

**Az európai adatvédelmi biztos véleménye „Az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé” című, az Európai Parlamenthez és a Tanácshoz intézett bizottsági közleményről**

(2011/C 101/02)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

tekintettel az Európai Unió működéséről szóló szerződésre, és különösen annak 16. cikkére,

tekintettel az Európai Unió Alapjogi Chartájára, és különösen annak 7. és 8. cikkére,

tekintettel 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 irányelvre <sup>(1)</sup>,

tekintettel 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 <sup>(2)</sup> szerinti véleménykérésre, és különösen a rendelet 41. cikkére,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

### I. BEVEZETÉS

1. A Bizottság 2010. november 22-én „Az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé” címmel közleményt fogadott el (a továbbiakban: a közlemény) <sup>(3)</sup>. A közleményt konzultáció céljából elküldték az európai adatvédelmi biztosnak.
2. Az európai adatvédelmi biztos üdvözli azt a tényt, hogy a Bizottság konzultált vele. Az adatvédelmi biztos már a közlemény elfogadása előtt előterjesztette a szövegtervezettel kapcsolatos nem hivatalos észrevételeit, amelyek közül néhányat figyelembe vettek a közlemény végleges változatának elkészítésekor.

### A közlemény háttere

3. A közlemény tárgyát képező uniós belső biztonsági stratégiát (ISS) 2010. február 23-án, a spanyol elnökség idején fogadták el <sup>(4)</sup>. A stratégia egy olyan európai biztonsági modellt vázol fel, amely ötvözi többek között a bűnüldözési és igazságügyi együttműködést, a határigazgatást és a polgári védelmet érintő intézkedéseket, miközben megfele-

lően tiszteletben tartja a közös európai értékeket, például az alapvető jogokat. Fő célkitűzései a következők:

- azon meglévő uniós eszközök bemutatása a nyilvánosság számára, amelyek jelenleg is segítenek garantálni az uniós polgárok szabadságát és biztonságát, valamint azt a hozzáadott értéket, amelyet az uniós fellépés e területen nyújt;
- a közös eszközök és politikák továbbfejlesztése egy integráltabb megközelítés keretében, amely a biztonság hiányának nemcsak a következményeit, hanem az okait is kezeli;
- a bűnüldözési és igazságügyi együttműködés, a határigazgatás, a polgári védelem és a katasztrófavédelem megerősítése.

4. A belső biztonsági stratégia elsősorban az EU biztonságát fenyegető legsürgetőbb veszélyek és kihívások, például az súlyos és szervezett bűnözés, a terrorizmus és a számítástechnikai bűnözés kezelésére, az EU külső határainak igazgatására, valamint a természeti és ember által előidézett katasztrófákkal szembeni ellenálló képesség kialakítására törekszik. Általános iránymutatásokkal, elvekkkel és útmutatással szolgál az e kérdésekkel kapcsolatos uniós fellépéshez, és felkéri a Bizottságot, hogy javasoljon ütemezett lépéseket a stratégia végrehajtására.
5. Ebben az összefüggésben mindenképpen meg kell említeni továbbá a Bel- és Igazságügyi Tanács közelmúltbeli következtetéseit a szervezett és súlyos nemzetközi bűnözésre vonatkozó európai uniós szakpolitikai ciklus meghatározásáról és végrehajtásáról, amelyet 2010. november 8–9-én fogadtak el <sup>(5)</sup> (a továbbiakban: a 2010. novemberi következtetések). Ez a dokumentum a belbiztonság felépítéséről szóló 2006. évi tanácsi következtetések nyomán született <sup>(6)</sup>, és felhívja a Tanácsot és a Bizottságot arra, hogy az átfogó belső biztonsági stratégia kidolgozása során vegyék figyelembe az EU Alapjogi Chartájában megerősített közös uniós értékeket és elveket <sup>(7)</sup>.

<sup>(1)</sup> HL L 281., 1995.11.23., 31. o.

<sup>(2)</sup> HL L 8., 2001.1.12., 1. o.

<sup>(3)</sup> COM(2010) 673 végleges.

<sup>(4)</sup> 5842/2/10. sz. dokumentum.

<sup>(5)</sup> A Bel- és Igazságügyi Tanács 3043. ülése, 2010. november 8–10., Brüsszel.

<sup>(6)</sup> 7039/2/06 JAI 86 CATS 34 sz. dokumentum.

<sup>(7)</sup> A 2010. novemberi következtetésben tárgyalt, a szervezett és súlyos nemzetközi bűnözésre vonatkozó európai uniós szakpolitikai ciklus négy lépésből áll: 1) a szakpolitika kidolgozása a súlyos és szervezett bűnözésre vonatkozó európai uniós fenyegetésvértékelés (EU SOCTA) alapján, 2) a szakpolitika meghatározása és döntéshozatal a Tanács részéről, kis számú prioritás meghatározásával, 3) évenkénti operatív cselekvési tervek (OAP) végrehajtása és nyomon követése és 4) a szakpolitikai ciklus végén alapos értékelés, amelynek eredményeit felhasználják a következő szakpolitikai ciklus meghatározásakor.

6. A belső biztonsági stratégia végrehajtásához javasolt iránymutatások és célok között a 2010. novemberi következtetések említik a proaktív és a hírszerzésre épülő megközelítés beépítését, az uniós egységek közötti szoros együttműködést, ideértve az általuk folytatott információcsere további javítását is, valamint a védelmüket szolgáló uniós munka jelentőségének tudatosítását a polgároknál. A következtetések ezenkívül felhívják a Bizottságot, hogy az érintett uniós ügynökségek és a tagállamok szakembereivel együtt minden egyes prioritás vonatkozásában dolgozzon ki többéves stratégiai tervet (a továbbiakban: MASP), amely meghatározza a legmegfelelőbb stratégiát a probléma megoldására. Emellett felszólítja a Bizottságot, hogy a tagállamok és az uniós ügynökségek szakembereivel folytatott konzultáció alapján dolgozzon ki egy független mechanizmust a többéves stratégiai terv végrehajtásának értékelésére. Az európai adatvédelmi biztos e vélemény későbbi részében kitér majd ezekre a kérdésekre, mivel ezek szorosan összefüggnek a személyes adatok, a magánélet, valamint más kapcsolódó alapvető jogok és szabadságok védelmével, illetve jelentős hatást gyakorolnak azokra.

#### A közlemény tartalma és célja

7. A közlemény öt stratégiai célkitűzést javasol, amelyek mindegyike kapcsolatban áll a magánélet és az adatok védelmével:

- a nemzetközi bűnözői hálózatok felgöngyölítése,
- a terrorizmus, a radikalizálódás és a toborzás megelőzése,
- a virtuális tér biztonságának növelése a polgárok és a vállalkozások számára,
- a biztonság megerősítése a határigazgatás útján és
- Európa válságokkal és katasztrófákkal szembeni ellenálló képességének javítása.

8. A *belső biztonsági stratégia megvalósítása* a közlemény által javasoltak szerint közös menetrendet irányoz elő a tagállamok, az Európai Parlament, a Bizottság, a Tanács, az ügynökségek és mások, többek között a civil társadalom és a helyi hatóságok számára, és javaslatot tesz arra, hogy az elkövetkező négy évben hogyan valósítsák meg az együttműködést a belső biztonsági stratégiai céljainak elérése érdekében.

9. A közlemény a Lisszaboni Szerződést veszi alapul, és elismeri a stockholmi program (és cselekvési terv) által nyújtott iránymutatást, amely a 4.1. fejezetben hangsúlyozza az alapvető jogok, a nemzetközi védelem és a jogállamiság tiszteletben tartásán alapuló átfogó belső biztonsági stratégia szükségességét. Ezenkívül, a stockholmi programmal összhangban a belső biztonsági stratégia kialakítása, nyomon követése és végrehajtása az EUMSz. 71. cikke

alapján létrehozott Belső Biztonsági Állandó Bizottság (COSI) egyik kiemelt feladata kell, hogy legyen. A belső biztonsági stratégia eredményes érvényesítése érdekében ki kell terjednie az integrált határigazgatás biztonsági vonatkozásaira, valamint adott esetben a belső biztonság területén folytatott operatív együttműködés szempontjából releváns, büntetőügyekben folytatott igazságügyi együttműködésre is. Ebben a vonatkozásban fontos még megemlíteni, hogy a stockholmi program a belső biztonsági stratégiával kapcsolatban integrált megközelítést szorgalmaz, amelynek figyelembe kell vennie az Unió által kidolgozott külső biztonsági stratégiát, valamint egyéb – különösen a belső piacot érintő – uniós politikákat is.

#### A vélemény célja

10. A közlemény számos olyan szakpolitikai területet említ, amelyek az Európai Unión belül a „belső biztonság” tágan értelmezett fogalmának részét képezik vagy azt befolyásolják.

11. E véleménynek nem a közleményben foglalt valamennyi szakpolitikai terület és konkrét témakör elemzése a célja, hanem az, hogy:

- a belső biztonsági stratégia közleményben javasolt egyes céljait a magánélet és az adatok védelmének konkrét szempontjából vizsgálja, és – e tekintetben – hangsúlyozza az uniós szinten jelenleg tárgyalt és elfogadott más stratégiákkal való szükséges kapcsolatokat;
- meghatározzon egy sor olyan adatvédelmi fogalmat és elképzelést, amelyeket a belső biztonsági stratégia uniós szintű tervezése, kidolgozása és végrehajtása során figyelembe kell venni;
- adott és szükséges esetben javaslatokat tegyen arra vonatkozóan, hogy a közleményben javasolt intézkedések végrehajtása során hogyan lehet a legjobban figyelembe venni az adatvédelmi megfontolásokat.

12. Az európai adatvédelmi biztos ennek során különösen rá fog mutatni a belső biztonsági stratégia és az információkezelési stratégia, illetve az átfogó adatvédelmi kerettel kapcsolatos munka közötti összefüggésekre. Az adatvédelmi biztos ezenkívül olyan fogalmakra fog hivatkozni, mint például: a rendelkezésre álló legjobb technikák és a „beépített adatvédelem”, magánélet- és adatvédelmi hatásvizsgálat, valamint az érintettek jogai, amelyek közvetlenül befolyásolják a belső biztonsági stratégia tervezését és végrehajtását. A vélemény emellett észrevételeket fűz néhány kiválasztott szakpolitikai területre, úgymint integrált határigazgatás, ideértve az EUROSUR-t és a személyes adatok FRONTEX általi feldolgozását, valamint egyéb területeket, például a virtuális teret és a terrorizmus finanszírozásának felderítését célzó programot (TFTP).

## II. ÁLTALÁNOS ÉSZREVÉTELEK

### A belső biztonsági stratégiához kapcsolódó uniós stratégiákkal szembeni átfogóbb, inkluzívabb és „stratégiaibb” megközelítés szükségessége

13. Uniós szinten jelenleg számos olyan stratégiáról folyik egyeztetés és készül javaslat, amelyek a Lisszaboni Szerződés és a stockholmi program alapján jöttek létre, és közvetlen vagy közvetett módon befolyásolják az adatvédelmet. A belső biztonsági stratégia ezek egyike, és szoros kapcsolatban áll más (akár az újabb bizottsági közleményekben tárgyalt, akár a közeljövőre tervezett) stratégiákkal; ilyenek az EU információkezelési stratégiája és az európai információcsere-modell, az EU Alapjogi Chartájának érvényesítésére irányuló stratégia, az átfogó adatvédelmi stratégia és az EU terrorizmusellenes politikája. E véleményében az európai adatvédelmi biztos kiemelten foglalkozik az információkezelési stratégiával és az EUMSz. 16. cikkén alapuló átfogó adatvédelmi kerettel való kapcsolatokkal, adatvédelmi szempontból ugyanis nyilvánvaló e két kezdeményezés és a belső biztonsági stratégia között fennálló politikai összefüggés.
14. Az említett stratégiák együttesen egymással összefüggő szakpolitikai iránymutatások, programok és cselekvési tervek bonyolult szövevényét alkotják, ami uniós szinten átfogó és integrált megközelítést tesz szükségessé.
15. Általánosabban fogalmazva, amennyiben a jövőbeni intézkedésekben alkalmaznánk a „stratégiák összekapcsolása” megközelítést, az bebizonyítaná, hogy az uniós stratégiákat illetően létezik európai szintű jövőkép, valamint hogy ezek a stratégiák, illetve az őket részletező, közelmúltban elfogadott közlemények szorosan összefüggnek, ami így is van, még hozzá a valamennyiük számára közös hivatkozási pontként szolgáló stockholmi program révén. Mindez továbbá kedvező szinergiákat hozna létre a szabadság, a biztonság és a jog érvényesülésének térségéhez tartozó különböző szakpolitikák között, és megelőzné az e területen végzendő munka és erőfeszítések esetleges megkettőzését. Ugyanilyen fontos, hogy ez a megközelítés valamennyi kapcsolódó stratégia tekintetében hatékonyabbá és egységesebbé tenné az adatvédelmi szabályok alkalmazását.
16. Az európai adatvédelmi biztos rámutat, hogy a belső biztonsági stratégia egyik pillére az Európai Unión belüli hatékony információkezelés, amelynek a szükségesség és az arányosság elvére kell épülnie ahhoz, hogy indokolja az információcsere iránti igényt.
17. Továbbá, amint az adatvédelmi biztos információkezelésről szóló véleményében is olvasható<sup>(8)</sup>, az adatvédelmi biztos hangsúlyozza, hogy csak abban az esetben kellene a személyes adatok tárolását és cseréjét megkönnyítő új jogalkotási intézkedést javasolni, ha konkrét bizonyítékok támasztják

alá annak szükségességét<sup>(9)</sup>. A belső biztonsági stratégia végrehajtása során ezt a jogi követelményt proaktív szakpolitikai megközelítéssel kell alakítani. A belső biztonsági stratégiára vonatkozó átfogó megközelítés igényének szükségszerű következménye, hogy a belbiztonság területén már meglévő valamennyi eszközt értékelni kell, mielőtt újakat javasolnának.

18. Ebben az összefüggésben az európai adatvédelmi biztos ugyancsak javasolja a meglévő eszközök rendszeres értékelését előíró záradékok gyakoribb alkalmazását, amilyen például a jelenleg értékelés alatt álló adatmegőrzési irányelvben<sup>(10)</sup> szerepel.

### Az adatvédelem mint a belső biztonsági stratégia célkitűzése

19. A közlemény a „Közös értékeken alapuló biztonsági politikák” című bekezdésben utal a személyes adatok védelmére, megemlítve, hogy a belső biztonsági stratégiát végrehajtó eszközöknek és fellépéseknek közös értékeken kell alapulniuk, úgymint a jogállamiság és az alapvető jogok tiszteletben tartása, az Európai Unió Alapjogi Chartájában rögzítettek szerint. Ebben az összefüggésben előírja, hogy „bár az EU-n belüli hatékony bűnüldözést segíti az információcsere, az egyének magánéletét, valamint személyes adataik védelméhez való alapvető jogukat is védenünk kell”.
20. Ez üdvözlendő kijelentés. Önmagában azonban nem állíthatjuk, hogy megfelelően megoldaná az adatvédelem kérdését a belső biztonsági stratégiában. A közlemény nem részletezi az adatvédelmet<sup>(11)</sup>, és azt sem fejt ki, a gyakorlatban hogyan gondoskodnak majd a magánélet tiszteletben tartásáról és a személyes adatok védelméről a belső biztonsági stratégiát végrehajtó intézkedésekben.

<sup>(9)</sup> Ez egy jogi követelmény; lásd különösen a Bíróság C-92/09. és C-93/09. egyesített ügyekben hozott 2010. november 2-i ítéletét. Konkrétan összefüggésekben az európai adatvédelmi biztos a szabadság, a biztonság és a jog érvényesülésének térségéhez kapcsolódó jogalkotási javaslatokról szóló egyéb véleményeiben is szorgalmazta ezt a megközelítést: pl. 2005. október 19-i vélemény a Schengeni információs rendszer második generációjával (SIS II) kapcsolatos három javaslatról; 2007. december 20-i vélemény az utas-nyilvántartási adatok (PNR) bűnüldözési célú felhasználásáról szóló tanácsi kerethatározati javaslat tervezetéről; 2009. február 18-i vélemény az (egy harmadik ország állampolgára vagy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló) [...] EK rendelet hatékony alkalmazása érdekében az üjlyenyomatok összehasonlítására irányuló „Eurodac” létrehozásáról szóló rendeletjavaslatról; 2009. február 18-i vélemény az egy harmadik ország állampolgára, illetve hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló rendelethez kapcsolódó javaslatról; és 2009. október 7-i vélemény az EURODAC-hoz való bűnüldözési célú hozzáféréséről szóló javaslatokról.

<sup>(10)</sup> 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 keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról, (HL L 105., 2006.4.13., 54. o.).

<sup>(11)</sup> Az adatvédelem konkrétan csak a személyes adatok FRONTEX általi feldolgozásával összefüggésben jelenik meg.

<sup>(8)</sup> 2010. szeptember 30-i vélemény a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben folytatott információkezelés áttekintéséről szóló, az Európai Parlamenthez és a Tanácshoz intézett bizottsági közleményről.

21. Az európai adatvédelmi biztos szerint a *belső biztonsági stratégia megvalósítása* egyik célkitűzésének az átfogó értelemben vett *védelemnek* kellene lennie, amely gondoskodna az egyrészről a polgárok meglévő veszélyekkel szembeni védelme, másrészről pedig a magánéletük, illetve a személyes adataik védelméhez való joguk tiszteletben tartása közötti *megfelelő* egyensúlyról. Más szóval a biztonsági és az adatvédelmi megfontolásokat egyformán komolyan kell venni a *belső biztonsági stratégia kidolgozása* során, a stockholmi programmal és a tanácsi következtetésekkel összhangban.

22. Röviden, a biztonság szavatolásának a magánélet és az adatok védelmének teljes körű tiszteletben tartása mellett konkrét célkitűzésként kellene szerepelnie az EU *belső biztonsági stratégiájában*. Ezt a stratégia végrehajtása érdekében a tagállamok és az uniós intézmények által hozott valamennyi intézkedésnek tükröznie kell.

23. Ebben az összefüggésben az európai adatvédelmi biztos megemlíti a személyes adatok Európai Unión belüli védelmének átfogó megközelítéséről szóló COM(2010) 609 közleményt.<sup>(12)</sup> Az adatvédelmi biztos hamarosan véleményt készít a közleményről, de hangsúlyozza, hogy csak úgy léptethető életbe egy hatékony *belső biztonsági stratégia*, ha azt egy megbízható adatvédelmi rendszer egészíti ki, amely gondoskodik a kölcsönös bizalomról és a jobb hatékonyságról.

### III. A BELSŐ BIZTONSÁGI STRATÉGIA TERVEZÉSÉRE ÉS VÉGREHAJTÁSÁRA ALKALMAZANDÓ ELKÉPZELÉSEK ÉS FOGALMAK

24. Egyértelmű, hogy a *belső biztonsági stratégia* célkitűzéseiből eredő intézkedések némelyike fokozott veszélyt jelenthet a személyek magánéletére és adataik védelmére. E kockázatok ellensúlyozása érdekében az európai adatvédelmi biztos különösen fel szeretné hívni a figyelmet az olyan fogalmakra, mint a „beépített adatvédelem”, a magánélet- és adatvédelmi hatásvizsgálat, az érintettek jogai és a rendelkezésre álló legjobb technikák. Az említettek kivétel nélkül figyelembe kell venni a *belső biztonsági stratégia* végrehajtása során, azok pedig eredményesen elősegíthetik a magánélet szempontjából kedvezőbb és az adatvédelmet középpontba helyező politikák létrehozását ezen a területen.

#### Beépített adatvédelem

25. Az európai adatvédelmi biztos több ízben, különböző véleményekben népszerűsítette a „beépített” adatvédelem elvét („Privacy by design” vagy „Privacy by default”). Jelenleg zajlik e fogalom részletes kidolgozása az állami és a magánszféra számára egyaránt, ezért az uniós *belső biztonság*, valamint a rendőrségi és igazságügyek területén is fontos szerepet kell játszania.<sup>(13)</sup>

<sup>(12)</sup> A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek és az Európai Gazdasági és Szociális Bizottságnak – A személyes adatok Európai Unión belüli védelmének átfogó megközelítése, COM (2010) 693.

<sup>(13)</sup> Az európai adatvédelmi biztos a stockholmi programról szóló biztonsági közleménnyel kapcsolatos véleményében azt javasolta, hogy írjanak elő jogi kötelezettséget az információs rendszerek kiépítői és felhasználói számára arra vonatkozóan, hogy a „beépített adatvédelem” elvével összhangban álló rendszereket hozzanak létre és alkalmazzanak.

26. A közleményben nem szerepel ez a fogalom. Az európai adatvédelmi biztos javasolja, hogy a *belső biztonsági stratégia* végrehajtása érdekében javasolt és végrehajtott célzott intézkedések között említsék meg ezt a fogalmat, különösen „A biztonság megerősítése a határigazgatás útján” című 4. célkitűzéssel összefüggésben, amelyben egyértelműen megemlítik a határellenőrzések és a határőrizet új technológiáinak fokozott használatát.

#### Magánélet- és adatvédelmi hatásvizsgálat

27. Az európai adatvédelmi biztos szorgalmazza, hogy a Bizottság – a közlemény alapján a *belső biztonsági stratégia* tervezésével és végrehajtásával kapcsolatban végzendő jövőbeni munka részeként – vizsgálja meg, mit jelentene az *igazi magánélet- és adatvédelmi hatásvizsgálat* a szabadság, a biztonság és a jog érvényesülésének térségében, és különösen a *belső biztonsági stratégiában*.

28. A közlemény említi a fenyegetés- és kockázatértékeléseket. Ez üdvözlendő. A magánélet- és adatvédelmi hatásvizsgálatra azonban egyetlen ízben sem utal. Az európai adatvédelmi biztos véleménye szerint a *belső biztonsági stratégia*ról szóló közlemény végrehajtását célzó munka megfelelő alkalmat kínál az ilyen magánélet- és adatvédelmi hatásvizsgálatok kidolgozására a belbiztonsággal összefüggésben. Az európai adatvédelmi biztos megjegyzi, hogy sem a közlemény, sem pedig a Bizottság hatásvizsgálattal kapcsolatos iránymutatásai<sup>(14)</sup> nem határozzák meg ezt a szempontot és alakítják azt szakpolitikai követelménnyé.

29. Az európai adatvédelmi biztos ezért azt javasolja, hogy a jövőbeli eszközök végrehajtása során a magánélet és az adatok védelméről konkrétabb és szigorúbb hatásvizsgálatot végezzenek, akár egy külön értékelés, akár az alapvető jogokra vonatkozó általános bizottsági hatásvizsgálat formájában. Ennek a hatásvizsgálatnak túl kell lépnie a jelenlegi gyakorlaton, azaz az általános elvek megfogalmazásán vagy a szakpolitikai lehetőségek elemzésén, és egyedi, konkrét garanciákat kell javasolnia.

30. Következésképpen egyedi mutatókat és jellemzőket kell kidolgozni annak biztosításához, hogy az uniós belbiztonság terén a magánélet és az adatok védelmére hatást gyakorló javaslatokat alapos megfontolásnak vessék alá, többek között az arányosság, a szükségesség és a célhoz kötöttség elve tekintetében.

31. Ezenfelül ebben az összefüggésben hasznos lehet utalni a rádiófrekvenciás azonosításról szóló ajánlás<sup>(15)</sup> 4. cikkére, amelyben a Bizottság felhívta a tagállamokat annak biztosítására, hogy az ágazat a civil társadalom érintett szereplőivel együttműködve alakítsa ki a magánélet védelmére és az adatvédelemre irányuló hatásvizsgálat kereteit. Az adatvédelmi biztosok nemzetközi konferenciája által 2009

<sup>(14)</sup> SEC(2009) 92, 2009.1.15.

<sup>(15)</sup> C(2009) 3200 végleges, 2009.5.12.

novemberében elfogadott madridi állásfoglalás szintén azt szorgalmazta, hogy a személyes adatok feldolgozását vagy a jelenlegi feldolgozás érdemi módosítását szolgáló új információ rendszerek és technológiák megvalósítása előtt hajtják végre a magánélet-védelmi hatásvizsgálatokat.

### Az érintettek jogai

32. Az európai adatvédelmi biztos megállapítja, hogy a közlemény nem tárgyalja konkrétan az érintettek jogainak kérdését, amely az adatvédelem egyik kulcsfontosságú elemét alkotja, és szerepet kellene játszania a belső biztonsági stratégia kialakításában. Alapvetően fontos annak biztosítása, hogy az azok hatálya alá tartozó polgárok az uniós belbiztonságot szolgáló valamennyi rendszer és eszköz tekintetében azonos jogokat élvezzenek a személyes adatok feldolgozásának módja terén.
33. A közleményben említettek közül számos rendszer konkrét szabályokat állapít meg az érintettek jogaira vonatkozóan (többek között a személyek olyan kategóriáit illetően is, mint az áldozatok, a bűncselekménnyel gyanúsított személyek vagy a migránsok), a rendszerek és eszközök között azonban indokolatlanul sok az eltérés.
34. Az európai adatvédelmi biztos ezért felkéri a Bizottságot, hogy a közeljövőben vizsgálja meg körültekintőbben az érintettek jogai Unión belüli összehangolásának kérdését a belső biztonsági stratégiával és az információkezelési stratégiával összefüggésben.
35. Kiemelt figyelmet kell fordítani a jogorvoslati mechanizmusokra. A belső biztonsági stratégiának garantálnia kell, hogy arra az esetre, ha a személyek jogai sérülnének, az adatkezelők könnyen hozzáférhető, hatékony és megfizethető panaszvételi eljárásról gondoskodjanak.

### Rendelkezésre álló legjobb technikák

36. A belső biztonsági stratégia végrehajtása szükségképpen olyan informatikai infrastruktúra igénybevételével fog történni, amely támogatja a közleményben előirányzott intézkedéseket. A rendelkezésre álló legjobb technikákra a belső biztonsági stratégia célkitűzéseinek elérése és a személyek jogainak védelme közötti helyes egyensúly megteremtését elősegítő eszközként kell tekinteni. Az aktuális összefüggésben az európai adatvédelmi biztos meg kívánja ismételni azt a korábbi véleményeiben tett ajánlását,<sup>(16)</sup> hogy a Bizottság az ágazati érdekeltekkel közösen határozza meg és népszerűsítsen a rendelkezésre álló

legjobb technikák alkalmazására irányuló konkrét intézkedéseket. Az ilyen alkalmazás a tevékenységek és működési módjaik fejlődésének leghatékonyabb és legfejlettebb szakaszát jelenti, ami azt jelzi, hogy egy adott technika a gyakorlatban lehetővé teszi-e – az adatok és a magánélet védelmével kapcsolatos uniós kerettel összhangban – a tervezett eredmények hatékony megvalósítását. Ez a megközelítés teljes körűen megfelel a korábban említett „beépített adatvédelem” elvnek.

37. Adott esetben, és ha erre lehetőség van, a rendelkezésre álló legjobb technikákra vonatkozó referenciadokumentumokat kell kidolgozni, amelyek iránymutatással szolgálnának és nagyobb jogbiztonságot teremtenének a belső biztonsági stratégia keretébe tartozó intézkedések tényleges végrehajtásához. Ez az ilyen intézkedések tagállamok közötti harmonizációját is előmozdíthatja. Végül, de nem utolsósorban, a rendelkezésre álló legjobb, magánélet- és biztonságbarát technikák fogalmának meghatározása megerősíti az adatvédelmi hatóságok felügyeleti szerepét azáltal, hogy az adatkezelők által elfogadott, a magánélet és az adatok védelmével összhangban álló műszaki hivatkozásokat biztosít számukra.
38. Az európai adatvédelmi biztos megjegyzi továbbá, hogy a belső biztonsági stratégiát megfelelően össze kell hangolni a hetedik kutatási és technológiafejlesztési keretprogramon, valamint a biztonság és a szabadságjogok védelmezése nevű keretprogramon belül már végrehajtott intézkedésekkel. A rendelkezésre álló legjobb technikák biztosítására törekvő közös jövőkép lehetővé teszi a polgárok védelméhez szükséges ismeretek és képességek terén történő innovációt az alapvető jogok tiszteletben tartása mellett.
39. Végül, az európai adatvédelmi biztos felhívja a figyelmet arra, hogy az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) fontos szerepet játszhat az iránymutatások kidolgozásában és az informatikai rendszerek sértetlenségének és rendelkezésre állásának biztosításához szükséges biztonsági képességek értékelésében, valamint a rendelkezésre álló legjobb technikák népszerűsítésében. Ezt figyelembe véve az adatvédelmi biztos üdvözli, hogy az ügynökség kulcsszerepet kap a számítástechnikai támadások kezelését és a számítástechnikai bűnözés elleni küzdelmet segítő képességek javításában.<sup>(17)</sup>

### A szereplők és feladataik tisztázása

40. Ebben az összefüggésben a belső biztonsági stratégia felépítésének képező vagy annak kialakításában közreműködő szereplők tekintetében is további tisztázásra van szükség. A közlemény számos szereplőt és érdekelt felet említ, például a polgárokat, az igazságszolgáltatást, az uniós ügynökségeket, a nemzeti hatóságokat, a rendőrséget és a vállalkozásokat. Az őket megillető egyedi szerep-

<sup>(16)</sup> Az európai adatvédelmi biztos véleménye az intelligens közlekedési rendszerekről, 2009. július; az európai adatvédelmi biztos véleménye a rádiófrekvenciás azonosításról szóló közleményről, 2007. december; lásd még az európai adatvédelmi biztos 2006. évi éves jelentésének 48. oldalát.

<sup>(17)</sup> Az európai adatvédelmi biztos tervei szerint még 2010 decemberében véleményt fogad el az ENISA jogi keretére vonatkozóan.

és jogköröket a belső biztonsági stratégia végrehajtásának keretében javasolt konkrét intézkedésekben pontosítani kell.

#### IV. A BELSŐ BIZTONSÁGI STRATÉGIÁHOZ KAPCSOLÓDÓ SZAKPOLITIKAI TERÜLETEKRE VONATKOZÓ EGYEDI ÉSZREVÉTELEK

##### Integrált határigazgatás

41. A közlemény utal arra, hogy a Lisszaboni Szerződéssel az EU-nak több lehetősége van a személyekkel és árukkal kapcsolatos határigazgatási szakpolitikák közötti szinergiák kihasználására. A személyek mozgásával kapcsolatban megemlíti, hogy „az EU az integrált határigazgatási stratégia ikercélkitűzéseiként kezelheti a migrációkezelést és a bűncselekmények elleni küzdelmet”. A dokumentum megítélése szerint a határigazgatás a súlyos és szervezett bűnözés felgöngyölítésének potenciálisan hatékony eszköze <sup>(18)</sup>.
42. Az európai adatvédelmi biztos megállapítja továbbá, hogy a közlemény az alábbi három stratégiai pillért határozza meg: 1) a határellenőrzések új technológiáinak fokozott használata (a SIS II, a VIS, a határregisztrációs rendszer és a regisztráltutas-program); 2) a határőrizet új technológiáinak fokozott használata (az európai határőrizeti rendszer, EUROSUR) és 3) a tagállamok közti fokozott koordináció a FRONTEX keretében.
43. Az adatvédelmi biztos meg kívánja ragadni az alkalmat, hogy e véleményében emlékeztessen arra a több korábbi véleményben megfogalmazott kérésére, hogy uniós szinten a határigazgatás terén világos – az adatvédelmi szabályokat maradéktalanul tiszteletben tartó – politikát hozzanak létre. Az adatvédelmi biztos úgy véli, hogy a belső biztonsági és az információkezelési stratégiával kapcsolatos jelenlegi munka nagyszerű alkalmat teremt az e területekre vonatkozó egységes szakpolitikai megközelítés irányába tett konkrétabb lépésekhez.
44. Az adatvédelmi biztos megállapítja, hogy a közlemény nem csupán a meglévő és a közeljövőben működésbe léptetendő nagyméretű rendszereket említi (például SIS, SIS II és VIS), hanem – ebben a szellemben – azokat a rendszereket is, amelyekre a Bizottság a jövőben javaslatot tehet, de amelyekről egyelőre még nem született döntés (pl. regisztráltutas-program, határregisztrációs rendszer). Ebben az összefüggésben emlékeztetni kell arra, hogy e rendszerek bevezetésének céljait és jogszerűségét még tisztázni és bizonyítani kell, többek között a Bizottság által végzett célzott hatásvizsgálatok eredményeinek fényében. Ha erre nem kerül sor, a közlemény a döntéshozatali folyamat előrevetéseiként értelmezhető, amely következképpen nem veszi figyelembe, hogy a regisztráltutas-program és a határregisztrációs rendszer európai uniós bevezetésére vonatkozó végleges döntés még nem született meg.

<sup>(18)</sup> Sajtóközlemény – Az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé, Memo 10/598.

45. Az adatvédelmi biztos ezért azt javasolja, hogy a belső biztonsági stratégia végrehajtásával kapcsolatos jövőbeni munka során kerüljék az ilyen jellegű előrevetéseket. Amint azt korábban említettük, a magánéletbe beavatkozó új, nagyméretű rendszerek bevezetéséről szóló döntésekre minden esetben csak a meglévő rendszerek megfelelő értékelését követően kerülhet sor, kellő figyelemmel a szükségesség és az arányosság elvére.

##### EUROSUR

46. A közlemény utal arra, hogy a Bizottság jogalkotási javaslatot fog benyújtani az EUROSUR 2011-es létrehozásáról a belső biztonsághoz és a bűnözés elleni küzdelemhez való hozzájárulás érdekében. Megemlíti továbbá, hogy az EUROSUR hasznosítani fogja az EU által támogatott kutatási projektek és tevékenységek segítségével kifejlesztett új technológiákat, mint például a műholdképek használata a célpontok felderítésére és nyomon követésére a tengeri határokon, pl. az EU-ba kábítószereket szállító gyors hajók esetében.
47. Ebben az összefüggésben az európai adatvédelmi biztos megjegyzi, hogy nem világos, vajon az EUROSUR-ra vonatkozóan 2011-ben előterjesztendő jogalkotási javaslat a személyes adatoknak az EUROSUR-ral összefüggésben történő feldolgozását is elő fogja-e irányozni, és ha igen, milyen mértékben. A Bizottság a közleményben erre vonatkozóan nem foglalt egyértelműen állást. A kérdés annál is inkább releváns, mivel a közlemény taktikai, operatív és stratégiai szinten nyilvánvalóan kapcsolatot teremt az EUROSUR és a FRONTEX között (lásd alább a FRONTEX-szel kapcsolatos észrevételeket), és a két szerv közötti szoros együttműködésre szólít fel.

##### A személyes adatok feldolgozása a FRONTEX által

48. Az európai adatvédelmi biztos 2010. május 17-én véleményt adott ki a FRONTEX-rendelet felülvizsgálatára vonatkozóan <sup>(19)</sup>, amelyben valódi vitára és alapos mérlegelésre hívott fel az adatvédelem kérdésével kapcsolatban, a FRONTEX jelenlegi feladatainak megerősítésével és új hatáskörökkel való felruházásával összefüggésben.
49. A közlemény *A biztonság megerősítése a határigazgatás útján* című 4. célkitűzésen belül utal arra, hogy meg kell erősíteni a FRONTEX szerepét a külső határokon. Ebben az összefüggésben a közlemény megemlíti, hogy a tapasztalatok alapján, valamint az EU általános információkezelési megközelítésének keretében a Bizottság áttekinti a Frontex ezen információk korlátozott keretek között és világosan meghatározott személyesadat-kezelési szabályok szerinti feldolgozására és felhasználására való felhatalmazásának lehetőségét, ami jelentősen hozzájárulna a bűnszervezetek

<sup>(19)</sup> Az európai adatvédelmi biztos 2010. május 17-i véleménye az Európai Unió Tagállamai Külső Határain Való Operatív Együttműködési Igazgatásért Felelős Európai Ügynökség (FRONTEX) felállításáról szóló 2007/2004/EK tanácsi rendelet módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról.

felgöngyölítéséhez. A FRONTEX-rendelet felülvizsgálatára vonatkozó bizottsági javaslattal összehasonlítva ez új megközelítés; a javaslatról, amely nem említi a személyes adatok feldolgozását, az Európai Parlament és a Tanács jelenleg egyeztet.

50. Ennek fényében az európai adatvédelmi biztos üdvözlí azt a tényt, hogy a közlemény érinti azokat a körülményeket, amelyek esetén az effajta feldolgozásra szükség lehet (pl. kockázatelemzés, a közös műveletek célpontjainak jobb meghatározása vagy információcseré az Európával). Konkrétabban a közlemény kifejti, hogy a csempészhalozatokban szerepet játszó bűnözőkre vonatkozó információk – amelyek a FRONTEX birtokába kerülnek – nem használhatók fel további kockázatelemzések céljából vagy a jövőbeni közös műveletek célpontjainak jobb meghatározására. Sőt, a bűncselekményekkel gyanúsított személyekre vonatkozó információk nem is jutnak el a hatáskörrel rendelkező nemzeti hatóságokhoz vagy az Európolhoz további vizsgálat céljából.
51. Az európai adatvédelmi biztos mindazonáltal megjegyzi, hogy a közlemény nem említi a FRONTEX jogi keretének felülvizsgálatáról jelenleg zajló egyeztetést, amely, amint azt már említettük, a jogszabályi megoldások biztosítása érdekében foglalkozik a kérdéssel. Továbbá, a közlemény megfogalmazása, amely a bünszervezetek felszámolására irányuló célkitűzéssel összefüggésben hangsúlyozza a FRONTEX szerepét, a FRONTEX mandátumának bővítéseként értelmezhető. Az adatvédelmi biztos javasolja, hogy ezt a szempontot a FRONTEX-rendelet felülvizsgálata és a belső biztonsági stratégia végrehajtása során egyaránt vegyék figyelembe.
52. Az európai adatvédelmi biztos felhívja a figyelmet arra is, hogy gondoskodni kell a feladatok Európol és FRONTEX közötti megkettőzésének elkerüléséről. Ehhez kapcsolódóan az adatvédelmi biztos üdvözlí, hogy a közlemény utal arra: el kell kerülni a feladatoknak a Frontex és az Európol közötti megkettőzését. Erre a kérdésre azonban a felülvizsgált FRONTEX-rendeletben és a belső biztonsági stratégiát végrehajtó azon intézkedésekben is pontosabban ki kell térni, amelyek a FRONTEX és az Európol közötti szoros együttműködésről rendelkeznek. Ez a célhoz kötöttség és az adatminőség elve szempontjából kiemelt jelentőséggel bír. Ez az észrevétel az olyan ügynökségekkel folytatott jövőbeni együttműködésre is vonatkozik, mint az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) vagy az Európai Menekültügyi Támogató Hivatal.

#### A biometrikus adatok felhasználása

53. A közlemény nem foglalkozik konkrétan azzal az aktuális jelenséggel, hogy a szabadság, a biztonság és a jog érvényesülésének térségében egyre fokozottabban használják a biometrikus adatokat, ideértve az EU nagyszabású informatikai rendszereit és az egyéb határigazgatási eszközöket is.
54. Az európai adatvédelmi biztos ezért megragadja az alkalmat, hogy elismételje javaslatát,<sup>(20)</sup> miszerint ezt az

<sup>(20)</sup> Lásd különösen az európai adatvédelmi biztos 8. lábjegyzetben említett, a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben folytatott információkezelés áttekintéséről szóló véleményét.

adatvédelem szempontjából kényes kérdésnek számító szempontot komolyan figyelembe kell venni a belső biztonsági stratégia végrehajtásában, különösen a határigazgatással összefüggésben.

55. Az európai adatvédelmi biztos a biometrikus adatok felhasználása szükségességének alapos értékelése és eseti alapon történő megvizsgálása alapján világos és szigorú politikák kidolgozását javasolja a biometrikus adatoknak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben történő felhasználására vonatkozóan, amelyek során teljes mértékben tiszteletben kell tartani az olyan alapvető adatvédelmi elveket, mint az arányosság, a szükségesség és a célhoz kötöttség.

#### A terrorizmus finanszírozásának felderítését célzó program (TFTP)

56. A közlemény bejelenti, hogy a Bizottság 2011-ben uniós szakpolitikát fog kidolgozni az EU területén tárolt pénzügyi üzenetadatok kivonatolására és elemzésére. Ebben az összefüggésben az európai adatvédelmi biztos felhívja a figyelmet az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program (TFTP II) céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról szóló 2010. június 22-i véleményére<sup>(21)</sup>. Az ebben a véleményben kifejtett kritikus észrevételek a pénzügyi üzenetadatok uniós keretere vonatkozó tervezett munkával összefüggésben is hasonlóképpen érvényesek és alkalmazandók. Eppen ezért azokat az e kérdéssel kapcsolatos egyeztetések során figyelembe kell venni. Kiemelt figyelmet kell szentelni a gyanúsítottak nem minősülő személyekre vonatkozó nagy mennyiségű adatok kivonatolásának és feldolgozásának arányosságára, valamint a független hatóságok és az igazságügyi szervek általi hatékony ellenőrzés kérdésére.

#### A virtuális tér biztonságának növelése a polgárok és a vállalkozások számára

57. Az európai adatvédelmi biztos örömmel veszi tudomásul, hogy a közlemény nagy jelentőséget tulajdonít az uniós szintű megelőző intézkedéseknek, és úgy véli, hogy az informatikai hálózatok biztonságának megerősítése nélkülözhetetlen eleme a jól működő információs társadalom kialakításának. Az európai adatvédelmi biztos támogatja az olyan konkrét intézkedéseket is, mint a számítástechnikai támadások kezelésére irányuló képességek javítása, a bűnüldözés és az igazságszolgáltatás terén történő kapacitásépítés, valamint az iparral való partnerségek létrehozása a polgárok és vállalkozások felhatalmazása érdekében. Ezenfelül üdvözlí az ENISA facilitátori szerepét, amelyet az e célkitűzésben meghatározott tevékenységek sokaságával kapcsolatban ellát.

<sup>(21)</sup> Az európai adatvédelmi biztos 2010. június 22-i véleménye – Tanácsi határozatra irányuló javaslat az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program (TFTP II) céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról szóló megállapodás megkötéséről.

58. A *belső biztonsági stratégia megvalósítása* azonban nem ismereti részletesen a virtuális térben előirányzott bűnüldözési célú intézkedéseket, hogy ezek hogyan veszélyeztethetik az egyes személyek jogait, és milyen biztosítékokra lenne szükség. A megfelelő garanciákra vonatkozóan az európai adatvédelmi biztos ambiciózusabb megközelítést szorgalmaz; erre az egyének alapvető jogainak védelme érdekében van szükség, ideértve azokat is, akiket az e területen lehetséges bűncselekmények megakadályozását célzó intézkedések hátrányosan érinthetnek.

#### V. ÖSSZEZÉS ÉS AJÁNLÁSOK

59. Az európai adatvédelmi biztos a különböző uniós stratégiák és közlemények összekapcsolását kéri a belső biztonsági stratégia végrehajtása során. Ezt a megközelítést konkrét, a tényleges igények felmérésén alapuló cselekvési tervnek kell követnie, amelynek eredményeképpen a belső biztonsági stratégiával kapcsolatos átfogó, integrált és jól szervezett uniós politikának kell létrejönnie.

60. Az európai adatvédelmi biztos továbbá megragadja az alkalmat, hogy hangsúlyozza azon jogi követelmény jelentőségét, amelynek értelmében a belső biztonsági stratégiával és az információcserével összefüggésben felhasználandó valamennyi meglévő eszközt ténylegesen értékelni kell, mielőtt újakat javasolnának. Ebben az összefüggésben határozottan javasolt a vonatkozó eszközök hatékonyságának rendszeres értékelését előíró rendelkezések beillesztése.

61. Az európai adatvédelmi biztos javasolja, hogy a 2010. novemberi tanácsi következtetésekben előírt többéves stratégiai terv elkészítése során vegyék figyelembe az EUMSz.

16. cikke alapján az átfogó adatvédelmi kerettel kapcsolatos jelenleg folyó munkát, különösen a COM(2010) 609 közleményt.

62. Az európai adatvédelmi biztos számos javaslattal él azokra az adatvédelmi szempontból fontos elképzelésekre és fogalmakra vonatkozóan, amelyeket a belső biztonsági stratégia területén figyelembe kell venni, úgymint a beépített adatvédelem, a magánélet- és adatvédelmi hatásvizsgálat és a rendelkezésre álló legjobb technikák.

63. Az európai adatvédelmi biztos azt javasolja, hogy a jövőbeli eszközök végrehajtása során végezzenek hatásvizsgálatot a magánélet és az adatok védelméről, akár egy külön értékelés, akár az alapvető jogokra vonatkozó általános bizottsági hatásvizsgálat formájában.

64. Egyben felkéri a Bizottságot, hogy dolgozzon ki koherensebb és következetesebb politikát a biometrikus adatok felhasználásának előfeltételeire vonatkozóan a belső biztonsági stratégia területén, és uniós szinten alakítson ki nagyobb fokú összhangot az érintettek jogai tekintetében.

65. Az európai adatvédelmi biztos végül számos észrevételt tesz a személyes adatoknak a határigazgatással összefüggésben, és különösen a FRONTEX, illetve esetlegesen az EUROSUR által történő feldolgozására vonatkozóan.

Kelt Brüsszelben, 2010. december 17-én.

Peter HUSTINX  
európai adatvédelmi biztos