperes esetében azonban az illegális prostitúció vádja túl tágnak és általánosnak tűnik, és konkrét tények nem is támasztják alá, mivel a felperest soha nem ítélték el illegális prostitúcióért, ezért a vád nem tekinthető olyannak, amely megfelel az EJEE 8. cikkének értelemben vett „kényszerítő társadalmi szükségletnek". Figyelemmel arra, hogy a hatóságoknak kell bizonyítaniuk a felperesről tárolt adatok pontosságát, továbbá a felperes jogaiba való beavatkozás súlyosságára, a Bíróság úgy ítélte meg, hogy a „prostituált" szó évekig való fenntartása a rendőrségi adatállományban nem szükséges egy demokratikus társadalomban. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

113 EJEB, 44647/98. sz. *Peck kontra Egyesült Királyság* ügy, 2003. január 28., különösen a 85. pont.

114 EJEB, *Leander kontra Svédország* (9248/81), 1985. július 11., 58. pont.

115 EJEB, *Khelili kontra Svájc* (16188/07), 2011. október 18.

Példa: A *Leander kontra Svédország* ügyben[116] az EJEB megállapította, hogy nemzetbiztonsági szempontból fontos állásra pályázó személyek titkos ellenőrzése önmagában nem ellentétes a demokratikus társadalomban való szükségesség követelményével. Az érintett érdekeinek védelmére a nemzeti jogban megállapított külön biztosítékok – például a parlament és az igazságügyi miniszter által gyakorolt ellenőrzés – eredményeként az EJEB arra a következtetésre jutott, hogy a svéd személyzeti ellenőrzési rendszer megfelel az EJEE 8. cikkének (2) bekezdésében szereplő követelményeknek. Tekintettel a rendelkezésére álló tág mérlegelési mozgástérre, az alperes állam megfontolhatta, hogy a felperes esetében a nemzetbiztonsági érdek elsőbbséget élvez-e az egyéni érdekkel szemben. A Bíróság arra a következtetésre jutott, hogy nem sértették meg az EJEE 8. cikkét.

3.1.2. A jogszerű korlátozások feltételei az Európai Unió Chartája szerint

A Charta szerkezete és szóhasználata is eltér az EJEE-étől. A Charta nem szól a garantált jogokkal való ütközésekről, de tartalmaz egy rendelkezést a Charta által elismert jogok és szabadságok gyakorlásának korlátozásáról.

Az 52. cikk (1) bekezdése szerint a Charta által elismert jogok és szabadságok gyakorlására, és ennek megfelelően a személyes adatok védelméhez való jog gyakorlására vonatkozó korlátozások csak akkor elfogadhatók, ha:

- jogszabály rendelkezik róluk; és
- tiszteletben tartják az adatvédelemhez való jog lényegét; és
- az arányosság elvének figyelembevétele mellett szükségesek; és
- az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálják.

116 EJEB, *Leander kontra Svédország* (9248/81), 1985. július 11., 59. és 67. pont.

Példák: A *Volker és Markus Schecke* ügyben[117] az EUB arra a következtetésre jutott, hogy a Tanács és a Bizottság azzal, hogy kötelezővé tette [bizonyos mezőgazdasági alapokból] nyújtott támogatások valamennyi természetes személy kedvezményezettjeire vonatkozó személyes adatoknak a közzétételét – anélkül, hogy különbséget tett volna lényeges kritériumok alapján (ilyenek például az időszak, amelyen keresztül a szóban forgó személyek a támogatást kapták, a támogatás gyakorisága, jelleg vagy összege) –, túllépett az arányosság elve tiszteletben tartása által megkövetelt határokon.

Ezért az EUB szükségesnek találta az 1290/2005/EK tanácsi rendelet bizonyos rendelkezéseinek érvénytelenítését, továbbá a 259/2008/EK rendeletet teljes egészében érvénytelennek nyilvánította.[118]

Az eltérő szóhasználat ellenére, a jogszerű adatfeldolgozásra vonatkozó, a Charta 52. cikkének (1) bekezdésében foglalt feltételek emlékeztetnek az EJEE 8. cikkének (2) bekezdésére. A Charta 52. cikkének (1) bekezdésében felsorolt feltételek nyilvánvalóan megfelelnek az EJEE 8. cikkének (2) bekezdésében leírtaknak, mivel a Charta 52. cikke (3) bekezdésének első mondata szerint „amennyiben a Charta olyan jogokat tartalmaz, amelyek megfelelnek az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményben biztosított jogoknak, akkor e jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az említett egyezményben szerepelnek."

Az 52. cikk (3) bekezdésének utolsó mondata szerint azonban „ez a rendelkezés nem akadályozza meg azt, hogy az Unió joga kiterjedtebb védelmet nyújtson". Az EJEE 8. cikke (2) bekezdésének és az 52. cikk (3) bekezdése első mondatának összehasonlítása szempontjából ez csak azt jelenti, hogy az EJEE 8. cikke (2) bekezdése szerinti igazolható sérelem feltételei a Charta szerinti adatvédelemhez való jog törvényes korlátozására vonatkozó minimumkövetelmények. Következésképpen személyes adatok jogszerű feldolgozásához az uniós jog szerint legalább az EJEE 8. cikkének (2) bekezdésében meghatározott feltételek teljesülése szükséges; az uniós jog azonban egyedi esetekre vonatkozóan további követelményeket is előírhat.

117 EUB, C-92/09. és C-93/09. sz. *Volker és Markus Schecke GbR (C-92/09) és Hartmut Eifert kontra Land Hessen (C-93/09)* egyesített ügyek, 2010. november 9., 89. és 86. pont.

118 A Tanács 1290/2005/EK rendelete (2005. június 21.) a közös agrárpolitika finanszírozásáról, HL L 209., 2005; valamint A Bizottság 259/2008/EK rendelete (2008. március 18.) az 1290/2005/EK tanácsi rendeletnek az Európai Mezőgazdasági Garanciaalapból (EMGA) és az Európai Mezőgazdasági Vidékfejlesztési Alapból (EMVA) származó pénzeszközök kedvezményezettjeire vonatkozó információk nyilvánosságra hozatalának tekintetében történő alkalmazása részletes szabályainak megállapításáról, HL L 76., 2008.

Azt, hogy a jogszerű adatfeldolgozás uniós jog szerinti elve megfelel az EJEE vonatkozó rendelkezéseinek, az EUSZ 6. cikkének (3) bekezdése is alátámasztja, amely a következőképpen rendelkezik: „Az alapvető jogok, ahogyan azokat az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény biztosítja […], az uniós jogrend részét képezik mint annak általános elvei".

3.2. A célmeghatározás és a célhoz kötöttség elve

Főbb pontok

- Az adatkezelés célját világosan meg kell határozni még az adatkezelés megkezdése előtt.
- Az uniós jog szerint az adatfeldolgozás célját kifejezetten meg kell határozni; az Európa Tanács joga ezt a kérdést a hazai jogra hagyja.
- A meg nem határozott célokra történő adatkezelés nem áll összhangban az adatvédelmi joggal.
- Adatok más célra való további felhasználásához kiegészítő jogalapra van szükség, ha az adatfeldolgozás új célja nem összeegyeztethető az eredeti céllal.
- Adatok harmadik feleknek való továbbítása új célnak minősül, amelyhez további jogalap szükséges.

A célmeghatározás és a célhoz kötöttség lényegében azt jelenti, hogy a személyesadat-feldolgozás törvényessége az adatkezelés céljától függ.[119] Az adatkezelőnek még az adatfeldolgozás megkezdése előtt meg kell jelölnie és nyilvánvalóvá kell tennie a célt.[120] Az **uniós jog** szerint ezt vagy a megfelelő hatósághoz benyújtott nyilatkozattal, más szóval bejelentéssel, vagy legalább belső dokumentummal kell megtenni, amelyet az adatkezelő köteles betekintés céljából a felügyelő hatóság rendelkezésére bocsátani, továbbá hozzáférhetővé tenni az érintett számára.

Személyes adatok meg nem határozott és/vagy korlátlan célokra való feldolgozása jogellenes.

119 108. egyezmény, 5. cikk, b) pont; adatvédelmi irányelv, 6. cikk, (1) bekezdés, b) pont.

120 Lásd még a 29. cikk szerinti munkacsoport *03/2013. számú, a célhoz kötöttségről szóló véleményét (2013)*, WP 203, Brüsszel, 2013. április 2.

Minden új személyesadat-feldolgozási célhoz saját konkrét jogalapnak kell tartoznia; nem lehet arra hivatkozni, hogy az adatokat eredetileg más jogszerű célra szerezték be vagy dolgozták fel. Másrészt a jogszerű feldolgozás az eredetileg megjelölt célra korlátozódik, minden új feldolgozási célhoz külön új jogalap szükséges. Adatok harmadik felekkel való közlését különösen gondosan kell mérlegelni, mivel az ilyen közlés rendszerint új célnak minősül, ezért az adatgyűjtéshez használttól eltérő jogalap szükséges hozzá.

Példa: Egy légitársaság a járat megfelelő üzemeltetését szolgáló foglalásokhoz adatokat gyűjt utasaitól. A légitársaságnak a következő adatokra lesz szüksége: az utasok ülésszáma; speciális fizikai korlátozások, például kerekesszék-igény; valamint speciális élelmiszer-igények, köztük a kóser vagy halal élelmiszer. Ha a légitársaságokat az utas-nyilvántartási adatállományban található adatoknak a célállomás helye szerinti bevándorlási hatóságokhoz való továbbítására kérik, a szóban forgó adatokat ezt követően idegenrendészeti ellenőrzés céljára használják fel, ami eltér az adatgyűjtés eredeti céljától. Ezen adatoknak a bevándorlási hatósághoz történő továbbításához tehát új, külön jogalapra lesz szükség.

Egy adott cél terjedelmének és korlátainak mérlegelésekor a 108. egyezmény és az adatvédelmi irányelv az összeegyeztethetőség fogalmát hívja segítségül: az adatok összeegyeztethető célokra való felhasználása az eredeti jogalap alapján engedélyezett. Az azonban nincs meghatározva, hogy mit jelent az „összeegyeztethető" – a fogalmat eseti alapon kell értelmezni.

Példa: A Sunshine vállalat ügyféladatait, amelyekre a cég ügyfélkapcsolat-kezelési (CRM) tevékenysége során tett szert, egy direkt marketing cégnek, a Moonlight vállalatnak értékesíti, amely harmadik cégek marketing kampányainak támogatására kívánja azokat felhasználni; ez új cél, amely összeegyeztethetetlen a CRM-mel, azaz a Sunshine vállalat eredeti céljával, amelyre az ügyféladatokat gyűjtötte. Az adatok Moonlight vállalatnak történő értékesítéséhez tehát saját jogalap szükséges.

Ezzel szemben, ha a Sunshine vállalat a CRM-adatokat saját marketing céljaira használja fel, például a saját termékeire vonatkozó marketing üzeneteket küld a saját ügyfeleinek, az általában elfogadott, mint összeegyeztethető cél.

Az adatvédelmi irányelv kifejezetten kimondja, hogy „a személyes adatok további feldolgozása történelmi, statisztikai vagy tudományos célokra nem

tekintendő összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat".[121]

Példák: A Sunshine vállalat CRM-adatokat gyűjtött és tárolt vásárlóiról. Ezen adatok Sunshine vállalat általi, a vásárlók vásárlási szokásainak statisztikai elemzése céljára való további felhasználása megengedhető, mivel a statisztikai elemzés összeegyeztethető cél. Nincs szükség további jogalapra, például az érintettek hozzájárulására.

Ha ugyanezen adatokat harmadik félnek, a Starlight vállalatnak szeretnék továbbítani kizárólag statisztikai célokra, a továbbítás további jogalap nélkül megengedhető lenne, de csak azzal a feltétellel, hogy megfelelő garanciákat biztosítanak, például elfedik az érintettek személyazonosságát, hiszen statisztikai célokra általában nincs szükség a személyazonosságra.

3.3. Az adatminőségre vonatkozó elvek

Főbb pontok

- Az adatminőségre vonatkozó elveket az adatkezelőnek minden adatkezelési művelet során érvényesítenie kell.
- A korlátozott adatmegőrzés elve előírja, hogy az adatokat törölni kell, amint már nincs rájuk szükség arra a célra, amelyre gyűjtötték őket.
- A korlátozott adatmegőrzés elve alóli kivételeket törvényben kell meghatározni, és az érintettek védelme érdekében minden ilyen esetben külön biztosítékokra van szükség.

3.3.1. Az adatok relevanciájának elve

Csak olyan adatok kezelhetők, amelyek „gyűjtésük és/vagy további feldolgozásuk célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek".[122] A kiválasztott adatkategóriáknak az adatkezelési műveletek általános célja eléréséhez

121 Ilyen nemzeti rendelkezésre példa az osztrák adatvédelmi törvény (*Datenschutzgesetz),* Fed. Law Gazette I 165/1999. szám, 46. pont, angol nyelven elérhető a következő címen: www.dsk.gv.at/DocView.axd?CobId=41936.

122 108. egyezmény, 5. cikk, c) pont; adatvédelmi irányelv, 6. cikk, (1) bekezdés, c) pont.

szükségesnek kell lenniük, és az adatkezelőnek szigorúan azon információkra kell korlátoznia az adatgyűjtést, amelyek a feldolgozás által támogatott konkrét cél szempontjából közvetlenül relevánsak.

A mai társadalomban az adatok relevanciája elvéhez még egy szempont kapcsolódik: a speciális adatvédelmi technológia segítségével olykor a személyesadat-felhasználás teljes kiküszöbölése, vagy akár álnéven kezelt adatok használata is lehetséges, ami a magánélet tiszteletben tartását biztosító megoldást eredményez. Ez a kiterjedtebb adatfeldolgozó rendszerekben különösen helyénvaló.

Példa: Egy városi tanács bizonyos díj ellenében chipkártyát ad a városi tömegközlekedést rendszeresen igénybevevő közlekedőknek. A kártya felületén szerepel a használó neve írásos formában, és a chipben elektronikus formában is rögzítve van. Ha a közlekedő személy autóbuszt vagy villamost vesz igénybe, a chipkártyát el kell húzni a buszra vagy villamosra felszerelt leolvasókészülék előtt. A készülék által leolvasott adatokat elektronikusan összevetik egy adatbázissal, amely az utazási kártyát megvásárolt személyek nevét tartalmazza.

Ez a rendszer nem tartja be optimálisan az adatok relevanciájának elvét: annak ellenőrzése, hogy egy személy használhatja-e a közlekedési eszközöket, anélkül is megoldható, hogy összevetnék a chipen található személyes adatokat egy adatbázissal. Elég lenne például egy speciális elektronikus kép, pl. vonalkód a kártya chipjében, amely, ha elhúzzák a leolvasókészülék előtt, igazolná a kártya érvényességét. Egy ilyen rendszer nem rögzítené, hogy ki, mikor, milyen közlekedési eszközt használt. Személyes adatok gyűjtésére nem kerülne sor, ami a relevancia elve értelmében optimális megoldás lenne, mivel ez az elv végső fokon az adatgyűjtés minimalizálására vonatkozó kötelezettséget ír elő.

3.3.2. Az adatok pontosságának elve

A személyes információkat birtokló adatkezelő anélkül nem használhatja fel ezeket az információkat, hogy lépéseket tenne annak kellő bizonyossággal történő biztosítására, hogy az adatok pontosak és naprakészek.

Az adatok pontosságának biztosítására irányuló kötelezettséget az adatkezelés céljával összefüggésben kell megítélni.

Példa: Egy bútorkereskedelmi vállalat számla kiállításához begyűjtötte egy vásárló személyazonossági és lakcímadatait. Hat hónappal később ugyanez a cég marketing kampányt kíván indítani, és meg szeretné keresni a korábbi vevőit. Ennek érdekében hozzá szeretne férni a nemzeti lakcímnyilvántartáshoz, amely valószínűsíthetően tartalmazza a legfrissebb címeket, mivel az állampolgárok jogszabály erejénél fogva kötelesek bejelenteni aktuális címüket. E nyilvántartás adataihoz csak olyan személyek/szervezetek férhetnek hozzá, akik/amelyek alapos indokot tudnak megjelölni.

Ebben a helyzetben a vállalat nem hivatkozhat arra, hogy az adatokat pontosan és naprakészen kell tartani és ő jogosult a korábbi vásárlóinak új lakcímadatait a lakcímnyilvántartásból kigyűjteni. Az adatokat a számlázás során gyűjtötték; ebből a szempontból az értékesítés időpontjában érvényes cím a releváns. Új lakcímadatok gyűjtésére nincs jogalap, mivel a marketing nem olyan érdek, amely előnyben részesítendő az adatvédelemhez való joggal szemben, a nyilvántartás adataihoz való hozzáférést tehát nem indokolhatja.

Lehetnek olyan esetek is, amikor a tárolt adatok frissítését jogszabály tiltja, mert az adatok tárolásának elsődleges célja események dokumentálása.

Példa: Egy orvosi beavatkozás jegyzőkönyvét nem szabad megváltoztatni, más szóval „frissíteni" még akkor sem, ha a jegyzőkönyvben szereplő megállapítások később tévesnek bizonyulnak. Ilyen körülmények között csupán a jegyzőkönyvben szereplő észrevételekhez fűzhetők kiegészítések, amennyiben egyértelműen megjelölik, hogy utólagos hozzájárulásokról van szó.

Másrészt viszont vannak olyan helyzetek, amikor az adatok pontosságának rendszeres ellenőrzése, a frissítést is beleértve, feltétlenül szükséges, mert ha az adatokat pontatlanul hagyják, az kárt okozhat az érintettnek.

Példa: Ha valaki szerződést akar kötni egy bankkal, a bank általában ellenőrzi a leendő ügyfél hitelképességét. E célból elérhetők speciális adatbankok, amelyek magánszemélyek hiteltörténetére vonatkozóan tartalmaznak adatokat. Ha egy ilyen adatbázis helytelen vagy idejétmúlt adatokat tartalmaz valakiről, ez súlyos problémákat okozhat a személy számára. Ezért az ilyen adatbázisok kezelőinek különösen törekedniük kell a pontosság elvének betartására.

Ezenfelül a nem tényekre, hanem gyanúra – például bűnügyi nyomozásra – vonatkozó adatok addig gyűjthetők és tárolhatók, amíg az adatkezelő jogalappal rendelkezik a szóban forgó információk gyűjtésére, és gyanúja kellően igazolt.

3.3.3. Az adatok korlátozott ideig történő megőrzésének elve

Az adatvédelmi irányelv 6. cikke (1) bekezdésének e) pontja és ehhez hasonlóan a 108. egyezmény 5. cikkének e) pontja kötelezően előírja a tagállamok számára, hogy a személyes adatok „tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatok gyűjtése vagy további feldolgozása céljainak eléréséhez szükséges ideig teszi lehetővé". Az adatokat tehát törölni kell, amint a célok teljesültek.

Az *S. és Marper* ügyben az EJEB megállapította, hogy az Európa Tanács vonatkozó eszközeinek alapelvei, valamint a többi szerződő fél joga és gyakorlata előírja, hogy az adatmegőrzésnek az adatgyűjtés céljával arányosnak és időben korlátozottnak kell lennie, különösen a rendőrségi ágazatban.[123]

A személyes adatok tárolására vonatkozó időbeli korlátozás azonban csak olyan adatokra vonatkozik, amelyeket az érintett azonosítását lehetővé tevő formában tárolnak. Azon adatok jogszerű tárolása is lehetséges tehát, amelyekre már nincs szükség, ha az adatokat anonimizálják vagy pszeudoanonimizálják.

Az adatok történelmi, statisztikai vagy tudományos célból történő tárolását az adatvédelmi irányelv kifejezetten mentesíti a korlátozott adatmegőrzés elve alól.[124] A személyes adatok ilyen jellegű folyamatos tárolásához és felhasználásához azonban a nemzeti jognak külön biztosítékokat kell elrendelnie.

123 EJEB, *S. és Marper kontra Egyesült Királyság* (30562/04 és 30566/04), 2008. december 4.; például lásd még EJEB, *M.M. kontra Egyesült Királyság* (24029/07), 2012. november 13.

124 Adatvédelmi irányelv, 6. cikk, (1) bekezdés, e) pont.

3.4. A tisztességes adatkezelés elve

Főbb pontok

- A tisztességes adatkezelés átláthatóságot jelenti – különösen az érintettek felé.
- Az adatkezelés megkezdése előtt az adatkezelőknek legalább az adatkezelés céljáról és az adatkezelő kilétéről és címéről tájékoztatniuk kell az érintetteket.
- Kifejezett jogszabályi előírás hiányában a személyes adatok kezelése nem lehet titkos vagy rejtett.
- Az érintettek az adatkezelés helyén hozzáférhetnek adataikhoz.

A tisztességes adatkezelés elve elsősorban az adatkezelő és az érintett közötti jogviszonyra vonatkozik.

3.4.1. Átláthatóság

Ez az elv azt a kötelezettséget állapítja meg az adatkezelő számára, hogy folyamatosan tájékoztassa az érintetteket adataik felhasználásának módjáról.

Példa: A *Haralambie kontra Románia* ügyben[125] a felperes hozzáférést kért a róla szóló titkosszolgálati aktához, de kérésének csak öt évvel később tettek eleget. Az EJEB ismételten rámutatott, hogy azon egyéneknek, akikről állami hatóságok személyes aktát tárolnak, elemi érdeke fűződik ahhoz, hogy hozzáférhessenek a szóban forgó adatállományhoz. A hatóságoknak az információkhoz való hozzáférés megszerzésével kapcsolatban hatékony eljárásról kellett volna rendelkezniük. Az EJEB úgy vélte, hogy sem a továbbított adatállományok mennyisége, sem az irattári rendszer hiányosságai nem indokolnak ötéves késedelmet a felperesi kérelem megadása tekintetében. A hatóságok nem biztosítottak a felperesnek hatékony és elérhető eljárást arra, hogy ésszerű időn belül hozzáférést szerezhessen személyes adatainak állományához. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Az adatkezelési műveleteket könnyen érthető módon el kell magyarázni az érintetteknek, hogy megértsék, mi történik adataikkal. Az érintettnek ahhoz is joga van,

125 EJEB, *Haralambie kontra Románia* (21737/03), 2009. október 27.

hogy az adatkezelő kérésére tájékoztassa arról, hogy adatait kezelik-e, és ha igen, melyeket.

3.4.2. A bizalom kiépítése

Az adatkezelőknek dokumentálniuk kell az érintettek és a nagyközönség felé, hogy jogszerűen és átláthatóan kezelik az adatokat. A műveletek nem történhetnek titokban, és nem járhatnak előre nem látható negatív hatásokkal. Az adatkezelőknek biztosítaniuk kell, hogy a vásárlók, ügyfelek vagy polgárok tájékoztatást kapjanak adataik felhasználásáról. Emellett az adatkezelőknek – amennyire lehetséges – úgy kell eljárniuk, hogy azonnal teljesítsék az érintettek kéréseit, különösen ha hozzájárulásuk jelenti az adatkezelés jogalapját.

Példa: A *K.H. és mások kontra Szlovákia* ügyben[126] nyolc roma származású nő volt a felperes, akiket két kelet-szlovákiai kórházban kezeltek terhességük és szülésük során. Később egyikük sem tudott teherbe esni, többszöri kísérletre sem. A nemzeti bíróságok elrendelték, hogy a kórházak engedélyezzék a felperesek és képviselőik számára, hogy konzultáljanak és készítsenek írásos kivonatokat a kórlapokról, de – állítólag a visszaélés megelőzése érdekében – elutasították a dokumentumok fénymásolására irányuló kérésüket. Az államoknak az EJEE 8. cikke alapján fennálló pozitív kötelezettségei feltétlenül magukban foglalják azt a kötelezettséget is, hogy az érintettnek másolatot adjanak a saját adatállományáról. Az államnak kellett volna meghatároznia a személyes adatállományok fénymásolására vonatkozó intézkedéseket, illetve adott esetben megjelölnie az elutasítás kényszerű indokait. A felperesek ügyében a hazai bíróságok elsősorban a vonatkozó információk visszaéléssel szembeni védelmének szükségességével indokolták a kórlapok fénymásolásának tiltását. Az EJEB azonban nem látta be, hogyan tudtak volna az alperesek, akik mindenképpen hozzáférhettek teljes orvosi kartonjukhoz, visszaélni a saját magukra vonatkozó információkkal. Ezenfelül a visszaélés kockázata a fénymásolatok alperesektől való megtagadásán kívül más eszközökkel – például a kórlapokhoz való hozzáférésre jogosult személyek körének korlátozásával – is kivédhető lett volna. Az állam nem tudott kellően kényszerítő okokat kimutatni ahhoz, hogy az alperesektől megtagadják az egészségi állapotukkal kapcsolatos információkhoz való tényleges hozzáférést. A Bíróság arra a következtetésre jutott, hogy megsértették a 8. cikket.

126 EJEB, *K.H. és társai kontra Szlovákia* (32881/04), 2009. április 28.

Internetes szolgáltatásokkal kapcsolatban az adatfeldolgozó rendszerek tulajdonságainak lehetővé kell tenniük, hogy az érintettek valóban megtudják, mi történik az adataikkal.

A tisztességes adatkezelés azt is jelenti, hogy az adatkezelők készek arra, hogy a szolgáltatásra kötelező jogi minimumkövetelményeken túl az érintett rendelkezésére álljanak, amennyiben az érintett törvényes érdekei úgy kívánják.

3.5. Az elszámoltathatóság elve

Főbb pontok

- Az elszámoltathatósághoz az szükséges, hogy az adatkezelők adatkezelési tevékenységük során aktívan hajtsák végre az adatvédelem előmozdítására és biztosítására irányuló intézkedéseket.
- Adatkezelési műveleteik során az adatkezelők felelősek az adatvédelmi jog betartásáért.
- Az adatkezelőknek bármikor tudniuk kell bizonyítani az adatvédelmi rendelkezések betartását az érintettek, a nyilvánosság és a felügyeleti hatóságok felé.

2013-ban a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) adatvédelmi iránymutatásokat fogadott el, amelyek kiemelték az adatkezelők fontos szerepét az adatvédelem gyakorlati megvalósulása terén. Az iránymutatásokban szerepelt az elszámoltathatóság elve, miszerint „az adatkezelőnek elszámoltathatónak kell lennie azon intézkedések betartásáért, amelyek érvényre juttatják a fenti [fő] elveket."[127]

Míg a 108. egyezmény nem említi az adatkezelők elszámoltathatóságát, azaz lényegében a hazai jogra hagyja ezt a kérdést, az adatvédelmi irányelv 6. cikkének (2) bekezdése kimondja, hogy az adatkezelő feladata gondoskodni az (1) bekezdésben szereplő, az adatok minőségével kapcsolatos elvek betartatásáról.

Példa: Az elszámoltatás elvének hangsúlyozására vonatkozó jogalkotási példa a 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) 2009-es

127 OECD (2013): *Az adatvédelemre és az országhatárokat átlépő személyesadat-áramlásra vonatkozó iránymutatások*, 14. cikk.

módosítása.[128] A módosított 4. cikk szerint az irányelv kötelezettséget ír elő „a személyes adatok feldolgozásának biztonságára vonatkozó politika" biztosítására. Ami tehát a szóban forgó irányelv biztonsági rendelkezéseit illeti, a jogalkotó úgy döntött, hogy kifejezett követelményként kell bevezetni a biztonsági politika létrehozását és végrehajtását.

A 29. cikk szerinti munkacsoport véleménye szerint[129] az elszámoltathatóság lényege az adatkezelő arra vonatkozó kötelezettsége, hogy:

- olyan intézkedéseket hozzon, amelyek az adatkezelési műveletekkel összefüggésben – rendes körülmények között – garantálják az adatvédelmi szabályok betartását; és

- olyan dokumentációval rendelkezzen, amely bizonyítja az érintettek és a felügyeleti hatóságok számára, hogy milyen intézkedéseket hoztak az adatvédelmi szabályok betartatására.

Az elszámoltathatóság elvéhez tehát az adatkezelőknek aktívan bizonyítaniuk kell a szabályok betartását, nem szabad csupán arra várniuk, hogy az érintettek vagy a felügyeleti hatóságok mutassanak rá a hiányosságokra.

128 Az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról, HL L 337., 2009, 11. o.

129 A 29. cikk szerinti munkacsoport *3/2010. sz. véleménye az elszámoltathatóság elvéről*, WP 173, Brüsszel, 2010. július 13.

4

Az európai adatvédelmi jog szabályai

EU	Tárgyalt kérdések	Európa Tanács
A nem érzékeny adatok jogszerű kezelésére vonatkozó szabályok		
Adatvédelmi irányelv, 7. cikk, a) pont	**Hozzájárulás**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk, b) pont és 3.6. cikk
Adatvédelmi irányelv, 7. cikk, b) pont	**Szerződéses (illetve szerződéskötés előtti) jogviszony**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk, b) pont
Adatvédelmi irányelv, 7. cikk, c) pont	**Az adatkezelő jogi kötelezettségei**	A profilalkotásra vonatkozó ajánlás, 3,4. cikk, a) pont
Adatvédelmi irányelv, 7. cikk, d) pont	**Az érintett létfontosságú érdekei**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk, b) pont
Adatvédelmi irányelv, 7. cikk, e) pont és 8. cikk, (4) bekezdés EUB, C-524/06. sz. *Huber kontra Németország* ügy, 2008. december 16.	**Közérdek és hivatali hatáskör gyakorlása**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk, b) pont
Adatvédelmi irányelv, 7. cikk f) pont, 8. cikk, (2) és (3) bekezdés EUB, C-468/10. és C-469/10. sz. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) kontra Administración del Estado* egyesített ügyek, 2011. november 24.	**Mások törvényes érdekei**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk, b) pont

EU	Tárgyalt kérdések	Európa Tanács
Az érzékeny adatok jogszerű kezelésére vonatkozó szabályok		
Adatvédelmi irányelv, 8. cikk, (1) bekezdés	A kezelés általános tilalma	108. egyezmény, 6. cikk
Adatvédelmi irányelv, 8. cikk, (2)–(4) bekezdés	Kivételek az általános tilalom alól	108. egyezmény, 6. cikk
Adatvédelmi irányelv, 8. cikk, (5) bekezdés	(Büntető)ítéletekre vonatkozó adatok kezelése	108. egyezmény, 6. cikk
Adatvédelmi irányelv, 8. cikk, (7) bekezdés	Személyazonosító számok kezelése	
A biztonságos kezelésre vonatkozó szabályok		
Adatvédelmi irányelv, 17. cikk	Kötelezettség a biztonságos kezelés biztosítására	108. egyezmény, 7. cikk
		EJEB, *I. kontra Finnország* (20511/03. sz. ügy), 2008. július 17.
Elektronikus hírközlési adatvédelmi irányelv, 4. cikk, (2) bekezdés	Adatsértés bejelentése	
Adatvédelmi irányelv, 16. cikk	Titoktartási kötelezettség	
Az adatkezelés átláthatóságára vonatkozó szabályok		
	Az átláthatóság általában	108. egyezmény, 8. cikk, a) pont
Adatvédelmi irányelv, 10. és 11. cikk	Tájékoztatás	108. egyezmény, 8. cikk, a) pont
Adatvédelmi irányelv, 10. és 11. cikk	A tájékoztatási kötelezettség alóli kivételek	108. egyezmény, 9. cikk
Adatvédelmi irányelv, 18. és 19. cikk	Értesítés	A profilalkotásra vonatkozó ajánlás, 9.2. cikk, a) pont
Az előírások betartásának előmozdítására vonatkozó szabályok		
Adatvédelmi irányelv, 20. cikk	Előzetes ellenőrzés	
Adatvédelmi irányelv, 18. cikk, (2) bekezdés	Adatvédelmi felelősök	A profilalkotásra vonatkozó ajánlás, 8,3. cikk
Adatvédelmi irányelv, 27. cikk	Eljárási szabályzatok	

Az elvek szükségképpen általános jellegűek. Konkrét helyzetekre való alkalmazásuk során van bizonyos értelmezési mozgástér, és az eszközök is megválaszthatók. Az **Európa Tanács joga** szerint a 108. egyezmény részes felei hazai jogukban maguk pontosíthatják az értelmezést. Az **uniós jogban** más a helyzet: a belső piacon

az adatvédelem létrehozása érdekében már uniós szinten részletesebb szabályozást tartottak szükségesnek, hogy összehangolják a tagállamok nemzeti jogszabályainak adatvédelmi szintjét. Az adatvédelmi irányelv a 6. cikkben meghatározott elvek alapján részletes szabályok együttesét hozza létre, amelyet a nemzeti jogban hűen végre kell hajtani. Az európai szintű részletes adatvédelmi szabályokkal kapcsolatos alábbi észrevételek ezért túlnyomórészt az uniós joggal foglalkoznak.

4.1. A jogszerű adatkezelésre vonatkozó szabályok

Főbb pontok

- Személyes adatok akkor kezelhetők jogszerűen, ha:
  - az érintett hozzájárulásán alapul; vagy
  - az érintettek létfontosságú érdeke miatt szükséges; vagy
  - a z adatkezelés okát mások törvényes érdekei jelentik, de csak annyiban, amennyiben ezt az indokot az érintettek alapvető jogainak védelme nem írja felül.
- Az érzékeny adatok jogszerű kezelése speciális, szigorúbb rend szerint történik.

Az adatvédelmi irányelv két különböző szabályrendszert állapít meg az adatok kezelésére: egyet a 7. cikkben a nem érzékeny adatokra, egyet pedig a 8. cikkben az érzékeny adatokra vonatkozóan.

4.1.1. Nem érzékeny adatok jogszerű feldolgozása

A 95/46/EK irányelvnek „A személyes adatok kezelésének jogszerűségére vonatkozó általános szabályok" című II. fejezete úgy rendelkezik, hogy valamennyi személyesadat-kezelésnek – a 13. cikk alapján engedélyezett kivételekkel – elsőként az adatvédelmi irányelv 6. cikkében meghatározott, az adatok minőségére vonatkozó elveknek, másodsorban pedig az adatkezelés jogszerűvé tételére vonatkozó, a

7. cikkben felsorolt kritériumoknak kell megfelelnie.[130] Ez megmagyarázza azokat az eseteket, amelyek a nem érzékeny személyes adatok kezelését jogszerűvé teszik.

Hozzájárulás

Az **Európa Tanács jogát** tekintve, a hozzájárulást sem az EJEE 8. cikke, sem a 108. egyezmény nem említi. Az EJEB joggyakorlatában és számos európa tanácsi ajánlásban viszont szerepel. Az **uniós jogban** a hozzájárulás mint a jogszerű adatfeldolgozás alapja egyértelműen megjelenik az adatvédelmi irányelv 7. cikkének a) pontjában, és a Charta 8. cikke is kifejezetten említi.

Szerződéses jogviszony

Az **uniós jogban** a személyes adatok jogszerű kezelésének másik jogalapja, amit az adatvédelmi irányelv 7. cikkének b) pontja is megnevez, az az eset, amikor „az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél". Ez a rendelkezés a szerződéskötés előtti jogviszonyokra is vonatkozik. Például: egy fél szerződést kíván kötni, de még nem kötötte meg – esetleg mert még bizonyos ellenőrzések hátra vannak. Ha ehhez az egyik félnek adatokat kell feldolgoznia, ez az adatkezelés törvényes, amennyiben „az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges".

Ami az **Európa Tanács jogát** illeti, az EJEE 8. cikkének (2) bekezdésében az adatvédelemhez való jogba való igazolható beavatkozás indokaként szerepel a „mások jogainak és szabadságainak védelme".

Az adatkezelő jogi kötelezettségei

Az **uniós jog** kifejezetten említést tesz egy másik kritériumról, ami jogszerűvé teszi az adatkezelést: ha „az adatkezelés az adatkezelőre vonatkozó jogi kötelezettségnek teljesítéséhez szükséges" (az adatvédelmi irányelv 7. cikkének c) pontja). Ez a rendelkezés a magánszektorban tevékenykedő adatkezelőkre utal; a közszférabeli adatkezelők az irányelv 7. cikke e) pontjának hatálya alá tartoznak. Számos olyan eset van, amikor magánszektorbeli adatkezelőket jogszabály kötelez arra, hogy

130 EUB, C-465/00., C-138/01. és C-139/01. sz. *Österreichischer Rundfunk és mások* egyesített ügyek, 2003. május 20., 65. pont; EUB, C-524/06. sz. *Huber kontra Németország* ügy, 2008. december 16., 48. pont; EUB, C-468/10. és C-469/10. sz. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) kontra Administración del Estado* egyesített ügyek, 2011. november 24., 26. pont.

másokról adatokat dolgozzanak fel; pl. az orvosok és a kórházak jogszabályi kötelezettsége, hogy a betegek kezelésével kapcsolatos adatokat több évig tárolják, a munkavállalóknak társadalombiztosítási és adózási okokból adatokat kell feldolgozniuk munkavállalóikról, továbbá a vállalkozásoknak adózási okokból adatokat kell feldolgozniuk ügyfeleikről.

Azzal összefüggésben, hogy a légitársaságok kötelesek az utas-nyilvántartási adatokat külföldi idegenrendészeti hatóságoknak továbbítani, felmerült a kérdés, hogy az uniós jog szerinti adatkezelés törvényes jogalapját alkothatja-e *külföldi* jogszabály alapján fennálló jogi kötelezettség (ezt a kérdést részletesebben a *6.2.* szakaszban tárgyaljuk).

Az adatkezelő jogi kötelezettségei az **Európa Tanács jogában** is szolgálhatnak a törvényes adatkezelés alapjául. Ahogyan fentebb már rámutattunk, egy magánszektorbeli adatkezelő jogi kötelezettségei – az EJEE 8 cikkének (2) bekezdése szerint – a mások törvényes érdekeinek csak egy konkrét esetét alkotják. A fenti példa tehát az Európa Tanács joga esetében is releváns.

Az érintett létfontosságú érdekei

Az **uniós jogban** az **adatvédelmi irányelv** 7. cikkének d) pontja úgy rendelkezik, hogy a személyes adatok kezelése akkor jogszerű, ha „az érintett létfontosságú érdekei védelméhez szükséges". Ezek az érdekek, amelyek szorosan összefüggnek az érintett továbbélésével, alkothatják például az egészségi állapotra vonatkozó adatok vagy az eltűnt személyekkel kapcsolatos adatok törvényes felhasználásának jogalapját.

Az **Európa Tanács joga** szerint az EJEE 8. cikkében az adatvédelemhez való jogba való igazolható beavatkozás indokaként nem szerepelnek az érintett létfontosságú érdekei. A bizonyos területeken a108. egyezményt kiegészítő egyes európa tanácsi ajánlások azonban kifejezetten említik az érintett létfontosságú érdekeit mint a jogszerű adatkezelés egyik jogalapját.[131] Az érintett létfontosságú érdekeinek az adatkezelést igazoló indokok közé való felvételét nyilvánvalóan mérlegelik: az alapvető jogok védelme soha nem veszélyeztetheti a védendő személy létfontosságú érdekeit.

131 A profilalkotásra vonatkozó ajánlás, 3.4. cikk, b) pont.

Közérdek és hivatali hatáskör gyakorlása

Figyelemmel a közügyek szervezésének számos lehetséges módjára, az adatvédelmi irányelv 7. cikkének e) pontja úgy rendelkezik, hogy személyes adatok akkor is jogszerűen kezelhetők, ha „az adatkezelés közérdekből elvégzendő feladat végrehajtásához vagy az adatkezelőre, illetve az adatokról tudomást szerző harmadik félre ruházott hivatali hatáskör gyakorlásához szükséges".[132]

Példa: A *Huber kontra Németország* ügyben[133] Huber úr, egy Németországban élő osztrák állampolgár azzal a kéréssel fordult a Szövetségi Bevándorlási és Menekültügyi Hivatalhoz, hogy a külföldiek központi nyilvántartásából („AZR") töröljék a rá vonatkozó adatokat. Ezt a nyilvántartást, amely nem német, de a három hónapnál hosszabb ideig Németországban élő uniós állampolgárok személyes adatait tartalmazza, bűnüldöző és igazságügyi hatóságok használják statisztikai célokra, amikor bűncselekmények vagy a közbiztonságot veszélyeztető tevékenységek ügyében nyomoznak és emelnek vádat. A kérdést előterjesztő bíróság azt a kérdést tette fel, hogy az olyan nyilvántartásban végzett személyesadat-kezelés, mint pl. a külföldiek központi nyilvántartása, amelyhez más hatóságoknak is van hozzáférésük, összhangban áll-e az uniós joggal – tekintettel arra, hogy német állampolgárokra vonatkozóan ilyen nyilvántartás nem létezik.

Az EUB először is megállapítja, hogy az irányelv 7. cikkének e) pontja értelmében személyes adatok csak akkor kezelhetők jogszerűen, ha ez közérdekből elvégzendő feladat végrehajtásához vagy hivatali hatáskör gyakorlásához szükséges.

A Bíróság szerint „tekintettel arra a célkitűzésre, hogy valamennyi tagállamban azonos védelmi szintet kell biztosítani, a 95/46/EK irányelv 7. cikkének e) pontja szerinti szükségesség fogalma [...] nem lehet eltérő tartalmú az egyes tagállamokban. Ennek következtében önálló közösségi jogi fogalomról van szó, amelyet oly módon kell értelmezni, hogy az maradéktalanul megfeleljen ezen irányelv célkitűzésének, amint az annak 1. cikke (1) bekezdéséből következik."[134]

132 Lásd még az adatvédelmi irányelv (32) preambulumbekezdését.

133 EUB, C-524/06. sz. *Huber kontra Németország* ügy, 2008. december 16.

134 *Uo.*, 52. pont.

A Bíróság megjegyzi, hogy az uniós polgároknak egy olyan másik tagállam területén történő tartózkodáshoz való joga, amelynek nem állampolgárai, nem feltétlen, hanem a Szerződésben, valamint a végrehajtására hozott rendelkezésekben előírt korlátozások és feltételek betartásához köthető. Ennek megfelelően, ha főszabályként jogszerű, hogy egy tagállam az AZR-hez hasonló nyilvántartással támogassa a tartózkodási joggal kapcsolatos jogszabályok alkalmazásáért felelős hatóságokat, egy ilyen nyilvántartás kizárólag az adott célhoz szükséges információkat tartalmazhatja. A Bíróság megállapítja, hogy egy ilyen személyesadat-kezelési rendszer akkor felel meg az uniós jognak, ha kizárólag a szóban forgó jogszabályok alkalmazásához szükséges adatokat tartalmazza, és ha központi jellege e jogszabályok alkalmazását hatékonyabbá teszi. A nemzeti bíróság feladata, hogy ezeket a körülményeket a konkrét ügyben megvizsgálja. Semmiképpen sem tekinthető azonban a 95/46/EK irányelv 7. cikkének e) pontja értelmében szükségesnek a névhez kötődő személyes adatoknak az AZRhez hasonló nyilvántartásban statisztikai célból történő feldolgozása.[135]

Végül, a nyilvántartásban szereplő adatoknak a bűnözés elleni küzdelem céljára való felhasználásával kapcsolatban a Bíróság megállapítja, hogy ez a cél „szükségszerűen a bűncselekményeknek és szabálysértéseknek az elkövetők állampolgárságától függetlenül történő üldözését jelenti". A szóban forgó nyilvántartás nem tartalmaz az érintett tagállam állampolgáraira vonatkozó személyes adatokat, ez az eltérő bánásmód viszont kimeríti az EUMSZ 18. cikke által tiltott megkülönböztetés fogalmát. Következésképpen ez a rendelkezés a Bíróság értelmezése szerint „azzal ellentétes, ha valamely tagállam a bűnözés elleni küzdelem céljából a személyes adatok kezelésének olyan rendszerét vezeti be, amely csak azon uniós polgárokra vonatkozik, akik nem e tagállam állampolgárai".[136]

A személyes adatok közügyekben eljáró hatóságok általi felhasználása az EJEE 8. cikkének hatálya alá is tartozik.

Az adatkezelő vagy harmadik fél által előmozdított jogos érdekek

Nem az érintett az egyetlen, akinek jogos érdekei vannak. Az **adatvédelmi irányelv** 7. cikkének f) pontja úgy rendelkezik, hogy személyes adatok akkor kezelhetők

135 *Uo.*, 54., 58., 59., 66–68. pont.

136 *Uo.*, 78. és 81. pont.

jogszerűen, ha „az adatkezelés az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintett [...] védelmet élvező érdekei az alapvető jogok és szabadságok tekintetében".

Az alábbi ítéletben az EUB kifejezetten állást foglalt az irányelv 7. cikkének f) pontjával kapcsolatban:

Példa: Az *ASNEF és FECEMD* ügyben[137] az EUB tisztázta, hogy a nemzeti jog nem egészítheti ki az irányelv 7. cikkének f) pontjában a jogszerű adatkezelésre vonatkozóan említett feltételeket. Az ügyben az alaphelyzet az volt, hogy a spanyol adatvédelmi törvény olyan rendelkezést tartalmazott, miszerint személyesadat-kezelés kapcsán más magánfelek csak akkor hivatkozhatnak jogos érdekre, ha az adatok a nyilvánosság számára hozzáférhető forrásokban már szerepeltek.

A Bíróság először is megjegyezte, hogy a 95/46/EK irányelv célja, hogy minden tagállamban azonossá tegye az egyének jogai és szabadságai védelmének szintjét a személyes adatok kezelése terén. Ugyanígy, az ezen a területen alkalmazandó nemzeti jogszabályok közelítése nem vezethet az általuk nyújtott védelem szintjének csökkenéséhez. Sőt, magas védelmi szintet kell, hogy biztosítson az Unión belül.[138] Következésképpen az EUB megállapította, hogy „abból a célkitűzésből, amelynek lényege az azonos védelmi szint biztosítása valamennyi tagállamban, az következik, hogy a 95/46 irányelv 7. cikke kimerítő és korlátozó jellegű felsorolását írja elő azon eseteknek, amelyekben a személyes adatok kezelése jogszerűnek minősíthető". Ezenfelül, „a tagállamok nem alkothatnak a személyes adatok kezelésének megengedhetőségére vonatkozó, az ezen irányelv 7. cikkében szereplőkhöz képest új elveket, és olyan további követelményeket sem írhatnak elő, amelyek módosítanák az e cikkben előírt elvek akár egyikének a hatályát".[139]A Bíróság elismerte, hogy „a 95/46 irányelv 7. cikkének f) pontja értelmében szükséges súlyozást illetően figyelembe vehető, hogy az érintett személy alapvető jogainak a hivatkozott adatkezelés

137 EUB, C-468/10. és C-469/10. sz. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) kontra Administración del Estado* egyesített ügyek, 2011. november 24.

138 *Uo.*, 28. pont. Lásd az adatvédelmi irányelv (8) és (10) preambulumbekezdését.

139 EUB, C-468/10. és C-469/10. sz. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) kontra Administración del Estado* egyesített ügyek, 2011. november 24., 30. és 32. pont.

általi sérelme súlyossága azon ténytől függően változhat, hogy a szóban forgó adatok szerepelneke már a nyilvánosság által hozzáférhető forrásokban, vagy sem".

Azonban az „irányelv 7. cikkének f) pontjával ellentétes az, ha valamely tagállam bizonyos kategóriákba tartozó személyes adatok tekintetében kategorikusan és általánosan kizárja ezek kezelhetőségét anélkül, hogy lehetővé tenné a szóban forgó ellentétes érdekek és jogok súlyozását az egyes esetekben".

A fenti megfontolásokra figyelemmel a Bíróság arra a következtetésre jutott, hogy „a 95/46 irányelv 7. cikkének f) pontját úgy kell értelmezni, hogy azzal ellentétes az olyan nemzeti szabályozás, amely az érintett hozzájárulásának hiányában, és annak érdekében, hogy lehetővé tegye az érintett személyes adatainak kezelését– ami az adatkezelő vagy azon harmadik személyek jogos érdekének kielégítéséhez szükséges, akikkel az adatokat közlik –, azt is előírja azonfelül, hogy ne sérüljenek a személy alapvető jogai és szabadságai, hogy adatai a nyilvánosság számára hozzáférhető forrásokban szerepeljenek, kategorikusan és általánosan kizárva ily módon az ilyen forrásokban nem szereplő adatok bármely kezelését".[140]

Az Európa Tanács ajánlásaiban is hasonló megfogalmazások szerepelnek. A profilalkotási ajánlás akkor ismeri el jogszerűnek a profilalkotási célokra végzett személyesadat-feldolgozást, ha az mások jogos érdekeinek védelme érdekében szükséges, „kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett alapvető jogai és szabadságai".[141]

4.1.2. Érzékeny adatok jogszerű feldolgozása

Az **Európa Tanács joga** a hazai jogra hagyja az érzékeny adatok felhasználásának megfelelő védelmét biztosító szabályok megalkotását, az **uniós jog** viszont az adatvédelmi irányelv 8. cikkében részletesen szabályozza az alábbiakra utaló adatkategóriák feldolgozását: a faji vagy etnikai hovatartozás, a politikai vélemény, a vallási vagy világnézeti meggyőződés, a szakszervezeti tagság, valamint az egészségi állapotra vagy a szexuális életre vonatkozó adatok. Főszabályként a különleges adatok kezelése nem megengedett.[142] Az irányelv 8. cikkének (2) és (3) bekezdése

140 *Uo.*, 40., 44., 48. és 49. pont.

141 A profilalkotásra vonatkozó ajánlás, 3.4. cikk, b) pont.

142 Adatvédelmi irányelv, 8. cikk (1) bekezdés.

azonban számos kivételt sorol fel e tiltás alól. A kivételek közé tartozik az érintett kifejezett hozzájárulása, az érintett létfontosságú érdekeinek védelme, mások jogos érdekei és a közérdek.

Az érzékeny adatok esetében – a nem érzékeny adatok feldolgozásától eltérően – az érintettel való szerződéses kapcsolatot nem tekintik a jogszerű adatfeldolgozás általános jogalapjának. Ezért ha az érintettel kötött szerződéssel összefüggésben érzékeny adatok feldolgozására kerülne sor, ezen adatok felhasználásához – a szerződéskötésbe való beleegyezésen kívül – az érintett kifejezett hozzájárulása szükséges. Ha azonban az érintett kifejezetten olyan árukat vagy szolgáltatásokat kér, amelyek szükségképpen érzékeny adatokat fednek fel, azt a kifejezett hozzájárulással egyenértékűnek kell tekinteni.

Példa: Ha egy légi utas egy foglalás kapcsán azt kéri, hogy a légitársaság kerekesszéket és kóser ételt bocsásson a rendelkezésére, a légitársaság akkor is felhasználhatja ezeket az adatokat, ha az utas nem írt alá külön hozzájáruló záradékot, melyben beleegyezik az egészségi állapotára és vallás meggyőződésére vonatkozó információkra utaló adatainak felhasználásába.

Az érintett kifejezett hozzájárulása

Bármely adat jogszerű kezelésének első feltétele – függetlenül attól, hogy érzékeny vagy nem érzékeny adatról van-e szó – az érintett hozzájárulása. Érzékeny adatok esetében a hozzájárulásnak kifejezettnek kell lennie. A nemzeti jog azonban úgy rendelkezhet, hogy az érzékeny adatok felhasználásához való hozzájárulás nem nyújt elegendő jogalapot ahhoz, hogy engedélyezzék ezen adatok feldolgozását[143] például akkor, amikor – kivételes esetekben – a feldolgozás szokatlan kockázattal jár az érintett számára.

Egyetlen speciális esetben még a hallgatólagos hozzájárulást is elismerik az érzékeny adatok feldolgozásának jogalapjául: az irányelv 8. cikke (2) bekezdésének e) pontja úgy rendelkezik, hogy az adatfeldolgozás nem tilos, ha olyan adatokra vonatkozik, amelyeket az érintett egyértelműen nyilvánosságra hozott. Ez a rendelkezés nyilvánvalóan abból indul ki, hogy az érintett cselekményét – adatainak nyilvánosságra hozását – úgy kell értelmezni, mint amely a szóban forgó adatok felhasználásához adott hozzájárulást is magában foglalja.

143 *Uo.*, 8. cikk (2) bekezdés, a) pont.

Az érintett létfontosságú érdekei

A nem érzékeny adatokhoz hasonlóan az érzékeny adatok is feldolgozhatók az érintett létfontosságú érdekeinek védelmében.[144]

Ahhoz, hogy a különleges adatok e jogcímen való feldolgozása jogszerű legyen, szükséges, hogy a döntésre irányuló kérdést nem lehetett korábban feltenni az érintettnek például azért, mert nem volt tudatánál, távol volt vagy nem volt elérhető.

Mások törvényes érdekei

A mások törvényes érdekei az érzékeny adatok esetében is – a nem érzékeny adatokhoz hasonlóan – szolgálhatnak az adatkezelés jogalapjául. Az érzékeny adatok esetében azonban ez – az adatvédelmi irányelv 8. cikkének (2) bekezdése szerint is – csak a következő esetekre vonatkozik:

- ha az adatkezelés más személy létfontosságú érdekeinek védelméhez szükséges,[145] amennyiben az érintett fizikailag vagy jogilag képtelen a hozzájárulását adni;

- ha az érzékeny adatok a foglalkoztatási jog területén relevánsak, ide tartoznak például az egészségi állapotra vonatkozó adatok, a különösen veszélyes munkavégzési hellyel kapcsolatos adatok, illetve a vallásos meggyőződésre vonatkozó, köztük a szabadsággal kapcsolatos adatok;[146]

- ha alapítvány, egyesület vagy bármely más nonprofit szervezet politikai, világnézeti, vallási vagy szakszervezeti céllal dolgoz fel adatokat a tagjairól, támogatóiról vagy más érdekelt felekről (az ilyen adatok azért minősülnek érzékeny adatnak, mert valószínűsíthetően az érintett egyének vallási vagy politikai meggyőződésére utalnak);[147]

144 *Uo.*, 8. cikk, (2) bekezdés, c) pont.

145 *Uo.*

146 *Uo.*, 8. cikk, (2) bekezdés, b) pont.

147 *Uo.*, 8. cikk, (2) bekezdés, d) pont.

- ha az érzékeny adatok feldolgozására bíróság vagy közigazgatási hatóság előtt folyó jogi eljárásban, jogi követelések megállapítása, gyakorlása vagy védelme céljából kerül sor.[148]

- Ezenfelül az adatvédelmi irányelv 8. cikkének (3) bekezdése szerint, ha egészségügyi szolgáltatók orvosi vizsgálathoz és kezeléshez használnak fel egészségügyi állapotra vonatkozó adatokat, az említett szolgáltatások igazgatása is e kivétel alá tartozik. Külön biztosítékként, a személyek csak akkor minősülnek „egészségügyi szolgáltatónak", ha egyedi szakmai titoktartási kötelezettség alá esnek.

Közérdek

Ezen kívül az adatvédelmi irányelv 8. cikkének (4) bekezdése szerint a tagállamok további célokat is megállapíthatnak, amelyek érdekében különleges adatok feldolgozhatók, amennyiben:

- az adatkezelés alapvető közérdekből történik; és

- az adatkezelést nemzeti jogszabály vagy a felügyelő hatóság határozata írja elő; és

- a nemzeti jogszabály vagy a felügyelő hatóság határozata megfelelő garanciákat tartalmaz az érintettek érdekeinek hatékony védelmére.[149]

Ennek egyik kiemelkedő példáját az elektronikus egészségügyi dokumentum-nyilvántartó rendszerek alkotják, amelyek létrehozását számos tagállamban tervezik. Az ilyen rendszerek nagymértékben, rendszerint országos szinten lehetővé teszik, hogy a beteg kezelése során az egészségügyi szolgáltatók által gyűjtött egészségügyi adatokhoz a beteg más egészségügyi szolgáltatói is hozzáférjenek.

A 29. cikk szerinti munkacsoport arra a következtetésre jutott, hogy az adatkezelésre vonatkozó meglévő jogszabályok szerint, amelyek az adatvédelmi irányelv 8. cikkének (3) bekezdésén alapulnak, ilyen rendszereket nem volna szabad létrehozni. Azt feltételezve azonban, hogy az ilyen elektronikus egészségügyi dokumentum-nyilvántartó rendszerek megléte alapvető közérdek, e rendszerek az irányelv

148 *Uo.*, 8. cikk, (2) bekezdés, e) pont.

149 *Uo.*, 8. cikk, (4) bekezdés.

8. cikkének (4) bekezdése alapján létrehozhatók, mely bekezdés kifejezett jogalapot ír elő a létrehozásukhoz, továbbá megfelelő garanciák nyújtását a rendszer biztonságos üzemeltetésére.[150]

4.2. Az adatkezelés biztonságára vonatkozó szabályok

Főbb pontok

- Az adatkezelés biztonságára vonatkozó szabályok az adatkezelő és az adatfeldolgozó azon kötelezettségére is kiterjednek, hogy megfelelő technikai és szervezési intézkedéseket hajtsanak végre az adatfeldolgozási műveletekbe való jogosulatlan beavatkozás megakadályozására.
- Az adatbiztonság szükséges szintjét a következők határozzák meg:
  - az adott típusú feldolgozás esetében a piacon elérhető biztonsági funkciók; és
  - a költségek; és
  - a feldolgozott adatok érzékenysége.
- A biztonságos adatfeldolgozást az az általános kötelezettség is garantálja, hogy valamennyi személy, adatkezelő és adatfeldolgozó köteles biztosítani az adatok titkosságát.

Az adatkezelők és -feldolgozók azon kötelezettségét tehát, hogy megfelelő intézkedésekkel biztosítsák az adatbiztonságot, az **Európa Tanács adatvédelmi joga** és az **EU adatvédelmi joga** is előírja.

4.2.1. Az adatbiztonság elemei

Az **uniós jog** vonatkozó rendelkezései szerint:

> *„A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése,*

150 29. cikk szerinti munkacsoportnak az elektronikus egészségügyi nyilvántartásban tárolt, *egészségi állapotra vonatkozó személyes adatok feldolgozásáról szóló munkadokumentuma (2007)*, WP 131., Brüsszel, 2007. február 15.

megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a feldolgozás közben az adatokat hálózaton keresztül továbbítják, továbbá a feldolgozás minden más jogellenes formája ellen."[151]

Hasonló rendelkezés az **Európa Tanács jogában** is létezik:

„Megfelelő biztonsági intézkedéseket kell tenni az automatizált adatállományokban tárolt személyes adatok védelme érdekében a véletlen vagy jogtalan megsemmisítés, vagy véletlen elvesztés, valamint a jogtalan hozzáférés, megváltoztatás vagy terjesztés megakadályozására."[152]

A biztonságos adatfeldolgozás érdekében számos esetben ágazati, nemzeti és nemzetközi normákat dolgoztak ki. Az európai adatvédelmi megfelelőségi címke (EuroPriSe) például az EU egyik eTEN (transzeurópai távközlési hálózatokra vonatkozó) projektje, amely a termékek, különösen szoftverek adatvédelmi tanúsításával – azaz az európai adatvédelmi jogszabályoknak való megfelelés igazolásával – kapcsolatos lehetőségeket tárta fel. Az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (ENISA) azért hozták létre, hogy fokozzák a Közösség, a tagállamok, és következésképpen az üzleti szféra képességét a hálózat- és információbiztonsággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálásra.[153] Az ENISA rendszeresen közzétesz elemzéseket az aktuális biztonsági fenyegetésekről, és tanácsokat ad azok kezelésével kapcsolatban.

Az adatbiztonság nem pusztán a megfelelő berendezések – hardver és szoftver – meglétével érhető el. Megfelelő belső szervezeti szabályok is szükségesek hozzá. A belső szabályok ideális esetben a következő kérdéseket érintik:

- valamennyi munkavállaló rendszeres tájékoztatása az adatbiztonsági szabályokról, valamint a munkavállalóknak az adatvédelmi jog alapján fennálló kötelezettségeiről, különösen a titoktartási kötelezettségről;

151 Adatvédelmi irányelv, 17. cikk (1) bekezdés.

152 108. egyezmény, 7. cikk.

153 Az Európai Parlament és a Tanács 2004. március 10-i 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról, HL L 77., 2004.

- világos feladatkör-megosztás és a hatáskörök egyértelmű meghatározása adatkezelési kérdésekben, különösen a személyes adatok kezelésére és harmadik feleknek történő továbbítására irányuló döntésekkel kapcsolatban;

- a személyes adatok kizárólag az illetékes személy utasításai vagy az általánosan elfogadott szabályok szerinti felhasználása;

- az adatkezelő, illetve az adatfeldolgozó telephelyeihez és hardveréhez, szoftveréhez való hozzáférés védelme, a hozzáférési engedélyek ellenőrzését is beleértve;

- annak biztosítása, hogy a személyes adatokhoz való hozzáférési engedélyt az illetékes személy adja ki, és az engedély megadásához megfelelő dokumentáció szükséges;

- automatizált protokollok a személyes adatokhoz elektronikus úton történő hozzáféréshez, és e protokollok belső felügyeleti részleg általi rendszeres ellenőrzése;

- az automatizált hozzáférésen kívüli más közlési formák alapos dokumentálása annak igazolására, hogy nem történt jogellenes adattovábbítás.

Az adatbiztonsággal kapcsolatos megfelelő betanítás és képzés a személyzet tagjai számára szintén a hatékony biztonsági óvintézkedések egyik fontos eleme. Ellenőrzési eljárásokat is telepíteni kell annak biztosítására, hogy a megfelelő intézkedések nem csupán papíron léteznek, hanem a gyakorlatban is végrehajtják őket és működnek (pl. belső vagy külső ellenőrzések).

Az adatkezelő vagy -feldolgozó biztonsági szintjének javítását célzó intézkedések közé tartoznak az adatvédelmi felelősök, a munkavállalók biztonsággal kapcsolatos oktatása, a rendszeres ellenőrzések, penetrációs tesztek és minőségi tanúsítványok.

Példa: Az *I. kontra Finnország* ügyben[154] a felperes nem tudta bizonyítani, hogy orvosi adataihoz a munkahelyéül szolgáló kórház más alkalmazottai jogellenesen hozzáfértek. Ezért a hazai bíróságok elutasították az adatvédelemhez való jogának megsértése miatt benyújtott keresetét. Az EJEB megállapította, hogy

154 EJEB, *I. kontra Finnország* (20511/03. sz. ügy), 2008. július 17.

megsértették az EJEE 8. cikkét, mivel a kórház kórlap-nyilvántartási rendszere „úgy volt kialakítva, hogy visszamenőlegesen nem lehetett tisztázni a betegek adatainak felhasználását, mivel a rendszer csupán az öt legutóbbi konzultációt mutatta ki, és ezt az információt törölte, amint a fájl visszakerült az archívumba". A Bíróság számára az volt a döntő, hogy a kórházban alkalmazott nyilvántartási rendszer egyértelműen nem állt összhangban a hazai jog által előírt jogi követelményekkel – aminek a hazai bíróságok nem tulajdonítottak kellő jelentőséget.

Adatsértés bejelentése

Számos európai ország adatvédelmi jogában új eszközt vezettek be az adatbiztonság megsértésének kezelésére: az elektronikus hírközlési szolgáltatók arra vonatkozó kötelezettségét, hogy a valószínű áldozatokat és a felügyeleti hatóságokat értesítsék az adatsértésekről. A távközlési szolgáltatók számára az uniós jog szerint ez már kötelező.[155] Az érintettek értesítése az adatsértésekről a kármegelőzést szolgálja: az értesítés és annak lehetséges következményei minimalizálják az érintettekre gyakorolt negatív hatások kockázatát. Súlyos gondatlanság esetén a szolgáltatók meg is bírságolhatók.

A biztonsági szabályok megsértésének hatékony kezelése és bejelentése érdekében előzetesen belső eljárásokat kell bevezetni, mivel az érintettek és/vagy a felügyeleti hatóság értesítésére a nemzeti jogban előírt határidő rendszerint meglehetősen rövid.

4.2.2. Az adatok bizalmas kezelése

Az **uniós jogban** a biztonságos adatkezelést az az általános kötelezettség is garantálja, hogy valamennyi személy, adatkezelő és adatfeldolgozó köteles biztosítani az adatok titkosságát.

155 Lásd az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelvet *(„elektronikus hírközlési adatvédelmi irányelv")*, HL L 201., 2002., 4. cikk, (3) bekezdés, módosította az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról szóló, 2009. november 25-i 2009/136/EK európai parlamenti és tanácsi irányelv, HL L 337., 2009.

Példa: Egy biztosítótársaság alkalmazottja a munkahelyén telefonhívást kap, és a hívó, aki önmagáról azt állítja, hogy ügyfél, a biztosítási szerződésével kapcsolatban kér tájékoztatást.

Az ügyfelek adatainak bizalmas kezelésére vonatkozó kötelezettség miatt az alkalmazottnak legalább minimális biztonsági intézkedéseket kell alkalmaznia, mielőtt személyes adatokat közöl. Ez történhet például úgy, hogy visszahívást ajánl az ügyfél aktájában szereplő telefonszámon.

Az adatvédelmi irányelv 16. cikke a titkosságot csak az adatkezelő és az adatfeldolgozó közötti jogviszonyban szabályozza. Azzal a kérdéssel, hogy az adatkezelőknek titkosan kell-e kezelniük az adatokat abban az értelemben, hogy harmadik felekkel nem közölhetik azokat, az irányelv 7. és 8. cikke foglalkozik.

A titkos kezelési kötelezettség nem terjed ki olyan helyzetekre, amikor az adatok magánszemélyként, nem pedig valamely adatkezelő vagy -feldolgozó alkalmazottjaként jutnak a személy tudomására. Ebben az esetben az adatvédelmi irányelv 16. cikke nem alkalmazandó, mivel a személyes adatok magánszemélyek általi felhasználása egyáltalán nem tartozik az irányelv hatálya alá, amennyiben a felhasználás az úgynevezett háztartási mentesség körébe esik.[156] A háztartási mentesség „a természetes személy által kizárólag személyes célra, vagy háztartási tevékenysége keretében végzett" személyesadat-kezelést jelenti.[157] Az EUB-nak a *Bodil Lindqvist* ügyben[158] hozott ítélete óta azonban ezt a mentességet szűken kell értelmezni, különösen adatok szolgáltatásával kapcsolatban. Konkrétan, a háztartási mentesség nem terjed ki személyes adatoknak az interneten, korlátlan számú címzett részére történő közzétételére (az ügy további részleteit lásd a *2.1.2., 2.2., 2.3.1. és 6.1. szakaszban*).

Az **Európa Tanács joga** szerint a 108. egyezmény 7. cikkében szereplő „adatbiztonság" fogalma magában foglalja a titkos kezelési kötelezettséget.

Az adatfeldolgozók számára a titkosság azt jelenti, hogy az adatkezelők által rájuk bízott személyes adatokat kizárólag az adatkezelő utasításainak megfelelően használhatják fel. Az adatkezelők vagy -feldolgozók alkalmazottai – a titkossági

156 Adatvédelmi irányelv, 3. cikk, (2) bekezdés, második francia bekezdés.

157 *Uo.*

158 EUB, C-101/01. sz. *Bodil Lindqvist ügy*, 2003. november 6.

követelmény miatt – a személyes adatokat kizárólag illetékes feletteseik utasításainak megfelelően használhatják fel.

A titkos kezelési kötelezettséget az adatkezelők a feldolgozóikkal kötött szerződésekben is kötelesek feltüntetni. Ezenkívül az adatkezelőknek és -feldolgozóknak egyedi intézkedésekkel – általában a munkaszerződésben egy titoktartási záradék szerepeltetésével – a munkavállalóik számára is elő kell írniuk a titkos kezelésre vonatkozó jogi kötelezettséget.

A szakmai titoktartási kötelezettség megszegése több uniós tagállam és a 108. egyezmény részes országainak büntetőjoga szerint is büntetendő.

4.3. Az adatkezelés átláthatóságára vonatkozó szabályok

Főbb pontok

- Személyes adatok kezelésének megkezdése előtt az adatkezelő köteles tájékoztatni az érintetteket legalább az adatkezelő kilétéről és a feldolgozás céljáról, kivéve, ha az érintett már rendelkezik ezekkel az információkkal.
- Ha az adatgyűjtés harmadik felektől történik, a tájékoztatási kötelezettség nem alkalmazandó, ha:
  - az adatkezelést jogszabály rendeli el; vagy
  - a tájékoztatás lehetetlennek bizonyul vagy aránytalan erőfeszítést igényelne.
- Személyes adatok kezelésének megkezdése előtt az adatkezelőnek ezenfelül:
  - értesítenie kell a felügyeleti hatóságot a tervezett feldolgozási műveletekről; vagy
  - a független belső adatvédelmi felelőssel házon belül dokumentáltatni kell az adatfeldolgozást, ha az ilyen eljárást nemzeti jogszabály előírja.

A tisztességes adatkezelés elve előírja az átláthatóságot. Az **Európa Tanács joga** e célból rögzíti, hogy minden személynek ismernie kell az adatállományok létezéséről, céljáról és a felelős adatkezelő kilétéről.[159] Annak meghatározása, hogy mindezt hogyan kell megvalósítani, a hazai jog feladata. Az **uniós jog** konkrétabb, az érintett

159 108. egyezmény, 8. cikk, a) pont.

számára úgy biztosít átláthatóságot, hogy az adatkezelőt kötelezi az érintett és a nagyközönség értesítés útján történő tájékoztatására.

A nemzeti jog mindkét jogrendszerben megállapíthat kivételeket és korlátozásokat az adatkezelő átláthatósági kötelezettsége alól, amikor a korlátozás bizonyos közérdekek védelme, illetve az érintett védelme vagy mások jogainak és szabadságainak védelme érdekében szükséges intézkedést jelent, amennyiben erre egy demokratikus társadalomban szükség van.[160] Ilyen kivételekre szükség lehet például bűnügyi nyomozással összefüggésben, de más körülmények között is indokoltak lehetnek.

4.3.1. Tájékoztatás

A feldolgozási műveletek adatkezelői **az Európa Tanács és az EU joga szerint is** kötelesek a tervezett feldolgozásról előre tájékoztatni az érintettet.[161] Ez a kötelezettség nem függ az érintett kérésétől, az adatkezelőnek aktívan eleget kell tennie e kötelezettségnek függetlenül attól, hogy az érintett érdeklődést mutat-e a tájékoztatás iránt.

A tájékoztatás tartalma

A tájékoztatásnak az adatkezelés céljára, valamint az adatkezelő kilétére és kapcsolattartási adataira is ki kell terjednie.[162] Az adatvédelmi irányelv további tájékoztatást is előír, „amennyiben e további információk, tekintettel az adatgyűjtés sajátos körülményeire, az érintett vonatkozásában a tisztességes adatkezelés biztosításához szükségesek". Az irányelv 10. és 11. cikke többek között ismerteti a feldolgozott adatok kategóriáit és ezen adatok címzettjeit, továbbá az adatokhoz való hozzáférési jog és az adatok helyesbítéséhez való jog meglétét. Ha az adatgyűjtés az érintettektől történik, a tájékoztatásnak egyértelműen tartalmaznia kell, hogy a válaszadás önkéntes vagy kötelező-e, és meg kell jelölnie a válaszadás elmulasztásának lehetséges következményeit.[163]

Az **Európa Tanács jogának** szempontjából e tájékoztatás nyújtása a tisztességes adatfeldolgozás elve szerinti helyes gyakorlatnak tekinthető, és ennyiben az Európa Tanács jogának részét is képezi.

160 *Uo*. 9. cikk (2) bekezdés; és adatvédelmi irányelv, 13. cikk, (1) bekezdés.

161 108. egyezmény, 8. cikk, a) pont; és adatvédelmi irányelv, 10. és 11. cikk.

162 108. egyezmény, 8. cikk, a) pont; és adatvédelmi irányelv, 10. cikk, a) és b) pont.

163 Adatvédelmi irányelv, 10. cikk c) pont.

A tisztességes adatfeldolgozás elve szerint a tájékoztatásnak az érintettek számára könnyen érthetőnek kell lennie. A címzettek számára megfelelő nyelvezetet kell használni. A nyelvezet szintjét és típusát szükség szerint a célközönséghez kell igazítani; más-más nyelvezetet kell használni pl. felnőttek és gyermekek, a nagyközönség vagy tudósok esetében.

Egyes érintettek csak rövid tájékoztatást igényelnek arról, hogy adataikat hogyan és miért dolgozzák fel, mások viszont részletesebb magyarázatot kérnek. Hogyan találjuk meg az egyensúlyt a tisztességes tájékoztatás e szempontjával kapcsolatban – ezt tárgyalja a 29. cikk szerinti munkacsoport egyik véleménye, amely az úgynevezett többszintű közleményekre[164] vonatkozó elképzelést pártolja, ami lehetővé teszi az érintettek számára, hogy eldöntsék, mennyire részletes tájékoztatást igényelnek.

A tájékoztatás határideje

Az adatvédelmi irányelv eléggé különböző rendelkezéseket tartalmaz arra vonatkozóan, hogy mikor kell a tájékoztatást megadni – attól függően, hogy az adatgyűjtés az érintettől (10. cikk) vagy harmadik féltől (11. cikk) történik. Ha az adatokat az érintettől gyűjtik, a tájékoztatást legkésőbb az adatgyűjtéskor meg kell adni. Ha az adatgyűjtés harmadik felektől történik, a tájékoztatást legkésőbb akkor kell megadni, amikor az adatkezelő rögzíti az adatokat, vagy mielőtt az adatokat első alkalommal közlik harmadik féllel.

A tájékoztatási kötelezettség alóli kivételek

Az **uniós jogban** általános kivétel létezik az érintett tájékoztatására vonatkozó kötelezettség alól abban az esetben, ha az érintett már rendelkezik a szóban forgó információkkal.[165] Ez olyan esetekre vonatkozik, amikor az érintett – az ügy körülményeiből fakadóan – már tudomást szerzett arról, hogy adatait egy bizonyos adatkezelő egy bizonyos célra fel fogja dolgozni.

Az irányelv 11. cikke, amely az érintett tájékoztatására vonatkozó kötelezettségről szól abban az esetben, ha az adatokat nem az érintettől szerezték be, azt is kimondja, hogy nincs ilyen kötelezettség – különösen a statisztikai célú vagy a történelmi, vagy tudományos célú adatkezelés esetében –, ha:

164 A 29. cikk szerinti munkacsoport 10/2004. sz. *véleménye az összehangoltabb tájékoztatási rendelkezésekről*, WP 100, Brüsszel, 2004. november 25.

165 Adatvédelmi irányelv, 10. cikk és 11. cikk, (1) bekezdés.

- a kérdéses információk rendelkezésre bocsátása lehetetlennek bizonyul; vagy
- aránytalanul nagy erőfeszítést igényel; vagy
- ha a rögzítést vagy a közlést jogszabály kifejezetten előírja.[166]

Csak az adatvédelmi irányelv 11. cikkének (2) bekezdése rendelkezik úgy, hogy az érintetteket nem kell tájékoztatni az adatkezelési műveletekről, ha azokat jogszabály írja elő. Figyelemmel arra az általános jogi vélelemre, hogy a jogalanyok ismerik a rájuk vonatkozó jogszabályokat, kijelenthető, hogy amennyiben az adatgyűjtés – az irányelv 10. cikke szerint – az érintettől történik, az érintett rendelkezik ezekkel az információkkal. Tekintve viszont, hogy a jogszabályok ismerete csupán feltételezés, a tisztességes adatkezelés elve a 10. cikk értelmében megkövetelné, hogy az érintettet akkor is tájékoztassák, ha a feldolgozást jogszabály írja elő, különösen mivel az érintett tájékoztatása nem különösebben terhes, ha az adatgyűjtés éppen közvetlenül tőle történik.

Az **Európa Tanács joga** szerint a 108. egyezmény rendelkezik a 8. cikke alóli kifejezett kivételekről. Az adatvédelmi irányelv 10. és 11. cikkében meghatározott kivételek ismét csak a 108. egyezmény 9. cikke alóli kivételekre vonatkozó helyes gyakorlat példáinak tekinthetők.

A tájékoztatás különböző módjai

A tájékoztatás nyújtásának ideális módja minden egyes érintett – szóbeli vagy írásbeli – megkeresése volna. Ha az adatokat az érintettől gyűjtik, a tájékoztatásnak az adatgyűjtéssel párhuzamosan kell történnie. Akkor azonban, ha az adatgyűjtés harmadik felektől történik, a tájékoztatás – figyelemmel az érintettek személyes elérésével kapcsolatos nyilvánvaló gyakorlati nehézségekre – megfelelő közlemény útján is megadható.

A tájékoztatás egyik leghatékonyabb módja a megfelelő információs közlemények közzététele az adatkezelő honlapján, például internetes adatvédelmi politika formájában. A lakosság jelentős hányada azonban nem használja az internetet, és egy cég vagy hatóság tájékoztatási politikájának figyelembe kell ezt vennie.

166 Uo., (40) preambulumbekezdés és 11. cikk, (2) bekezdés.

4.3.2. Értesítés

Nemzeti jogszabály kötelezheti az adatkezelőket, hogy értesítsék tevékenységükről az illetékes felügyeleti hatóságot, hogy közzé tudja tenni az adatkezelés tényét. A másik lehetőség, hogy nemzeti jogszabály úgy rendelkezik, hogy az adatkezelő jelöljön ki egy belső adatvédelmi felelőst, aki elsősorban az adatkezelő által végzett adatkezelési műveletek nyilvántartásának vezetéséért felelős.[167] Ezt a belső nyilvántartást kérésre hozzáférhetővé kell tenni a nagyközönség számára.

Példa: Az értesítésnek és a belső személyesadat-védelmi tisztviselő dokumentációjának le kell írnia az adott adatkezelés legfontosabb jellemzőit. Ide tartoznak az adatkezelővel kapcsolatos információk, az adatkezelés célja, jogalapja, a feldolgozott adatok kategóriái, a valószínű harmadik fél címzettek köre és az, hogy terveznek-e országhatárokat átlépő adatáramlást, és ha igen, melyek ezek.

A felügyeleti hatóságnak az értesítéseket külön nyilvántartás formájában kell közzétennie. A nyilvántartás céljának teljesüléséhez a nyilvántartásnak könnyen és ingyenesen hozzáférhetőnek kell lennie. Ugyanez vonatkozik az adatkezelő személyesadat-védelmi tisztviselője által vezetett dokumentációra.

Nemzeti jogszabály olyan adatfeldolgozási műveletek esetében rendelkezhet az illetékes felügyeleti hatóság értesítésére vagy belső adatvédelmi tisztviselő alkalmazására vonatkozó kötelezettség alóli mentességről, amelyek valószínűleg nem jelentenek különös veszélyt az érintettekre – ezek felsorolását az adatvédelmi irányelv 18. cikkének (2) bekezdése tartalmazza.[168]

4.4. Az előírások betartásának előmozdítására vonatkozó szabályok

Főbb pontok

- Az elszámoltathatóság elvét továbbfejlesztve az adatvédelmi irányelv számos eszközt említ az előírások betartásának előmozdítására:

167 Uo., 18. cikk, (2) bekezdés, második francia bekezdés.

168 Uo., 18. cikk (2) bekezdés első francia bekezdése.

- a tervezett adatfeldolgozási műveletek előzetes ellenőrzése, amit a nemzeti felügyelő hatóság végez el;
- belső adatvédelmi felelősök, akik speciális szakmai tudásukkal segítik az adatkezelőt az adatvédelem terén;
- eljárási szabályzatok, amelyek egy-egy társadalmi területen, különösen az üzleti szférában felsorolják a meglévő adatvédelmi szabályokat.

- Az Európa Tanács profilalkotási ajánlásában hasonló eszközöket javasol az előírások betartásának előmozdítására.

4.4.1. Előzetes ellenőrzés

Az adatvédelmi irányelv 20. cikke szerint a felügyelő hatóságnak az adatkezelés megkezdése előtt ellenőriznie kell azokat a műveleteket, amelyek – az adatkezelés célja vagy körülményei miatt – külön kockázatot jelenthetnek az érintettek jogaira és szabadságaira nézve. A nemzeti jognak kell meghatároznia, mely műveletek tartoznak az előzetes ellenőrzés hatálya alá. Az ellenőrzés nyomán a felügyelő hatóság egyes adatkezelési műveleteket megtilthat, vagy határozatban elrendelheti a művelet tervezett kialakítása egyes jellemzőinek megváltoztatását. Az irányelv 20. cikkének célja annak biztosítása, hogy a szükségtelenül kockázatos adatkezelést el se kezdjék, mivel a felügyelő hatóság jogosult az ilyen műveleteket megtiltani. E mechanizmus hatékonyságának előfeltétele, hogy a felügyelő hatóságot valóban értesítsék. Annak biztosítása érdekében, hogy az adatkezelők eleget tesznek értesítési kötelezettségüknek, a felügyelő hatóságoknak kényszerítő jogkörökre – például az adatkezelők megbírságolására irányuló hatáskörre – lesz szükségük.

Példa: Ha egy cég olyan adatkezelési műveleteket végez, amelyek a nemzeti jog szerint előzetes ellenőrzés hatálya alá tartoznak, a cégnek dokumentációt kell benyújtania a tervezett feldolgozási műveletekről a felügyelő hatósághoz. A cég nem kezdheti meg az adatfeldolgozási műveleteket, mielőtt pozitív választ kap a felügyelő hatóságtól.

Néhány tagállamban a nemzeti jog úgy rendelkezik, hogy az adatkezelés megkezdhető, ha a felügyelő hatóság bizonyos határidőn, például három hónapon belül nem válaszol.

4.4.2. Belső adatvédelmi felelősök

Az adatvédelmi irányelv értelmében nemzeti jogszabály úgy rendelkezhet, hogy az adatkezelők kijelölhetnek egy tisztviselőt, aki belső adatvédelmi felelősként jár el.[169] A tisztséget betöltő személy célja annak biztosítása, hogy az adatfeldolgozási műveletek várhatóan ne befolyásolják hátrányosan az érintettek jogait és szabadságait.[170]

> Példa: Németországban a német adatvédelmi törvény (*Bundesdatenschutzgesetz*) 4f. szakaszának (1) bekezdése szerint a magántulajdonban lévő társaságok kötelesek belső adatvédelmi felelőst kijelölni, ha az automatizált személyesadat-feldolgozás során legalább 10 főt tartósan foglalkoztatnak.

Ahhoz, hogy az adatvédelmi tisztviselő elérje ezt a célt, tisztségének bizonyos mértékű függetlenséget kell élveznie az adatkezelő szervezetén belül, ahogyan erre az irányelv kifejezetten rámutat. E tisztség hatékony működésének támogatása érdekében erős munkavállalói jogokra is szükség van, amelyek védelmet nyújtanak az olyan eshetőségekkel szemben, mint például az indokolatlan elbocsátás.

A nemzeti adatvédelmi jogszabályok betartásának előmozdítása érdekében az Európa Tanács egyes ajánlásai is átvették a belső adatvédelmi felelős koncepcióját.[171]

4.4.3. Eljárási szabályzatok

Az előírások betartásának érdekében az üzleti és egyéb szektorok részletes szabályokat állapíthatnak meg tipikus adatkezelési tevékenységeikre vonatkozóan, amelyekben a bevált gyakorlatokat összegzik. Az ágazatban tevékenykedők szakmai tudásuk alapján olyan megoldásokat fognak előnyben részesíteni, amelyek gyakorlatiasak, azaz amelyeket minden valószínűség szerint követni fognak. Ennek megfelelően a tagállamok és a Bizottság ösztönzik az irányelvnek megfelelően a tagállamok által elfogadott nemzeti rendelkezések helyes végrehajtásának elősegítésére szánt eljárási szabályzatok kidolgozását, figyelembe véve a különböző ágazatok egyedi jellemzőit.[172]

169 Uo., 18. cikk, (2) bekezdés, második francia bekezdés.

170 Uo.

171 Lásd például a profilalkotásra vonatkozó ajánlás 8.3. cikkét.

172 Lásd az adatvédelmi irányelv 27. cikkének (1) bekezdését.

Annak biztosítása érdekében, hogy ezek az eljárási szabályzatok összhangban legyenek az irányelvnek megfelelően elfogadott nemzeti rendelkezésekkel, a tagállamoknak eljárást kell kidolgozniuk a szabályzatok értékelésére. Az eljárásba rendszerint a nemzeti hatóságot, valamint szakmai szövetségeket és az egyéb adatkezelőket képviselő más szerveket is bevonnának.[173]

A közösségi szabályzattervezetek, továbbá a meglévő közösségi szabályzatok módosításai vagy bővítései benyújthatók értékelésre a 29. cikk szerinti munkacsoporthoz. E munkacsoport jóváhagyását követően az Európai Bizottság megfelelő nyilvánosságot biztosíthat a szóban forgó szabályzatok számára.[174]

Példa: Az Európai Direkt és Interaktív Marketing Szövetség (FEDMA) európai eljárási szabályzatot dolgozott ki a személyes adatok közvetlen üzletszerzés során történő felhasználására vonatkozóan. A szabályzatot sikerrel nyújtották be a 29. cikk szerinti munkacsoporthoz. 2010-ben a szabályzatot az elektronikus marketing kommunikációval kapcsolatos melléklettel egészítették ki.[175]

173 Uo., 27. cikk, (2) bekezdés.

174 Uo., 27. cikk ,(3) bekezdés.

175 A 29. cikk szerinti munkacsoport *4/2010. sz. véleménye a FEDMA-nak a személyes adatok közvetlen üzletszerzés során történő felhasználására vonatkozó európai eljárási szabályzatáról*, WP 174., Brüsszel, 2010. július 13.

5

Az érintett jogai és e jogok érvényesítése

EU	Tárgyalt kérdések	Európa Tanács
A hozzáférési jog		
Adatvédelmi irányelv, 12. cikk EUB, C-553/07. sz. *College van burgemeester en wethouders van Rotterdam kontra M.E.E. Rijkeboer ügy*, 2009. május 7.	**Hozzáférés a személy saját adataihoz**	108. egyezmény, 8. cikk, b) pont
	A helyesbítéshez, törléshez vagy zároláshoz való jog	108. egyezmény, 8. cikk, c) pont EJEB, *Cemalettin Canli kontra Törökország* (22427/04), 2008. november 18. EJEB, *Segerstedt-Wiberg és társai kontra Svédország* (62332/00), 2006. június 6. EJEB, *Ciubotaru kontra Moldova* (27138/04), 2010. április 27.
A tiltakozás joga		
Adatvédelmi irányelv, 14. cikk (1) bekezdés a) pont	**Tiltakozási jog az érintett konkrét helyzete alapján**	A profilalkotásra vonatkozó ajánlás, 5,3. cikk
Adatvédelmi irányelv, 14. cikk, (1) bekezdés, b) pont	**Tiltakozási jog az adatok marketing célokra történő további felhasználásával kapcsolatban**	A közvetlen üzletszerzésre vonatkozó ajánlás, 4.1. cikk

EU	Tárgyalt kérdések	Európa Tanács
Adatvédelmi irányelv, 15. cikk	Tiltakozási jog az automatizált döntésekkel kapcsolatban	A profilalkotásra vonatkozó ajánlás, 5.5. cikk
Független felügyelet		
Charta, 8. cikk, (3) bekezdés Adatvédelmi irányelv, 28. cikk Uniós intézmények, V. fejezet Adatvédelmi rendelet EUB, C-518/07. sz. *Európai Bizottság kontra Német Szövetségi Köztársaság* ügy, 2010. március 9. EUB, C-614/10. sz. *Európai Bizottság kontra Ausztria ügy*, 2012. október 16. EUB, C-288/12. sz. *Európai Bizottság kontra Magyarország ügy*, 2014. április 8.	Nemzeti felügyeleti hatóságok	108. egyezmény, Kiegészítő jegyzőkönyv, 1. cikk
Jogorvoslatok és szankciók		
Adatvédelmi irányelv, 12. cikk	Az adatkezelőhöz intézett kérés	108. egyezmény, 8. cikk, b) pont
Adatvédelmi irányelv, 28. cikk, (4) bekezdés Uniós intézmények, adatvédelmi rendelet, 32. cikk, (2) bekezdés	A felügyelő hatósághoz benyújtott követelések	108. egyezmény, Kiegészítő jegyzőkönyv, 1. cikk, (2) bekezdés, b) pont
Charta, 47. cikk	Bíróságok (általában)	EJEE, 13. cikk
Adatvédelmi irányelv, 28. cikk, (3) bekezdés	Nemzeti bíróságok	108. egyezmény, Kiegészítő jegyzőkönyv, 1. cikk, (4) bekezdés
EUMSZ, 263. cikk, (4) bekezdés Uniós intézmények, adatvédelmi rendelet, 32. cikk, (1) bekezdés EUMSZ, 267. cikk	EUB	
	EJEB	EJEE, 34. cikk
Jogorvoslatok és szankciók		
Charta, 47. cikk Adatvédelmi irányelv, 22. és 23. cikk EUB, C-14/83. sz. *Sabine von Colson és Elisabeth Kamann kontra Land Nordrhein-Westfalen ügy*, 1984. április 10. EUB, C-152/84. sz. *M.H. Marshall kontra Southampton and South-West Hampshire Area Health Authority* ügy, 1986. február 26.	A nemzeti adatvédelmi jogszabályok megsértése esetén	EJEE, 13. cikk (csak az Európa Tanács tagállamai számára) 108. egyezmény, 10. cikk EJEB, *K. U. kontra Finnország* (2872/02. sz. ügy), 2008. december 2. EJEB, *Biriuk kontra Litvánia* ügy, 23373/03, 2008. november 25.

EU	Tárgyalt kérdések	Európa Tanács
Uniós intézmények, adatvédelmi rendelet, 34. és 49. cikk EUB, C-28/08 P. sz. *Európai Bizottság kontra The Bavarian Lager Co. Ltd ügy*, 2010. június 29.	Az uniós jog uniós intézmények és szervek általi megsértése esetén	

Általánosságban a jogi előírások és konkrétan az érintettek jogai hatékonysága jelentős mértékben attól függ, hogy léteznek-e megfelelő mechanizmusok ezen előírások, illetve jogok érvényesítésére. Az európai adatvédelmi jogban az érintettet nemzeti jogszabálynak kell feljogosítania adatainak védelmére. A nemzeti jogszabályoknak független felügyelő hatóságokat is létre kell hozniuk, amelyek segítik az érintetteket jogaik gyakorlásában, és felügyelik a személyesadat-feldolgozást. Ezen felül az EJEE-ben és a Chartában is garantált hatékony jogorvoslathoz való jog megköveteli, hogy a bírósági jogorvoslat lehetősége mindenki számára rendelkezésre álljon.

5.1. Az érintettek jogai

Főbb pontok

- A nemzeti jog alapján mindenkinek joga van ahhoz, hogy bármely adatkezelőtől tájékoztatást kérjen arról, hogy az adatkezelő dolgoz-e fel rá vonatkozó adatokat.
- Az érintettek a nemzeti jog alapján jogosultak arra, hogy:
  - saját adataikhoz hozzáférjenek bármely adatkezelőnél, amely ezeket az adatokat feldolgozza;
  - adataikat a feldolgozó adatkezelővel helyesbíttessék (vagy szükség esetén zároltassák), ha az adatok nem pontosak;
  - adataikat az adatkezelővel töröltessék vagy adott esetben zároltassák, ha az adatkezelő jogellenesen dolgozza fel azokat.
- Ezenfelül az érintettek tiltakozhatnak az adatkezelőnél a következők miatt:
  - automatizált döntések (amelyeket kizárólag automatizált módon feldolgozott személyes adatok felhasználásával kapcsolatban hoztak);
  - adataik feldolgozása, ha a feldolgozás aránytalan eredményekhez vezet;
  - adataik közvetlen üzletszerzési célokra való felhasználása.

5.1.1. A hozzáférési jog

Az **EU jogban** az adatvédelmi irányelv 12. cikke tartalmazza az érintett hozzáférési jogának elemeit, beleértve azt a jogát, hogy az adatkezelőtől „megerősítést kapjon arról, hogy rá vonatkozóan adatok kezelése folyamatban van-e, továbbá, hogy információt kapjon legalább az adatkezelés céljáról, az érintett adatkategóriákról, a címzettekről vagy a címzettek kategóriáiról, akik felé az adatokat továbbítják", valamint hogy „kérje az olyan adatok helyesbítését, törlését vagy zárolását, amelyek kezelése nem felel meg ezen irányelv rendelkezéseinek, különösen az ilyen adatok hiányos vagy hibás volta miatt".

Az **Európa Tanács jogában** is léteznek ugyanezek a jogok, és ezekről a hazai jognak kell rendelkeznie (a 108. egyezmény 8. cikke). Számos európa tanácsi ajánlás használja a „hozzáférés" fogalmát, és a hazai jog az előző bekezdésben foglaltakkal azonos módon leírja a hozzáférési jog különböző vonatkozásait, és javaslatot tesz azok végrehajtására.

A 108. egyezmény 9. cikke és az adatvédelmi irányelv 13. cikke szerint az adatkezelők azon kötelezettsége, hogy válaszoljanak az érintett hozzáférési kérelmére, mások magasabb rendű jogos érdekei miatt korlátozható. A magasabb rendű jogos érdekek közé tartozhat a közérdek, például a nemzetbiztonság, a közbiztonság és a bűncselekmények üldözése, valamint a magánérdek, amely megelőzi az adatvédelemhez fűződő érdekeket. Minden kivételnek vagy korlátozásnak egy demokratikus társadalomban szükségesnek, valamint a kitűzött jogszerű céllal arányosnak kell lennie. Igen kivételes esetekben – például orvosi javallat miatt – pusztán az érintett védelme miatt is szükség lehet az átláthatóság korlátozására; ez különösen a minden érintett számára biztosított hozzáférési jog korlátozásához kapcsolódik.

Amennyiben az adatokat kizárólag tudományos kutatás céljára vagy statisztikai célokra dolgozzák fel, az adatvédelmi irányelv engedélyezi, hogy nemzeti jogszabály korlátozza a hozzáférési jogokat; megfelelő jogi biztosítékokat kell azonban életbe léptetni. Különösen azt kell biztosítani, hogy a szóban forgó adatfeldolgozással összefüggésben nem hoznak meghatározott egyénre vonatkozó intézkedéseket vagy döntéseket, és „nyilvánvalóan nem áll fenn annak a veszélye, hogy az érintett magánélethez való jogát sérelem éri".[176] A 108. egyezmény 9. cikkének (3) bekezdése hasonló rendelkezéseket tartalmaz.

176 Adatvédelmi irányelv, 13. cikk (2) bekezdés.

Hozzáférés a személy saját adataihoz

Az **Európa Tanács joga** szerint a 108. egyezmény 8. cikke kifejezetten elismeri a személy jogát a saját adataihoz való hozzáféréshez. Az EJEB többször is megállapította, hogy a személy hozzáférési joggal rendelkezik a saját, mások által tárolt vagy használt személyes adataihoz, és hogy ez a jog a magánélet tiszteletben tartásához való jogból fakad.[177] A *Leander* ügyben[178] az EJEB kimondta, hogy a hatóságok által tárolt személyes adatokhoz való hozzáférés mindazonáltal – bizonyos körülmények között – korlátozható.

Az **uniós jogban** az adatvédelmi irányelv 12. cikke kifejezetten szól a személy saját adataihoz való hozzáférési jogáról, és arról, hogy e jogot a Charta 8. cikkének (2) bekezdése alapvető jognak ismeri el.

Az irányelv 12. cikkének a) pontja előírja, hogy a tagállamoknak biztosítaniuk kell minden érintett számára a hozzáférési jogot személyes adataikhoz és a tájékoztatáshoz. Minden érintettnek joga van arra, hogy megerősítést kapjon az adatkezelőtől arról, hogy rá vonatkozóan adatok kezelése folyamatban van-e, továbbá, hogy információt kapjon legalább a következőkről:

- az adatkezelés céljai;
- az érintett adatkategóriák;
- az adatkezelés alatt álló adatok;
- az adatok címzettjei, illetve a címzettek kategóriái, akik felé az adatokat továbbítják;
- az adatkezelés alatt álló adatok forrásával kapcsolatos minden rendelkezésre álló információ;
- automatizált döntések esetében az adatok automatizált feldolgozása során alkalmazott logika.

177 EJEB, *Gaskin kontra Egyesült Királyság* (10454/83), 1989. július 7.; EJEB, *Odièvre kontra Franciaország* [nagytanács] (42326/98), 2003. február 13.; EJEB, *K.H. és mások kontra Szlovákia* (32881/04), 2009. április 28.; EJEB, *Godelli kontra Olaszország (33783/09)*, 2012. szeptember 25.

178 EJEB, *Leander kontra Svédország* (9248/81), 1985. július 11.

Nemzeti jogszabály a fentieket további, az adatkezelő által megadandó információkkal is kiegészítheti, például azzal, hogy az adatkezelő jelölje meg az adatkezelést lehetővé tevő jogalapot.

Példa: Ha a személy hozzáfér a saját személyes adataihoz, meg tudja ítélni, hogy az adatok pontosak-e. Ezért feltétlenül szükséges, hogy az érintett tájékoztatást kapjon a feldolgozott adatkategóriákról és az adatok tartalmáról. Nem elég tehát, ha az adatkezelő egyszerűen csak elmondja az érintettnek, hogy kezeli nevét, címét, születési idejét és érdeklődési körét, hanem pontosan közölnie kell az érintettel, hogy feldolgozza a következőket: „név: N.N.; cím: 1040 Bécs, Schwarzenbergplatz 11, Ausztria; születési idő: 1974. 10. 10.; érdeklődési kör (az érintett nyilatkozata szerint): komolyzene." Az utolsó tétel ezen felül információt tartalmaz az adatok forrásáról.

A személyes adatokkal és az adatok forrásával kapcsolatos minden rendelkezésre álló információt érthető formában – adott esetben részletesen is - közölni kell az érintettel. Ha például egy hozzáférés iránti kérelemre válaszul csupán műszaki rövidítéseket vagy orvosi szakszavakat adnak meg, az általában nem elegendő – még akkor sem, ha csupán a szóban forgó rövidítéseket vagy fogalmakat tárolják.

Az adatkezelőnek – hozzáférés iránti kérelemre válaszul – tájékoztatást kell adnia az adatok forrásával kapcsolatban, amennyiben ez az információ rendelkezésre áll. E rendelkezés a tisztességesség és az elszámoltathatóság elvére figyelemmel értendő. Az adatkezelő nem semmisítheti meg az adatok forrására vonatkozó információkat azért, hogy mentesüljön azok közlése alól, nem hagyhatja továbbá figyelmen kívül a tevékenységi területén szokásos dokumentálási normákat és általánosan elismert igényeket. Ha nem őrzik meg az adatok forrására vonatkozó dokumentációt, azzal rendszerint nem tesznek eleget az adatkezelő hozzáférési jog alapján fennálló kötelezettségének.

Amennyiben automatizált értékelést végeznek, az értékelés általános logikáját nem kell megmagyarázni, beleértve a konkrét kritériumokat is, amelyeket az érintett értékelése során mérlegeltek.

Az irányelv nem teszi egyértelművé, hogy az információkhoz való hozzáférés a múltra vonatkozik-e, és ha igen, milyen múltbeli időszakot érint. Ezzel kapcsolatban – ahogyan az EUB ítélkezési gyakorlata is kiemeli – a személy saját adataihoz való hozzáférési joga határidőkkel indokolatlanul nem korlátozható. Az érintetteknek

ezenkívül ésszerű lehetőséget kell adni arra, hogy korábbi adatkezelési műveletekről tájékoztatást kapjanak.

Példa: A *Rijkeboer* ügyben[179] az EUB-ot annak megállapítására kérték, hogy az irányelv 12. cikkének a) pontja szerint valamely személynek a rá vonatkozó személyes adatok címzettjeire vagy a címzettek kategóriájára vonatkozó információkhoz való hozzáférés joga korlátozhatóe az adathozzáférés iránti kérelem benyújtását megelőző egyéves időtartamra.

Annak meghatározásához, hogy az irányelv 12. cikkének a) pontja lehetővé tesze, vagy sem ilyen időbeli korlátozást, a Bíróság úgy döntött, hogy a szóban forgó cikket az irányelv célkitűzéseinek fényében értelmezi. A Bíróság először is megállapította, hogy a hozzáféréshez való jog szükséges ahhoz, hogy az érintett gyakorolja azon jogát, hogy kérelmére az adatkezelő helyesbítse, törölje vagy zárolja az adatait (12. cikk, b) pont), vagy kérelmére az adatkezelő értesítse az adatokról tudomást szerző harmadik feleket e helyesbítésről, törlésről vagy zárolásról (12. cikk, c) pont). E hozzáféréshez való jog szükséges ahhoz is, hogy az érintett gyakorolja az adatok feldolgozása elleni tiltakozáshoz való jogát (14. cikk) vagy kártérítési igényét, ha őt kár érte (22. és 23. cikk).

A fenti rendelkezések hatékony érvényesülése érdekében a Bíróság megállapította, hogy „e jognak szükségszerűen a múltra is vonatkoznia kell. Ellenkező esetben ugyanis az érintett személy nem gyakorolhatná eredményesen a jogszerűtlennek vagy helytelennek vélt adatok helyesbítéséhez, törléséhez vagy zárolásához fűződő, valamint jogorvoslati és kártérítéshez való jogát."

Az adatok helyesbítéséhez, törléséhez és zárolásához való jog

„Minden személynek lehetővé kell tenni a rá vonatkozó, adatkezelés alatt álló adatokhoz való hozzáférés jogának gyakorlását, különösen az adatok helyességének és az adatfeldolgozás jogszerűségének ellenőrzése céljából."[180] Ezen elvekkel összhangban az érintettnek a nemzeti jogban jogosultsággal kell bírnia, hogy az adatkezelőtől kérje az olyan adatok helyesbítését, törlését vagy zárolását, amelyek kezelése

179 EUB, C-553/07. sz. *College van burgemeester en wethouders van Rotterdam kontra M.E.E. Rijkeboer ügy*, 2009. május 7.

180 Adatvédelmi irányelv, (41) preambulumbekezdés.

nem felel meg ezen irányelv rendelkezéseinek, különösen az ilyen adatok hiányos vagy hibás volta miatt.[181]

Példa: A *Cemalettin Canli kontra Törökország* ügyben[182] az EJEB megállapította az EJEE 8. cikkének megsértését büntetőeljárásban történt hibás rendőrségi jelentés miatt.

A felperest kétszer vonták büntetőeljárás alá illegális szervezetben való állítólagos tagság miatt, de soha nem ítélték el. Amikor a felperest újra letartóztatták és más bűncselekmény miatt elítélték, a rendőrség *„tájékoztató további bűncselekményekről"* címmel jelentést nyújtott be a büntetőbíróságra, amelyben a felperest két illegális szervezet tagjaként tüntette fel. A felperesnek a jelentés és a rendőrségi nyilvántartás módosítására irányuló kérését elutasították. Az EJEB megállapította, hogy a rendőrségi jelentésben szereplő információk az EJEE 8. cikkének hatálya alá tartoznak, mivel a nyilvános információk is a „magánélet" körébe tartozhatnak, ha szisztematikusan gyűjtötték és a hatóságok által vezetett aktákban tárolják azokat. Ezenfelül, a rendőrségi jelentés valótlan volt, az elkészítése és a büntetőbírósághoz való benyújtása pedig nem felelt meg a jogszabályoknak. A Bíróság arra a következtetésre jutott, hogy megsértették a 8. cikket.

Példa: A *Segerstedt-Wiberg és mások kontra Svédország* ügyben[183] a felperesek tagjai voltak bizonyos liberális és kommunista politikai pártoknak. A felperesek gyanították, hogy adataikat felvették a rendőrségi nyilvántartásba. Az EJEB meggyőződött arról, hogy a kérdéses adatok tárolására volt jogalap, és az adatok tárolása jogszerű célt szolgált. Egyes felperesek esetében az EJEB úgy találta, hogy az adatok tartós megőrzése aránytalan beavatkozást jelent e személyek magánéletébe. Schmid úr esetében például a hatóságok megőrizték azt az információt, hogy 1969-ben tüntetések során Schmid úr állítólag erőszakosan ellenállt a rendőri ellenőrzésnek. Az EJEB megállapította, hogy ez az információ – figyelembe véve különösen azt, hogy milyen régen keletkezett – semmiféle releváns nemzetbiztonsági érdeket nem szolgálhat. Az EJEB azt

181 Uo., 12. cikk, b) pont.

182 EJEB, *Cemalettin Canli kontra Törökország* (22427/04), 2008. november 18., 33., 42. és 43. pont; EJEB, *Dalea kontra Franciaország* (964/07), 2010. február 2.

183 EJEB, *Segerstedt-Wiberg és mások kontra Svédország* (62332/00), 2006. június 6., 89. és 90. pont; lásd még például: EJEB, *M.K. kontra Franciaország* (19522/09), 2013. április 18.

állapította meg, hogy az öt felperes közül négy esetében megsértették az EJEE 8. cikkét.

Egyes esetekben elegendő, ha az érintett egyszerűen csak kéri például neve betűzésének helyesbítését, megváltozott címének vagy telefonszámának kijavítását. Ha azonban az ilyen kéréshez jogi kérdés kapcsolódik – például az érintett jogi személyisége, vagy a jogi dokumentumok kézbesítése szempontjából helyes tartózkodási helye –, előfordulhat, hogy a helyesbítés iránti kérelem nem elegendő, és az adatkezelő követelheti az állítólagos valótlanság bizonyítását. E követelés nem róhat túl nagy bizonyítási terhet az érintettre, és ezáltal nem akadályozhatja meg az érintettet abban, hogy adatait helyesbíttesse. Az EJEB számos olyan esetben megállapította az EJEE 8. cikkének megsértését, amikor a felperes nem tudta vitatni a titkos nyilvántartásokban tárolt információk helyességét.[184]

Példa: A *Ciubotaru kontra Moldova* ügyben[185] a felperes állítólag azért nem tudta moldávról románra változtatni az etnikai származására vonatkozó bejegyzést a hivatalos nyilvántartásban, mert kérelmét nem támasztotta alá bizonyítékkal. Az EJEB megítélése szerint elfogadható, ha az állam az egyén etnikai származásának nyilvántartásba vételekor objektív bizonyítékot kér. Amennyiben az állítás pusztán szubjektív, bizonyítékkal alá nem támasztott, a hatóságok visszautasíthatják azt. A felperes állítása azonban nem csupán saját etnikai hovatartozásának szubjektív megítélésén alapult; objektíven ellenőrizhető kapcsolódási pontokat tudott kimutatni – például a nyelv, a név, az együttérzés és egyebek tekintetében – a román etnikumhoz. A hazai jog szerint azonban a felperesnek bizonyítania kellett, hogy szülei a román etnikumhoz tartoztak. Figyelembe véve Moldova történelmi realitását, egy ilyen követelmény leküzdhetetlen akadályt jelentett azzal kapcsolatban, hogy a felperes a szovjet hatóságok által a szüleire vonatkozóan bejegyzett etnikai identitástól eltérő etnikai származást vetessen nyilvántartásba. Az állam azzal, hogy megakadályozta, hogy a felperes állítását objektíven ellenőrizhető bizonyítékok fényében vizsgálják, nem tett eleget azon pozitív kötelezettségének, hogy biztosítsa a felperes magánélethez való jogának tényleges tiszteletben tartását. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Az adatok helyességének megállapítására indított polgári peres eljárásban vagy hatósági eljárásban az érintett kérheti, hogy adatállományában bejegyzést vagy

184 EJEB, *Rotaru kontra Románia* (28341/95), 2000. május 4.

185 EJEB, *Ciubotaru kontra Moldova* (27138/04), 2010. április 27., 51. és 59. pont.

megjegyzést helyezzenek el, miszerint az adatok helyességét vitatják, és az erre vonatkozó hivatalos döntés folyamatban van. Ezen időszak alatt az adatkezelő – különösen harmadik felek felé – nem állíthatja be az adatokat bizonyosnak vagy véglegesnek.

Az érintett adatok törlése iránti kérelme gyakran azon az állításon alapszik, hogy az adatfeldolgozásnak nincs törvényes jogalapja. Ez akkor szokott felmerülni, ha a hozzájárulást visszavonták, vagy ha az adatgyűjtés céljának teljesítéséhez bizonyos adatokra már nincs szükség. Az adatkezelés jogszerűségére vonatkozó bizonyítási teher az adatkezelőt terheli, mivel az adatkezelő felel az adatfeldolgozás jogszerűségéért. Az elszámoltathatóság elve szerint az adatkezelőnek bármikor tudnia kell igazolni, hogy szilárd jogalappal rendelkezik az általa végzett adatgyűjtéshez, ellenkező esetben a feldolgozást le kell állítani.

Ha az adatok kezelését vitatják, mert az adatok állítólag valótlanok vagy feldolgozásuk jogellenesen történt, az érintett a tisztességes adatkezelés elvének megfelelően követelheti a vitatott adatok zárolását. Ez azt jelenti, hogy az adatokat nem törlik, de az adatkezelő a zárolás ideje alatt nem használhatja fel őket. Erre különösen akkor lenne szükség, ha a valótlan vagy jogellenesen tárolt adatok kárt okozhatnának az érintettnek. A nemzeti jognak kell részletesebben szabályoznia, hogy az adatok felhasználásának zárolására irányuló kötelezettség mikor merülhet fel, és hogyan kell az ehhez való jogot gyakorolni.

Az érintettek ezenfelül jogosultak kérni az adatkezelőtől a zárolásra, helyesbítésre vagy törlésre vonatkozó, harmadik feleknek szóló értesítést, ha azok a szóban forgó műveletek előtt kaptak adatokat. Mivel az adatkezelőnek dokumentálnia kellett az adatok harmadik felekkel való közlését, a címzetteknek azonosíthatónak kell lenniük, és a törlés kérésére lehetőséget kell biztosítani. Ha azonban időközben az adatokat közzétették például az interneten, nem kizárt, hogy az adatokat minden esetben töröltetni kell, mivel az adatok címzettjei nem lelhetők fel. Az adatvédelmi irányelv szerint helyesbítés, törlés, vagy zárolás céljából a címzettek megkeresése kötelező, „hacsak ez lehetetlennek nem bizonyul, vagy aránytalanul nagy erőfeszítést nem igényel”.[186]

186 Adatvédelmi irányelv, 12. cikk, c) pont, utolsó félmondat.

5.1.2. A tiltakozás joga

A tiltakozás joga az automatizált egyedi döntések kifogásolására, az érintett sajátos helyzetéből fakadó kifogásolási jogára, valamint az adatok közvetlen üzletszerzés céljára történő további felhasználása elleni tiltakozásra egyaránt kiterjed.

Tiltakozási jog az automatizált egyedi döntésekkel kapcsolatban

Az automatizált döntések olyan döntések, amelyeket kizárólag automatizált módon feldolgozott személyes adatok felhasználásával kapcsolatban hoztak. Ha az ilyen döntés valószínűleg jelentős mértékben érintené mások életét, mivel például a hitelképességgel, a munkahelyi teljesítménnyel, az életvitellel vagy a megbízhatósággal kapcsolatos, a nem kívánatos következmények elkerülése érdekében különleges védelemre van szükség. Az adatvédelmi irányelv úgy rendelkezik, hogy automatizált döntések nem határozhatnak meg olyan kérdéseket, amelyek fontosak az egyének számára, és előírja, hogy az egyén számára biztosítani kell a jogot az automatizált döntés felülvizsgálatára.[187]

Példa: Fontos gyakorlati példa az automatizált döntésre a hitelbírálati minősítés. Annak érdekében, hogy gyorsan dönthessenek egy jövőbeli ügyfél hitelképességéről, bizonyos adatokat, köztük a foglalkozásra és a családi állapotra vonatkozó információkat gyűjtenek az ügyféltől, és összekapcsolják ezeket az érintettre vonatkozó, más forrásból – például hitelinformációs rendszerekből – származó adatokkal. Ezeket az adatokat automatikusan beviszik egy minősítő algoritmussal működő rendszerbe, amely kiszámítja a potenciális ügyfél hitelképességét jelző összesített értéket. Így a cég alkalmazottja másodperceken belül el tudja dönteni, hogy az érintett ügyfélként elfogadható-e vagy sem.

Mindazonáltal az irányelv szerint a tagállamok úgy is rendelkezhetnek, hogy az automatizált döntés hatálya kiterjedhet a személyre – vagy olyan esetben, amikor a döntés az érintett számára kedvező volt, vagy amennyiben az érintett érdekeit más megfelelő biztosítékokkal védik.[188] Az automatizált döntésekkel szembeni tiltakozás joga az **Európa Tanács jogában** is megtalálható, ahogyan a profilalkotásra vonatkozó ajánlásból is kitűnik.[189]

187 Uo., 15. cikk, (1) bekezdés.

188 Uo., 15. cikk, (2) bekezdés.

189 A profilalkotásra vonatkozó ajánlás, 5. cikk, (5) bekezdés.

Tiltakozási jog az érintett konkrét helyzete alapján

Az érintettek nem rendelkeznek általános tiltakozási joggal adataik feldolgozása ellen.[190] Az adatvédelmi irányelv 14. cikkének a) pontja azonban feljogosítja az érintettet arra, hogy sajátos helyzetével kapcsolatos lényeges jogos érdekből tiltakozzon. Az Európa Tanács profilalkotásra vonatkozó ajánlása is elismer ehhez hasonló jogot.[191] E rendelkezések célja az érintett adatainak kezelése során a megfelelő egyensúly megtalálása az érintett adatvédelmi jogai és mások törvényes jogai között.

Példa: Egy bank hét évig tárol a hitelek visszafizetésével késedelembe esett ügyfeleire vonatkozó adatokat. Egy ügyfél, akinek adatait a szóban forgó adatbázisban tárolják, újabb hitelért folyamodik. Megnézik az adatbázist, a pénzügyi helyzetre vonatkozó értékelést is elkészítik, és az ügyfél hiteligénylését elutasítják. Az ügyfél azonban tiltakozhat személyes adatainak az adatbázisban történő tárolása ellen, és kérheti az adatok törlését, ha bizonyítani tudja, hogy a fizetési késedelem csupán egy hibából fakadt, amelyet a tudomásszerzést követően azonnal kijavítottak.

A sikeres tiltakozás joghatása az, hogy az adatkezelő a továbbiakban már nem kezelheti a szóban forgó adatokat. Az érintett adatain a tiltakozás előtt végzett műveletek azonban továbbra is jogszerűek.

Tiltakozási jog adatok közvetlen üzletszerzési célokra történő további felhasználásávalkapcsolatban

Az adatvédelmi irányelv 14. cikkének b) pontja egyedi tiltakozási jogról rendelkezik a személy adatainak közvetlen üzletszerzési célokra történő felhasználása ellen. Ezt a jogot az Európa Tanács közvetlen üzletszerzésre vonatkozó ajánlása is tartalmazza.[192] Az ilyen típusú tiltakozást azelőtt kell benyújtani, hogy az adatokat közvetlen üzletszerzési célra harmadik felek rendelkezésére bocsátják. Az érintett számára tehát lehetőséget kell biztosítani a tiltakozásra, mielőtt az adatokat továbbítják.

190 Lásd még EJEB, *M.S. kontra Svédország* (20837/92), 1997. augusztus 27., amelyben orvosi adatokat hozzájárulás és a tiltakozás lehetősége nélkül közöltek; vagy EJEB, *Leander kontra Svédország* (9248/81), 1987. március 26.; vagy EJEB, *Mosley kontra Egyesült Királyság (48009/08)*, 2011. május 10.

191 A profilalkotásra vonatkozó ajánlás, 5. cikk, (3) bekezdés.

192 Az Európa Tanács Miniszteri Bizottsága (1985) (85)20. sz., a tagállamoknak szóló ajánlása a közvetlen üzletszerzési célokra felhasznált személyes adatok védelméről, 1985. október 25., 4. cikk, (1) bekezdés.

5.2. Független felügyelet

Főbb pontok

- A hatékony adatvédelem biztosítása érdekében a nemzeti jogszabályokban független felügyelő hatóságokat kell létrehozni.
- A nemzeti felügyelő hatóságoknak teljes függetlenséggel kell eljárniuk, amit az őket létrehozó törvénynek és a felügyelő hatóság egyedi szervezeti struktúrájának is tükröznie kell.
- A felügyelő hatóságok egyedi feladatokat látnak el, többek között az alábbiakat:
  - nemzeti szinten nyomon követik és előmozdítják az adatvédelmet;
  - tanácsadással segítik az érintetteket és az adatkezelőket, valamint a kormányt és a nagyközönséget;
  - megtárgyalják a panaszokat, és segítséget nyújtanak az érintettnek a feltételezett adatvédelmi jogsértésekkel kapcsolatban;
  - felügyelik az adatkezelőket és az adatfeldolgozókat;
  - szükség esetén beavatkoznak:
    - figyelmeztetésben vagy megrovásban részesítik, sőt akár meg is bírságolják az adatkezelőket és az adatfeldolgozókat,
    - elrendelik adatok helyesbítését, zárolását vagy törlését,
    - megtiltják az adatfeldolgozást;
  - ügyeket bíróság elé utalnak.

Az adatvédelmi irányelv a független felügyeletet a hatékony adatvédelem biztosításához szükséges fontos mechanizmusnak tartja., Ez először még nem jelent meg a 108. egyezményben vagy az OECD adatvédelmi iránymutatásaiban.

Figyelemmel arra, hogy a hatékony adatvédelem kialakítása szempontjából a független felügyelet nélkülözhetetlennek bizonyult, a 2013-ban elfogadott átdolgozott OECD adatvédelmi iránymutatás egyik új rendelkezése felhívja a tagállamokat, hogy „hozzanak létre és tartsanak fenn adatvédelmi végrehajtási hatóságokat, amelyek rendelkeznek a jogkörük hatékony gyakorlásához és az objektív, pártatlan és

következetes döntéshozatalhoz szükséges irányítással, erőforrásokkal és műszaki szaktudással".[193]

Az **Európa Tanács joga** szerint a 108. egyezményhez fűzött kiegészítő jegyzőkönyv kötelezővé tette a felügyelő hatóságok létrehozását. Ez az eszköz az 1. cikkben megjelöli a független felügyelő hatóságok jogi keretét, amelyet a szerződő feleknek a saját belső jogukban végre kell hajtaniuk és az adatvédelmi irányelvben szereplőhöz hasonló szavakkal írja le e hatóságok feladatait és hatáskörét. Elvileg tehát a felügyelő hatóságoknak az EU és az Európa Tanács joga szerint azonos módon kellene működniük.

Az **uniós jogban** a felügyelő hatóságok hatáskörét és szervezeti struktúráját először az adatvédelmi irányelv 28. cikkének (1) bekezdése körvonalazta. Az uniós intézmények adatvédelmi rendelete[194] létrehozza az európai adatvédelmi biztos intézményét, amely az uniós szervek és intézmények által végzett adatfeldolgozás felügyelő hatósága. Amikor a rendelet leírja a felügyelő hatóság szerepét és feladatkörét, az adatvédelmi irányelv kihirdetése óta összegyűlt tapasztalatokra épít.

Az adatvédelmi hatóságok függetlenségét az EUMSZ 16. cikkének (2) bekezdése és a Charta 8. cikkének (3) bekezdése garantálja. Ez utóbbi rendelkezés a független hatóság általi ellenőrzést kifejezetten az adatvédelemhez való alapvető jog elengedhetetlen elemének tartja. Ezenfelül az adatvédelmi irányelv előírja, hogy a tagállamok hozzanak létre teljes függetlenségben eljáró felügyelő hatóságokat az irányelv alkalmazásának nyomon követésére.[195] Nemcsak a felügyelő hatóság létrehozását megalapozó jogszabálynak kell a függetlenséget kifejezetten garantáló rendelkezéseket tartalmaznia, hanem a hatóság egyedi szervezeti felépítésének is alá kell támasztania a függetlenséget.

193 OECD (2013): *Az adatvédelemre és az országhatárokat átlépő személyesadat-áramlásra vonatkozó iránymutatások*, 19. cikk, c) pont.

194 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, HL 2001 L 8., 41–48. cikk.

195 Adatvédelmi irányelv, 28. cikk, (1) bekezdés, utolsó mondat; 108. egyezmény, kiegészítő jegyzőkönyv, 1. cikk, (3) bekezdés.

Az EUB 2010-ben foglalkozott először az adatvédelmi felügyelő hatóságok függetlenségére irányuló követelmény terjedelmének kérdésével.[196] Az alábbi példák jól szemléltetik az EUB gondolkodásmódját.

Példa: A *Bizottság kontra Németország* ügyben[197] az Európai Bizottság annak megállapítására kérte az EUB-ot, hogy Németország helytelenül ültette át az adatvédelem biztosításáért felelős hatóságok „teljes függetlenségére" vonatkozó követelményt, azaz nem teljesítette a 95/46/EK irányelv 28. cikke (1) bekezdéséből eredő kötelezettségeit. A Bizottság álláspontja szerint az volt a probléma, hogy Németország a személyes adatoknak a nem állami szektorban történő kezelését ellenőrző hatóságokat egyes tartományokban *(Länder)* állami felügyelet alá vonta.

A kereset megalapozottságának értékelése a Bíróság szerint az említett bekezdésben foglalt függetlenség követelményének hatályától, következésképpen e rendelkezés értelmezésétől függött.

A Bíróság kiemelte, hogy az irányelv 28. cikkének (1) bekezdésében szereplő „teljes függetlenséggel" kifejezést a rendelkezés szövegezése, valamint az adatvédelmi irányelv céljai és szerkezete alapján kell értelmezni.[198] A Bíróság hangsúlyozta, hogy a felügyelő hatóságok az irányelvben biztosított személyesadat-feldolgozással kapcsolatos jogok „őrzői", ennélfogva létrehozásuk a tagállamokban „alapvető eleme az egyének védelmének a személyes adatok kezelése tekintetében".[199] A Bíróság megállapította, hogy „feladataik gyakorlása során az ellenőrző hatóságoknak objektíven és pártatlanul kell eljárniuk. Ezért minden külső befolyástól mentesnek kell lenniük, ideértve az állam vagy a tartományok által gyakorolt közvetlen vagy közvetett befolyást is, nemcsak az ellenőrzött szervezetek általi befolyást."[200]

Az EUB azt is megállapította, hogy a „teljes függetlenséget" az európai adatvédelmi biztosnak az uniós intézmények adatvédelmi rendeletében

196 Lásd FRA (2010), *Alapvető jogok: kihívások és eredmények 2010-ben* – Az FRA éves jelentése (2010), 59. o. Az FRA a 2010 májusában közzétett, *Adatvédelem az Európai Unióban: a nemzeti adatvédelmi hatóságok szerepe* című jelentésében részletesebben is foglalkozott ezzel a kérdéssel.

197 EUB, C-518/07. sz. *Európai Bizottság kontra Német Szövetségi Köztársaság ügy*, 2010. március 9., 27. pont.

198 *Uo.*, 17. és 29. pont.

199 *Uo.*, 23. pont.

200 *Uo.*, 25. pont.

meghatározott függetlensége fényében kell értelmezni. Ahogyan a Bíróság hangsúlyozta, a rendelet 44. cikkének (2) bekezdése pontosítja a függetlenség fogalmát azzal, hogy hozzáteszi: „az európai adatvédelmi biztos feladatkörének ellátása során senkitől nem kérhet és nem fogadhat el utasítást". Ez kizárja a független adatvédelmi felügyelő hatóság állami felügyeletét.[201]

Ennek megfelelően az EUB megállapította, hogy a szövetségi államok szintjén működő, a személyes adatok nem állami szervek általi feldolgozását ellenőrző német adatvédelmi intézmények nem kellőképpen függetlenek, mivel állami felügyelet alatt állnak.

Példa: A *Bizottság kontra Ausztria* ügyben[202] az EUB hasonló problémákra világított rá az osztrák adatvédelmi hatóság (Adatvédelmi Bizottság, DSK) egyes tagjainak és személyi állományának helyzetével kapcsolatban. A Bíróság ebben az ügyben arra a következtetésre jutott, hogy az osztrák jogszabályok nem teszik lehetővé a DSK számára, hogy a feladatai ellátása során az adatvédelmi irányelv értelmében vett teljes függetlenségben járjon el. Az osztrák adatvédelmi hatóság függetlensége nem volt kellően biztosított, mert a szövetségi kancellária látja el a DSK-t munkaerővel, felügyeli a DSK-t, továbbá mindenkor tájékoztatást kérhet a DSK munkájáról.

Példa: A *Bizottság kontra Magyarország* ügyben[203] az EUB rámutatott arra, hogy a követelmény, miszerint biztosítani kell, hogy a rájuk ruházott feladatok gyakorlása során minden egyes hatóság teljes függetlenségben járjon el, magában foglalja azt a kötelezettséget, hogy az érintett tagállamnak e hatóság megbízatását az eredetileg megállapított időtartam leteltéig tiszteletben kell tartania. A bíróság azt is megállapította, hogy Magyarország,mivel idő előtt megszüntette a személyes adatok védelmét felügyelő hatóság megbízatását, nem teljesítette a 95/46/EK irányelvből eredő kötelezettségeit.

A felügyelő hatóságok a nemzeti jog alapján többek között a következő hatáskörökkel és jogosultságokkal rendelkeznek:[204]

201 *Uo.*, 27. pont.

202 EUB, C-614/10. sz. *Európai Bizottság kontra Ausztria ügy*, 2012. október 16., 59. és 63. pont.

203 EUB, C-288/12. sz. *Európai Bizottság kontra Magyarország ügy*, 2014. április 8., 50. és 67. pont.

204 Adatvédelmi irányelv, 28. cikk; lásd még a 108. egyezmény kiegészítő jegyzőkönyvének 1. cikkét.

- tanácsot adhatnak az adatkezelőknek és az érintetteknek adatvédelmi kérdésekben;
- vizsgálhatják az adatkezelési műveleteket, és ennek megfelelően beavatkozhatnak;
- figyelmeztethetik vagy megrovásban részesíthetik az adatkezelőket;
- elrendelhetik adatok helyesbítését, zárolását, törlését vagy megsemmisítését;
- elrendelhetik az adatkezelés átmeneti vagy végleges tilalmát;
- ügyet bíróság elé utalhatnak.

Feladatainak gyakorlásához a felügyelő hatóságnak a vizsgálathoz szükséges valamennyi személyes adathoz és információhoz hozzáféréssel kell rendelkeznie, továbbá belépési joggal kell rendelkeznie minden olyan telephelyre, ahol az adatkezelő releváns információkat tárol.

A felügyelő hatóság eljárásai és megállapításainak jogi hatása tekintetében jelentős eltérések vannak a különböző belföldi joghatóságok között. A skála az ombudsman-szerű ajánlásoktól egészen az azonnal végrehajtható határozatokig terjedhet. Ezért az adott joghatóságon belül rendelkezésre álló jogorvoslati lehetőségek hatékonyságának elemzésekor a jogorvoslati eszközöket a saját összefüggésükben kell megítélni.

5.3. Jogorvoslatok és szankciók

Főbb pontok

- A 108. egyezmény és az adatvédelmi irányelv szerint a nemzeti jognak megfelelő jogorvoslati lehetőségeket és szankciókat kell megállapítania az adatvédelemhez való jog megsértése esetére.
    - Az EU joga értelmében a hatékony jogorvoslathoz való jog megköveteli, hogy a nemzeti jog az adatvédelmi jogok megsértésének esetére biztosítson bírósági jogorvoslatot – függetlenül attól, hogy a felügyelő hatósághoz lehet-e fordulni az ügyben.

  - A szankciókat nemzeti jogszabálynak kell megállapítania, és hatékonynak, egyenértékűnek, arányosnak és visszatartó erejűnek kell lenniük.
- Mielőtt valaki bírósághoz fordul, először az adatkezelőt kell megkeresnie. Azt, hogy bírósághoz fordulás előtt kötelező-e a felügyelő hatóság megkeresése, a nemzeti jognak kell szabályoznia.
- Az érintettek – végső megoldásként, bizonyos körülmények között – az adatvédelmi jogsértéseket az EJEB elé vihetik.
- Ezenfelül az érintettek az EUB-hoz is fordulhatnak, de csak igen korlátozott mértékben.

Az adatvédelmi jogszabályok értelmében fennálló jogokat csak az a személy gyakorolhatja, akinek jogai érintettek; ez a személy az érintett, vagy legalábbis aki magát érintettnek mondja. E személyeket jogaik gyakorlása során azon személyek képviselhetik, akik a nemzeti jog szerint megfelelnek a szükséges követelményeknek. A kiskorúakat szüleik vagy gyámjuk képviselheti. A személyt olyan szervezet is képviselheti a felügyelő hatóságok előtt, amelynek törvényes célja az adatvédelmi jogok előmozdítása.

5.3.1. Az adatkezelőhöz intézett kérések

A *3.2.* szakaszban említett jogok gyakorlása elsőként az adatkezelőn keresztül történhet. A nemzeti felügyelő hatóság vagy bíróság közvetlen megkeresése nem célravezető, mivel a hatóság csak azt tanácsolhatja, hogy először forduljanak az adatkezelőhöz, és a bíróság a kereseti kérelmet elutasítja. Nem szükséges, hogy nemzeti jogszabály szabályozza az adatkezelőhöz intézett, jogilag releváns kérelem formai követelményeit – különösen azt, hogy a kérelmet írásba kell-e foglalni.

Az adatkezelőként megkeresett jogalanynak válaszolnia kell a kérelemre akkor is, ha nem ő az adatkezelő. A választ minden esetben a nemzeti jogszabályban megállapított határidőn belül kell kézbesíteni az érintett részére – akkor is, ha csak az szerepel benne, hogy nem kezelnek a kérelmezőre vonatkozó adatokat. Az adatvédelmi irányelv 12. cikkének a) pontjában és a 108. egyezmény 8. cikkének b) pontjában foglalt rendelkezésekkel összhangban a kéréssel „túlzott késedelem nélkül" kell foglalkozni. A nemzeti jogszabálynak tehát olyan válaszadási határidőt kell előírnia, amely eléggé rövid, ugyanakkor lehetővé teszi, hogy az adatkezelő megfelelően foglalkozzon a kéréssel.

A kérés megválaszolása előtt az adatkezelőként megkeresett jogalanynak meg kell állapítania a kérelmező személyazonosságát, hogy meggyőződjön arról, a

kérelmező valóban az a személy, akinek magát állítja, így elkerülhető a titoktartás súlyos megsértése. Ha a személyazonosság megállapítására vonatkozó követelményeket nemzeti jogszabály kifejezetten szabályozza, az adatkezelőnek döntenie kell ezekről. A tisztességes adatkezelés elve azonban megkövetelné, hogy az adatkezelők ne írjanak elő túlzottan terhes feltételeket az azonosításra (és a kérelem hitelességének megállapítására, amit a *2.1.1.* szakaszban tárgyalunk).

A nemzeti jogszabálynak azzal a kérdéssel is foglalkoznia kell, hogy az adatkezelők, mielőtt válaszolnának a kérésre, kérhetnek-e díjat a kérelmezőtől: az irányelv 12. cikkének a) pontja és a 108. egyezmény 8. cikkének b) pontja úgy rendelkezik, hogy a hozzáférés iránti kérelemre „túlzott [...] költség nélkül" kell válaszolni. Számos európai ország nemzeti joga úgy rendelkezik, hogy az adatvédelmi törvény alapján benyújtott kérelmeket ingyenesen kell megválaszolni, amennyiben a válaszadás nem jár túlzott vagy szokatlan erőfeszítéssel; másfelől az adatkezelőket általában nemzeti jogszabály védi a kérelem megválaszolásához való joggal való visszaéléssel szemben.

Ha az adatkezelőként megkeresett személy, intézmény vagy szervezet nem tagadja, hogy ő az adatkezelő, a nemzeti jogban előírt határidőn belül köteles:

- vagy eleget tenni a kérelemnek és értesíteni a kérelmező személyt arról, hogy hogyan teljesítette kérelmét; vagy

- tájékoztatni a kérelmezőt, miért nem teljesíti a kérését.

5.3.2. A felügyelő hatósághoz benyújtott kérelmek

Ha egy személy, aki hozzáférés iránti kérelmet vagy tiltakozást nyújtott be az adatkezelőhöz, nem kap határidőre megfelelő választ, segítséget kérhet a nemzeti adatvédelmi felügyelő hatóságtól. A felügyelő hatóság előtti eljárás folyamán tisztázni kell, hogy a kérelmező által megkeresett személy, intézmény vagy szervezet valóban köteles volt-e válaszolni a kérelemre, és a válaszadás megfelelő és elegendő volt-e. A felügyelő hatóságnak értesítenie kell az érintett személyt a kérelmet tárgyaló eljárás eredményéről.[205] A nemzeti felügyelő hatóságok előtt folyó eljárások eredményének jogi hatása – az, hogy a hatóság határozata jogilag végrehajtható-e, azaz a határozat hivatalos hatóság által kikényszeríthető, vagy hogy bírósághoz

205 Adatvédelmi irányelv, 28. cikk (4) bekezdés.

kell-e fellebbezni, ha az adatkezelő nem tesz eleget a felügyelő hatóság határozatának (véleményének, megrovásának stb.) – a nemzeti jogtól függ.

Az EUMSZ 16. cikke által biztosított adatvédelmi jogok uniós intézmények vagy szervek általi állítólagos megsértése esetén az érintett panaszt tehet az európai adatvédelmi biztosnál,[206] amely az uniós intézmények adatvédelmi rendelete szerinti független adatvédelmi felügyelő hatóság, melynek feladatait és hatáskörét is a rendelet határozza meg. Ha az európai adatvédelmi biztos hat hónapon belül nem válaszol, a panaszt elutasítottnak kell tekinteni.

A nemzeti felügyelő hatóság döntései ellen lehetőséget kell biztosítani bírósági fellebbezésre. Ez az érintettre és az adatkezelőkre egyaránt vonatkozik, akik felügyelő hatóság előtt lefolytatott eljárásban félként vettek részt.

Példa: Az Egyesült Királyság információs biztosa 2013. július 24-én határozatot adott ki, melyben arra kérte a hertfordshire-i rendőrséget, hogy ne használjon egy általa jogellenesnek minősített rendszámtábla-követő rendszert. A kamerák által gyűjtött adatokat a helyi rendőrségi adatbázisokban és egy központi adatbázisban is tárolták. A rendszámtáblákról készített fényképeket két évig, a gépkocsik fényképét pedig 90 napig őrizték meg. A biztos megállapítása szerint egy ilyen kiterjedt kamerahasználat és a megfigyelés más formái nem állnak arányban a kezelni kívánt problémával.

5.3.3. Bíróságra benyújtott kérelem

Az adatvédelmi irányelv szerint, ha a személy, aki az adatvédelmi törvény szerint kérelmet nyújtott be az adatkezelőhöz, nem elégedett az adatkezelő válaszával, jogosult panaszával bírósághoz fordulni.[207]

Azt, hogy bírósághoz fordulás előtt először a felügyelő hatóságot kell-e megkeresni, a nemzeti jognak kell szabályoznia. A legtöbb esetben azonban előnyös az adatvédelmi jogaikat gyakorló személyek számára, ha először a felügyelő hatósághoz fordulnak, mivel az ő eljárásuk egyszerű és ingyenes. A felügyelő hatóság

206 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, HL 2001 L 8.

207 Adatvédelmi irányelv, 22. cikk.

határozatában (véleményében, megrovásában stb.) dokumentált szakvélemény is segítheti az érintettet abban, hogy jogait bíróság előtt érvényesítse.

Az **Európa Tanács joga** szerint az adatvédelmi jogok feltételezett megsértése, amit az EJEE egyik részes fele nemzeti szinten követett el és ami az EJEE 8. cikkét is sérti, ezenfelül az EJEB elé is vihető, ha az összes hazai jogorvoslati lehetőséget már kimerítették. Ahhoz, hogy az EJEE 8. cikkének megsértését az EJEB elé vigyék, más elfogadhatósági kritériumoknak is meg kell felelni (az EJEE 34–37. cikke).[208]

Bár az EJEB-hez intézett kereseti kérelmek közvetlenül a szerződő felek ellen is benyújthatók, közvetve magánfelek cselekményeivel vagy mulasztásaival is foglalkozhatnak, amennyiben egy szerződő fél nem tett eleget az EJEE értelmében fennálló pozitív kötelezettségeinek, és nemzeti jogában nem nyújtott elegendő védelmet az adatvédelmi jogok megsértése ellen.

Példa: A *K.U. kontra Finnország* ügyben[209] a kiskorú felperes azért tett panaszt, mert egy internetes társkereső oldalon szexuális tartalmú hirdetést tettek közzé róla. A szolgáltató a finn jogban előírt titoktartási kötelezettség miatt nem fedte fel az információt közzétevő személy kilétét. A felperes azt állította, hogy a finn jog nem nyújt elegendő védelmet a felperesről az interneten terhelő adatokat elhelyező magánszemély ilyen jellegű cselekményeivel szemben. Az EJEB megállapította, hogy az államok nemcsak kötelesek tartózkodni az egyének magánéletébe való önkényes beavatkozástól, hanem pozitív kötelezettségek is terhelhetik őket, amelyek „a magánélet tiszteletben tartásának biztosítására irányuló intézkedések elfogadását" jelentik „akár az egyének egymás közötti kapcsolatainak szférájában is". A felperes esetében a gyakorlati és hatékony védelem megkövetelte volna, hogy tegyenek tényleges lépéseket az elkövető azonosítására és vád alá helyezésére. Az állam azonban nem biztosított ilyen védelmet, ezért a Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Példa: A *Köpke kontra Németország* ügyben[210] a felperest a munkahelyén elkövetett lopással gyanúsították meg, és ezért rejtett videomegfigyelés alá helyezték. Az EJEB megállapította, hogy „semmi nem mutat arra, hogy a

208 EJEE, 34–37. cikk, elérhető a következő címen: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 EJEB, *K. U. kontra Finnország* (2872/02), 2009. március 2.

210 EJEB, *Köpke kontra Németország* (hat.) (420/07), 2010. október 5.

belföldi hatóságok mérlegelési mozgásterükön belül nem teremtettek megfelelő egyensúlyt egyfelől a felperes magánéletének tiszteletben tartásához való, 8. cikk szerinti joga, másfelől munkáltatójának a tulajdon védelméhez fűződő érdeke és a gondos igazságszolgáltatáshoz fűződő közérdek között". A keresetet ezért elutasították.

Ha az EJEB megállapítja, hogy egy részes fél megsértette az EJEE által oltalomban részesített bármelyik jogot, a részes fél köteles az EJEB ítéletét végrehajtani. A végrehajtási intézkedéseknek először is véget kell vetniük a jogsértésnek, és – amennyire lehetséges – orvosolniuk kell a jogsértés felperest érintő negatív következményeit. Az ítéletek végrehajtásához a Bíróság által megállapítotthoz hasonló jogsértések megelőzésére irányuló általános intézkedések is szükségesek, amelyek lehetnek jogszabály-módosítások, az ítélkezési gyakorlatban bekövetkező változások vagy egyéb intézkedések.

Ha az EJEB az EJEE megsértését állapítja meg, az EJEE 41. cikke értelmében az EJEB igazságos elégtételt ítélhet meg a felperesnek a részes fél költségére.

Az **uniós jogban**[211] az uniós adatvédelmi jogot végrehajtó nemzeti adatvédelmi jogszabályok megsértése esetén a sértettek egyes esetekben az EUB-hoz fordulhatnak. Két lehetséges forgatókönyv létezik arra, hogy az érintett adatvédelmi jogainak megsértése nyomán hogyan indítható eljárás az EUB előtt.

Az első forgatókönyv szerint az érintettnek az egyén adatvédelemhez való jogát sértő uniós igazgatási vagy szabályozási jogi aktus közvetlen sértettjének kell lennie. Az EUMSZ 263. cikkének (4) bekezdése szerint:

> *„[b]ármely természetes vagy jogi személy […] eljárást indíthat a neki címzett vagy az őt közvetlenül és személyében érintő jogi aktusok ellen, továbbá az őt közvetlenül érintő olyan rendeleti jellegű jogi aktusok ellen, amelyek nem vonnak maguk után végrehajtási intézkedéseket".*

Az uniós szerv által elkövetett jogellenes adatfeldolgozás sértettjei tehát közvetlenül az EUB Törvényszékéhez fellebbezhetnek, amely az EUB-nak az uniós intézmények adatvédelmi rendeletében szabályozott kérdésekben ítélethozatalra illetékes

211 EU (2007): Az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról szóló, Lisszabonban aláírt Lisszaboni Szerződés, 2007. december 13., HL C 306. Lásd még az Európai Unióról szóló szerződés (2012, HL C 326) és az EUMSZ egységes szerkezetbe foglalt változatát (2012, HL C 326.).

testülete. A közvetlenül az EUB-hoz fordulás lehetősége akkor is adott, ha egy uniós jogi rendelkezés közvetlenül érinti valakinek a jogi helyzetét.

A második forgatókönyv az EUB (a Bíróság) azon hatáskörével kapcsolatos, miszerint az EUB az EUMSZ 267. cikke szerint előzetes döntéseket hozhat.

Az érintettek a belföldi eljárások során kérhetik a nemzeti bíróságot, hogy forduljon a Bírósághoz pontosításért az uniós Szerződések értelmezésével, valamint az uniós intézmények, szervek, hivatalok vagy ügynökségek aktusainak értelmezésével és érvényességével kapcsolatban. Az ilyen pontosítások előzetes döntéshozatali eljárás néven ismertek. Az előzetes döntés nem nyújt közvetlen jogorvoslatot a panaszosnak, lehetővé teszi viszont a nemzeti bíróságok számára, hogy az unós jog helyes értelmezését alkalmazzák.

Ha a nemzeti bíróság előtt folyó eljárásban részt vevő egyik fél a kérdés EUB elé vitelét kéri, csak a végső fokon eljáró nemzeti bíróságok – azaz amelyek határozata ellen jogorvoslatnak helye nincs – kötelesek eleget tenni a fél kérésének.

Példa: A *Kärntner Landesregierung és mások* ügyben[212] az osztrák Alkotmánybíróság kérdéseket intézett az EUB-hoz – a Charta 7., 9. és 11. cikkének figyelembevételével – a 2006/24/EK irányelv (adatmegőrzési irányelv) 3–9. cikke érvényességével kapcsolatban, valamint arra vonatkozóan, hogy az adatmegőrzési irányelvet átültető osztrák távközlési szövetségi törvény bizonyos rendelkezései nem összeegyeztethetetlenek-e az adatvédelmi irányelv és az uniós intézmények adatvédelmi rendelete egyes vonatkozásaival.

Seitlinger úr, az alkotmánybírósági eljárás egyik felperese elmondta, hogy ő munkavégzési célból és a magánélete során egyaránt használja a telefont, az internetet és az emailt. Következésképpen az általa küldött és kapott információk a távközlési közszolgáltatási hálózatokon keresztül áramlanak. A 2003. évi osztrák távközlési törvény értelmében a távközlési szolgáltatót jogszabály kötelezi arra, hogy a hálózat Seitlinger úr általi használatáról adatokat gyűjtsön és tároljon. Seitlinger úr úgy értékelte, hogy személyes adatainak szóban forgó gyűjtése és tárolása semmiképpen sem volt szükséges azon technikai célok érdekében, hogy az információk a hálózaton A-ból B-be eljussanak, ezen adatok számlázási célokra való gyűjtésére és tartós tárolására sem volt szükség és

212 EUB, C-293/12. és C-594/12. sz., *Digital Rights Írország és Seitling és társai* egyesített ügyek, 2014. április 8.

nyilvánvalóan nem járult hozzá személyes adatainak ilyen felhasználásához. Mindezen kiegészítő adatok gyűjtésének és tárolásának egyetlen oka a 2003-as osztrák távközlési törvény.

Seitlinger úr ezért keresetet indított az osztrák Alkotmánybíróságon, amelyben azt állította, hogy a távközlési szolgáltatójával szemben előírt törvényi kötelezettségek sértik az EU Charta 8. cikke szerinti alapvető jogait.

Az EUB csupán az előzetes döntésre elé terjesztett kérelem alapelemeire vonatkozóan hoz határozatot. Az eredeti ügyben továbbra is a nemzeti bíróság illetékes.

Főszabály szerint a Bíróságnak meg kell válaszolnia az elé vitt kérdéseket. Azon az alapon nem tagadhatja meg az előzetes döntés meghozatalát, hogy válasza az eredeti ügy szempontjából nem releváns és nem is a kellő időben születik. Akkor azonban megtagadhatja, ha a kérdés nem tartozik a hatáskörébe.

Végül, ha az EUMSZ 16. cikkében garantált adatvédelmi jogokat uniós intézmény vagy szerv személyesadat-kezelés során feltételezhetően megsérti, az érintett az EUB Törvényszéke elé viheti az ügyet (az uniós intézmények adatvédelmi rendelete 32. cikkének (1) és (4) bekezdése). Ugyanez vonatkozik az európai adatvédelmi biztos ilyen jogsértésekkel kapcsolatos döntéseire is (az uniós intézmények adatvédelmi rendelete 32. cikkének (3) bekezdése).

Bár az EUB Törvényszéke illetékes az uniós intézmények adatvédelmi rendelete kérdéseiben történő ítélethozatalra, ha azonban egy személy mint uniós intézmény vagy szerv alkalmazottja jogorvoslatért folyamodik, az EU Közszolgálati Törvényszékéhez kell fellebbeznie.

Példa: Az *Európai Bizottság kontra The Bavarian Lager Co. Ltd* ügy[213] jól szemlélteti az adatvédelemmel foglalkozó uniós intézmények és szervek tevékenységével vagy döntéseivel szemben rendelkezésre álló jogorvoslati lehetőségeket.

A Bavarian Lager hozzáférést kért az Európai Bizottságtól egy, a Bizottság által tartott találkozó teljes jegyzőkönyvéhez, amely találkozó állítólag a társaság számára fontos jogi kérdéseket is érintett. A Bizottság magasabb rendű

213 EUB, C-28/08 P. sz. *Európai Bizottság kontra The Bavarian Lager Co. Ltd ügy*, 2010. június 29.

adatvédelmi érdekek címén elutasította a társaság hozzáférés iránti kérelmét.[214] A Bavarian Lager – az uniós intézmények adatvédelmi rendeletének 32. cikkét alkalmazva – panaszt nyújtott be e határozat ellen az EUB-hoz; pontosabban az Elsőfokú Bírósághoz (a Törvényszék elődjéhez). Az Elsőfokú Bíróság a T-194/04. sz. *Bavarian Lager kontra Bizottság* ügyben hozott határozatával megsemmisítette a Bizottságnak a hozzáférési kérelmet elutasító határozatát. Az Európai Bizottság fellebbezést nyújtott be a Bírósághoz e határozat ellen. A Bíróság (nagytanácsa) ítéletében hatályon kívül helyezte az Elsőfokú Bíróság ítéletét, és megerősítette az Európai Bíróság hozzáférés iránti kérelmet elutasító határozatát.

5.3.4. Szankciók

Az **Európa Tanács jogában** a 108. egyezmény 10. cikke szerint mindegyik Fél vállalja, hogy megfelelő szankciókat és jogorvoslatokat állapít meg a 108. egyezményben foglalt adatvédelmi alapelveket érvényesítő hazai jog rendelkezéseinek megsértése esetén.[215] Az **uniós jogban** az adatvédelmi irányelv 24. cikke előírja, hogy a tagállamok „elfogadják a megfelelő intézkedéseket ezen irányelv rendelkezéseinek maradéktalan végrehajtása érdekében és különösen megállapítják az [...] elfogadott rendelkezések megsértése esetén kiszabható szankciókat".

Mindkét jogi aktus széles körű mérlegelési jogkört biztosít a tagállamoknak a megfelelő szankciók és jogorvoslatok kiválasztása terén. Egyik jogi aktus sem ad konkrét iránymutatást a megfelelő szankciók jellegére vagy típusára vonatkozóan, és nem is közöl példákat e szankciókra.

Azonban:

> *„bár az uniós tagállamok mérlegelési mozgástérrel rendelkeznek abban a tekintetben, hogy meghatározzák, mely intézkedések a legmegfelelőbbek az uniós jog által az egyéneknek biztosított jogok oltalmazására, a hatékonyság, egyenértékűség, arányosság és a visszatartó erő*

214 Az érvelés elemzéséhez lásd: Európai adatvédelmi biztos: *A személyes adatokat tartalmazó dokumentumokhoz való nyilvános hozzáférés a Bavarian Lager ügyben hozott ítélet után* (2011), Brüsszel, európai adatvédelmi biztos**,** elérhető a következő címen: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

215 EJEB, 20511/03. sz. *I. kontra Finnország* ügy, 2008. július 17.; EJEB, 2872/02. sz. *K.U. kontra Finnország* ügy, 2008. december 2.

minimumkövetelményét – az EUSZ 4. cikkének (3) bekezdésében szereplő lojális együttműködés elvével összhangban – tiszteletben kell tartani."[216]

Az EUB megismételte, hogy a nemzeti jog nem teljesen szabadon határozhatja meg a szankciókat.

Példa: A *Von Colson és Kamann kontra Land Nordrhein-Westfalen* ügyben[217] az EUB rámutatott, hogy minden tagállam, amely egy irányelv címzettje, köteles az adott irányelv teljes körű érvényesítéséhez szükséges intézkedéseket – az irányelv által előmozdítani kívánt célnak megfelelően – a saját nemzeti jogrendszerében elfogadni. A Bíróság megállapította, hogy bár a tagállamok az irányelv végrehajtása biztosításának módját és eszközeit maguk választhatják meg, ez a szabadság a rájuk vonatkozó kötelezettséget nem érinti. A hatékony jogorvoslatnak elsősorban lehetővé kell tennie, hogy az egyén a szóban forgó jog minden lényeges elemét gyakorolhassa és érvényesíthesse. Az említett valódi és hatékony védelem megvalósítása érdekében a jogorvoslatoknak büntető- és/vagy kártérítési eljárást is maguk után kell vonniuk, amely visszatartó erejű szankciókhoz vezet.

Ami az uniós jog uniós intézmények vagy szervek általi megsértésének szankcióit illeti, szankciókat – az uniós intézmények adatvédelmi rendeletének speciális feladata miatt – kizárólag fegyelmi intézkedés formájában irányoznak elő. A rendelet 49. cikke szerint „ha az Európai Közösségek tisztviselője vagy más alkalmazottja az e rendeletben foglalt kötelezettségeit szándékosan vagy gondatlanságból megszegi, ellene [...] fegyelmi eljárás indul".

216 FRA (2012): *Az Európai Unió Alapjogi Ügynökségének 2/2012. sz. véleménye a javasolt adatvédelmi reformcsomagról*, Bécs, 2012. október 1., 27. o.

217 EUB, C-14/83. sz. *Sabine von Kolson és Elisabeth Kamman kontra Land Nordrhein-Westfalen* ügy, 1984. április 10.

6

Országhatárokat átlépő adatáramlás

EU	Tárgyalt kérdések	Európa Tanács
Országhatárokat átlépő adatáramlás		
Adatvédelmi irányelv, 25. cikk (1) bekezdés EUB, C-101/01. sz. *Bodil Lindqvist ügy*, 2003. november 6.	Meghatározás	108. egyezmény, Kiegészítő jegyzőkönyv, 2. cikk, (1) bekezdés
Szabad adatáramlás		
Adatvédelmi irányelv, 1. cikk, (2) bekezdés	Az uniós tagállamok között	
	A 108. egyezmény részes felei között	108. egyezmény, 12. cikk, (2) bekezdés
Adatvédelmi irányelv, 25. cikk	Megfelelő adatvédelmi szinttel rendelkező harmadik országokba	108. egyezmény, Kiegészítő jegyzőkönyv, 2. cikk, (1) bekezdés
Adatvédelmi irányelv, 26. cikk, (1) bekezdés	Harmadik országokba egyedi esetekben	108. egyezmény, Kiegészítő jegyzőkönyv, 2. cikk, (2) bekezdés, a) pont
Korlátozott adatáramlás harmadik országokba		
Adatvédelmi irányelv, 26. cikk, (2) bekezdés Adatvédelmi irányelv, 26. cikk, (4) bekezdés	Szerződéses záradékok	108. egyezmény, Kiegészítő jegyzőkönyv, 2. cikk, (2) bekezdés, b) pont Iránymutatás szerződéses záradékok kidolgozásához
Adatvédelmi irányelv, 26. cikk, (2) bekezdés	Kötelező erejű vállalati szabályok	

EU	Tárgyalt kérdések	Európa Tanács
Példák: EU-USA megállapodás az utas-nyilvántartási adatállományról (PNR) EU-USA SWIFT-megállapodás	Speciális nemzetközi megállapodások	

Az adatvédelmi irányelv nemcsak a tagállamok közötti szabad adatáramlásról rendelkezik, hanem a személyes adatok Unión kívüli harmadik országokba történő továbbítására vonatkozó követelményekkel kapcsolatos rendelkezéseket is tartalmaz. Az Európa Tanács az országhatárokat átlépő adatáramlásra vonatkozó végrehajtási szabályok fontosságát is felismerte, és 2001-ben elfogadta a 108. egyezményhez fűzött kiegészítő jegyzőkönyvet. Ez a jegyzőkönyv az országhatárokat átlépő adatáramlásra vonatkozó főbb szabályozási elemeket átvette az egyezmény részes feleitől és az uniós tagállamoktól.

6.1. Az országhatárokat átlépő adatáramlás jellege

Fő pont

- Az országhatárokat átlépő adatáramlás személyes adatok olyan címzettnek történő továbbítása, aki vagy amely külföldi joghatóság alá tartozik.

A 108. egyezményhez fűzött kiegészítő jegyzőkönyv 2. cikkének (1) bekezdése úgy írja le az országhatárokat átlépő adatáramlást, mint személyes adatok olyan címzettnek történő továbbítása, aki vagy amely külföldi joghatóság alá tartozik. Az adatvédelmi irányelv 25. cikkének (1) bekezdése „a feldolgozásra kerülő vagy továbbítás után feldolgozásra szánt személyes adatok" harmadik országba való továbbítását szabályozza. Az ilyen adattovábbítás csak a 108. egyezményhez fűzött kiegészítő jegyzőkönyv 2. cikkében, továbbá – az uniós tagállamok tekintetében – az adatvédelmi irányelv 25. és 26. cikkében meghatározott szabályok szerint engedélyezett.

Példa: A *Bodil Lindqvist* ügyben[218] az EUB megállapította, hogy „internetes oldalon több személyre történő hivatkozás, és azoknak akár nevükkel, akár más módon – például telefonszámukkal vagy munkakörülményeikre és időtöltésükre vonatkozó információkkal – történő azonosítása a 95/46 irányelv 3. cikkének (1) bekezdése értelmében „személyes adatok részben vagy egészben automatizált módon való feldolgozásá[nak]" minősül".

A Bíróság arra is rámutatott, hogy az irányelv sajátos szabályokat is meghatároz, amelyek célja, hogy a személyes adatok harmadik országokba irányuló továbbítását a tagállamok ellenőrizhessék.

Tekintettel azonban egyrészt az internetnek az irányelv kidolgozásakor elért fejlettségére, másrészt pedig arra, hogy az irányelv nem tartalmaz internethasználatra alkalmazandó szempontokat, „nem vélelmezhető, hogy a közösségi jogalkotó a jövőre vonatkozóan az „adatok harmadik országba irányuló továbbítása" fogalomba bele szándékozott foglalni az adatoknak valamely internetes oldalra [...]" való „feltöltését, még akkor sem, ha ezen adatok így hozzáférhetővé váltak a hozzáférésükhöz technikai eszközökkel rendelkező harmadik országbeli személyek részére".

Ellenkező esetben, ha az irányelvet „úgy lehetne értelmezni, hogy minden alkalommal fennáll az „adatok harmadik országba irányuló továbbítása", akkor ha internetes oldalra töltenek fel személyes adatokat, e továbbítás szükségszerűen minden olyan harmadik országba irányuló továbbítást jelentene, ahol rendelkezésre állnak az internethez való csatlakozáshoz szükséges technikai eszközök. Az [irányelvben] előírt különleges szabályozás így szükségszerűen – az interneten végrehajtott műveleteket illetően – az általánosan alkalmazandó szabályozássá válna. Amennyiben ugyanis a Bizottság [...] megállapítaná, hogy egyetlen harmadik ország sem biztosít megfelelő szintű védelmet, a tagállamok kötelesek lennének megakadályozni a személyes adatok internetre való bármilyen feltöltését."

Az elv, miszerint „személyes" adatok puszta közzététele nem tekinthető országhatárokat átlépő adatáramlásnak, online nyilvántartásokra és a tömegmédiumokra, köztük az (elektronikus) újságokra és a televízióra is vonatkozik. Csak a konkrét címzettekhez intézett kommunikáció tartozhat az „országhatárokat átlépő adatáramlás" fogalmába.

218 EUB, C-101/01. sz. *Bodil Lindqvist ügy*, 2003. November 6., 27., 68. és 69. pont.

6.2. Tagállamok vagy részes felek közötti szabad adatáramlás

Főbb pontok

- Személyes adatoknak az Európai Gazdasági Térség más tagállamába vagy a 108. egyezmény más részes fele részére történő továbbításának korlátozásoktól mentesnek kell lennie.

A 108. egyezmény 12. cikkének (2) bekezdése szerint **az Európa Tanács joga értelmében** a személyesadat-áramlásnak szabadon kell történnie az egyezmény részes felei között. A belföldi jog nem korlátozhatja személyes adatoknak az egyik részes fél részére történő kivitelét, kivéve ha:

- az adatok jellege úgy kívánja;[219] vagy
- a korlátozás annak érdekében szükséges, hogy megakadályozza, hogy az országhatárokat átlépő, harmadik felek részére történő adatáramlásra vonatkozó belföldi jogszabályokat kijátsszák.[220]

Az **uniós jogban** az adatvédelmi irányelv 1. cikkének (2) bekezdése értelmében a személyes adatok tagállamok közötti szabad áramlása nem korlátozható és nem tiltható. Az Európai Gazdasági Térségről (EGT) szóló megállapodás,[221] amely Izlandot, Liechtensteint és Norvégiát is a belső piachoz csatolta, kibővítette a szabad adatáramlás területét.

Példa: Ha egy több uniós tagállamban, köztük Szlovéniában és Franciaországban is letelepedett nemzetközi vállalatcsoport egyik leányvállalata Szlovéniából Franciaországba továbbít személyes adatokat, az ilyen adatáramlást szlovén nemzeti jogszabály nem korlátozhatja és nem tilthatja.

219 108. egyezmény, 12. cikk, (3) bekezdés, a) pont.

220 Uo., 12. cikk, (3) bekezdés, b) pont.

221 A Tanács és a Bizottság 1993. december 13i határozata az Európai Közösségek, azok tagállamai, valamint az Osztrák Köztársaság, a Finn Köztársaság, az Izlandi Köztársaság, a Liechtensteini Hercegség, a Norvég Királyság, a Svéd Királyság és a Svájci Államszövetség között az Európai Gazdasági Térségről létrejött megállapodás megkötéséről, HL 1994. L 1.

Ha azonban ugyanez a szlovén leányvállalat ugyanezeket a személyes adatokat az egyesült államokbeli anyavállalatának kívánja továbbítani, a szlovén adatátadónak át kell esnie a megfelelő adatvédelemmel nem rendelkező harmadik országokba történő, határokon átnyúló adatáramlásra vonatkozó, a szlovén jogban előírt eljáráson, kivéve, ha az anyavállalat csatlakozott a védett adatkikötőre (Safe Harbour) vonatkozó alapelvekhez, amely a megfelelő adatvédelmi szint biztosítására vonatkozó önkéntes magatartási kódex (lásd a 6.3.1 szakaszt).

Az EGT-tagállamokba irányuló, a belső piaci feladatokon kívüli célokat – például bűncselekmények nyomozását – szolgáló, országhatárokat átlépő adatáramlás azonban nem tartozik az adatvédelmi irányelv rendelkezéseinek hatálya alá, ezért a szabad adatáramlás elve sem vonatkozik rá. Ami az Európa Tanács jogát illeti, mindezen területek a 108. egyezmény és a 108. egyezményhez fűzött kiegészítő jegyzőkönyvben is megtalálhatók, bár a részes felek kivételeket is megállapíthatnak ezek alól. Az EGT valamennyi tagja egyben a 108. egyezményben is részes fél.

6.3. Harmadik országba irányuló szabad adatáramlás

Főbb pontok

- A harmadik országba irányuló személyesadat-továbbítást a nemzeti adatvédelmi jogszabályok nem korlátozzák, ha:
  - megállapítást nyert, hogy a címzett megfelelő adatvédelemmel rendelkezik; vagy
  - az érintett egyedi érdekei vagy mások jogos érdekei – különösen fontos közérdekek – miatt a továbbításra szükség van.
- A harmadik országban fennálló adatvédelem megfelelősége azt jelenti, hogy a fő adatvédelmi elveket ténylegesen átültették ezen ország nemzeti jogába.
- Az uniós jog szerint a harmadik országban fennálló adatvédelem megfelelőségét az Európai Bizottság értékeli. Az Európa Tanács joga szerint a megfelelőség értékelésének módját a belföldi jognak kell szabályoznia.

6.3.1. Szabad adatáramlás megfelelő védelem esetén

Az **Európa Tanács joga** lehetővé teszi, hogy a nemzeti jog az egyezményhez nem csatlakozott államokba is engedélyezze a szabad adatáramlást, ha a címzett állam vagy szervezet a tervezett adattovábbítás tekintetében megfelelő szintű védelmet biztosít.[222] A külföldi országban fennálló adatvédelmi szint értékelésének módját és azt, hogy az értékelést ki végezze el, a hazai jog határozza meg.

Az **uniós jogban** a megfelelő szintű védelmet biztosító harmadik országokba irányuló szabad adatáramlásról az adatvédelmi irányelv 25. cikkének (1) bekezdése rendelkezik. Az, hogy egyenértékűség helyett a megfelelőség a követelmény, lehetővé teszi, hogy az adatvédelem különböző módon történő megvalósítási formáit egyaránt tiszteletben tartsák. Az irányelv 25. cikkének (6) bekezdése szerint az Európai Bizottság illetékes a külföldi országokban fennálló adatvédelmi szint – a megfelelőségre vonatkozó megállapításokkal történő – értékelésére, és az értékelésről konzultál a 29. cikk szerinti munkacsoporttal, amely jelentősen hozzájárult a 25. és 26. cikk értelmezéséhez.[223]

Az Európai Bizottság megfelelőségre vonatkozó megállapítása kötelező erejű. Ha az Európai Bizottság egy adott ország tekintetében megfelelőségre vonatkozó megállapítást tesz közzé az *Európai Unió Hivatalos Lapjában,* valamennyi EGT-tagország és szerveik kötelesek követni a határozatot, ami azt jelenti, hogy a szóban forgó országba az adatáramlás ellenőrzés, illetve a nemzeti hatóságok előtt lefolytatott engedélyezési eljárás nélkül történhet.[224]

Az Európai Bizottság egy ország jogrendszerének egyes részeit is értékelni tudja, illetve értékelését egy-egy témakörre is korlátozhatja. A Bizottság megfelelőségre vonatkozó megállapítást tett például Kanada magánkereskedelmi jogszabályaira

222 108. egyezmény, Kiegészítő jegyzőkönyv, 2. cikk, (1) bekezdés.

223 Lásd például a 29. cikk szerinti munkacsoport *„Munkadokumentum személyes adatok harmadik országokba való továbbításáról: az uniós adatvédelmi irányelv 26. cikke (2) bekezdésének alkalmazása a nemzetközi adattovábbításokra vonatkozó kötelező erejű vállalati szabályokra" című dokumentumát* (2003), WP 74, Brüsszel, 2003. június 3.; és a 29. cikk szerinti munkacsoport *„Munkadokumentum a 95/46/EK irányelv 26. cikke (1) bekezdésének egységes értelmezéséről"*, 1995. Október 24., WP 114, Brüsszel, 2005. November 25.

224 A megfelelőségre vonatkozó megállapítást elnyert országok folyamatosan frissülő listáját lásd az Európai Bizottság honlapján a Jogérvényesülési Főigazgatóságnál a következő címen: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

vonatkozóan.[225] Az EU és külföldi államok közötti megállapodásokon alapuló továbbítások tekintetében is számos megfelelőségre vonatkozó megállapítás létezik. Ezek a határozatok egyetlen adattípus továbbítására vonatkoznak, például az utas-nyilvántartási adatok légitársaságok által a külföldi határellenőrző hatóságok részére történő továbbítására, amikor a légitársaság az EU-ból bizonyos tengerentúli célállomásokra repül (lásd a 6.4.3 szakaszt). Az EU és harmadik országok közötti külön megállapodásokon alapuló adattovábbítás újabban megvalósuló gyakorlata nyomán általában nincs már szükség megfelelőségre vonatkozó megállapításokra – feltéve, hogy maga a megállapodás megfelelő adatvédelmi szintet biztosít.[226]

Az egyik legfontosabb megfelelőségi határozat nem is hivatkozik jogszabályi rendelkezésekre.[227] Inkább szabályokra, köztük olyan magatartási kódexekre, mint például a védett adatkikötőre (Safe Harbour) vonatkozó alapelvek. Ezeket az alapelveket az EU és az Amerikai Egyesült Államok amerikai üzleti vállalkozásokra vonatkozóan dolgozták ki. A védett adatkikötőbe az USA Kereskedelmi Minisztériumában tett önkéntes kötelezettségvállalással lehet belépni, mely kötelezettségvállalást a minisztérium által közzétett jegyzékben dokumentálják. Mivel a megfelelőség egyik fontos eleme az adatvédelem megvalósításának hatékonysága, a védett adatkikötőre vonatkozó szabályozás is előír bizonyos állami felügyeletet: csak azok a vállalatok csatlakozhatnak a védett adatkikötőhöz, amelyek az USA Szövetségi Kereskedelmi Bizottságának felügyelete alá tartoznak.

6.3.2. Szabad adatáramlás egyedi esetekben

Az **Európa Tanács joga** szerint a 108. egyezményhez fűzött kiegészítő jegyzőkönyv 2. cikkének (2) bekezdése személyes adatok olyan országokba történő továbbítását

225 Európai Bizottság (2002), 2002/2/EK határozat (2001. december 20.) a 95/46/EK európai parlamenti és tanácsi irányelv értelmében a személyes adatoknak a személyes információk védelméről és az elektronikus dokumentumokról szóló kanadai törvény által biztosított megfelelő védelméről, HL L 2., 2002.

226 Például az Amerikai Egyesült Államok és az Európai Unió közötti, az utas-nyilvántartási adatállomány (PNR) felhasználásáról és az Egyesült Államok Belbiztonsági Minisztériuma részére történő továbbításáról szóló megállapodás (2012, HL L 215., 5–14. o.) vagy az Európai Unió és az Amerikai Egyesült Államok között a pénzügyi üzenetadatoknak az Európai Unió általi feldolgozásáról és az Egyesült Államok részére a „terrorizmus finanszírozásának felderítését célzó program" céljára történő továbbításáról szóló megállapodás (2010, HL L 8., 11–16. o.).

227 Európai Bizottság (2000), 2000/520/EK határozat (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott biztonságos kikötő adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről, HL L 215., 2000.

is lehetővé teszi, ahol az adatvédelem nem megfelelő, ha az adattovábbítást belföldi jogszabály rendeli el a következők érdekében:

- az érintett egyéni érdekei; vagy
- mások jogos, magasabb érdekei, különösen fontos közérdek.

Az **uniós jogban** az adatvédelmi irányelv 26. cikkének (1) bekezdése a 108. egyezményhez fűzött kiegészítő jegyzőkönyvben foglaltakhoz hasonló rendelkezéseket tartalmaz.

Az irányelv értelmében az érintett érdekei indokolhatják a harmadik országba irányuló szabad adatáramlást, ha:

- az érintett egyértelműen hozzájárult az adatkivitelhez; vagy
- az érintett olyan szerződéses jogviszonyra lép vagy készül lépni, amelyhez egyértelműen szükséges az adatok külföldi címzettnek történő továbbítása; vagy
- az adatkezelő és egy harmadik fél közötti szerződés az érintett érdekében lezárásra került; vagy
- a továbbítás az érintett létfontosságú érdekének védelme miatt szükséges.
- arra adatok nyilvántartásokból való továbbításához van szükség; ez jó példa a nyilvánosság ahhoz fűződő magasabb érdekére, hogy hozzáférhessen a nyilvántartásokban tárolt információkhoz.

Mások jogos érdekei indokolhatják az országhatárokat átlépő adatáramlást:[228]

- fontos közérdekből – a nemzet- vagy közbiztonság kérdéseinek kivételével, amelyekre az adatvédelmi irányelv nem vonatkozik; vagy
- jogi követelések létrejötte, érvényesítése vagy védelme miatt.

A fent említett esetek kivételként értendők azon szabály alól, hogy a más országba irányuló, minden kötöttségtől mentes adattovábbításhoz szükséges, hogy a fogadó ország megfelelő adatvédelmi szinttel rendelkezzen. A kivételeket minden esetben

228 Adatvédelmi irányelv, 26. cikk, (1) bekezdés, d) pont.

szűken kell értelmezni. Ezt az adatvédelmi irányelv 26. cikkének (1) bekezdése kapcsán a 29. cikk szerinti munkacsoport többször is hangsúlyozta, különösen ha az adattovábbítás alapját a hozzájárulás alkotja.[229] A 29. cikk szerinti munkacsoport arra a következtetésre jutott, hogy a hozzájárulás jogi jelentőségére vonatkozó általános szabályok az irányelv 26. cikkének (1) bekezdésére is vonatkoznak. Ha például a munkaügyi kapcsolatok terén nem egyértelmű, hogy a munkavállalók hozzájárulása valóban szabad hozzájárulás volt-e, az irányelv 26. cikke (1) bekezdésének a) pontja nem képezheti az adattovábbítás jogalapját. Ilyen esetben a 26. cikk (2) bekezdése alkalmazandó, amely szerint a nemzeti adatvédelmi hatóságoknak kell engedélyezniük az adattovábbítást.

6.4. Harmadik országokba irányuló korlátozott adatáramlás

Főbb pontok

- Mielőtt olyan harmadik országba történő adatkivitelre kerül sor, amely ország nem biztosít megfelelő szintű adatvédelmet, az adatkezelő kötelezhető arra, hogy a tervezett adatáramlást a felügyelő hatósággal megvizsgáltassa.
- A vizsgálat során az adatkivitelt tervező adatkezelőnek két kérdést kell bizonyítania:
  - a címzettnek történő adattovábbításnak van jogalapja; és
  - a címzettnél intézkedéseket vezettek be az adatok megfelelő védelmének biztosítására.
- A címzettnél a megfelelő adatvédelem létrehozására irányuló intézkedések közé tartoznak a következők:
  - szerződéses kikötések az adatokat exportáló adatkezelő és az adatok külföldi címzettje között; vagy
  - kötelező erejű vállalati szabályok, amelyek általában egy multinacionális vállalatcsoporton belüli adattovábbításokra alkalmazandók.
- A külföldi hatóságoknak történő adattovábbításokat szintén szabályozhatja nemzetközi különmegállapodás.

229 Lásd különösen a 29. cikk szerinti munkacsoport *munkadokumentumát az 1995. Október 24-i 95/46/EK irányelv 26. cikke (1) bekezdésének egységes értelmezéséről*, 2005, WP 114, Brüsszel, 2005. November 25.

Az adatvédelmi irányelv és a 108. egyezményhez fűzött kiegészítő jegyzőkönyv engedélyezi, hogy a hazai jog adattovábbítási rendszereket hozzon létre olyan harmadik országokba, amelyek nem biztosítanak megfelelő adatvédelmet, amennyiben az adatkezelő speciális szabályokkal biztosítja a címzettnél a megfelelő adatvédelmet, és amennyiben az adatkezelő az illetékes hatóságnak ezt bizonyítani tudja. Ezt a követelményt csak a 108. egyezményhez fűzött kiegészítő jegyzőkönyv említi kifejezetten; mindez azonban az adatvédelmi irányelv alapján is általános eljárásnak tekinthető.

6.4.1. Szerződési feltételek

Az **Európa Tanács joga** és az **uniós jog** egyaránt említi az adatokat exportáló adatkezelő és a harmadik országban lévő címzett közötti szerződési feltételeket mint a címzettnél a megfelelő adatvédelmi szint biztosításának egyik lehetséges eszközét.

Uniós szinten az Európai Bizottság a 29. cikk szerinti munkacsoport segítségével általános szerződési feltételeket dolgozott ki, amelyeket egy bizottsági határozat hivatalosan is a megfelelő adatvédelem bizonyítékának minősített.[230] Mivel a Bizottság határozatai teljes egészében kötelező erejűek a tagállamokban, az országhatárokat átlépő adatáramlás felügyeletével megbízott nemzeti hatóságoknak eljárásaik során el kell ismerniük ezen általános szerződési feltételeket.[231] Ha tehát az adatokat exportáló adatkezelő és a harmadik országbeli címzett megállapodnak és aláírják a szóban forgó feltételeket, ennek elegendő bizonyítékul kell szolgálnia a felügyelő hatóság felé a megfelelő biztosítékok meglétére.

Az uniós jogi keretben az általános szerződési feltételek létezése nem tiltja, hogy az adatkezelők más eseti szerződéses kikötéseket megfogalmazzanak. Ezeknek azonban ugyanolyan szintű adatvédelmet kell eredményezniük, mint amit az általános szerződési feltételek biztosítanak. Az általános szerződési feltételek legfontosabb elemei a következők:

- egy harmadik fél kedvezményezettre vonatkozó feltétel, amely lehetővé teszi, hogy az érintettek akkor is gyakorolhassák a szerződéses jogokat, ha maguk nem felek a szerződésben;

230 Adatvédelmi irányelv, 26. cikk (4) bekezdés.

231 EUMSZ, 288. cikk.

- az adatok címzettje vagy az adatátvevő jogvita esetén aláveti magát az adatokat exportáló adatkezelő nemzeti felügyelő hatósága és/vagy nemzeti bíróságai eljárásának.

Jelenleg az adatkezelőtől adatkezelőig terjedő adattovábbításokra vonatkozó általános feltételeknek két csomagja létezik, ezek közül választhat az adatokat exportáló adatkezelő.[232] Az adatkezelőtől adatfeldolgozóig terjedő adattovábbításokra vonatkozóan csak egyetlen, az általános szerződési feltételeket tartalmazó csomag létezik.[233]

Az **Európa Tanács jogában** a 108. egyezmény konzultatív bizottsága iránymutatást készített a szerződési feltételek kidolgozására vonatkozóan.[234]

6.4.2. Kötelező erejű vállalati szabályok

A többoldalú kötelező erejű vállalati szabályok igen gyakran egyidejűleg több európai adatvédelmi hatóságot is érintenek.[235] A kötelező erejű vállalati szabályok jóváhagyásához e szabályok tervezetét a kérelem beadására szolgáló formanyomtatvánnyal együtt el kell küldeni a vezető hatósághoz.[236] A vezető hatóság a kérelem beadására szolgáló formanyomtatványról azonosítható. Ezután a szóban forgó hatóság tájékoztatja mindazon EGT-tagországokban működő felügyelő hatóságokat, ahol a vállalatcsoportnak letelepedett leányvállalata működik, de e hatóságoknak

232 Az I. csomag a 95/46/EK irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről szóló, 2001. Június 15-i 2001/497/EK európai bizottsági határozat (2001, HL L 181.) mellékletében található; a II. csomag a 2001/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről szóló, 2004. December 27-i 2004/915/EK bizottsági határozat (2004, HL L 385.) mellékletében található.

233 A 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2010. Február 5-i 2010/87/EK európai bizottsági határozat, 2010, HL L 39.

234 Európa Tanács, a 108. egyezmény konzultatív bizottságának *„Iránymutatás az adatvédelemre vonatkozó szerződési feltételek előkészítéséről személyes adatoknak olyan harmadik országokba való továbbítása során, amelyekre nem vonatkozik a megfelelő adatvédelmi szint biztosítása”* c. dokumentuma, 2002.

235 A megfelelő kötelező erejű vállalati szabályok magyarázatát a 29. cikk szerinti munkacsoport 2008-as, *„Munkadokumentum a kötelező erejű vállalati szabályok keretének létrehozásáról”* c. dokumentuma (WP 154, Brüsszel, 2008. Június 24.), valamint a 29. cikk szerinti munkacsoport 2008-as, *„Munkadokumentum a kötelező erejű vállalati szabályokban szerepeltetendő elemeket és elveket tartalmazó táblázat létrehozásáról”* c. dokumentum tartalmazza (WP 153, Brüsszel, 2008. Június 24.).

236 A 29. cikk szerinti munkacsoport *1/2007. sz. ajánlása a személyes adatok továbbítására vonatkozó kötelező erejű vállalati szabályok jóváhagyása iránti kérelem beadására szolgáló formanyomtatványról*, WP 133, Brüsszel, 2007. Január 10.

a kötelező erejű vállalati szabályok értékelésében való részvétele önkéntes. Bár az értékelés eredménye nem kötelező erejű, minden érintett adatvédelmi hatóságnak be kell azt építenie a hivatalos engedélyezési eljárásába.

6.4.3. Nemzetközi külön megállapodások

Az EU két adattovábbítás-típusra vonatkozóan kötött külön megállapodásokat:

Utas-nyilvántartási adatállományok

Utas-nyilvántartási (PNR) adatokat légitársaságok gyűjtenek a foglalási eljárás során; ezen adatok közé a légi utasok neve, címe, hitelkártya-adatai és ülésszáma tartozik. Az Amerikai Egyesült Államok joga szerint a légitársaságok kötelesek ezen adatokat az utas indulása előtt a Belbiztonsági Minisztérium részére továbbítani. Ez az Egyesült Államokból induló és oda érkező légi járatokra vonatkozik.

Hogy a PNR-adatok megfelelő védelmét biztosítsák a 95/46/EK irányelvvel összhangban, egy PNR-csomag[237] került elfogadásra 2004-ben. A csomag tartalmazta az USA Belbiztonsági Minisztériuma által kezelt adatkezelések megfelelőségét is.

A PNR-csomag EUB[238] általi érvénytelenítését követően az EU és az USA két különálló megállapodást írt alá kettős céllal; először is hogy jogalapot nyújtsanak a PNR-adatok külföldi hatóságok részére történő felfedéséhez; másodszor hogy megteremtsék a megfelelő adatvédelmet a fogadó országban.

Az első megállapodás az adatok megosztásának és kezelésének módjáról az uniós országok és az Amerikai Egyesült Államok között 2012-ben került aláírásra, amelynek számos hiányossága volt ezért a jogbiztonság érdekében egy új megállapodás

237 Az Európai Unió és az Egyesült Államok közötti, a PNR adatoknak a légi szállítók általi feldolgozásáról és az Egyesült Államok Belbiztonsági Minisztériuma Vámügyi és Határvédelmi Irodájának történő továbbításáról szóló megállapodás kötéséről szóló, 2004. Május 17-i 2004/496/EK tanácsi határozat, 2004, HL L 183., 83. o.; és az Egyesült Államok Vámügyi és Határvédelmi Irodája rendelkezésére bocsátott, a légiutasok utasnyilvántartási adatállományában tárolt személyes adatok megfelelő védelméről szóló, 2004. Május 14-i 2004/535/EK bizottsági határozat, 2004, HL L 235., 11. o.

238 EUB, C-317/04. és C-318/04. sz., *Európai Parlament kontra Európai Unió Tanácsa* egyesített ügyek, hozott 2006. Május 30., 57. pont, 58. pont és 59. pont., amelyben a Bíróság arról döntött, hogy mind a megfelelőségi döntés, mind az adatkezelésről szóló egyezmény ki van zárva az irányelv hatálya alól.

lépett helyébe még ugyanabban az évben.[239] Az új megállapodás jelentős pontosításokat tartalmaz. Korlátozza és pontosítja a célokat, amelyekre az információk felhasználhatók, ezek közé tartoznak például a súlyos nemzetközi bűncselekmények és a terrorizmus, és meghatározza azt az időkorlátot, amely ideig a személyes adatokat meg kell őrizni: 6 hónap után a személyes adatokat anonimizálni vagy maszkírozni kell. Amennyiben az egyének személyes adataival visszaélnek, a sértettek az amerikai jog szerint jogosultak közigazgatási vagy bírósági jogorvoslatra. Hozzáférhetnek továbbá a saját PNR-adataikhoz, és helyesbítést – akár törlést is – kérhetnek az USA Belbiztonsági Minisztériumától.

A megállapodás, amely 2012. július 1-jén lépett hatályba, hét évig, 2019-ig marad hatályban.

2011 decemberében az Európai Unió Tanácsa jóváhagyta az Európai Unió és Ausztrália közötti, az utas-nyilvántartási adatállomány feldolgozásáról és továbbításáról szóló megállapodás frissített változatának megkötését.[240] Az EU és Ausztrália közötti, a PNR-adatokról szóló megállapodás egy újabb lépés az EU ütemtervében, amelyben globális PNR-iránymutatások,[241] egy új uniós PNR-rendszer létrehozása,[242] valamint harmadik országokkal kötendő megállapodások tárgyalása is szerepel.[243]

239 Az Amerikai Egyesült Államok és az Európai Unió közötti, az utas-nyilvántartási adatállomány felhasználásáról és az Egyesült Államok Belbiztonsági Minisztériuma részére történő továbbításáról szóló megállapodás megkötéséről szóló, 2012. április 26-i 2012/472/EU tanácsi határozat, HL L 215/4. A megállapodás szövegét csatolták e határozathoz, 2012, HL L 215., 5–14. o.

240 Az Európai Unió és Ausztrália közötti, az utas-nyilvántartási adatállomány (PNR) adatainak feldolgozásáról és a légi fuvarozók által az Ausztrál Vámügyi és Határvédelmi Szolgálatnak való továbbításáról szóló megállapodás megkötéséről szóló, 2011. December 13-i 2012/381/EU tanácsi határozat, HL L 186/3. A megállapodás szövegét, amely a korábbi 2008.évi egyezményt váltotta fel, csatolták e határozathoz, 2012, HL L 186., 4-16. o.

241 Lásd különösen az utas-nyilvántartási adatállomány (PNR) adatainak harmadik országok részére történő továbbításával kapcsolatos általános megközelítésről szóló, 2010. szeptember 21-i bizottsági közleményt, COM(2010) 492, Brüsszel, 2010. Szeptember 21. Lásd a 29. cikk szerinti munkacsoport *7/2010. sz. véleményét az Európai Bizottság közleményéről a PNR-adatok harmadik országba való való továbbításának globális megközelítésével kapcsolatban*, WP 178, 2010. November 12.

242 Javaslat európai parlamenti és tanácsi irányelvre az utas-nyilvántartási adatállomány (PNR) felhasználásáról a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása érdekében, COM(2011) 32, Brüsszel, 2011. február 2. 2011. Április 2-án az Európai Parlament felkérte az FRA-t, hogy véleményezze a javaslatot és azt, hogy a javaslat megfelel-e az Európai Unió Alapjogi Chartájának. Lásd: az FRA *1/2011. sz. véleménye – Utas-nyilvántartási adatállomány,* Bécs, 2011. június 14.

243 Az EU jelenleg tárgyalásokat folytat Kanadával egy új PNR-megállapodásról, amely fel fogja váltani a jelenleg érvényben lévő 2006-os egyezményt.

Pénzügyi üzenetadatok

Az európai bankokból kiinduló legtöbb pénzátutalást a belga székhelyű Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) dolgozza fel, amely egy kisebb számítógépközponttal működik az Amerikai Egyesült Államokban; a SWIFT azzal a kéréssel szembesült, hogy terrorizmussal kapcsolatos nyomozás céljából közöljön adatokat az USA Pénzügyminisztériumával.[244]

Uniós szemszögből ezen alapvetően európai adatok közlésének nem volt kellő jogalapja, hiszen az adatok csak azért voltak hozzáférhetőek az Egyesült Államokban, mert a SWIFT egyik adatfeldolgozó központja ott található. Figyelemmel arra, hogy az USA Pénzügyminisztériuma általi hozzáférés az adatvédelmi irányelv 26. cikke szerint adattovábbításnak minősült, az e rendelkezésben foglalt követelményeknek meg kellene felelni.

„SWIFT megállapodás" néven 2010-ben külön megállapodás jött létre az EU és az Amerikai Egyesült Államok között, amelynek célja az volt, hogy megteremtse a szükséges jogalapot, és biztosítsa a megfelelő adatvédelmet.[245]

E megállapodás alapján – a terrorizmus vagy a terrorizmus finanszírozásának megakadályozása, kivizsgálása, felderítése, illetve büntetőeljárás alá vonása céljából – a SWIFT által tárolt pénzügyi adatok továbbra is átadásra kerülnek az USA Pénzügyminisztériumának. Az USA Pénzügyminisztériuma pénzügyi adatokat kérhet a SWIFT-től, amennyiben a kérés:

- a lehető legpontosabban megjelöli a pénzügyi adatokat;
- egyértelműen megindokolja az adat szükségességét;

244 Ezzel összefüggésben lásd a 29. cikk szerinti munkacsoport *14/2011. sz. véleményét a pénzmosás és a terrorizmusfinanszírozás megelőzése kapcsán felmerülő adatvédelmi kérdésekről*, WP 186, 2011. június 13.; a 29. cikk szerinti munkacsoport *10/2006. sz. véleményét a személyes adatok Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) általi feldolgozásáról*, WP 128, Brüsszel, 2006. november 22.; a belga adatvédelmi bizottság (Commission de la protection de la vie privée) 2008-as), „A SWIFT scrl vállalattal kapcsolatban indított ellenőrzési és ajánlási eljárás" c. határozatát, 2008. december 9.

245 Az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról szóló megállapodás megkötéséről szóló, 2010. július 13-i 2010/412/EU tanácsi határozat, HL L 195., 3. és 4. o. A megállapodás szövegét csatolták e határozathoz, 2010, HL L 195., 5–14. o.

- megfogalmazása a lehető legpontosabb annak érdekében, hogy a kért adatok mennyisége a lehető legkisebb legyen;

- nem az egységes eurofizetési térséget (SEPA) érintő adat megszerzésére irányul.

Az Europolnak az USA Pénzügyminisztériuma által benyújtott minden kérésből kapnia kell egy példányt, és ellenőriznie kell, hogy betartják-e a SWIFT-megállapodás elveit.[246] Ha megerősíti, hogy igen, a SWIFT-nek közvetlenül az USA Pénzügyminisztériuma részére kell átadnia a pénzügyi adatokat. A minisztériumnak a pénzügyi adatokat biztonságos fizikai környezetben kell tárolnia, ahol kizárólag a terrorizmust vagy annak finanszírozását vizsgáló elemzők férhetnek hozzájuk, és a pénzügyi adatok nem kapcsolhatók össze más adatbázisokkal. Általában a SWIFT-től kapott adatokat legkésőbb öt évvel a kézhezvételt követően törölni kell. A konkrét nyomozáshoz vagy büntetőeljáráshoz lényeges pénzügyi adatok az adott nyomozáshoz vagy büntetőeljáráshoz szükséges ideig megőrizhetők.

Az USA Pénzügyminisztériuma a SWIFT által kapott adatokból származó információkat egyesült államokbeli vagy az Egyesült Államokon kívüli, bűnüldözéssel, közbiztonsággal vagy terrorizmus elleni küzdelemmel foglalkozó hatóságoknak továbbíthatja – csakis a terrorizmus vagy a terrorizmus finanszírozásának megakadályozása, kivizsgálása, felderítése, illetve büntetőeljárás alá vonása céljából. Ha a pénzügyi adatok harmadik fél részére történő továbbítása uniós tagállam állampolgárát vagy lakosát érinti, az információ harmadik ország hatóságának való bármely továbbadása az érintett tagállam illetékes hatóságainak előzetes hozzájárulásával történhet. Kivétel megállapítható, ha az adat továbbadása a közbiztonságot közvetlenül és súlyosan fenyegető veszély elhárításához elengedhetetlenül szükséges.

A SWIFT-megállapodás elveinek betartását független ellenőrök – köztük az Európai Bizottság által kinevezett személy – ellenőrzik.

Az érintetteknek joguk van ahhoz, hogy az illetékes uniós adatvédelmi hatóságtól megerősítést kapjanak arról, hogy személyes adataik védelméhez fűződő jogaikat tiszteletben tartották. Az érintettek a SWIFT-megállapodás alapján az USA Pénzügyminisztériuma által gyűjtött és tárolt adataik helyesbítését, törlését vagy zárolását is kérhetik. Az érintettek hozzáférési joga azonban bizonyos jogszabályi korlátozások

246 Az EUROPOL Közös Ellenőrző Hatósága számos auditot folytatott az EUROPOL tevékenységeivel kapcsolatban ezen a területen, az eredményei elérhetőek: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

alá eshet. Ha a hozzáférést megtagadják, az érintettet írásban tájékoztatni kell az elutasításról, valamint az Egyesült Államokban igénybe vehető közigazgatási és bírósági jogorvoslati lehetőségekről.

A SWIFT-megállapodás öt évig, 2015 augusztusáig érvényes. Automatikusan mindig további egy évvel meghosszabbodik, kivéve, ha valamelyik fél a másikat írásban, legalább hat hónappal korábban azon szándékáról értesíti, hogy a megállapodás hatályát meghosszabbítani nem kívánja.

7

Az EU joga a rendőrségi és büntetőjogi területen megvalósuló adatvédelemmel kapcsolatban

EU	Tárgyalt kérdések	Európa Tanács
	Általánosságban	108. egyezmény
	Rendőrség	Rendőrségi ajánlás
		EJEB, *B. B. kontra Franciaország* (5335/06), 2009. december 17.
		EJEB, *S. és Marper kontra Egyesült Királyság* (30562/04 és 30566/04), 2008. december 4.
		EJEB, *Vetter kontra Franciaország* (59842/00), 2005. május 31.
	Számítástechnikai bűnözés	A számítástechnikai bűnözéssel szembeni egyezmény
Adatvédelem a rendőrségi és a bírói hatóságok határokon átnyúló együttműködésével összefüggésben		
Adatvédelmi kerethatározat	Általánosságban	108. egyezmény
		Rendőrségi ajánlás
Prümi határozat	A különleges adatok tekintetében: ujjlenyomat, DNS, huliganizmus stb.	108. egyezmény
		Rendőrségi ajánlás
Europol-határozat	Szakügynökségek részéről	108. egyezmény
Eurojust-határozat		A rendőrségi adatokra vonatkozó ajánlás
Frontex-rendelet		
Schengen II határozat	Speciális közös információs rendszerek által	108. egyezmény
VIS-rendelet		Rendőrségi ajánlás
Eurodac-rendelet		EJEB, *Dalea kontra Franciaország* (964/07), 2010. február 2.
CIS-határozat		

Az egyén adatvédelemhez fűződő érdekei és a társadalomnak – a bűnözés elleni küzdelem, továbbá a nemzet- és közbiztonság biztosítása okán – az adatgyűjtéshez fűződő érdekei közötti egyensúly megteremtése érdekében az Európa Tanács és az EU egyedi jogi aktusokat fogadott el.

7.1. Az Európa Tanács joga a rendőrségi és büntető igazságügyi területen megvalósuló adatvédelemmel kapcsolatban

Főbb pontok

- A 108. egyezmény és az Európa Tanács rendőrségi ajánlása a rendőrségi munka valamennyi területének adatvédelmi vonatkozásait érinti.
- A számítástechnikai bűnözéssel szembeni egyezmény *(Budapesti Egyezmény)* kötelező erejű nemzetközi jogi aktus, amely az elektronikus hálózatok ellen, illetve segítségével elkövetett bűncselekményekkel foglalkozik.

Európai szinten a 108. egyezmény a személyesadat-feldolgozás valamennyi területét érinti, és rendelkezései általánosságban a személyes adatok feldolgozását kívánják szabályozni. Ezért a 108. egyezmény a rendőrségi és büntető igazságügyi területen megvalósítandó adatvédelemre is vonatkozik, bár a részes felek korlátozhatják alkalmazását.

A rendőrségi és büntető igazságügyi hatóságok jogszabályi feladataihoz gyakran van szükség személyes adatok feldolgozására, ami súlyos következményekkel járhat az érintett egyénekre nézve. Az Európa Tanács által 1987-ben elfogadott, a rendőrségi adatokra vonatkozó ajánlás iránymutatást ad a részes feleknek arról, hogy milyen módon kell megvalósítaniuk a 108. egyezménynek a rendőri szervek általi személyesadat-feldolgozással kapcsolatos alapelveit.[247]

247 Az Európa Tanács Miniszteri Bizottságának 1987. szeptember 17-én elfogadott R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról.

7.1.1. A rendőrségi ajánlás

Az EJEB állandó ítélkezési gyakorlatából kitűnik, hogy a személyes adatok rendőri vagy nemzetbiztonsági hatóságok általi tárolása és megőrzése az EJEE 8. cikkének (1) bekezdésébe ütközik. Az EJEB számos ítélete foglalkozik az ilyen beavatkozás indokoltságával.[248]

Példa: A *B.B. kontra Franciaország* ügyben[249] az EJEB úgy döntött, hogy egy szexuális bűncselekmény miatt elítélt személynek egy nemzeti igazságügyi adatbázisban való szerepeltetése az EJEE 8. cikkének hatálya alá tartozik. Figyelemmel azonban arra, hogy megfelelő adatvédelmi biztosítékokat alkalmaztak – köztük azt, hogy az érintett kérheti az adatok törlését, továbbá az adatok tárolásának ideje és az adatokhoz való hozzáférés korlátozott –, megteremtették a megfelelő egyensúlyt a versengő magán- és közérdekek között. A Bíróság arra a következtetésre jutott, hogy nem sértették meg az EJEE 8. cikkét.

Példa: Az *S. és Marper kontra Egyesült Királyság* ügyben[250] mindkét felperest bűncselekményekkel vádolták meg, de egyiket sem ítélték el. Ennek ellenére a rendőrség megtartotta és tárolta ujjlenyomataikat, DNS profiljukat és sejtmintáikat. Törvény engedélyezte a biometrikus adatok korlátlan megőrzését, ha valakit bűncselekménnyel gyanúsítottak – még akkor is, ha a gyanúsítottat a későbbiekben felmentették vagy szabadlábra helyezték. Az EJEB megállapította, hogy a személyes adatok válogatás nélküli, általános megőrzése, amely időben nem korlátozott és a felmentett egyénnek csekély lehetősége van arra, hogy kérje az adatok törlését, aránytalan beavatkozásnak minősül a felperesek magánélet tiszteletben tartásához való jogába. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

A felügyeletnek az adatvédelmi jogban való beavatkozása indokoltságával az EJEB számos további ítélete foglalkozik.

248 Lásd például: EJEB, 9248/81. sz. *Leander kontra Svédország* ügy, 1987. március 26.; EJEB, 24029/07. sz. *M .M. kontra Egyesült Királyság* ügy, 2012. november 13.; EJEB, 19522/09. sz., *M. K. kontra Franciaország* ügy, 2013. április 18.

249 EJEB, *B. B. kontra Franciaország* (5335/06), 2009. december 17.

250 EJEB, *S. és Marper kontra Egyesült Királyság* (30562/04 és 30566/04), 2008. december 4., 119. és 125. pont.

Példa: Az *Allan kontra Egyesült Királyság* ügyben[251] a hatóságok titokban felvételt készítettek egy fogvatartottnak a börtönben őt meglátogató barátjával, valamint az ugyanabban a cellában lakó rabtársával folytatott magánbeszélgetéséről. Az EJEB megállapította, hogy az audio- és videokészülékeknek a felperes cellájában, a börtönbeli látogatóteremben és a rabtárson való elhelyezése és használata beavatkozásnak minősül a felperes magánélethez való jogába. Mivel a rejtett felvevőkészülékek rendőrség általi használatát az adott időben törvényi rendszer nem szabályozta, a szóban forgó beavatkozás nem felelt meg a jogszabályoknak. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Példa: A *Klass és társai kontra Németország* ügyben[252] a felperesek azt állították, hogy több német jogalkotási aktus, amely engedélyezi a levelek, postai küldemények és a távközlés titkos megfigyelését, megsérti az EJEE 8. cikkét, mégpedig azért, mert az érintett személyt nem tájékoztatják a megfigyelési intézkedésekről, és a szóban forgó intézkedések hatályon kívül helyezése után sem tud bírósághoz fordulni. Az EJEB megállapította, hogy a megfigyelés veszélye szükségképpen sérti a postai és távközlési szolgáltatásokat igénybe vevő felhasználók közötti szabad kommunikációt. Megítélése szerint azonban megfelelő biztosítékok léteztek a visszaélés ellen. A német törvényhozás joggal vélhette úgy, hogy a szóban forgó intézkedések egy demokratikus társadalomban a nemzetbiztonság és a zavargás vagy bűncselekmény megelőzése érdekében szükségesek. A Bíróság arra a következtetésre jutott, hogy nem sértették meg az EJEE 8. cikkét.

Mivel a rendőri hatóságok által végzett adatfelkezelés jelentős hatással lehet az érintett személyekre, különösen szükséges, hogy az ezen a területen létező adatbázisok fenntartására vonatkozóan részletes adatvédelmi szabályok legyenek érvényben. Az Európa Tanács rendőrségi ajánlása úgy próbálta kezelni a kérdést, hogy iránymutatást adott arra vonatkozóan, hogyan kell az adatokat gyűjteni a rendőrségi munkához; ezen a területen hogyan kell az adatállományokat tárolni; kinek kell hozzáférést biztosítani, a külföldi rendőri hatóságok részére történő adattovábbítás feltételeit is beleértve; hogyan kell az érintettek számára biztosítani adatvédelmi jogaik gyakorlását; és hogyan kell megvalósítani a független hatóságok általi ellenőrzést. Az ajánlás a megfelelő adatbiztonság biztosítására irányuló kötelezettséggel is foglalkozik.

251 EJEB, *Allan kontra Egyesült Királyság* (48539/99), 2002. november 5.

252 EJEB, *Klass és társai kontra Németország* (5029/71), 1978. szeptember 6.

Az ajánlás nem ír elő nem korlátozott, válogatás nélküli adatgyűjtést a rendőri hatóságok számára. A rendőri hatóságok általi személyesadat-gyűjtést az adatok azon körére korlátozza, amely valós veszély megelőzéséhez vagy egy konkrét bűncselekmény felszámolásához szükséges. Minden további adatgyűjtésnek egyedi nemzeti jogszabályon kell alapulnia. Az érzékeny adatok feldolgozását azon adatokra kell korlátozni, amelyek egy konkrét nyomozással összefüggésben feltétlenül szükségesek.

Ha az érintett tudomása nélkül kerül sor személyes adatok gyűjtésére, az érintettet tájékoztatni kell az adatgyűjtés tényéről, amint ez a közlés már nem akadályozza a nyomozást. A műszaki megfigyeléssel vagy más automatizált módon történő adatgyűjtésnek szintén egyedi jogi rendelkezéseken kell alapulnia.

Példa: A *Vetter kontra Franciaország* ügyben[253] anonim tanúk megvádolták a felperest emberöléssel. Mivel a felperes rendszeresen meglátogatta otthonában az egyik barátját, a rendőrség a vizsgálóbíró engedélyével lehallgató készüléket telepített a lakásba. A rögzített beszélgetések alapján a felperest letartóztatták, és elítélték emberölés miatt. A felperes kérte, hogy a felvételt minősítsék elfogadhatatlan bizonyítéknak; konkrétan azzal érvelt, hogy a felvételről jogszabály nem rendelkezett. Az EJEB számára az ügyben az volt a kérdés, hogy a lehallgató készülék alkalmazása „megfelelt-e a jogszabályoknak" vagy sem. A magáncélú helyiségek lehallgató készülékkel való felszerelése kétségtelenül nem tartozott a büntető eljárási törvény 100. és azt követő cikkeinek hatálya alá, mivel ezek a rendelkezések telefonvonalak lehallgatására vonatkoznak. A büntető eljárási törvény 81. cikke nem határozta meg kellően pontosan a hatóságok magánbeszélgetések nyomon követésének engedélyezésével kapcsolatos mérlegelési jogkörének terjedelmét és gyakorlásának módját. Ennek megfelelően a felperes a minimális védelemben sem részesült, amelyre egy demokratikus társadalomban a polgárok a jogállamiság elve alapján jogosultak. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Az ajánlás megállapítja, hogy személyes adatok tárolásakor világosan különbséget kell tenni a következők között: igazgatási adatok és rendőrségi adatok; az érintettek különböző típusai, mint például gyanúsítottak, elítéltek, áldozatok és tanúk; továbbá a konkrét ténynek minősülő, illetve gyanún vagy spekuláción alapuló adatok.

253 EJEB, *Vetter kontra Franciaország* (59842/00), 2005. május 31.

A rendőrségi adatoknak szigorúan célhoz kötöttnek kell lenniük. Ez a rendőrségi adatok harmadik felekkel való közlése szempontjából következményekkel jár: a rendőrségen belül az adatok továbbítását vagy közlését annak kell meghatároznia, hogy fűződik-e jogos érdek az információk megosztásához. Az ilyen adatok rendőrségen kívülre történő továbbítását vagy közlését csak akkor kellene engedélyezni, ha erre vonatkozóan egyértelmű jogi kötelezettség vagy engedély áll fenn. Nemzetközi továbbításra vagy közlésre kizárólag külföldi rendőri hatóságok részére kerülhet sor, és mindennek külön jogi rendelkezéseken – lehetőleg nemzetközi megállapodásokon – kell alapulnia, kivéve, ha a továbbításra vagy közlésre súlyos és közvetlen veszély kiküszöbölése érdekében van szükség.

A belföldi adatvédelmi jog betartásának biztosítása érdekében a rendőrségi adatkezelést független felügyelet alá kell helyezni. Az érintetteknek a 108. egyezményben foglalt valamennyi hozzáférési joggal rendelkezniük kell. Amennyiben az érintettek hozzáférési jogait a 108. egyezmény 9. cikke szerint a hatékony rendőrségi nyomozás érdekében korlátozzák, a belföldi jognak biztosítania kell az érintett számára a jogot ahhoz, hogy a nemzeti adatvédelmi felügyeleti hatósághoz vagy egy másik független szervhez fellebbezzen.

7.1.2. A számítógépes bűnözésről szóló egyezmény (Budapesti Egyezmény)

Mivel a bűnözői tevékenység egyre növekvő mértékben használ és érint elektronikus adatfeldolgozó rendszereket, e kihívás leküzdéséhez új büntetőjogi rendelkezésekre van szükség. Ezért az Európa Tanács – az elektronikus hálózatok ellen, illetve segítségével elkövetett bűncselekmények kérdésének kezelése céljából – elfogadta a számítógépes bűnözésről szóló egyezményt, azaz a Budapesti Egyezmény néven ismert nemzetközi jogi eszközt.[254] Ez az egyezmény azon országok számára is csatlakozásra nyitva áll, akik nem tagjai az Európa Tanácsnak, és 2013 közepéig négy, Európa Tanácson kívüli állam – Ausztrália, a Dominikai Köztársaság, Japán és az Amerikai Egyesült Államok – csatlakozott félként az egyezményhez, 12 másik, ugyancsak az Európa Tanácson kívüli állam pedig aláírta az egyezményt vagy felkérték a csatlakozásra.

Továbbra is a számítógépes bűnözésről szóló egyezmény a legbefolyásosabb nemzetközi szerződés, amely az interneten vagy más nemzetközi hálózaton elkövetett jogsértésekkel foglalkozik. Arra kötelezi a részes feleket, hogy tegyék naprakésszé

254 Az Európa Tanács Miniszteri Bizottsága (2001): A számítógépes bűnözésről szóló egyezmény, CETS 185., Budapest, 2001. november 23., hatálybalépés napja: 2004. július 1.

és hangolják össze a feltöréssel és más biztonsági jogsértésekkel, köztük a szerzői jog megsértésével, a számítógépes csalással, a gyermekpornográfiával és más jogellenes számítástechnikai tevékenységekkel szembeni büntető jogszabályaikat. Az egyezmény eljárási jogköröket is biztosít, amelyek a számítástechnikai bűnözéssel összefüggésben a számítógépes hálózatokon való keresésre és a kommunikáció feltartóztatására terjednek ki. Ezen felül az egyezmény lehetővé teszi a hatékony nemzetközi együttműködést. Az egyezményhez fűzött kiegészítő jegyzőkönyv a számítógépes hálózatokon megjelenő rasszista és idegengyűlölő propaganda büntethetőségével foglalkozik.

Bár az egyezmény nem közvetlenül az adatvédelem előmozdítására irányuló jogi aktus, büntetni azokat a tevékenységeket, amelyek valószínűleg sértik az érintett saját adatainak védelméhez való jogát. Ezenkívül kötelezi a részes feleket, hogy a végrehajtás során segítsék elő az emberi jogok és szabadságok megfelelő védelmét, az EJEE által garantált jogokat, köztük az adatvédelemhez való jogot is beleértve.[255]

7.2. Az EU joga a rendőrségi és büntetőjogi területen megvalósuló adatvédelemmel kapcsolatban

Főbb pontok

- Európai uniós szinten a rendőrségi és büntető igazságügyi területen az adatvédelmet kizárólag a rendőrségi és igazságügyi hatóságok közötti, határokon átnyúló együttműködéssel összefüggésben szabályozzák.
- Különleges adatvédelmi rendszerek léteznek az Európai Rendőrségi Hivatalra (Europol) és az EU Igazságügyi Együttműködési Egységére (Eurojust) vonatkozóan, amelyek a határokon átnyúló bűnüldözést segítő és támogató uniós szervek.
- Külön adatvédelmi rendszerek léteznek a közös információs rendszerekre vonatkozóan is, amelyeket uniós szinten az illetékes rendőrségi és igazságügyi hatóságok közötti, határokon átnyúló információcsere céljából hoztak létre. Fontos példák a Schengen II, a vízuminformációs rendszer (VIS) és az Eurodac, amely az uniós tagállamok valamelyikében menedékjogot kérő harmadik országbeli állampolgárok ujjlenyomatait tartalmazó központi rendszer.

255 Uo., 15. cikk (1) bekezdés.

Az adatvédelmi irányelv a rendőrségi és büntető igazságügyi területre nem vonatkozik. A *7.2.1. szakasz* számba veszi az ezen a területen meglévő legfontosabb jogi aktusokat.

7.2.1. Az adatvédelmi kerethatározat

A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében kezelt személyes adatok védelméről szóló 2008/977/IB tanácsi kerethatározat *(adatvédelmi kerethatározat)*[256] célja a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából történő személyesadat-feldolgozás során a természetes személyek személyes adatai védelmének biztosítása. A tagállamok, illetve az EU részéről a rendőrségi és büntető igazságügyi területen dolgozó illetékes hatóságok járnak el. Ezek a hatóságok uniós ügynökségek vagy szervek, valamint tagállami hatóságok.[257] A kerethatározat kizárólag az e hatóságok közötti, határokon átnyúló együttműködés során az adatvédelem biztosítására alkalmazható, a nemzetbiztonságra nem terjed ki.

Az adatvédelmi kerethatározat javarészt a 108. egyezményben és az adatvédelmi irányelvben szereplő elvekre és fogalom meghatározásokra támaszkodik.

Az adatokat kizárólag illetékes hatóság használhatja fel és csakis arra a célra, amelyre azokat továbbították vagy rendelkezésre bocsátották. A fogadó tagállamnak a továbbító tagállam jogszabályai által az adatcserére előírt minden korlátozást tiszteletben kell tartania. Mindazonáltal a fogadó állam bizonyos körülmények között más célra is felhasználhatja az adatokat. A továbbítások naplózása és dokumentálása az illetékes hatóságok külön feladata; ennek célja, hogy segítse a panaszokból fakadó felelősség tisztázását. A határokon átnyúló együttműködés során kapott adatok harmadik feleknek történő továbbküldéséhez azon tagállam hozzájárulása is szükséges, ahonnan az adatok származnak, bár sürgős esetekben léteznek kivételek ez alól.

A személyes adatok jogellenes feldolgozásával szembeni védelem érdekében az illetékes hatóságoknak meg kell hozniuk a szükséges biztonsági intézkedéseket.

256 A Tanács 2008/977/IB kerethatározata (2008. november 27.) a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről *(adatvédelmi kerethatározat)*, 2008, HL L 350.

257 Uo., 2. cikk h) pont.

Minden tagállamnak gondoskodnia kell arról, hogy az adatvédelmi kerethatározat szerint elfogadott rendelkezések alkalmazását egy vagy több független nemzeti felügyeleti hatóság segítse tanácsadással és ellenőrizze. E hatóságok az említetteken kívül befogadják az illetékes hatóságok által végzett személyesadat-feldolgozással összefüggően az adott személyt megillető jogok és szabadságok védelmével kapcsolatban e személy által benyújtott kérelmeket.

Az érintett tájékoztatásra jogosult személyes adatainak kezeléséről, és a hozzáférés, a helyesbítés, a törlés és a zárolás joga is megilleti őt. Amennyiben kényszerítő okok miatt e jogok gyakorlását megtagadják, az érintettnek rendelkeznie kell fellebbezési joggal az illetékes nemzeti felügyeleti hatósághoz és/vagy a bírósághoz. Ha a személy az adatvédelmi kerethatározatot végrehajtó nemzeti jogszabály megsértése miatt kárt szenved, az adatkezelőtől kártérítésre jogosult.[258] Az érintettnek általánosságban jogot kell biztosítani arra, hogy az adatvédelmi kerethatározatot végrehajtó nemzeti jogszabályok szerint őt megillető jogok megsértése esetén bírósági jogorvoslatot vehessen igénybe.[259]

Az Európai Bizottság adatvédelmi reformcsomagja egy általános adatvédelmi rendeletből[260] és egy általános adatvédelmi irányelvből áll.[261] Ez az új irányelv a jelenleg hatályos adatvédelmi kerethatározat helyébe lépne, és a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésre alkalmazna általános elveket és szabályokat.

258 Uo., 19. cikk.

259 Uo., 20. cikk.

260 Európai Bizottság (2012), A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslat (általános adatvédelmi rendelet), COM(2012) 0011, Brüsszel, 2012. január 25.

261 Európai Bizottság (2012), Javaslat európai parlament és tanácsi irányelvre a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi irányelv), COM(2012) 0010, Brüsszel, 2012. január 25.

7.2.2. Egyedi jogi eszközök az adatvédelemben a rendőrségi és bűnüldözési területen megvalósuló határokon átnyúló együttműködés terén

Az adatvédelmi kerethatározaton kívül a tagállamok által speciális területeken tárolt információk cseréjét több jogi eszköz szabályozza, köztük a bűnügyi nyilvántartásból származó információk tagállamok közötti cseréjének megszervezéséről és azok tartalmáról szóló 2009/315/IB tanácsi kerethatározat és a tagállamok pénzügyi információs egységeinek az információcsere terén folytatott együttműködésére vonatkozó rendelkezésekről szóló tanácsi határozat.[262]

Lényeges, hogy az illetékes hatóságok közötti, határokon átnyúló együttműködés[263] egyre nagyobb mértékben együtt jár a bevándorlási adatok cseréjével. Ez a jogi terület nem tartozik a rendőrségi és igazságügyi kérdések közé, de számos vonatkozásban lényeges a rendőrségi és igazságügyi hatóságok munkája szempontjából. Ugyanez igaz az EU-ba bevitt vagy onnan kivitt árukkal kapcsolatos adatokra is. Az EU-n belüli belső határellenőrzés megszüntetése megnövelte a csalás kockázatát, aminek következtében a tagállamoknak intenzívebbé kell tenniük az együttműködést – különösen a határokon átnyúló információcsere fokozásával –, hogy eredményesebben derítsék fel és vonják büntetőeljárás alá a nemzeti és az uniós vámszabálysértéseket.

A prümi határozat

A nemzeti szinten tárolt adatok cseréjével megvalósuló, intézményesített határokon átnyúló együttműködés egyik példája a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló 2008/615/IB tanácsi határozat (*prümi határozat*), amely

262 Az Európai Unió Tanács (2009): A Tanács 2009/315/IB kerethatározata (2009. február 26.) a bűnügyi nyilvántartásból származó információk tagállamok közötti cseréjének megszervezéséről és azok tartalmáról, 2009, HL L 93.; az Európai Unió Tanácsa (2000): A Tanács 2000/642/IB határozata (2000. október 17.) a tagállamok pénzügyi információs egységeinek az információcsere terén folytatott együttműködésére vonatkozó rendelkezésekről, 2000, HL L 271.

263 Európai Bizottság (2012): A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – Az EU-n belüli bűnüldözési együttműködés erősítése: az európai információcsere-modell, COM(2012) 735, Brüsszel, 2012. december 7.

2008-ban az uniós jogba emelte a Prümi Szerződést.[264] A Prümi Szerződés egy 2005-ben létrejött nemzetközi rendőrségi együttműködési megállapodás, amelyet Ausztria, Belgium, Franciaország, Hollandia, Luxemburg, Németország és Spanyolország írt alá.[265]

A prümi határozat célja, hogy segítséget nyújtson a tagállamoknak három területen – a terrorizmus, a határokon átnyúló bűnözés, valamint az illegális migráció terén – a bűncselekmények megelőzését és az ellenük való küzdelmet szolgáló fokozottabb információcsere megvalósításában. E célból a határozat a következőkkel kapcsolatban állapít meg rendelkezéseket:

- automatizált hozzáférés DNS-profilokhoz, ujjlenyomat-adatokhoz és bizonyos nemzeti gépjármű-nyilvántartási adatokhoz;
- határon átnyúló dimenzióval rendelkező nagyszabású eseményekkel kapcsolatos adatok átadása;
- információátadás terrorcselekmények megelőzése érdekében;
- egyéb intézkedések a határon átnyúló rendőrségi együttműködés megerősítésére.

A prümi határozat alapján rendelkezésre bocsátott adatbázisok teljes egészében a nemzeti jog hatálya alá tartoznak, az adatok cseréjére azonban a határozat, valamint újabban az adatvédelmi kerethatározat az irányadó. A szóban forgó adatforgalom felügyeletét ellátó illetékes szervek a nemzeti adatvédelmi felügyeleti hatóságok.

264 Az Európai Unió Tanácsa (2008): A Tanács 2008/615/IB határozata (2008. június 23.) a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről, 2008, HL L 210.

265 A Belga Királyság, a Németországi Szövetségi Köztársaság, a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság és az Osztrák Köztársaság között létrejött, különösen a terrorizmus, a határokon átnyúló bűnözés, valamint az illegális migráció elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló egyezmény; elérhető a következő címen: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

7.2.3. Adatvédelem az Europolnál és az Eurojustnál

Europol

Az Europol, az EU hágai székhelyű bűnüldözési ügynöksége, amelynek minden tagállamban vannak nemzeti egységei (EUROPOL nemzeti egységek). Az Europolt 1998-ban hozták létre; jelenlegi jogállása – uniós intézmény – az Európai Rendőrségi Hivatalt létrehozó tanácsi határozaton (*Europol-határozat*) alapszik.[266] Az Europol célja az Europol-határozat mellékletében felsorolt, két vagy több tagállamot érintő szervezett bűncselekmények, terrorizmus és a szervezett bűnözés más formáinak megelőzése és kivizsgálása.

Céljainak eléréséhez az Europol létrehozta az Europol Információs Rendszert, amely adatbázison keresztül a tagállamok – EUROPOL nemzeti egységeik (ENU-k) útján – kicserélhetik a bűnügyi hírszerzési adatokat és információkat. Az Europol Információs Rendszer a következőkkel kapcsolatos adatok rendelkezésére bocsátására használható: az Europol hatáskörébe tartozó bűncselekménnyel gyanúsított vagy ilyen bűncselekményért elítélt személyek; illetve olyan személyek, akikkel kapcsolatban tényszerű jelek alapján feltételezhető, hogy ilyen bűncselekményt fognak elkövetni. Az Europol és az ENU-k közvetlenül felvehetnek adatokat az Europol Információs Rendszerbe, és le is kérdezhetnek adatokat onnan. Csak az a fél módosíthatja, javíthatja vagy törölheti az adatokat, aki felvitte azokat a rendszerbe.

Ha a feladatainak ellátásához szükséges, az Europol elemzési munkafájlokban tárolhat, módosíthat és felhasználhat bűncselekményekkel kapcsolatos adatokat. Elemzési munkafájlt adatok összegyűjtése, feldolgozása vagy felhasználása céljából nyitnak annak érdekében, hogy az Europol által uniós tagállamokkal együtt folytatott konkrét bűnügyi nyomozást segítsék.

Az új fejleményekre reagálva 2013. január 1-jén létrehozták az Europolnál a Számítástechnikai Bűnözés Elleni Európai Központot.[267] A központ az EU számítástechnikai

266 Az Európai Unió Tanácsa (2009): Az Európai Rendőrségi Hivatalt (Europol) létrehozó, 2009. április 6-i tanácsi határozat, 2009, HL L 121. Lásd még a Bűnüldözési Együttműködés És Képzés Európai Ügynökségéről (Europol), valamint a 2009/371/IB és 2005/681/IB határozatok hatályon kívül helyezéséről szóló bizottsági rendeletjavaslatot, amely egy új Europol számára teremt jogi keretet; az e javaslat által létrehozott Europol a 2009. április 6-i 2009/371/IB tanácsi határozat által létrehozott Európai Rendőrségi Hivatal (Europol) és a 2005/681/IB tanácsi határozat által létrehozott Európai Rendőrakadémia (CEPOL) helyébe lép, és azok jogutódja; COM(2013) 173.

267 Lásd még az európai adatvédelmi biztos 2012-*es véleményét a Számítástechnikai Bűnözés Elleni Európai Központ létrehozásáról szóló, a Tanácshoz és az Európai Parlamenthez intézett bizottsági közleményről,* Brüsszel, 2012. június 29.

bűnözéssel kapcsolatos információs központja, amely lehetővé teszi a gyors reagálást online bűncselekmények elkövetése esetén, fejleszti és kialakítja a digitális igazságügyi képességeket, és közvetíti a számítástechnikai bűnözéssel kapcsolatos nyomozások során bevált gyakorlatokat. A központ elsősorban olyan számítástechnikai bűncselekményekkel foglalkozik, amelyek(et):

- szervezett csoportok követnek el bűncselekményekből származó tetemes nyereség érdekében (pl. online csalás);
- súlyos kárt okoznak áldozataiknak (pl. gyermekek szexuális kizsákmányolása);
- az Unión belüli kritikus információs és kommunikációs technológiai rendszereket érintik.

Az Europol tevékenységeire vonatkozó adatvédelmi rendszert megerősítették. Az Europol-határozat 27. cikke kimondja, hogy az Europol figyelembe veszi a 108. egyezmény és a rendőrségi adatokra vonatkozó ajánlás automatizált és nem automatizált adatfeldolgozással kapcsolatos elveit. Az Europol és a tagállamok közötti adattovábbításnak ezenkívül az adatvédelmi kerethatározatban foglalt szabályoknak is meg kell felelnie.

Az alkalmazandó adatvédelmi jogszabályok betartása és különösen annak biztosítása érdekében, hogy a személyesadat-kezelés ne sértse a magánszemélyek jogait, az Europol független közös ellenőrző szerve felügyeli és ellenőrzi az Europol tevékenységeit.[268] Minden magánszemély hozzáférési joggal rendelkezik az Europol által tárolt, rá vonatkozó személyes adatokhoz, továbbá a szóban forgó személyes adatok ellenőrzését, javítását vagy törlését is kérheti. Ha egy személy nem ért egyet az Europol e jogok gyakorlásával kapcsolatos határozatával, a közös ellenőrző szerv fellebbezési bizottságánál jogorvoslathoz folyamodhat.

Ha az Europolnál tárolt adatok jogi vagy ténybeli hibája miatt kár keletkezett, a sértett fél kizárólag a kárt előidéző esemény helye szerinti tagállam illetékes bíróságához fordulhat jogorvoslatért.[269] Az Europol visszatéríti a tagállamnak a kártérítésként kifizetett összeget, ha a kár abból eredt, hogy az Europol nem tett eleget jogszabályi kötelezettségeinek.

268 Europol-határozat, 34. cikk.

269 Uo., 52. cikk.

Eurojust

A 2002-ben létrehozott Eurojust hágai székhelyű uniós szerv, amely a legalább két tagállamot érintő súlyos bűncselekményekkel kapcsolatos nyomozás és büntetőeljárás terén előmozdítja az igazságügyi együttműködést.[270] Az Eurojust illetékességi körébe az alábbiak tartoznak:

- a nyomozások és a büntetőeljárások terén a tagállamok hatáskörrel rendelkező hatóságai közötti koordináció és együttműködés ösztönzése és fejlesztése;

- az igazságügyi együttműködésre irányuló megkeresések és határozatok végrehajtásának előmozdítása.

Az Eurojust feladatait nemzeti tagok látják el. Minden tagállam egy-egy, a nemzeti jog hatálya alá tartozó bírót vagy ügyészt delegál az Eurojustba, aki rendelkezik az igazságügyi együttműködés ösztönzését és fejlesztését szolgáló feladatok teljesítéséhez szükséges hatáskörökkel. Ezenfelül a nemzeti tagok közösen testületként látják el az Eurojust speciális feladatait.

Az Eurojust a célkitűzéseinek eléréséhez szükséges mértékben személyes adatokat is kezelhet. Ez a tevékenység azonban olyan személyekkel kapcsolatos konkrét adatokra korlátozódik, akiket az Eurojust hatáskörébe tartozó bűncselekmény elkövetésével vagy ilyen bűncselekmény elkövetésében való részvétellel gyanúsítanak, illetve akiket ilyen bűncselekmény miatt elítéltek. Az Eurojust a hatáskörébe tartozó bűncselekmények tanúira és sértettjeire vonatkozó bizonyos információkat is feldolgozhat.[271] Rendkívüli körülmények között az Eurojust – korlátozott ideig – a bűncselekmény körülményeire vonatkozóan szélesebb körű személyesadat-feldolgozást is végezhet, amennyiben ezek az adatok közvetlenül érintik a folyamatban lévő nyomozást. Az Eurojust a hatáskörének keretein belül más uniós intézményekkel, szervekkel és ügynökségekkel is együttműködhet, és velük személyes adatokat

270 Az Európai Unió Tanácsa (2002): A bűnözés súlyos formái elleni fokozott küzdelem céljából az Eurojust létrehozásáról szóló, 2002. február 28-i 2002/187/IB tanácsi határozat, 2002, HL L 63.; Az Európai Unió Tanácsa (2003): A bűnözés súlyos formái elleni fokozott küzdelem céljából az Eurojust létrehozásáról szóló 2002/187/IB határozat módosításáról szóló, 2003. június 18-i 2003/659/IB tanácsi határozat, 2003, HL L 44.; Az Európai Unió Tanácsa (2009): Az Eurojust megerősítéséről és az Eurojust létrehozásáról a bűnözés súlyos formái elleni fokozott küzdelem céljából szóló 2002/187/IB határozat módosításáról szóló, 2008. december 16-i 2009/426/IB tanácsi határozat, 2009, HL L 138. (*Eurojust-határozatok*).

271 A 2002/187/IB tanácsi határozatnak a 2003/659/IB tanácsi határozattal és a 2009/426/IB tanácsi határozattal történt módosítása egységes szerkezetbe foglalt változata, 15. cikk (2) bekezdés.

cserélhet. Az Eurojust harmadik országokkal és szervezetekkel is együttműködhet és személyes adatokat cserélhet.

Az adatvédelem terén az Eurojustnak legalább olyan szintű védelmet kell biztosítania, amely egyenértékű az Európa Tanács 108. egyezményében, illetve későbbi módosításaiban foglalt elvek alkalmazásából eredő védelemmel. Adatcsere esetén egyedi szabályokat és korlátozásokat kell betartani, amelyeket vagy együttműködési megállapodásban, vagy munkavégzésre vonatkozó rendelkezésben állapítanak meg az Eurojustra vonatkozó tanácsi határozatoknak és az Eurojust adatvédelmi szabályzatának megfelelően.[272]

Az Eurojustnál független közös ellenőrző szervet hoztak létre, amely az Eurojust által végzett személyesadat-kezelést kíséri figyelemmel. Magánszemélyek a közös ellenőrző szervhez nyújthatnak be fellebbezést, ha nem értenek egyet az adataikhoz való hozzáférés, adataik helyesbítése, zárolása vagy törlése iránti kérésükre az Eurojust által adott válasszal. Ha az Eurojust jogellenesen kezel személyes adatokat, a székhelye szerinti tagállam – Hollandia – nemzeti jogának megfelelően felel az érintettnek okozott minden kárért.

7.2.4. Adatvédelem az uniós szintű közös információs rendszerekben

A tagállamok közötti információcserén és a határokon átnyúló bűncselekmények elleni küzdelemre szakosodott uniós hatóságok létrehozásán túl számos közös információs rendszert hoztak létre uniós szinten, hogy meghatározott bűnüldözési célokra – köztük az idegenrendészeti jog és a vámjog területén – az adatcsere fórumaként szolgáljanak a hatáskörrel rendelkező nemzeti és uniós hatóságok számára. Néhány ilyen rendszer többoldalú megállapodások nyomán jött létre, amelyek később uniós jogi aktusokkal és rendszerekkel egészültek ki – ezek közé tartozik pl. a Schengeni Információs Rendszer, a Vízuminformációs Rendszer, az Eurodac, az Eurosur vagy a váminformációs rendszer.

272 Az Eurojust személyes adatok feldolgozására és védelmére vonatkozó eljárási szabályzata, 2005, HL C 68/01., 2005. március 19., 1. o.

A 2012-ben létrehozott, nagyméretű informatikai rendszerekkel foglalkozó európai ügynökség (eu-LISA)[273] feladata a második generációs Schengeni Információs Rendszer (SIS II), a Vízuminformációs Rendszer (VIS) és az Eurodac hosszú távú üzemeltetési igazgatása. Az eu-LISA alapfeladata az információtechnológiai rendszerek hatékony, biztonságos és folyamatos működésének biztosítása. Feladatai közé tartozik ezen kívül, hogy elfogadja a rendszerek biztonságossága és az adatbiztonság szavatolásához szükséges intézkedéseket.

A Schengeni Információs Rendszer

1985-ben a korábbi Európai Közösségek több tagállama, a Benelux Unió államai, Németország és Franciaország között megállapodás jött létre a közös határaikon történő ellenőrzések fokozatos megszüntetéséről (*Schengeni Megállapodás*), amelynek célja a személyek szabad, a schengeni területen belül határellenőrzéstől mentes mozgását biztosító térség létrehozása volt.[274] A nyitott határokból fakadó, a közbiztonságot fenyegető veszély ellensúlyozására megerősített határellenőrzést vezettek be a schengeni térség külső határain, és szoros együttműködést hoztak létre a nemzeti rendőri és igazságügyi hatóságok között.

Mivel a Schengeni Megállapodáshoz további államok is csatlakoztak, a schengeni rendszert végül az Amszterdami Szerződéssel beépítették az uniós jogi keretbe.[275] E határozat végrehajtására 1999-ben került sor. A Schengeni Információs Rendszer legújabb verziója, az ún. SIS II, 2013. április 9-én kezdte meg működését. Jelenleg az összes uniós tagállamot, valamint Izlandot, Liechtensteint, Norvégiát és Svájcot is kiszolgálja.[276] Az Europol és az Eurojust is rendelkezik hozzáféréssel a SIS II-höz.

A SIS II egy központi rendszerből (C-SIS), a tagállamokban található nemzeti rendszerekből, valamint a központi rendszer és a nemzeti rendszerek közötti kommunikációs

273 Az Európai Parlament és a Tanács 1077/2011/EU rendelete (2011. október 25.) a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai ügynökség létrehozásáról, 2011, HL L 286.

274 Megállapodás a Benelux Gazdasági Unió államai, a Németországi Szövetségi Köztársaság és a Francia Köztársaság kormányai között a közös határaikon történő ellenőrzések fokozatos megszüntetéséről, HL L 239., 2000.

275 Európai Közösségek (1997): Amszterdami Szerződés az Európai Unióról szóló szerződés, az Európai Közösségeket létrehozó szerződések és egyes kapcsolódó okmányok módosításáról, 1997, HL C 340.

276 Az Európai Parlament és a Tanács 1987/2006/EK rendelete (2006. december 20.) a Schengeni Információs Rendszer második generációjának (sis ii) létrehozásáról, működtetéséről és használatáról, HL L 381., 2006 *(SIS II)*; Az Európai Unió Tanácsa (2007): A Tanács 2007/533/IB határozata (2007. június 12.) a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról *(SIS II),* HL L 205., 2007.

infrastruktúrából áll. A C-SIS a tagállamok által a rendszerbe bevitt, személyekre és tárgyakra vonatkozó adatokat tartalmaz. A C-SIS-t az egész schengeni övezetben megtalálható nemzeti határellenőrzési, rendőri, vám-, vízum- és igazságügyi hatóságok használják. Minden tagállam a C-SIS nemzeti másolatát, a „nemzeti schengeni információs rendszerek" (N-SIS) néven ismert rendszereket üzemelteti, amelyeket folyamatosan frissítenek, így a C-SIS is frissül. Az N-SIS-szel egyeztetnek, és a rendszer figyelmeztető jelzést ad ki, ha:

- a személy nem jogosult a schengeni területre való belépésre vagy az ott tartózkodásra; vagy
- a személyt vagy tárgyat igazságügyi vagy bűnüldöző hatóságok keresik; vagy
- a személy eltűnését jelentették; vagy
- az árukat, köztük bankjegyeket, gépjárműveket, tehergépjárműveket, lőfegyvereket és azonosító okmányokat ellopott vagy elveszett dologként bejelentették.

Figyelmeztető jelzés esetén nyomon követést kell kezdeményezni a nemzeti schengeni információs rendszereken keresztül.

A SIS II-nek új funkciói is vannak, mint pl. a lehetőség a következők bevitelére a rendszerbe: biometrikus adatok, köztük ujjlenyomatok és fényképek; a figyelmeztető jelzések új kategóriái: pl. ellopott hajók, légi járművek, konténerek vagy fizetőeszközök; figyelmeztető jelzések személyekre és tárgyakra vonatkozóan; letartóztatás, átadás vagy kiadatás céljából körözött személyekre vonatkozó európai elfogatóparancsok másolatai.

A Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról szóló 2007/533/IB tanácsi határozat (Schengen II határozat) beépíti a 108. egyezmény következő rendelkezését: „Az e határozat alkalmazásában feldolgozott személyes adatok védelmére az Európa Tanács 108. egyezményével összhangban kerül sor."[277] Ha személyes adatok nemzeti rendőri hatóságok általi felhasználására a Schengen II határozat akalmazásában kerül sor, a 108. egyezmény és a rendőrségi adatokra vonatkozó ajánlás rendelkezéseinek alkalmazása a nemzeti jogban kötelező érvényű.

277 Az Európai Unió Tanácsa (2007): A Tanács 2007/533/IB határozata (2007. június 12.) a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról, 2007, HL L 205., 57. cikk.

A hatáskörrel rendelkező nemzeti felügyeleti hatóság minden tagállamban felügyeletet gyakorol a hazai N-SIS felett. Ellenőriznie kell különösen azon adatok minőségét, amelyeket a tagállam az N-SIS-en keresztül bevisz a C-SIS-be. A nemzeti felügyelő hatóságnak biztosítania kell, hogy legalább négyévente sor kerül a belföldi N-SIS-en belül az adatfeldolgozó tevékenységek ellenőrzésére. A nemzeti felügyeleti hatóságok és az európai adatvédelmi biztos együttműködnek egymással, és biztosítják a SIS összehangolt felügyeletét, míg az európai adatvédelmi biztos felel a C-SIS felügyeletéért. Az átláthatóság érdekében kétévente közös tevékenységi jelentést küldenek az Európai Parlamentnek, a Tanácsnak és az eu-LISA-nak.

A magánszemélyek bármelyik tagállamban gyakorolhatják a SIS II-höz való hozzáférési jogaikat, mivel minden N-SIS a C-SIS pontos másolata.

Példa: A *Dalea kontra Franciaország* ügyben[278] a felperestől megtagadták a francia beutazó vízumot, mivel a francia hatóságok bejelentették a Schengeni Információs Rendszerben, hogy a felperes beutazási kérelmét el kell utasítani. A felperes sikertelenül kérte a francia adatvédelmi hatóságtól, majd az Államtanácstól az adataihoz való hozzáférést, továbbá adatainak helyesbítését vagy törlését. Az EJEB megállapította, hogy a felperes Schengeni Információs Rendszerbe történt bejelentése megfelelt a jogszabályoknak, és a nemzetbiztonság védelmének törvényes célját szolgálta. Mivel a felperes nem mutatta ki, hogy ténylegesen milyen hátrányt szenvedett a schengeni övezetbe való belépésének meghiúsulása miatt, és mivel megfelelő intézkedések álltak rendelkezésre arra, hogy megvédjék őt az önkényes döntéshozataltól, a magánélet tiszteletben tartásához való jogába való beavatkozás arányos volt. A felperes 8. cikk szerinti panaszát ezért elfogadhatatlannak nyilvánították.

A Vízuminformációs Rendszer

A szintén az eu-LISA által üzemeltetett Vízuminformációs Rendszert (VIS) a közös uniós vízumpolitika végrehajtásának támogatására fejlesztették ki.[279] Lehetővé

278 EJEB, *Dalea kontra Franciaország* (hat.) (964/07), 2010. február 2.

279 Az Európai Unió Tanácsa (2004): a Vízuminformációs Rendszer létrehozásáról (VIS) szóló, 2004. június 8-i tanácsi határozat, HL L 213., 2004; Az Európai Parlament és a Tanács 767/2008/EK rendelete (2008. július 9.) a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről *(VIS-rendelet)*, HL L 218., 2008; Az Európai Unió Tanácsa (2008): A Tanács 2008/633/IB határozata (2008. június 23.) a vízuminformációs rendszerhez (VIS) a tagállamok kijelölt hatóságai, valamint az Europol számára a terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében, betekintés céljából történő hozzáférésről, HL L 218., 2008.

teszi, hogy egy, a schengeni államok nem uniós országokban található konzulátusait az összes schengeni állam külső határátkelőhelyeivel összekötő rendszeren keresztül kicseréljék a vízumadatokat. A VIS a schengeni térségben való rövid távú tartózkodásra vagy a schengeni térségen való átutazásra jogosító vízumok iránti kérelmek adatait dolgozza fel és a határőrizeti hatóságok biometrikus adatok segítségével ellenőrizhetik, hogy a vízumot bemutató személy annak jogos tulajdonosa-e, továbbá azonosíthatják a hamis dokumentumokkal rendelkező vagy dokumentumokkal egyáltalán nem rendelkező személyeket.

A Vízuminformációs Rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló 767/2008/EK európai parlamenti és tanácsi rendelet (*VIS-rendelet*) szerint csak a kérelmezőre, a kérelmező vízumaira, fényképeire, ujjlenyomataira, a korábbi kérelmeihez való kapcsolódásokra, valamint a vele együtt utazó személyek kérelmeire vonatkozó adatok rögzíthetők a Vízuminformációs Rendszerben.[280] Adatok bevitele, módosítása vagy törlése céljából kizárólag a tagállami vízumhatóságok férhetnek hozzá a nyilvántartáshoz, míg adategyeztetés céljából a vízumhatóságokon kívül a külső határátkelőhelyeken végzett ellenőrzésekre, az idegenrendészeti ellenőrzésre hatáskörrel rendelkező, valamint a menekültügyi hatóságok is hozzáférhetnek a rendszerhez. Bizonyos körülmények között – súlyos bűncselekmény megelőzése, felderítése vagy kivizsgálása céljából – az illetékes nemzeti rendőri hatóságok és az Europol is hozzáférést kérhetnek a VIS-be bevitt adatokhoz.[281]

Eurodac

Az Eurodac neve az ujjlenyomatokra (daktilogramokra) utal. Az Eurodac a valamelyik uniós tagállamban menedékjogot kért harmadik országbeli állampolgárok ujjlenyomat-adatait tartalmazó központi rendszer.[282] A rendszer 2003. január óta

280 A vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló, 2008. július 9-i 767/2008/EK európai parlamenti és tanácsi rendelet *(VIS-rendelet)* 5. cikke, 2008, HL L 218.

281 Az Európai Unió Tanácsa (2008): A Tanács 2008/633/IB határozata (2008. június 23.) a vízuminformációs rendszerhez (VIS) a tagállamok kijelölt hatóságai, valamint az Europol számára a terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében, betekintés céljából történő hozzáférésről, 2008, HL L 218.

282 A Tanács 2725/2000/EK rendelete (2000. december 10.) a dublini egyezmény hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítására irányuló „Eurodac" létrehozásáról, 2000, HL L 316.; A Tanács 407/2002/EK rendelete (2002. február 28.) a Dublini Egyezmény hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítására irányuló „Eurodac" létrehozásáról szóló 2725/2000/EK rendelet végrehajtására vonatkozó egyes szabályok megállapításáról, 2002, HL L 62. *(Eurodac-rendeletek).*

működik azzal a céllal, hogy segítse annak eldöntését, hogy az egy harmadik ország állampolgára által a tagállamok egyikében benyújtott menedékjog iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó szempontok és eljárási szabályok megállapításáról szóló 343/2003/EK tanácsi rendelet *(Dublin II rendelet)* alapján melyik tagállam feladata egy adott menedékkérelem vizsgálata.[283] Az EURODAC-ban tárolt személyes adatok kizárólag a dublini rendelet alkalmazásának megkönnyítése céljából használhatók fel; bármely egyéb felhasználás büntetendő.

Az Eurodac egy, az eu-LISA által működtetett, az ujjlenyomatok tárolására és összehasonlítására szolgáló központi egységből, valamint a tagállamok és a központi adatbázis közötti elektronikus adattovábbításokat végző rendszerből áll. A tagállamok minden olyan, 14. életévét betöltött nem uniós állampolgár vagy hontalan személy ujjlenyomatát leveszik és továbbítják, aki a területükön menedékjogot kér, vagy akit a külső határok jogellenes átlépése miatt elfogtak. A tagállamok a területükön engedély nélkül tartózkodó nem uniós állampolgárok vagy hontalan személyek ujjlenyomatait is levehetik és továbbíthatják.

Az ujjlenyomat-adatokat kizárólag pszeudoanonimizált módon tárolják az Eurodac-adatbázisban. Egyezés esetén az álnevet azon első tagállam megnevezésével együtt, amely az ujjlenyomat-adatot továbbította, a másik tagállam tudomására hozzák. E második tagállam ezután megkeresi az első tagállamot, mert a Dublin II rendelet szerint a menedékkérelem feldolgozása az első tagállam feladata.

Az Eurodac-ban tárolt, menedékkérőkre vonatkozó személyes adatokat az ujjlenyomat-vétel napjától számított 10 évig őrzik meg, kivéve, ha az érintett valamelyik uniós tagállamban állampolgárságot szerez. Ebben az esetben az adatokat azonnal törölni kell. A külső határok jogellenes átlépése miatt elfogott külföldi állampolgárokra vonatkozó adatokat két évig tárolják. Ezeket az adatokat azonnal törölni kell, ha az érintett tartózkodási engedélyt kap, elhagyja az EU területét, vagy uniós tagállamban állampolgárságot szerez.

Az uniós tagállamokon kívül – nemzetközi megállapodások alapján – Izland, Norvégia, Liechtenstein és Svájc is alkalmazza a nyilvántartást.

283 A Tanács 2003. február 18-i, 343/2003/EK rendelete egy harmadik ország állampolgára által a tagállamok egyikében benyújtott menedékjog iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó szempontok és eljárási szabályok megállapításáról, 2003, HL L 50. *(Dublin II rendelet)*.

Eurosur

Az európai határőrizeti rendszert (*Eurosur*)[284] a schengeni külső határok ellenőrzésének – az illegális bevándorlás és a határokon átnyúló bűnözés felderítése, megelőzése és az ellene való küzdelem útján történő – megerősítésére hozták létre. Fokozza az információcserét és az operatív együttműködést a nemzeti koordinációs központok és a Frontex között, mely utóbbi az integrált határigazgatás új koncepciójának kidolgozásáért és alkalmazásáért felelős uniós ügynökség.[285] Általános célkitűzései a következők:

- az EU-ba észrevétlenül bejutó illegális bevándorlók számának csökkentése;
- az illegális bevándorlókat érintő tengeri halálesetek számának csökkentése, azaz több emberi élet megmentése a tengeren;
- az EU egésze belső biztonságának növelése a határokon átnyúló bűnözés megelőzéséhez való hozzájárulás révén.[286]

Az Eurosur 2013. december 2-án kezdte meg működését a külső határokkal rendelkező összes tagállamban, a többi tagállamban pedig 2014. december 1-től indul. A rendelet a tagállamok szárazföldi és tengeri külső határainak, valamint légi határainak őrzésére alkalmazandó.

284 Az Európai Parlament és a Tanács 2013. október 22-i 1052/2013/EK rendelete az európai határőrizeti rendszer (EUROSUR) létrehozásáról, HL L 295., 2013.

285 Az Európai Parlament és a Tanács 2011. október 25-i 1168/2011/EU rendelete az Európai Unió Tagállamai Külső Határain Való Operatív Együttműködési Igazgatásért Felelős Európai Ügynökség felállításáról szóló 2007/2004/EK tanácsi rendelet módosításáról, 2011, HL L 394. *(Frontex-rendelet).*

286 Lásd még: Európai Bizottság (2008): A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdaásgi és Szociális Bizottságnak és a Régiók Bizottságának az európai határőrizeti rendszer (EUROSUR) kialakításának vizsgálatáról, COM(2008) 68, Brüsszel, 2008. gebruár 13.; Európai Bizottság (2011): A "Javaslat európai parlamenti és tanácsi rendeletre az európai határőrizeti rendszer (EUROSUR) létrehozásáról" című dokumentumot kísérő hatásvizsgálat, bizottsági szolgálati munkadokumentum, SEC(2011)1536, Brüsszel, 2011. december 12., 18. o.

Váminformációs rendszer

Egy másik, uniós szinten létrehozott, közös információs rendszer a váminformációs rendszer (VIR).[287] A belső piac kialakítása során az EU területén belül mozgó árukra vonatkozó ellenőrzéseket és formalitásokat teljesen eltörölték, ami megnövelte a csalás kockázatát. Ezt a veszélyt a tagállamok vámigazgatási szervei közötti fokozott együttműködéssel ellensúlyozták. A VIR célja, hogy elősegítse a tagállamok számára a nemzeti és uniós vám- és mezőgazdasági jogszabályok súlyos megsértésének megelőzését, felderítését és üldözését.

A VIR nyersanyagokkal, szállítóeszközökkel, vállalkozásokkal, személyekkel, valamint a visszatartott, lefoglalt vagy elkobozott árukkal és készpénzzel kapcsolatos személyes adatokat tartalmaz. Az említett információk kizárólag az alábbi célokból használhatók fel: megfigyelés és jelentéstétel, célzott megfigyelés, illetve stratégiai vagy operatív elemzés olyan személyre vonatkozóan, aki vámügyi jogszabályok megsértésével gyanúsítható.

A VIR-hez a nemzeti vám-, adó-, mezőgazdasági, közegészségügyi és rendőri hatóságok, valamint az Europol és az Eurojust rendelkezik hozzáférési jogosultsággal.

A személyes adatok feldolgozása során be kell tartani az 515/97 Rendeletben és a VIR-egyezményben meghatározott speciális szabályokat,[288] valamint az adatvédelmi irányelv, az uniós intézmények adatvédelmi rendelete, a 108. egyezmény és a rendőrségi adatokra vonatkozó ajánlás rendelkezéseit. Az európai adatvédelmi biztos felelős azért, hogy a CIS a 45/2001/EK rendeletnek megfeleljen, és évente legalább egyszer összehív egy találkozót az összes felügyeleti joggal rendelkező nemzeti adatvédelmi hatóságokkal.

287 Az Európai Unió Tanácsa (1995): A Tanács 1995. július 26-i jogi aktusa az informatika vámügyi alkalmazásáról szóló egyezmény létrehozásáról, 1995. HL C 316., módosította az Európai Unió Tanácsa (2009); A Tanács 1997. március 13.-i 515/97/EK rendelete a tagállamok közigazgatási hatóságai közötti kölcsönös segítségnyújtásról, valamint az utóbbiak és a Közösség közötti együttműködéséről a vám- és agrárügyekre vonatkozó jogszabályok korrekt alkalmazásáról; A Tanács 2009. november 30-i 2009/917/IB határozata az információs technológia vámügyi alkalmazásáról, 2009, HL L 323. *(VIR-határozat),*

288 Uo.

8

Egyéb speciális európai adatvédelmi jogszabályok

EU	Tárgyalt kérdések	Európa Tanács
Adatvédelmi irányelv Elektronikus hírközlési adatvédelmi irányelv	Elektronikus közlések	108. egyezmény Távközlési szolgáltatásokra vonatkozó ajánlás
Adatvédelmi irányelv, 8. cikk (2) bekezdés b) pont	Foglalkoztatási jogviszony	108. egyezmény Foglalkoztatásra vonatkozó ajánlás
		EJEB, *Copland kontra Egyesült Királyság* (62617/00), 2007. április 3.
Adatvédelmi irányelv, 8. cikk (3) bekezdés	Orvosi adatok	108. egyezmény Az orvosi adatokra vonatkozó ajánlás
		EJEB, *Z. kontra Finnország* (22009/93. sz. ügy), 1997. február 25.
A klinikai vizsgálatokról szóló irányelv	Klinikai vizsgálatok	
Adatvédelmi irányelv, 6. cikk (1) bekezdés b) pont, 13. cikk (2) bekezdés	Statisztikák	108. egyezmény A statisztikai adatokra vonatkozó ajánlás
223/2009/EK rendelet az európai statisztikákról EUB, C-524/06. sz., *Huber kontra Németország* ügy, 2008. december 16.	Hivatalos statisztikák	108. egyezmény A statisztikai adatokra vonatkozó ajánlás

EU	Tárgyalt kérdések	Európa Tanács
2004/39/EK irányelv a pénzügyi eszközök piacairól 648/2012/EU rendelet a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról 1060/2009/EK rendelet a hitelminősítő intézetekről 2007/64/EK irányelv a belső piaci pénzforgalmi szolgáltatásokról	Pénzügyi adatok	108. egyezmény 90(19). számú, a kifizetésekre és más kapcsolódó műveletekre vonatkozó ajánlás EJEB, *Michaud kontra Franciaország* (12323/11), 2012. december 6.

Számos esetben speciális jogi aktusokat fogadtak el európai szinten, amelyek a 108. egyezményben és az adatvédelmi irányelvben foglalt általános szabályokat alkalmazzák részletesebben – konkrét helyzetekre.

8.1. Elektronikus közlések

Főbb pontok

- Az Európa Tanács 1995-ből származó ajánlása a távközlés területén – különös tekintettel a telefonszolgáltatásra – irányadó speciális adatvédelmi szabályokat tartalmaz.
- Az európai szintű kommunikációs szolgáltatásokhoz kapcsolódó személyesadat-feldolgozást az elektronikus hírközlési adatvédelmi irányelv szabályozza.
- Az elektronikus kommunikáció titkossága nemcsak a kommunikáció tartalmára vonatkozik, hanem a forgalmi adatokra is, köztük arra az információra, hogy ki kivel beszélt, mikor és mennyi ideig, valamint a helymeghatározási adatokra, pl. arra, hogy honnan közölték az adatokat.

A távközlési hálózatok fokozottan sérthetik a felhasználók magánszféráját, mivel több technikai lehetőséget nyújtanak az e hálózatokon zajló beszélgetésekbe való belehallgatásra, illetve e beszélgetések megfigyelésére. Következésképpen speciális adatvédelmi rendelkezések bevezetését tartották szükségesnek annak érdekében, hogy kezeljék azokat a kockázatokat, amelyeknek a távközlési szolgáltatásokat igénybe vevők ki vannak téve.

1995-ben az Európa Tanács ajánlást adott ki a távközlés területén az adatvédelemről, különös tekintettel a telefonszolgáltatásra.[289] Ezen ajánlás szerint a személyes adatok távközléssel összefüggésben történő gyűjtését és feldolgozását a következőkre kell korlátozni: a felhasználó bekötése a hálózatba, az adott távközlési szolgáltatás elérhetővé tétele, számlázás, ellenőrzés, a technikai szempontból optimális működés biztosítása, valamint a hálózat- és szolgáltatás-fejlesztés.

Különleges figyelmet szenteltek a távközlési hálózatok közvetlen üzletszerzési célú (direkt marketing) üzenetek küldésére való használatának. Főszabályként direkt marketing üzenet olyan előfizetőhöz nem irányítható, aki kifejezetten kizárta a hirdetési célú üzenetek vételét. Előre felvett, hirdetési célú üzenetek továbbításához automatikus hívásokat lebonyolító eszközök kizárólag akkor használhatók, ha az előfizető ehhez kifejezetten hozzájárult. Az ezen a területen érvényes részletes szabályokat a nemzeti jog állapítja meg.

Ami az **uniós jogi keretet** illeti, az 1997-es első kísérletet követően 2002-ben fogadták el, majd 2009-ben módosították az adatvédelemről és az elektronikus hírközlésről szóló irányelvet *(elektronikus hírközlési adatvédelmi irányelv)* azzal a céllal, hogy a távközlési ágazatra vonatkozóan kiegészítsék és részletesebben meghatározzák az adatvédelmi irányelv rendelkezéseit.[290] Az elektronikus hírközlési adatvédelmi irányelv alkalmazása a nyilvános elektronikus hírközlő hálózatokon nyújtott hírközlési szolgáltatásokra korlátozódik.

Az elektronikus hírközlési adatvédelmi irányelv a kommunikáció során keletkező adatok három fő kategóriáját különbözteti meg:

- a kommunikáció során küldött üzenetek tartalmát alkotó adatok; ezek az adatok szigorúan titkosak;

289 Európa Tanács Miniszteri Bizottsága (1995) (95)4. sz., a tagállamoknak szóló ajánlása a távközlési szolgáltatások területén a személyes adatok védelméről, különös tekintettel a telefonszolgáltatásra, 1995. február 7.

290 Az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv *(„elektronikus hírközlési adatvédelmi irányelv")*, HL L 201., 2002,, módosította az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról szóló, 2009. november 25-i 2009/136/EK európai parlamenti és tanácsi irányelv, HL L 337., 2009.

- a kommunikáció létrehozásához és fenntartásához szükséges adatok, az ún. forgalmi adatok, mint pl. a kommunikációs partnerekre, a kommunikáció időpontjára és időtartamára vonatkozó információk;

- a forgalmi adatokon belül léteznek a kifejezetten a kommunikációs eszköz helyének meghatározására vonatkozó ún. helymeghatározó adatok; ezek az adatok egyidejűleg a kommunikációs eszközök *felhasználóinak* helyéről is adatokat szolgáltatnak, különös tekintettel a mobil kommunikációs eszközök felhasználóira.

A forgalmi adatokat a szolgáltató kizárólag a számlázás és a műszaki szolgáltatásnyújtás céljára használhatja fel. Az érintett hozzájárulásával azonban ezen adatok más, értéknövelt szolgáltatásokat kínáló adatkezelők számára is felfedhetők, mint pl. tájékoztatás a felhasználó helyéhez képest a legközelebbi metróállomásról vagy gyógyszertárról, vagy a felhasználó helye szerinti időjárás-előrejelzésről.

Az elektronikus hírközlési adatvédelmi irányelv 15. cikke szerint az elektronikus hálózatokon történő kommunikációra vonatkozó adatokhoz való egyéb hozzáféréseknek, köztük a bűncselekmény kivizsgálása céljából történő hozzáférésnek, meg kell felelniük az EJEE 8. cikkének (2) bekezdésében rögzített és a Charta 8. és 52. cikkében megerősített, az adatvédelemhez való jog igazolható sérelmére vonatkozó követelményeknek.

Az elektronikus hírközlési adatvédelmi irányelv 2009-et követő módosításai[291] a következőket vezették be:

- A direkt marketing céljából küldött e-mailekre vonatkozó korlátozásokat a rövid szöveges üzenet szolgáltatásokra (SMS), a multimédiás üzenetküldő szolgáltatásokra (MMS) és más hasonló típusú alkalmazásokra is kiterjesztették; marketing célú e-mailek küldése tilos, kivéve, ha beszerezték a címzett előzetes hozzájárulását. Ilyen hozzájárulás nélkül csak korábbi ügyfeleknek szabad marketing célú e-mailt küldeni, ha megadták e-mail-címüket, és nem emelnek kifogást.

291 Az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról, HL L 337., 2009.

- Arra kötelezték a tagállamokat, hogy a nem kívánt közlésekre vonatkozó tilalom megszegésének esetére biztosítsanak bírósági jogorvoslati lehetőséget.[292]

- A számítógép tulajdonosának hozzájárulása nélkül immár nem engedélyezett a sütik (a számítógép-tulajdonos aktivitását nyomon követő és rögzítő szoftver) beállítása. A nemzeti jognak részletesebben is szabályoznia kell, hogyan kell kifejezni és megszerezni a hozzájárulást ahhoz, hogy a védelem megfelelő legyen.[293]

Amennyiben jogosulatlan hozzáférés következtében adatsértés, adatvesztés vagy -megsemmisülés történik, azonnal tájékoztatni kell erről az illetékes felügyelő hatóságot. Az előfizetőket is tájékoztatni kell, hogy az adatsértés következtében káruk keletkezhet.[294]

Az adatmegőrzési irányelv[295] (érvénytelenítve 2014. április 8-án) arra kötelezte a hírközlési szolgáltatókat, hogy a forgalmi adatokat – kifejezetten a súlyos bűncselekmények elleni küzdelem céljából – legalább hat, de legfeljebb 24 hónapig őrizzék meg, függetlenül attól, hogy a szolgáltatónak számlázási célra vagy a szolgáltatás műszaki teljesítéséhez még mindig szüksége van-e ezekre az adatokra.

Az uniós tagállamok független hatóságokat jelölnek ki arra a feladatra, hogy ellenőrizzék a megőrzött adatok biztonságát.

292 Lásd a módosított irányelv 13. cikkét.

293 Lásd uo., 5. cikk; lásd még a 29. cikk szerinti munkacsoport *04/2012. számú, a sütikhez való hozzájárulás alóli mentességről szóló véleményét (2012)*, WP 194, Brüsszel, 2012. június 7.

294 Lásd még a 29. cikk szerinti munkacsoport *01/2011. sz., a személyes adatok sértésére vonatkozó, jelenleg hatályos európai uniós keretről és a jövőbeli szakpolitikai fejleményekkel kapcsolatos ajánlásokról szóló munkadokumentumát*, WP 184, Brüsszel, 2011. április 5.

295 Az Európai Parlament és a Tanács 2006. március 15-i 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról, HL L 105., 2006.

A távközlési adatok megőrzése egyértelműen ellentétes az adatvédelemhez való joggal.[296] Azt, hogy ez a jogba való beavatkozás indokolt-e vagy sem, az uniós tagállamokban lefolytatott [297] számos bírósági eljárás során tárgyalták.

Példák: Az EUB a Digital Rights Írország és Seitlinger és társai egyesített ügyekben[298] kimondta, hogy az Adatmegőrzési Irányelv érvénytelen. A Bíróság szerint az Adatmegőrzési Irányelv széles körben és különösen súlyosan beavatkozik az alapvető jogokba, és nem megfelelően körülhatárolt ahhoz, hogy a beavatkozás ténylegesen a feltétlenül szükséges mértékre korlátozódjon.

Az elektronikus kommunikációval kapcsolatos egyik döntő fontosságú kérdés a hatósági beavatkozás kérdése. A kommunikáció megfigyelésére vagy feltartóztatására szolgáló eszközök, köztük a lehallgató készülékek csak abban az esetben engedhető meg, amennyiben azt törvény írja elő, és egy demokratikus társadalomban az alábbiak érdekében szükséges intézkedésnek minősül: az állam- vagy a közbiztonság, illetve az állam pénzügyi érdekeinek védelme, vagy bűncselekmények visszaszorítása; továbbá az érintett vagy mások jogainak és szabadságainak védelme.

Példa: A *Malone kontra Egyesült Királyság* ügyben[299] a felperest lopott árukkal kapcsolatos orgazdasággal összefüggő több bűncselekményért elítélték. A tárgyalás folyamán felmerült, hogy egy általa folytatott telefonbeszélgetést – belügyminisztériumi államtitkár által kiadott végzés alapján – lehallgattak. Bár a mód, ahogyan a felperes beszélgetését lehallgatták, a hazai jogszabályok értelmében jogszerű volt, az EJEB mégis úgy vélte, hogy az ezen a területen fennálló hatósági mérlegelési jogkör terjedelmére és gyakorlásának módjára vonatkozóan nem voltak jogi előírások, ezért a szóban forgó gyakorlatból fakadó beavatkozás nem „állt összhangban a jogszabályokkal". A Bíróság megállapította, hogy megsértették az EJEE 8. cikkét.

296 Az európai adatvédelmi biztos 2011. május *31-i véleménye a Tanácsnak és az Európai Parlamentnek szóló, az adatvédelmi irányelvre (2006/24/EK irányelv) vonatkozó bizottsági értékelő jelentésről*, 2011. május 31.

297 Németország, Szövetségi Alkotmánybíróság (*Bundesverfassungsgericht*), 1 BvR 256/08. sz. ügy, 2010. március 2.; Románia, Szövetségi Alkotmánybíróság (*Curtea Constituțională a României*), 1258. sz. ügy, 2009. Október 8.; Csehország, Alkotmánybíróság (*Ústavní soud České republiky*), 94/2011. Coll. sz. ügy, 2011. március 22.

298 EUB, C-293/12. és C-594/12. sz., *Digital Rights Írország és Seitlinger és társai* egyesített ügyek, 2014. április 8., 65. pont

299 EJEB, *Malone kontra Egyesült Királyság* (8691/79), 1984. augusztus 2.

8.2. A foglalkoztatási jogviszonnyal kapcsolatos adatok

Főbb pontok

- A foglalkoztatási jogviszonyban fennálló adatvédelemre vonatkozó speciális szabályokat az Európa Tanács foglalkoztatási adatokra vonatkozó ajánlása tartalmazza.
- Az adatvédelmi irányelv a foglalkoztatási jogviszonyokat csak az érzékeny adatok feldolgozásával összefüggésben említi.
- Figyelemmel arra, hogy nincs gazdasági egyensúly a munkáltató és a munkavállalók között, a hozzájárulás – mint a munkavállalói adatok feldolgozásának jogalapja – érvényessége kétséges lehet. A hozzájárulás megadásának körülményeit alaposan meg kell vizsgálni.

Az EU-ban nem létezik a munkaviszonnyal összefüggő adatkezelésre irányadó konkrét jogi keret. Az adatvédelmi irányelv a foglalkoztatási jogviszonyokat konkrétan csak a 8. cikk (2) bekezdésében említi, amely az érzékeny adatokkal foglalkozik. Ami az Európa Tanácsot illeti, a foglalkoztatási adatokra vonatkozó ajánlást 1989-ben adták ki; az ajánlást jelenleg felülvizsgálják.[300]

A foglalkoztatással összefüggő személyes adatok kezeléséhez kapcsolódó leggyakoribb adatvédelmi problémák a 29. cikk szerinti munkacsoport munkadokumentumában találhatók.[301] A munkacsoport elemezte a hozzájárulás, mint adatkezelési jogalap jelentőségét[302] és megállapította, hogy mivel nincs egyensúly a hozzájárulást kérő munkáltató és a hozzájárulást megadó munkavállaló helyzete között, ez gyakran kételyeket vet fel azzal kapcsolatban, hogy a hozzájárulás megadása szabadon történt-e. Ezért a hozzájárulás érvényességének értékelése során gondosan meg kell vizsgálni a körülményeket, amelyek közepette a hozzájárulást kérik.

300 Európa Tanács Miniszteri Bizottsága (1989): (89)2. sz., a tagállamoknak szóló ajánlás a foglalkoztatási célokra felhasznált személyes adatok védelméről, 1989. január 18. Lásd továbbá a 108. egyezmény konzultatív bizottságának „Tanulmány a foglalkoztatási célokra felhasznált személyes adatok védelméről szóló (89)2. sz. ajánlással kapcsolatban, és az említett ajánlás felülvizsgálatával kapcsolatos javaslatok" c. dokumentumot, 2011. szeptember 9.

301 A 29. cikk szerinti munkacsoport (2001) *8/2001. sz. véleménye a foglalkoztatással összefüggő személyes adatok feldolgozásáról*, WP 48, Brüsszel, 2001. szeptember 13.

302 A 29. cikk szerinti munkacsoport (2005): *Munkadokumentum az 1995. október 24-i 95/46/EK irányelv 26. cikke (1) bekezdésének egységes értelmezéséről*, WP 114, Brüsszel, 2005. november 25.

A tipikus mai munkakörnyezetben az egyik szokásos adatvédelmi probléma a munkavállalók munkahelyi elektronikus kommunikációja figyelemmel kísérésének törvényes mértéke. Gyakori állítás, hogy ez a probléma könnyen megoldható azzal, ha megtiltják a munkahelyen lévő kommunikációs eszközök magáncélú használatát. Egy ilyen általános tiltás azonban aránytalan és irreális lehet. Ezzel kapcsolatban az EJEB alábbi ítélete különös jelentőséggel bír:

Példa: A *Copland kontra Egyesült Királyság* ügyben[303] titokban nyomon követték egy szakkollégiumi munkavállaló telefon-, e-mail- és internethasználatát, hogy megbizonyosodjanak arról, a munkavállaló túlzott mértékben személyes célokra használja a kollégiumi infrasturktúrát. Az EJEB megállapította, hogy a munkahelyről lebonyolított telefonhívásokra is vonatkozik a magánélet és a kapcsolattartás fogalma. Ennélfogva a munkahelyről indított ilyen hívások és e-mailek, valamint a személyes internethasználat nyomon követéséből származó információk is oltalomban részesülnek az EJEE 8. cikke alapján. A felperes esetében nem létezett olyan rendelkezés, amely azokat a körülményeket szabályozta volna, amelyek fennállása esetén a munkáltató megfigyelheti a munkavállalók telefon- e-mail- és internethasználatát. A beavatkozás tehát nem felelt meg a jogszabályoknak. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Az Európa Tanács foglalkoztatásra vonatkozó ajánlása szerint a foglalkoztatási célokra gyűjtött személyes adatokat közvetlenül a munkavállalótól kell beszerezni.

A toborzás céljából gyűjtött személyes adatok körét a jelöltek alkalmasságának és karrierlehetőségének értékeléséhez szükséges információkra kell korlátozni.

Az ajánlás kifejezetten említi az egyes munkavállalók teljesítményét vagy lehetőségeit minősítő adatokat. A minősítő adatoknak tisztességes, őszinte értékeléseken kell alapulniuk, és megfogalmazásuk semmiképpen sem lehet sértő. Ezt a tisztességes adatfeldolgozás és az adatok pontosságának elve is megköveteli.

A munkáltató-munkavállaló jogviszonyban az adatvédelmi jog egyik speciális vonatkozása a munkavállalók képviselőinek szerepe. Az ilyen képviselők csak olyan mértékben juthatnak hozzá a munkavállalók személyes adataihoz, amennyire ez a munkavállalók érdekeinek képviseletéhez szükséges.

303 EJEB, *Copland kontra Egyesült Királyság* (62617/00), 2007. április 3.

Foglalkoztatási célokra gyűjtött érzékeny személyes adatok kezelése kizárólag konkrét esetekben, és csakis a nemzeti jog által előírt biztosítékok mellett történhet. A munkáltatók csak akkor kérdezhetik a munkavállalókat vagy a pályázókat egészségi állapotukról, illetve akkor kérhetnek tőlük orvosi vizsgálatot, ha erre a munkára való alkalmasságuk megállapításához, preventív gyógyszer követelményeinek való megfeleléshez vagy szociális ellátások odaítéléséhez van szükség. Egészségügyi adatok az érintett munkavállalón kívüli forrásból nem gyűjthetők, kivéve, ha ehhez megszerezték a munkavállaló kifejezett beleegyező nyilatkozatát, vagy ha az adatgyűjtést nemzeti jogszabály írja elő.

A foglalkoztatásra vonatkozó ajánlás értelmében a munkavállalókat tájékoztatni kell személyes adataik feldolgozásának céljáról, a tárolt személyes adatok típusáról, azon jogalanyokról, akikkel az adatokat rendszeresen közlik, valamint e közlések céljáról és jogalapjáról. Ezen felül a munkáltatóknak előre tájékoztatniuk kell alkalmazottaikat, ha az alkalmazottak személyes adatainak feldolgozására, illetve mozgásuk vagy termelékenységük ellenőrzésére automatizált rendszert vezetnek be vagy alkalmaznak.

A munkavállalóknak hozzáférési joggal kell rendelkezniük a foglalkoztatási adataikhoz, továbbá a helyesbítés vagy törlés jogával is rendelkezniük kell. Minősítő adatok feldolgozása esetén a munkavállalóknak a minősítés vitatására is jogosultnak kell lenniük. E jogok azonban – belső vizsgálat céljára – ideiglenesen korlátozhatók. Ha egy munkavállalótól megtagadják a foglalkoztatáshoz kapcsolódó személyes adataihoz való hozzáférést, ezen adatok helyesbítését vagy törlését, nemzeti jogszabálynak kell rendelkeznie a megfelelő eljárásról, amelynek keretében az elutasító határozat vitatható.

8.3. Orvosi adatok

Fő pont

- Az orvosi adatok különleges adatok, ezért speciális védelmet élveznek.

Az érintett egészségi állapotára vonatkozó személyes adatok az adatvédelmi irányelv 8. cikkének (1) bekezdése és a 108. egyezmény 6. cikke értelmében érzékeny adatnak minősülnek. Az orvosi adatok ennélfogva a nem érzékeny adatoknál szigorúbb adatvédelmi rendszer alá tartoznak.

Példa: A *Z. kontra Finnország* ügyben[304] a felperes volt férje, aki HIV-fertőzött, több szexuális bűncselekményt követett el. Elítélték emberölésért azon az alapon, hogy szándékosan tette ki áldozatait a HIV-fertőzés kockázatának. A nemzeti bíróság az ítélet teljes egészét és az ügy dokumentumait 10 évre titkosította annak ellenére, hogy a felperes hosszabb titkosítási időszakot kért. Ezeket a kérelmeket a fellebbviteli bíróság elutasította, és ítélete a felperes és volt férje teljes nevét is tartalmazta. Az EJEB megállapította, hogy a beavatkozás nem minősül egy demokratikus társadalomban szükségesnek, mert az orvosi adatok védelme a magánélet és a családi élet tiszteletben tartásához való jog gyakorlása szempontjából alapvető fontosságú, különösen ha HIV-fertőzésre vonatkozó információkról van szó – tekintetbe véve, hogy számos társadalomban ehhez az állapothoz megbélyegzés kapcsolódik. Ezért a Bíróság arra a következtetésre jutott, hogy az, hogy a fellebbviteli bíróság ítéletében mindösszesze tíz évvel az ítélet kihirdetését követően megadja a hozzáférést a felperes személyazonosságához és egészségügyi állapotához, sérti az EJEE 8. cikkét.

Az adatvédelmi irányelv 8. cikkének (3) bekezdése engedélyezi orvosi adatok kezelését, amennyiben az megelőző egészségügyi, orvosi diagnosztikai célból, gondozás vagy egészségügyi szolgáltatások igazgatása céljából szükséges. A kezelés azonban kizárólag akkor engedélyezhető, ha egészségügyi szakember végzi szakmai titoktartási kötelezettség mellett, vagy más személy végzi, akit ezzel egyenértékű kötelezettség terhel.[305]

Az Európa Tanács 1997-es, orvosi adatokra vonatkozó ajánlása részletesebben is alkalmazza az egészségügyi területen végzett adatkezelésre a 108. egyezményben foglalt elveket.[306] A tervezett szabályok összhangban állnak az adatvédelmi irányelvnek az orvosi adatok törvényes célokra való feldolgozásával, az egészségügyi adatokat felhasználó személyek szükséges szakmai titoktartási kötelezettségével, valamint az érintettek átláthatósághoz, hozzáféréshez, helyesbítéshez és törléshez való jogával kapcsolatos rendelkezéseivel. Ezen kívül az egészségügyi szakemberek által törvényesen feldolgozott orvosi adatok bűnüldöző hatóságok részére is továbbíthatók, amennyiben „megfelelő biztosítékok" állnak rendelkezésre „az EJEE

304 EJEB, 22009/93. sz. *Z. kontra Finnország* ügy, 1997. február 25., 94. és 112. pont; lásd még EJEB, 20837/92. sz. *M.S. kontra Svédország* ügy, 1997. augusztus 27.; EJEB, 7508/02. sz. *L.L. kontra Franciaország* ügy, 2006. október 10.; EJEB, 20511/03. sz. *I. kontra Finnország* ügy, 2008. július 17.; EJEB, 32881/04. sz. *K.H. és társai kontra Szlovákia* ügy, 2009. április 28.; EJEB, 36936/05. sz. *Szuluk kontra Egyesült Királyság* ügy, 2009. június 2.

305 Lásd még EJEB, *Biriuk kontra Litvánia* (23373/03), 2008. november 25.

306 Az Európa Tanács Miniszteri Bizottságának a tagállamoknak szóló Rec(97)5. sz. ajánlása az orvosi adatok védelméről, 1997. február 13.

8. cikkében garantált [...] magánélet tiszteletben tartásához való joggal össze nem egyeztethető közlések megakadályozására".[307]

Az orvosi adatokra vonatkozó ajánlás a születendő gyermekek és korlátozottan cselekvőképes vagy cselekvőképtelen személyek orvosi adataira, valamint a genetikai adatok feldolgozására vonatkozóan speciális rendelkezéseket is tartalmaz. A tudományos kutatást kifejezetten elismerik az adatok szükségesnél hosszabb ideig való megőrzésének indokául, bár ehhez általában anonimizálás szükséges. Az orvosi adatokra vonatkozó ajánlás 12. cikke részletes szabályokat javasol olyan helyzetekre, amikor a kutatóknak személyes adatokra van szükségük, és az anonimizált adatok nem elegendőek.

Az álnéven kezelés megfelelő lehet a tudományos igények kielégítésére, ugyanakkor az érintett betegek érdekeit is megvédi. Az adatvédelemmel összefüggésben az adatok álnéven való kezelésének koncepcióját a *2.1.3.* szakaszban részletesebben is kifejtjük.

Nemzeti és európai szinten intenzív vitát folytattak le a beteg orvosi kezelésére vonatkozó adatainak elektronikus fájlban való tárolására irányuló kezdeményezésekről.[308] Az egészségügyi elektronikus fájlok nemzeti szintű rendszerei kiépítésének egyik speciális vonatkozása a szóban forgó rendszerek országhatárokon túli elérhetősége: ez az EU-ban a határokon átnyúló egészségügyi ellátással összefüggésben egyike a különös érdeklődésre számot tartó kérdéseknek.[309]

Az új rendelkezésekkel kapcsolatos vita egy másik területen, a klinikai vizsgálatok kapcsán is folyik, ami új gyógyszerek kutatási környezetben dokumentált, betegeken történő kipróbálását jelenti; ennek a témakörnek is jelentős adatvédelmi vonatkozásai vannak. Az emberi felhasználásra szánt gyógyszerekkel végzett klinikai vizsgálatokat az emberi felhasználásra szánt gyógyszerekkel végzett klinikai vizsgálatok során alkalmazandó helyes klinikai gyakorlat bevezetésére vonatkozó tagállami törvényi, rendeleti és közigazgatási rendelkezések közelítéséről szóló, 2001. április 4-i 2001/20/EK európai parlamenti és tanácsi irányelv *(klinikai*

307 EJEB, *Avilkina és társai kontra Oroszország* (1585/09), 2013. június 6., 53. pont (nem végleges).

308 29. cikk szerinti munkacsoportnak *az elektronikus egészségügyi nyilvántartásban tárolt, egészségi állapotra vonatkozó személyes adatok feldolgozásáról szóló munkadokumentuma (2007)*, WP 131., Brüsszel, 2007. február 15.

309 Az Európai Parlament és a Tanács 2011. október 25-i 2011/24/EU irányelve a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről, HL L 88., 2011.

vizsgálatokról szóló irányelv) szabályozza.[310] 2012 decemberében az Európai Bizottság a klinikai vizsgálatokról szóló irányelv helyébe lépő rendeletre irányuló javaslatot terjesztett elő, amelynek célja a klinikai vizsgálati eljárások egységesebbé és hatékonyabbá tétele.[311]

Az egészségügyi ágazatban a személyes adatokkal kapcsolatban uniós szinten számos más jogalkotási és egyéb kezdeményezés is folyamatban van.[312]

8.4. Statisztikai célú adatfeldolgozás

Főbb pontok

- A statisztikai célokra gyűjtött adatok semmilyen más célra nem használhatók fel.
- A bármilyen célra törvényesen gyűjtött adatok statisztikai célokra tovább hasznosíthatók, amennyiben a nemzeti jog megfelelő biztosítékokat ír elő, amelyeket a felhasználók betartanak. Erre a célra különösen a harmadik feleknek történő továbbítást megelőző anonimizálást vagy pszeudoanonimizálást kell előirányozni.

Az adatvédelmi irányelv a statisztikai célú adatfeldolgozást az adatvédelmi elvek alóli lehetséges kivételekkel összefüggésben említi. Az irányelv 6. cikke (1) bekezdésének b) pontjában a célhoz kötöttség elvétől nemzeti jogszabály alapján el lehet térni az adatok statisztikai célokra történő további feldolgozása érdekében, bár a nemzeti jogszabálynak biztosítania kell a megfelelő garanciákat. Az irányelv 13. cikkének (2) bekezdése közvetlenül engedélyezi a hozzáférési jogok nemzeti jogszabály általi korlátozását, ha az adatok feldolgozása kizárólag statisztikai célból történik; a nemzeti jogban ebben az esetben is léteznie kell a megfelelő garanciáknak. Ezzel összefüggésben az adatvédelmi irányelv azt az egyedi követelményt írja elő, hogy a statisztikai kutatás során megszerzett vagy létrejött egyetlen adat sem használható fel az érintettekre vonatkozó konkrét döntésekhez.

310 Az Európai Parlamenti és a Tanács 2001. április 4-i 2001/20/EK irányelve az emberi felhasználásra szánt gyógyszerekkel végzett klinikai vizsgálatok során alkalmazandó helyes klinikai gyakorlat bevezetésére vonatkozó tagállami törvényi, rendeleti és közigazgatási rendelkezések közelítéséről, 2001, HL L 121.

311 Európai Bizottság (2012): Európai parlamenti és tanácsi rendeletre irányuló javaslat az emberi felhasználásra szánt gyógyszerek klinikai vizsgálatairól és a 2001/20/EK irányelv hatályon kívül helyezéséről, COM(2012) 369, Brüsszel, 2012. július 17.

312 Európai adatvédelmi biztos (2013): Az európai adatvédelmi biztos véleménye az "E-egészségügyi cselekvési terv 2012-2020 – innovatív egészségügyi ellátás a 21. században" című bizottsági közleményről, Brüsszel, 2013. március 27.

Bár az adatkezelő által bármilyen célra törvényesen gyűjtött adatokat az adott adatkezelő a saját statisztikai céljaira ismételten felhasználhatja (ún. másodlagos statisztikák), mielőtt az adatokat statisztikai célokra harmadik félnek továbbítja, a tartalomtól függően anonimizálni vagy pszeudoanonimizálni kell azokat, kivéve, ha az érintett a továbbításhoz hozzájárult, vagy a továbbítást nemzeti jogszabály kifejezetten előírja. Ez az adatvédelmi irányelv 6. cikke (1) bekezdésének b) pontja szerinti megfelelő biztosítékok követelményéből következik.

Az adatok statisztikai célokra való felhasználásának legfontosabb esetei a nemzeti és uniós statisztikai hivatalok által a hivatalos statisztikákról szóló nemzeti és uniós jogszabályok alapján készített hivatalos statisztikák. E jogszabályok szerint a polgárok és a vállalkozások általában kötelesek adatokat közölni a statisztikai hatóságokkal. A statisztikai hivatalokban dolgozó tisztviselőkre speciális szakmai titoktartási kötelezettségek vonatkoznak, amelyeket gondosan be kell tartani, mivel a polgároknak a statisztikai hatóságok részére történő kötelező adatszolgáltatásba vetett bizalma szempontjából alapvető fontosságúak.

Az európai statisztikákról szóló 223/2009/EK rendelet *(európai statisztikákról szóló rendelet)* a hivatalos statisztikákra vonatkozó alapvető adatvédelmi szabályokat tartalmazza, ezért a nemzeti szintű hivatalos statisztikákra vonatkozó rendelkezések tekintetében is relevánsnak tekinthető.[313] A rendelet fenntartja az elvet, miszerint a hivatalos statisztikai műveletekhez kellően pontos jogalap szükséges.[314]

Példa: A *Huber kontra Németország* ügyben[315] az EUB megállapította, hogy személyes adatok hatóság általi, statisztikai célokra való gyűjtése és tárolása önmagában nem elegendő indok ahhoz, hogy az adatkezelés törvényes legyen. A vonatkozó jogszabálynak a szükségesség követelményének is meg kellett felelnie, ami a konkrét esetben nem teljesült.

313 Az Európai Parlament és a Tanács 2009. március 11-i 223/2009/EK rendelete az európai statisztikákról és a titoktartási kötelezettség hatálya alá tartozó statisztikai adatoknak az Európai Közösségek Statisztikai Hivatala részére történő továbbításáról szóló 1101/2008/EK, Euratom európai parlamenti és tanácsi rendelet, a közösségi statisztikákról szóló 322/97/EK tanácsi rendelet és az Európai Közösségek statisztikai programbizottságának létrehozásáról szóló 89/382/EGK, Euratom tanácsi határozat hatályon kívül helyezéséről, 2009, HL L 87.

314 Ezt az elvet az Eurostat gyakorlati kódexe részletesebben is kifejti, amely az európai statisztikákról szóló rendelet 11. cikkével összhangban etikai iránymutatást ad a hivatalos statisztikák elkészítésének módjára vonatkozóan, a személyes adatok körültekintő használatát is beleértve; elérhető a következő címen: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 EUB, C-524/06. sz., *Huber kontra Németország* ügy, 2008. december 16., különösen a 68. pont.

Ami az Európa Tanácsot illeti, az 1997-ben kiadott, statisztikai adatokra vonatkozó ajánlás vonatkozik a közszférában és a magánszektorban a statisztikák készítésére.[316] Ez az ajánlás olyan elveket vezetett be, amelyek egybeesnek az adatvédelmi irányelv fent leírt főbb szabályaival. Az alábbi kérdésekkel kapcsolatban az ajánlás részletesebb szabályokat is megállapít.

Míg az adatkezelő által statisztikai célokra gyűjtött adatok semmilyen más célra nem használhatók fel, a nem statisztikai célokra gyűjtött adatokat további statisztikai felhasználásra rendelkezésre kell bocsátani. A statisztikai adatokra vonatkozó ajánlás még az adatok harmadik felekkel való közlését is megengedi, ha ez kizárólag statisztikai célokra történik. Ilyen esetben a feleknek meg kell állapodniuk, és írásban rögzíteniük kell a statisztikai célú további törvényes felhasználás mértékét. Mivel ez nem helyettesítheti az érintett hozzájárulását, feltételezhető, hogy a személyes adatokkal való visszaélés kockázatainak minimalizálása érdekében nemzeti jogszabályban előírt további megfelelő garanciákra – például az adatok továbbítás előtti anonimizálására vagy álnevesítésére irányuló kötelezettségre – van szükség.

A hivatásszerűen statisztikai kutatással foglalkozó szakembereket a nemzeti jog szerint szakmai titoktartási kötelezettségnek kell terhelnie, ami a hivatalos statisztikák esetében szokásos. A titoktartásnak a kérdezőkre is ki kell terjednie, ha az érintettektől vagy más személyektől való adatgyűjtés a munkaköri kötelezettségük.

Ha a személyes adatok felhasználásával készített statisztikai felmérést nem jogszabály írja elő, ahhoz, hogy a felmérés törvényes legyen, az érintetteknek hozzá kellene járulniuk adataik felhasználásához, vagy legalább lehetőséget kellene biztosítani számukra a tiltakozásra. Ha kérdezők statisztikai célokra gyűjtenek személyes adatokat, egyértelműen tájékoztatni kell őket arról, hogy a nemzeti jog értelmében az adatok közlése kötelező-e vagy sem. Érzékeny adatokat soha nem szabad olyan módon gyűjteni, hogy a magánszemély azonosítható legyen, kivéve, ha ezt nemzeti jogszabály kifejezetten lehetővé teszi.

Ha a statisztikai felmérés anonim adatokkal nem végezhető el, és valóban szükség van személyes adatokra, az e célra gyűjtött adatokat a lehető leghamarabb anonimizálni kell. A statisztikai felmérés eredményei alapján az érintettek nem lehetnek azonosíthatók, kivéve, ha ez nyilvánvalóan semmiféle kockázatot nem jelentene.

316 Az Európa Tanács Miniszteri Bizottságának a tagállamoknak szóló Rec(97)18. sz. ajánlása a statisztikai célokra gyűjtött és feldolgozott személyes adatok védelméről, 1997. szeptember 30.

A statisztikai elemzés lezárását követően a felhasznált személyes adatokat törölni vagy anonimizálni kell. Ebben az esetben a statisztikai adatokra vonatkozó ajánlás azt javasolja, hogy az azonosító adatokat más személyes adatoktól elkülönítve kell tárolni. Ez azt jelenti, például hogy az adatokat álnevesíteni kell, és a titkosítási kulcsot, illetve az azonosító szinonimákat tartalmazó listát az álnevesített adatoktól elkülönítve kell tárolni.

8.5. Pénzügyi adatok

Főbb pontok

- Bár a pénzügyi adatok nem a 108. egyezmény vagy az adatvédelmi irányelv értelmében vett érzékeny adatok, kezelésük – a pontosság és az adatbiztonság szavatolása érdekében – különleges garanciákat igényel.
- Az elektronikus pénzforgalmi rendszerek esetében a rendszerbe eleve betervezett adatvédelem, az ún. beépített adatvédelem szükséges.
- Ezen a területen speciális adatvédelmi problémák merülnek fel a megfelelő hitelesítési mechanizmusok meglétének igényéből fakadóan.

Példa: A *Michaud kontra Franciaország* ügyben[317] a felperes, egy francia ügyvéd, vitatta a francia jog alapján fennálló azon kötelezettségét, hogy be kell jelentenie ügyfelei lehetséges pénzmosási tevékenységével kapcsolatos gyanúját. Az EJEB megállapította, hogy az ügyvédek arra való kötelezése, hogy jelentsenek olyan információkat a közigazgatási hatóságoknak egy másik személyről, amelyek a szóban forgó személlyel való információcsere során kerültek a birtokukba, beavatkozásnak minősül az ügyvéd – az EJEE 8. cikke alapján fennálló –kapcsolattartási jogának és magánéletének tiszteletben tartásához való jogába, mivel e fogalomba a szakmai vagy üzleti jellegű tevékenységek is beletartoznak. A beavatkozás azonban megfelelt a jogszabályoknak, és törvényes célt szolgált – nevezetesen a zavargás vagy bűncselekmény megelőzését. Mivel az ügyvédek csupán igen korlátozott körülmények fennállása esetén voltak kötelesek a gyanú bejelentésére, az EJEB megállapította, hogy ez

317 EJEB, 12323/11. sz. *Michaud kontra Franciaország* ügy, 2012. december 6.; lásd még EJEB, 13710/88. sz. *Niemietz kontra Németország* ügy, 1992. december 16., 29. pont, és EJEB, 20605/92. sz. *Halford kontra Egyesült Királyság* ügy, 1997. június 25., 42. pont.

a kötelezettség arányos, és arra a következtetésre jutott, hogy nem sértették meg a 8. cikket.

A 108. egyezményben foglalt általános adatvédelmi keretnek a pénzforgalommal összefüggésben történő alkalmazását az Európa Tanács 1990-es, (90)19. sz. ajánlásában dolgozták ki.[318] Ez az ajánlás a kifizetésekkel – különösen a bankkártyás fizetésekkel – összefüggésben pontosítja a törvényes adatgyűjtés és -felhasználás terjedelmét. Részletes szabályokat javasol továbbá a belföldi jogalkotóknak a fizetési adatok harmadik felekkel való közlésének határaira, az adatok megőrzésének időbeli korlátaira, az átláthatóságra, az adatbiztonságra és az országhatárokat átlépő adatáramlásra, valamint a felügyeletre és a jogorvoslatokra vonatkozóan. A javasolt megoldások megfelelnek a később az adatvédelmi irányelvben szereplő általános uniós adatvédelmi keretnek.

Számos jogi aktus van születőben a pénzügyi eszközök piacainak, valamint a hitelintézetek és a befektetési cégek tevékenységének szabályozására.[319] Más jogi aktusok a bennfentes kereskedelem és a piaci manipuláció elleni küzdelemhez nyújtanak segítséget.[320] Az említett területeken az adatvédelmet érintő legkritikusabb kérdések a következők:

- a pénzügyi tranzakciókra vonatkozó nyilvántartások megőrzése;
- személyes adatok harmadik országokba történő továbbítása;

318 Az Európa Tanács Miniszteri Bizottsága (1990) (90)19. sz. ajánlása a fizetéshez és más kapcsolódó műveletekhez használt személyes adatok védelméről, 1990. szeptember 13.

319 Európai Bizottság (2011): Európai parlamenti és tanácsi irányelvre irányuló javaslat a pénzügyi eszközök piacairól és a 2004/39/EK európai parlamenti és tanácsi irányelv hatályon kívül helyezéséről, COM(2011) 656, Brüsszel, 2011. október 20.; Európai Bizottság (2011): Európai parlamenti és tanácsi rendeletre irányuló javaslat a pénzügyi eszközök piacairól és a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról szóló [EMIR] rendelet módosításáról, COM(2011) 652, Brüsszel, 2011. október 20.; Európai Bizottság (2011): Európai parlamenti és tanácsi irányelvre irányuló javaslat a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek és befektetési vállalkozások prudenciális felügyeletéről, valamint a pénzügyi konglomerátumhoz tartozó hitelintézetek, biztosítóintézetek és befektetési vállalkozások kiegészítő felügyeletéről szóló 2002/87/EK európai parlamenti és tanácsi irányelv módosításáról, COM(2011) 453, Brüsszel, 2011. július 20.

320 Európai Bizottság (2011): Európai parlamenti és tanácsi rendeletre irányuló javaslat a bennfentes kereskedelemről és a piaci manipulációról (piaci visszaélés), COM(2011) 651, Brüsszel, 2011. október 20.; Európai Bizottság (2011): Európai parlamenti és tanácsi irányelvre irányuló javaslat a bennfentes kereskedelem és a piaci manipuláció büntetőjogi szankcióiról, COM(2011) 654, Brüsszel, 2011. október 20.

- telefonbeszélgetés vagy elektronikus kommunikáció felvétele, beleértve az illetékes hatóságok azon jogkörét, hogy telefon- és adatforgalmi nyilvántartásokat kérjenek;

- személyes információk közlése, a szankciók közzétételét is beleértve;

- az illetékes hatóságok felügyeleti és nyomozati hatásköre, a helyszíni szemlét és a dokumentumok lefoglalása céljából magánterületre való belépést is beleértve;

- jogsértések bejelentésére vonatkozó mechanizmusok, azaz visszaélés-jelentési rendszerek; és

- együttműködés az illetékes tagállami hatóságok és az Európai Értékpapír-piaci Hatóság között.

Vannak ezeken a területeken más kérdések is, amelyekkel jelenleg foglalkoznak, például az érintettek pénzügyi helyzetére vonatkozó adatok gyűjtése[321] vagy a banki átutalásokon keresztül történő, országhatárokat átlépő fizetés kérdése, amely elkerülhetetlenül személyes adatok áramlásához vezet.[322]

321 Az Európai Parlament és a Tanács 2009. szeptember 16-i 1060/2009/EK rendelete a hitelminősítő intézetekről, 2009, HL L 302.; Az Európai Bizottság európai parlamenti és tanácsi rendeletre irányuló javaslata a hitelminősítő intézetekről szóló 1060/2009/EK rendelet módosításáról, COM(2010) 289, Brüsszel, 2010. június 2.

322 Az Európai Parlament és a Tanács 2007. november 3-i 2007/64/EK irányelve a belső piaci pénzforgalmi szolgáltatásokról és a 97/7/EK, a 2002/65/EK, a 2005/60/EK és a 2006/48/EK irányelv módosításáról és a 97/5/EK irányelv hatályon kívül helyezéséről, 2007, HL L 319.

Irodalomjegyzék

1. fejezet

Araceli Mangas, M. (szerk.) (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*, Bécs, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi: *An introduction to data protection (Bevezetés az adatvédelembe)*, Brüsszel, elérhető a következő címen: www.edri.org/files/paper06_datap.pdf.

Frowein, J. és Peukert, W. (2009): *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. és Pabel, K. (2012): *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Harris, D.J., O'Boyle, M., Warbick, C. és Bates, E. (2009): *Law of the European Convention on Human Rights* [Az emberi jogok európai egyezményének joga], 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* [Jogesetek, anyagok és kommentár az emberi jogok európai egyezményéhez], Oxford, Oxford University Press.

Nowak, M., Januszewski, K. és Hofstätter, T. (2012): *All human rights for all – Vienna manual on human rights* [Az összes emberi jogot mindenkinek – Bécsi emberi jogi kézikönyv], Antwerpen, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. és Coutron, L. (2010) : *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brüsszel, Emile Bruylant.

Simitis, S. (1997): 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, 5. szám, 281–288. o.

Warren, S. és Brandeis, L. (1890): 'The right to privacy' [A magánélethez való jog], *Harvard Law Review,* 4. évf., 5. szám, 193–220. o., elérhető a következő címen: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. és Ovey, C. (2010): *The European Convention on Human Rights* [Az emberi jogok európai egyezménye], Oxford, Oxford University Press.

2. fejezet

Carey, P. (2009): *Data protection: A practical guide to UK and EU law* [Adatvédelem: gyakorlati útmutató az Egyesült Királyság és az EU jogához], 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*, Párizs, LexisNexis.

Di Martino, A. (2005): *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. és Boardman, R. (2012): *Data protection strategy: Implementing data protection compliance*, [Adatvédelmi stratégia: az adatvédelmi megfelelőség végrehajtása], London, Sweet & Maxwell.

Ohm, P. (2010): 'Broken promises of privacy: Responding to the surprising failure of anonymization' [Be nem váltott adatvédelmi ígéretek: válasz a névtelenítés meglepő sikertelenségére], *UCLA Law Review*, 57. évf., 6. szám, 1701–1777. o.

Tinnefeld, M., Buchner, B. és 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* [Névtelenítés: az adatvédelmi kockázat kezelése. Gyakorlati útmutató], elérhető a következő címen: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

3–5. fejezet

Brühann, U. (2012): 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. és Nettesheim, M. (szerk.), *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. és Simitis, S. (1997): *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (az Európai Unió Alapjogi Ügynöksége) (2010): *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)* [Adatvédelem az Európai Unióban: a nemzeti adatvédelmi hatóságok szerepe (Az alapjogi szerkezet erősítése az EU-ban II.)], Luxemburg, Az Európai Unió Kiadóhivatala (Kiadóhivatal).

FRA (2010): *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* [A gyermek jogainak az Európai Unióban történő védelmét, tiszteletben tartását és előmozdítását mérő mutatók kidolgozása] (konferencia-kiadás), Bécs, FRA.

FRA (2011): *Access to justice in Europe: an overview of challenges and opportunities* [Az igazságszolgáltatáshoz való hozzáférés Európában: a problémák és a lehetőségek áttekintése], Luxemburg, Kiadóhivatal.

Simitis, S. (2011): *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office: *Privacy Impact Assessment* [Adatvédelmi hatásvizsgálat], elérhető a következő címen: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

6. fejezet

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. és Nouwt, S. (2009): *Reinventing data protection?*, [Az adatvédelem megújítása], Berlin, Springer.

Kuner, C. (2007): *European data protection law* [Európai adatvédelmi jog], Oxford, Oxford University Press.

Kuner, C. (2013): *Transborder data flow regulation and data privacy law* [A határokon átnyúló adatáramlás szabályozása és az adatvédeli jog], Oxford, Oxford University Press.

7. fejezet

Europol (2012): *Data Protection at Europol* [Adatvédelem az Europolnál], Luxemburg, Kiadóhivatal, elérhető a következő címen: 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* [Adatvédelem az Eurojustnál: erős, hatékony és testre szabott rendszer], Hága, Eurojust.

Drewer, D., Ellermann, J. (2012): *Europol's data protection framework as an asset in the fight against cybercrime* [Az Europol adatvédelmi kerete mint a számítástechnikai bűnözés elleni küzdelem egyik eszköze], ERA Forum, 13. évf., 3. szám, 381–395. o.

Gutwirth, S., Poullet, Y. és De Hert, P. (2010): *Data protection in a profiled world* [Adatvédelem egy profilírozott világban], Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. és Leenes, R. (2011): *Computers, privacy and data protection: An element of choice* [Számítógépek, a magánélet védelme és adatvédelem: választási lehetőség], Dordrecht, Springer.

Konstadinides, T. (2011): *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem* [A demokrácia lerombolása a demokrácia megvédése címén? Az adatmegőrzési irányelv, a rendőrállam és alkotmányos ökoszisztémánk], *European Law Review*, 36. évf., 5. szám, 722–776. o.

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* [Az Európai Parlament szerepe a személyes adatok továbbításáról szóló transzatlanti szerződések megkötésében Lisszabon után], Centre for the Law of External Relations, CLEER 2013/2. sz. munkadokumentuma, elérhető a következő címen: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

8. fejezet

Büllesbach, A., Gijrath, S., Poullet, Y. és Hacon, R. (2010): *Concise European IT law* [Európai informatikai jog – összefoglaló], Amszterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. és Poullet, Y. (2012): *European data protection: In good health?*, [Egészséges európai adatvédelem?], Dordrecht, Springer.

Gutwirth, S., Poullet, Y. és De Hert, P. (2010): *Data protection in a profiled world* [Adatvédelem egy profilírozott világban], Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. és Leenes, R. (2011): *Computers, privacy and data protection: An element of choice* [Számítógépek, a magánélet védelme és adatvédelem: választási lehetőség], Dordrecht, Springer.

Konstadinides, T. (2011): Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem [A demokrácia lerombolása a demokrácia megvédése címén? Az adatmegőrzési irányelv, a rendőrállam és alkotmányos ökoszisztémánk], *European Law Review*, 36. évf., 5. szám, 722–776. o.

Rosemary, J. és Hamilton, A. (2012): *Data protection law and practice* [Adatvédelmi jog és gyakorlat], London, Sweet & Maxwell.

Ítélkezési gyakorlat

Az Emberi Jogok Európai Bíróságának válogatott jogesetei

Személyes adatokhoz való hozzáférés

10454/83. sz. *Gaskin kontra Egyesült Királyság* ügy, 1989. július 7.
33783/09. sz. *Godelli kontra Olaszország* ügy, 2012. szeptember 25.
32881/04. sz. *K.H. és társai kontra Szlovákia* ügy, 2009. április 28.
9248/81. sz. *Leander kontra Svédország* ügy, 1987. március 26.
42326/98. sz. *Odièvre kontra Franciaország* ügy [nagytanács], 2003. február 13.

Az adatvédelem és a véleménynyilvánítás szabadsága közötti egyensúly megteremtése

39954/08. sz. *Axel Springer AG kontra Németország* ügy [nagytanács], 2012. február 7.
59320/00. sz. *Von Hannover kontra Németország* ügy, 2004. június 24.
40660/08. és 60641/08. sz. *Von Hannover kontra Németország* egyesített ügyek [nagytanács], 2012. február 7.

Kihívások az online adatvédelem terén

2872/02. sz. *K.U. kontra Finnország* ügy, 2008. december 2.

Kapcsolattartás

27798/95. sz. *Amann kontra Svájc* ügy [nagytanács], 2000. február 16.
24117/08. sz. *Bernh Larsen Holding AS és társai kontra Norvégia* ügy, 2013. március 14.
22427/04. sz. *Cemalettin Canli kontra Törökország* ügy, 2008. november 18.
964/07. sz. *Dalea kontra Franciaország* ügy, 2010. február 2.
10454/83. sz. *Gaskin kontra Egyesült Királyság* ügy, 1989. július 7.
21737/03. sz. *Haralambie kontra Románia* ügy, 2009. október 27.
16188/07. sz. *Khelili kontra Svájc* ügy, 2011. október 18.
9248/81. sz. *Leander kontra Svédország* ügy, 1987. március 26.
8691/79. sz. *Malone kontra Egyesült Királyság* ügy, 1984. augusztus 2.
16424/90. sz. *McMichael kontra Egyesült Királyság* ügy, 1995. február 24.
39393/98. sz. *M. G. kontra Egyesült Királyság* ügy, 2002. szeptember 24.
28341/95. sz. *Rotaru kontra Románia* [nagytanács] ügy, 2000. május 4.
30562/04. és 30566/04. sz. *S. és Marper kontra Egyesült Királyság* ügyek, 2008. december 4.
30194/09. sz. *Shimovolos kontra Oroszország* ügy, 2011. június 21.
57986/00. sz. *Turek kontra Szlovákia* ügy, 2006. február 14.

Bűnügyi nyilvántartási adatbázisok

5335/06. sz. *B. B. kontra Franciaország* ügy, 2009. december 17.
24029/07. sz. *M. M. kontra Egyesült Királyság* ügy, 2012. november 13.

DNS-adatbázisok

30562/04. és 30566/04. sz. *S. és Marper kontra Egyesült Királyság* ügyek, 2008. december 4.

GPS-adatok

35623/05. sz. *Uzun kontra Németország* ügy, 2010. szeptember 2.

Egészségügyi adatok

Biriuk kontra Litvánia ügy 23373/03, 2008. november 25.
20511/03. sz. *I. kontra Finnország* ügy, 2008. július 17.
7508/02. sz. *L.L. kontra Franciaország* ügy, 2006. október 10.
34209/96. sz. *M.S. kontra Svédország* ügy, 2002. július 2.
36936/05. sz. *Szuluk kontra Egyesült Királyság* ügy, 2009. június 2.

22009/93. sz. *Z. kontra Finnország* ügy, 1997. február 25.

Személyazonosság

27138/04. sz. *Ciubotaru kontra Moldova* ügy, 2010. április 27.
33783/09. sz. *Godelli kontra Olaszország* ügy, 2012. szeptember 25.
42326/98. sz. *Odièvre kontra Franciaország* ügy [nagytanács], 2003. február 13.

Szakmai tevékenységgel kapcsolatos információk

12323/11. sz. *Michaud kontra Franciaország* ügy, 2012. december 6.
13710/88. sz. *Niemietz kontra Németország* ügy, 1992. december 16.

Beszélgetések lehallgatása

27798/95. sz. *Amann kontra Svájc* ügy [nagytanács], 2000. február 16.
62617/00. sz. *Copland kontra Egyesült Királyság* ügy, 2007. április 3.
38565/97. sz. *Cotlet kontra Románia* ügy, 2003. június 3.
11801/85. sz. *Kruslin kontra Franciaország* ügy, 1990. április 24.
23618/94. sz. *Lambert kontra Franciaország* ügy, 1998. augusztus 24.
58243/00. sz. *Liberty és társai kontra Egyesült Királyság* ügy, 2008. július 1.
8691/79. sz. *Malone kontra Egyesült Királyság* ügy, 1984. augusztus 2.
20605/92. sz. *Halford kontra Egyesült Királyság* ügy, 1997. június 25.
36936/05. sz. *Szuluk kontra Egyesült Királyság* ügy, 2009. június 2.

A jogalanyok kötelezettségei

5335/06. sz. *B. B. kontra Franciaország* ügy, 2009. december 17.
20511/03. sz. *I. kontra Finnország* ügy, 2008. július 17.
48009/08. sz. *Mosley kontra Egyesült Királyság* ügy, 2011. május 10.

Fényképek

50774/99. sz. *Sciacca kontra Olaszország* ügy, 2005. január 11.
59320/00. sz. *Von Hannover kontra Németország* ügy, 2004. június 24.

A személyes adatok tárolásának megszüntetéséhez való jog

62332/00. sz. *Segerstedt-Wiberg és társai kontra Svédország* ügy, 2006. június 6.

A tiltakozás joga

9248/81. sz. *Leander kontra Svédország* ügy, 1987. március 26.
48009/08. sz. *Mosley kontra Egyesült Királyság* ügy, 2011. május 10.
34209/96. sz. *M.S. kontra Svédország* ügy, 2002. július 2.
28341/95. sz. *Rotaru kontra Románia* [nagytanács] ügy, 2000. május 4.

Az adatok érzékeny kategóriái

20511/03. sz. *I. kontra Finnország* ügy, 2008. július 17.
12323/11. sz. *Michaud kontra Franciaország* ügy, 2012. december 6.
30562/04. és 30566/04. sz. *S. és Marper kontra Egyesült Királyság* ügyek, 2008. december 4.

Felügyelet és az előírások betartatása (a különböző szereplők, köztük az adatvédelmi hatóságok szerepe)

20511/03. sz. *I. kontra Finnország* ügy, 2008. július 17.
2872/02. sz. *K.U. kontra Finnország* ügy, 2008. december 2.
59320/00. sz. *Von Hannover kontra Németország* ügy, 2004. június 24.
40660/08. és 60641/08. sz. *Von Hannover kontra Németország* egyesített ügyek [nagytanács], 2012. február 7.

Felügyeleti módszerek

48539/99. sz. *Allan kontra Egyesült Királyság* ügy, 2002. november 5.
33810/07. és 18817/08. sz. *Association "21 Décembre 1989" és társai kontra Románia* egyesített ügyek, 2011. május 24.
4378/02. sz. *Bikov kontra Oroszország* ügy [nagytanács], 2009. március 10.
26839/05. sz. *Kennedy kontra Egyesült Királyság* ügy, 2010. május 18.
5029/71. sz. *Klass és társai kontra Németország* ügy, 1978. szeptember 6.
28341/95. sz. *Rotaru kontra Románia* [nagytanács] ügy, 2000. május 4.
47114/99. sz. *Taylor-Sabori kontra Egyesült Királyság* ügy, 2002. október 22.
35623/05. sz. *Uzun kontra Németország* ügy, 2010. szeptember 2.
59842/00. sz. *Vetter kontra Franciaország* ügy, 2005. május 31.

Video-megfigyelés

420/07. sz. *Köpke kontra Németország* ügy, 2010. október 5.
44647/98. sz. *Peck kontra Egyesült Királyság* ügy, 2003. január 28.

Hangminták

44787/98. sz. *P. G. és J. H. kontra Egyesült Királyság* ügy, 2001. szeptember 25.
71611/01. sz. *Wisse kontra Franciaország* ügy, 2005. december 20.

Az Európai Unió Bíróságának válogatott jogesetei

Az adatvédelmi irányelvvel kapcsolatos joggyakorlat

C-73/07. sz. *Tietosuojavaltuutettu kontra Satakunnan Markkinapörssi Oy és Satamedia Oy ügy*, 2008 december 16.
[Az adatvédelmi irányelv 9. cikke értelmében vett „újságírói tevékenység" fogalma]

C-92/09. és C-93/09. sz., *Volker és Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* egyesített ügyek, 2010. november 9.
[Az egyes uniós mezőgazdasági alapok kedvezményezettjei személyes adatainak közzétételére vonatkozó jogszabályi kötelezettség arányossága]

C-101/01. sz. *Bodil Lindqvist ügy*, 2003. november 6.
[Magánszemély által mások magánéletére vonatkozó adatok interneten való közzétételének jogszerűsége]

C-131/12. sz., *Google Spain, S.L., Google Inc. kontra Agencia Española de Protección de Datos, Mario Costeja González ügy, Az Audiencia Nacional (Spanyolország) által 2012. március 9-én*, 2012. május 25-én benyújtott előzetes döntéshozatal iránti kérelem, folyamatban
[A keresőmotor-szolgáltatók azon kötelezettsége, hogy az érintett kérésére tartózkodjanak személyes adatok megmutatásától a keresési eredmények között]

C-270/11. sz., *Európai Bizottság kontra Svéd Királyság ügy*, 2013. május 30.
[Bírság egy irányelv végrehajtásának elmaradása miatt]

C-275/06. sz., *Productores de Música de España (Promusicae) kontra Telefónica de España SAU ügy*, 2008. január 29.
[Internetszolgáltatók azon kötelezettsége, hogy szellemitulajdon-védő szervezetekkel közöljék a KaZaA fájlcserélő program felhasználóinak kilétét]

C-288/12. sz., *Európai Bizottság kontra Magyarország ügy*, 2014. április 8.
[A nemzeti adatvédelmi biztos hivatalból való felmentésének jogszerűsége]

C-291/12. sz., *Michael Schwarz kontra Stadt Bochum* ügy, A főtanácsnok véleménye, 2013. június 13.
[Az EU elsődleges joganyagának a 2252/2004/EK rendelettel való megsértése – azzal, hogy a rendelet kötelezővé teszi az útlevélben az ujjlenyomat tárolását]

C-293/12. és C-594/12. sz., *Digital Rights Írország és Seitling és társai* egyesített ügyek, 2014. április 8.
[Az EU elsődleges joganyagának az adatmegőrzési irányelv általi megsértése]

C-360/10. sz., *SABAM kontra Netlog N.V. ügy*, 2012. február 16.
[Közösségihálózat-szolgáltatók azon kötelezettsége, hogy megakadályozzák zeneművek és audiovizuális művek hálózat-felhasználók általi jogellenes használatát]

C-465/00., C-138/01. és C-139/01. sz., *Rechnungshof kontra Österreichischer Rundfunk és társai és Neukomm és Lauermann kontra Österreichischer Rundfunk egyesített ügyek*, 2003. május 20.
[A bizonyos kategóriákba tartozó közszférabeli intézmények alkalmazottainak fizetésére vonatkozó személyes adatok közzétételére vonatkozó jogi kötelezettség arányossága]

C-468/10. és C-469/10. sz., *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado* egyesített ügyek, 2011. november 24.
[Az adatvédelmi irányelv 7. cikke f) pontjának – „mások jogszerű érdekei" – megfelelő átültetése a nemzeti jogba]

C-518/07. sz. *Európai Bizottság kontra Német Szövetségi Köztársaság* ügy, 2010. március 9.
[Egy nemzeti felügyelő hatóság függetlensége]

C-524/06. sz., *Huber kontra Bundesrepublik Deutschland* ügy, 2008. december 16.
[Külföldiekre vonatkozó adatok statisztikai regiszterben való tárolásának jogszerűsége]

C-543/09. sz., *Deutsche Telekom AG kontra Bundesrepublik Deutschland* ügy, 2011. május 5.
[Újabb hozzájárulás szükségessége]

C-553/07. sz., *College van burgemeester en wethouders van Rotterdam kontra M.E.E. Rijkeboer ügy*, 2009. május 7.
[Az érintett hozzáférési joga]

C-614/10. sz., *Európai Bizottság kontra Ausztria ügy*, 2012. október 16.
[Egy nemzeti felügyelő hatóság függetlensége]

Az uniós intézmények adatvédelmi rendeletével kapcsolatos joggyakorlat

C-28/08 P. sz., *Európai Bizottság kontra The Bavarian Lager Co. Ltd ügy*, 2010. június 29.
[Dokumentumokhoz való hozzáférés]

C-41/00 P. sz., *Interporc Im- und Export GmbH kontra az Európai Közösségek Bizottsága ügy*, 2003. március 6.
[Dokumentumokhoz való hozzáférés]

F-35/08 sz., *Pachtitis kontra Bizottság és EPSO ügy*, 2010. június 15.
[Személyes adatok foglalkoztatással összefüggő felhasználása az uniós intézményekben]

F-46/09. sz., *V kontra Parlament* ügy, 2011. július 5.
[Személyes adatok foglalkoztatással összefüggő felhasználása az uniós intézményekben]

Tárgymutató

Az Európai Bíróság esetjoga

Az Emberi Jogok Európai Bíróságának esetjoga

A nemzeti bíróságok esetjoga

Az Európai Unió Alapjogi Ügynöksége
Európa Tanács - Emberi Jogok Európai Bírósága

Európai adatvédelmi jogi kézikönyv

2014 — 208 o. — 14,8 × 21 cm

ISBN 978-92-871-9944-7 (Európa Tanács)
ISBN 978-92-9239-334-2 (FRA)
doi:10.2811/5399

Bővebb információ elérhető az interneten az Európai Unió Alapjogi Ügynökségének (fra.europa.eu) honlapján keresztül.

Az Európa Tanácsról bővebb információ található az interneten (hub.coe.int).

Európa Tanács joggyakorlatával kapcsolatban további információ található a Bíróság honlapján: echr.coe.int. A HUDOC keresőportál révén hozzáférhetők az ítéletek és határozatok angolul ill. franciául, egyes esetekben azok fordítása más nyelveken, a havi esetjogi tájékoztatók, a sajtóközlemények, valamint a Bíróság munkájával kapcsolatos egyéb tudnivalók.

HOGYAN JUTHAT HOZZÁ AZ EU KIADVÁNYAIHOZ

Ingyenes kiadványok:

- egy példányt:
  az EU Bookshop által (http://bookshop.europa.eu);
- több mint egy példányt:
  az Európai Unió képviseletein és küldöttségein keresztül. (http://ec.europa.eu/represent_en.htm);
  a nem EU-s országok képviseletein (http://eeas.europa.eu/delegations/index_en.htm);
  az Europe Direct szolgáltatáson keresztül (http://europa.eu/europedirect/index_en.htm) vagy a 00 800 6 7 8 9 10 11 telefonszám hívásával (ingyenes szám bárhonnan az EU területéről) (*).

Megvásárolható kiadványok:

- az EU-könyvesbolton keresztül (http://bookshop.europa.eu);

Előfizetéses kiadványok (az *Európai Unió Hivatalos Lapjának sorozatai, az Európai Bírósági Határozatok Tára* stb.):

- az Európai Unió Kiadóhivatalának forgalmazó partnerein keresztül (http://publications.europa.eu/others/agents/index_en.htm).

(*) A kapott információ ingyenes, ahogy a legtöbb telefonhívás is (bár néhány szolgáltató, telefonfülke, vagy hotel díjat számolhat fel).

Az Európa Tanács publikációihoz való hozzáférés

Az Európa Tanács kiadója a szervezet hatáskörébe tartozó összes területen, köztük az emberi jogok, a jogtudomány, az egészségügy, az etika, a szociális ügyek, a környezetvédelem, az oktatás, a kultúra, a sport, a fiatalok és az építészeti örökség területén kiad műveket. Az átfogó katalógusból könyvek és elektronikus publikációk egyaránt rendelhetők online módon: (http://book.coe.int/).

A virtuális olvasószoba segítségével a felhasználók – ingyenesen – kivonatokat olvashatnak a közelmúltban megjelent jelentősebb művekből, illetve megtekinthetik egyes hivatalos dokumentumok teljes szövegét.

Az Európa Tanács egyezményeire vonatkozóan tájékoztatás, valamint az egyezmények teljes szövege elérhető az Európa Tanács szerződéseket kezelő irodájának honlapjáról: http://conventions.coe.int/.

10.2811/5399
TK-01-13-772-HU-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

Az információs és kommunikációs technológiák gyors fejlődésével egyre nagyobb szükség van a személyes adatok erőteljes védelmére, amely jogot az Európai Unió és az Európa Tanács jogi aktusai egyaránt biztosítják. A technológiai fejlesztések kiterjesztik például a felügyelet, a beszélgetések lehallgatása és az adatok tárolása határait, ami hatalmas kihívásokat állít az adatvédelemhez való jog elé. Ez a kézikönyv azon gyakorló jogászok számára készült, akiknek nem az adatvédelem a szakterülete. Áttekintést nyújt az EU és az Európa Tanács alkalmazandó jogi keretéről. Kifejti az irányadó joggyakorlatot, összefoglalja az Emberi Jogok Európai Bírósága (EJEE) és az Európai Unió Bírósága (EUB) legfontosabb döntéseit. Ahol ilyen ítélkezési gyakorlat nincs, hipotetikus esetekkel illusztrált gyakorlati példákat mutat be. Összegezve, a kézikönyv célja, hogy segítse az adatvédelemhez való jog határozott és elkötelezett biztosítását.

AZ EURÓPAI UNIÓ ALAPJOGI ÜGYNÖKSÉGE
Schwarzenbergplatz 11 - 1040 Bécs - Ausztria
Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

EURÓPA TANÁCS
EMBERI JOGOK EURÓPAI BÍRÓSÁGA
67075 Strasbourg Cedex - Franciaország
Tel. +33 (0) 3 88 41 20 00 - Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Kiadóhivatal
ISBN 978-92-871-9944-7 (Európa Tanács)
ISBN 978-92-9239-334-2 (FRA)