EURÓPAI ADATVÉDELMI BIZTOS

Az Európai Adatvédelmi Biztos véleménye

– a Schengeni információs rendszer második generációjának (SIS II) létesítéséről, működtetéséről és felhasználásáról (COM(2005) 230 végleges) szóló tanácsi határozati javaslatról,

– a Schengeni Információs Rendszer második generációjának (SIS II) létesítéséről, működtetéséről és felhasználásáról szóló európai parlamenti és tanácsi rendeletjavaslatról, és

– a járművek forgalmi engedélyének kiadására hatáskörrel rendelkező tagállami szolgálatoknak a Schengeni Információs Rendszer második generációjához (SIS II) való hozzáféréséről (COM(2005) 237 végleges) szóló európai parlamenti és tanácsi rendeletjavaslatról

(2006/C 91/11)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

tekintettel az Európai Közösséget létrehozó szerződésre, és különösen annak 286. cikkére,

tekintettel az Európai Unió alapjogi chartája, és különösen annak 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,

tekintettel a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 2001/45/EK európai parlamenti és tanácsi rendeletre, és különösen annak 41. cikkére,

tekintettel a Bizottságtól a 45/2001/EK rendelet 28. cikkének (2) bekezdése szerint kért, és 2005. június 17-én megkapott véleménykérelemre;

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

1. **BEVEZETÉS**

1.1. **Háttér**

A Schengeni Információs Rendszer (a továbbiakban: SIS) az EU nagyléptékű informatikai rendszere, melyet kiegyenlítő intézkedésként hoztak létre a schengeni térségen belül a belső határellenőrzések megszüntetését követően. Az SIS lehetővé teszi a tagállamok illetékes hatóságai számára az olyan információk cseréjét, melyeket a személyek és tárgyak külső határoknál vagy a nemzeti területen történő ellenőrzésekor, továbbá a vízumok és tartózkodási engedélyek kiállításakor használnak fel.

A Schengeni Egyezmény 1995-ben lépett hatályba kormányközi megállapodásként. Az SIS-t a Schengeni Egyezmény részeként az Amszterdami szerződés illesztette be az EU közös vívmányai közé.

Egy új, második generációs II. Schengeni Információs Rendszer fog a jelenlegi rendszer helyébe lépni, lehetővé téve a schengeni térség kibővítését az új EU-tagállamokra. Egyúttal a rendszer új funkciókat is fog nyújtani. A kormányközi keretben kidolgozott schengeni rendelkezések teljes mértékben klasszikus európai jogi eszközökké alakulnak át.

2005. június 1-én a SIS II. létrehozásához az Európai Bizottság három javaslatot nyújtott be. Ezek a javaslatok a következőket tartalmazzák:

– az EK-Szerződés IV. címe alapján javasolt rendelet (vízum, menedékjoggal kapcsolatos bevándorlás és a személyek szabad mozgásával kapcsolatos egyéb politikák), mely a SIS II. első pillérrel (bevándorlás) kapcsolatos szempontjait fogja szabályozni (a továbbiakban: *rendeletjavaslat*);

– az EK-Szerződés VI. címe alapján javasolt határozat (büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés), mely a SIS harmadik pillérrel kapcsolatos igénybevételét fogja szabályozni (a továbbiakban: *határozati javaslat*);

– az V. cím (Közlekedés) alapján javasolt rendelet, mely konkrétan a járművek nyilvántartásáért felelős hatóságok SIS adatokhoz történő hozzáférésére vonatkozik; ezzel a javaslattal külön foglalkozunk (lsd. alább a 4.6. pontot).

Érdemes megemlíteni ebben az összefüggésben, hogy a Bizottság az elkövetkező hónapokban közleményt fog kiadni az uniós adatbázisok közötti interoperabilitásról és az adatbázisok megnövelt hatékonyságú felhasználásáról (SIS, VIS, Eurodac).

A SIS II egy központi adatbázist tartalmaz, melyet „Központi Schengeni Információs Rendszernek" (a továbbiakban: *CS-SIS*) neveznek, és amelyhez a Bizottság olyan operatív irányítást fog biztosítani, mely minden tagállam által meghatározott országos hozzáférési pontokhoz kapcsolódik. A SIRENE hatóságok biztosítják valamennyi kiegészítő információ cseréjét (a SIS II. figyelmeztető jelzésekhez kapcsolódó, de a SIS II-ben nem tárolt információk).

A tagállamok a letartóztatás, átadás, kiadatás érdekében körözöttekről, igazságügyi eljárás lefolytatása érdekében körözöttekről, megfigyelés alá helyezendő, vagy meghatározott ellenőrzések tárgyát képező emberekről, olyan emberekről akinek belépését a külső határokon meg kell tagadni, valamint az elveszett vagy lopott tárgyakról adatokat szolgáltatnak a SIS II-nek. A a SIS-ben rögzített „figyelmeztető jelzések"-nek nevezett adathalmaz lehetővé teszi az illetékes hatóság számára, hogy azonosítson egy személyt vagy tárgyat.

A SIS II. új jellemzőket fejleszt ki: szélesebb körű hozzáférés a SIS-hez (Europol, Eurojust, a tagállamok ügyészsége, jármű forgalmi engedélyeket kiállító hatóságok), a figyelmeztető jelzések összekapcsolása, új adatkategóriákkal történő kiegészítés, beleértve a biometrikus adatokat (ujjlenyomatok és fényképek), valamint a Vízuminformációs Rendszerrel megosztandó technikai felület. Ezek a kiegészítések éveken keresztül folyó vitákat váltottak ki a SIS céljának az ellenőrzési eszköztől a kimutatási és nyomozási rendszer felé történő eltolódásáról.

1.2. **A javaslatok általános értékelése**

1. Az Európai Adatvédelmi Biztos üdvözli azt a tényt, hogy a 45/2001/EK rendelet 28. cikkének (2) bekezdése alapján bevonták a konzultációba. Azonban a 28. cikk (2) bekezdésének kötelező jellegénél fogva a jelen véleményt meg kell említeni a szövegek preambulumában.

2. Több okból kifolyólag az Európai Adatvédelmi Biztos üdvözli a javaslatokat. A kormányközi struktúra átalakítása európai jogi eszközökké több pozitív következménnyel jár: A SIS II-t meghatározó szabályok jogi értéke tisztázódni fog, (a Bíróság hatáskörébe fog esni az első pillér jogi eszközeinek értelmezése), és az Európai Parlament legalább részben szerepet kap (ámbátor kissé megkésve).

3. Továbbá tartalmukat tekintve, a javaslatok jelentős mértékben foglalkoznak az adatvédelemmel, néhány ponton a jelenlegi helyzethez képest üdvözlendő javulást jelentenek. Különösen megemlítendő a személyazonossággal való visszaélés áldozatainak érdekében megfogalmazott intézkedések, a 45/2001 rendelet kiterjesztése a Bizottságnak a VI. címmel kapcsolatos adatfeldolgozási tevékenységére, és a beléptetés megtagadásának céljából történő, egyénekkel kapcsolatos figyelmeztető jelzés alapját képező okok pontosabb meghatározása.

4. Az is nyilvánvaló, hogy a javaslatokat nagy körültekintéssel állították össze; bonyolultak ugyan, de ez csupán az általuk szabályozott rendszer inherens bonyolultságát tükrözi. A jelen véleményben szereplő legtöbb megjegyzés a rendelkezések tisztázása vagy kiegészítése érdekében született, és nem igényli az anyag teljes átdolgozását.

Viszont ezen általánosan pozitív méltatás ellenére némi fenntartásnak kell hangot adnunk, különösen a következők kapcsán:

1. Sok tekintetben nehéz megérteni a szöveg mögött rejlő szándékot; igencsak sajnálatos az Indokolás hiánya. Tekintve ezen anyagok rendkívüli bonyolultságát, az indokolás alapvető követelmény lett volna. Ennek hiányában az olvasó kénytelen jobb híján pusztán találgatásokra hagyatkozni.

2. Továbbá ugyancsak sajnálatos, hogy nem készült hatástanulmány. Az, hogy a rendszer első része már kész van, nem indokolja ezt, tekintve, hogy jelentős különbségek vannak a kettő között. Többek között a biometrikus adatok alkalmazásának hatásait is jobban végig kellett volna gondolni.

3. Az adatvédelmi jogi szabályozás nagyon bonyolult; a *lex generalis* és a *lex specialis* együttes alkalmazásán alapul. Biztosítani kellene, hogy amikor egy különös jogszabályt dolgoznak ki, a 95/46/EK irányelv és a 45/2001 rendelet által meghatározott meglévő adatvédelmi szabályozás teljes mértékben alkalmazható legyen. A különböző jogi eszközök együttes alkalmazása egyrészt az alapvető szempontokat érintő nemzeti szabályok között nem szabad, hogy eltéréseket eredményezzen, másrészt az adatvédelem jelenlegi szintjét sem szabad, hogy fellazítsa.

4. Az olyan hatóságok számára történő hozzáférés biztosítását, amely nem illeszthető „a személyeken és tárgyakon végzett ellenőrzések" eredeti célrendszeréhez, szigorú biztosítékok alkalmazása kell, hogy kísérje.

5. A javaslatok jelentős részben olyan egyéb jogi eszközökön alapulnak, melyek jelenleg készülőfélben vannak (néha még a javaslati szintnél sem tartanak). Az Európai Adatvédelmi Biztos megérti az összetett és folytonosan változó környezetben történő jogalkotás nehézségeit; ugyanakkor az adott személyeket érintő következményeket és az így teremtett jogbizonytalanságot tekintve azt mégsem véli elfogadhatónak.

6. Kissé elmosódottan van körvonalazva a tagállamok és a Bizottság közötti hatáskörmegosztás. A világos fogalmazás óriási jelentőségű, mivel az nem csak a rendszer zökkenőmentes üzemeltetéséhez szükséges, hanem a rendszer átfogó felügyeletének biztosításához is alapkövetelmény.

1.3. **A vélemény tagolása**

A véleményt a következőképpen tagoljuk: először tisztázza a SIS II-re vonatkozó jogi keretet. Ezután a SIS II. céljának és a jelenlegi rendszertől lényegesen eltérő elemeknek a meghatározásával foglalkozik. Az 5. pont a Bizottság és a tagállamok szerepmegosztását tartalmazza a SIS II. üzemeltetésének vonatkozásában. A 6. pont az érintettek jogaival foglalkozik, míg a 7. pont a nemzeti szintű ellenőrzést és az Európai Adatvédelmi Biztos által végzett ellenőrzést, valamint a ellenőrző szervek közötti együttműködést érinti. A 8. pont megjegyzéseket, és a biztonsággal kapcsolatos esetleges módosításokat javasol; a 9. és 10. pont a komitológiával illetve az interoperabilitással foglalkozik. Végezetül a következtetések összefoglalása kiemeli az egyes pontokhoz tartozó főbb következtetéseket.

2. A VONATKOZÓ JOGI KERET

2.1. **A SIS II-re vonatkozó adatvédelmi szabályozás**

A javaslatok a 95/46/EK irányelvet, a 108. számú egyezményt és a 45/2001 rendeletet említik, mint az adatvédelemre vonatkozó, általuk figyelembe vett jogi keretet. Egyéb eszközök szintén relevánsak.

Érdemes a következőket felsorolni ezen összefüggés tisztázása végett, valamint emlékeztetőül arra, hogy vizsgálódásunknak mi képezi a főbb vonatkoztatási pontjait:

– A magánélet tiszteletben tartását Európában az emberi jogok és alapvető szabadságok védelméről szóló, 1950-ben az Európa Tanács által elfogadott egyezmény biztosítja. Az emberi jogokról szóló európai egyezmény 8. cikke kimondja a „magán- és családi élet tiszteletben tartásához való jogot".

  A 8. cikk (2) bekezdése szerint „e jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban" fontos érdekek „védelme érdekében szükséges". Az Európai Emberjogi Bíróság esetjogában ezek a feltételek további követelményekhez vezettek a beavatkozás jogalapjának minőségét, valamely intézkedés arányosságát és a visszaélések elkerülését garantáló biztosítékok szükségességét tekintve.

– A magánélet tiszteletben tartásához és a személyes adatok védelméhez való jogot legutóbb az Európai Unió alapjogi chartájának 7. és 8. cikkében fektették le. A charta 52. cikke elismeri, hogy ezen jogok korlátozás alá eshetnek, feltéve, ha az emberi jogokról szóló európai egyezmény 8. cikkében említett feltételekhez hasonlóak teljesülnek.

– Az EU-Szerződés 6. cikkének (2) bekezdése úgy rendelkezik, hogy az Unió az emberi jogokról szóló európai egyezmény által garantált alapvető jogokat tiszteletben tartja.

A SIS II. javaslatokra kifejezetten alkalmazandó három szöveg a következő:

– Az egyéneknek a személyes adatok gépi feldolgozása során való védelméről szóló európa tanácsi 1981. január 28-i 108. számú egyezmény (a továbbiakban: *108. számú egyezmény*) a személyes adatok gépi feldolgozásával kapcsolatban alapelveket dolgozott ki a személyek védelme érdekében. Minden tagállam megerősítette a 108. számú egyezményt. Olyan tevékenységekre is vonatkozik, melyeket a rendőrségi munka és igazságszolgáltatás területén végeznek. Jelenleg a 108. számú egyezmény a SIS egyezményre alkalmazandó adatvédelmi szabályrendszer, valamint az Európa Tanács Miniszteri Bizottságának 1987. szeptember 17-i R(87)15. ajánlása, mely a rendőri ágazatban történő adatfelhasználást szabályozza.

– 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 (HL L 281., 31. o.). Erre az irányelvre a továbbiakban *95/46/EK irányelv*ként fogunk utalni. Érdemes megjegyezni, hogy a legtöbb tagországban az irányelvet végrehajtó jogszabályok a rendőrség és az igazságszolgáltatás területén történő feldolgozási tevékenységekre is kiterjednek.

– A személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 2001/45/EK európai parlamenti és tanácsi rendelet (HL L 8., 1. o.). Erre az irányelvre a továbbiakban *45/2001/EK rendelet*ként fogunk utalni.

A 95/46/EK irányelv és a 45/2001 rendelet értelmezése részben az Európai Emberjogi Bíróság vonatkozó esetjogától kell, hogy függjön az 1950-es emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény (ECHR) értelmében. Más szóval, az irányelv és a rendelet, amennyiben a személyes adatoknak az alapvető szabadságok, különösen a magánélet tiszteletben tartásához való jog megsértésének lehetőségét magában foglaló feldolgozásával foglalkozik, az alapvető jogokra figyelemmel értelmezendő. Ez egyben az Európai Bíróság esetjogából is következik ([1]).

([1]) Ezzel összefüggésben érdemes a Bíróság „Österreicher Rundfunk és mások" (a C-465/00., C-138/01. és C-139/01. egyesített ügyek, 2003. május 20-i ítélet, teljes kamara, (2003) ECR I-4989) ügyben hozott ítéletére hivatkozni. A Bíróság egy olyan osztrák törvényt vizsgált, amely előírta a közszférában dolgozók fizetésével kapcsolatos adatoknak az Osztrák Számvevőszék számára történő átadását, és ezen adatok ezt követően történő közzétételét. A Bíróság ítéletében számos, az emberi jogokról szóló európai egyezmény 8. cikkéből átvett kritériumot határoz meg, amelyeket a 95/46/EK irányelv alkalmazása során alkalmazni kell, amennyiben az irányelv a magánélethez való jog bizonyos korlátozását engedélyezi.

A Bizottság 2005. október 4-én kibocsátotta A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló tanácsi kerethatározatra vonatkozó javaslatot [1] (a továbbiakban: kerethatározat-tervezet). Szándéka szerint ez a kerethatározat, mint a SIS II. határozattervezethez tartozó jogszabályi hivatkozás lépne a 108. számú egyezmény helyébe, ami valószínűleg az ilyen összefüggésű adatvédelmi szabályozásra is kihatással lesz (lásd alább a 2.2.5. pontot).

2.2. **SIS II. adatvédelmi jogi szabályozás**

2.2.1. *Általános megjegyzés*

A SIS II. szabályozásához szükséges jogszabályi alapvetés különböző eszközökből áll; viszont, amint azt a preambulumbekezdésben említettük, ez „nem befolyásolja azt az elvet, hogy a SIS II egyetlen információs rendszert alkot, melyet ekként kell működtetni. Ezen eszközök bizonyos rendelkezéseinek ezért azonosnak kell lenniük”.

A két dokumentum felépítése alapvetően megegyezik, sőt valójában az I-III. fejezet csaknem azonos mindkét anyagban. A tény, hogy a SIS II-t egyetlen információs rendszerként kell felfogni, melyhez két különböző jogalap tartozik, tükröződik a meglehetősen összetett adatvédelmi szabályozásban is.

Az adatvédelmi szabályozást részben magukban a javaslatokban, *lex specialis*-ként határozzák meg, amit kiegészít szektoronként egy ettől különböző referencia joganyag (*lex generalis*) (Bizottság, az első pillérben lévő tagállamok, a harmadik pillérben lévő tagállamok).

Ez a szerkezet felveti azt a kérdést, hogy az általános joggal kapcsolatban hogyan foglalkozzunk a speciális szabályokkal. Ebben az esetben az Európai Adatvédelmi Biztos egy konkrét szabályt az általános szabály alkalmazásának tekint. Következésképp a *lex specialis*-nak mindig összhangban kell lennie a *lex generalis*-szal; kibontja (konkretizálja vagy kiegészíti) a lex *generalis*-t, de nem teremt kivételeket a *lex generalis* alól.

Arra a kérdésre, hogy melyik szabályt kellene konkrét esetekben alkalmazni, az az alapelv, hogy a *lex specialis* prioritásként alkalmazandó, de ahol a *lex specialis* hallgat, vagy nem egyértelmű, a *lex generalis*-hoz kell fordulni.

Ezen szerkezet szerint a *lex generalis* és a *lex specialis* három különböző kombinációja képzelhető el. A következőképp foglalható össze:

2.2.2. *A Bizottságra vonatkozó szabályozás*

Bárhol, ahol a Bizottság érintve van, a 45/2001 rendelet alkalmazandó, beleértve az Európai Adatvédelmi Biztos szerepét is, függetlenül attól, hogy a tevékenységeket az első (rendeletjavaslat) vagy a harmadik pillér (irányelvjavaslat) keretén belül végzik. A rendeletjavaslat 21. preambulumbekezdése a következőképpen szól: „A 45/2001EK (…) rendeletet kell alkalmazni a személyes adatoknak az Európai Bizottság által történő feldolgozására, ha a feldolgozás részben vagy teljes egészében a közösségi jog hatálya alá tartozó tevékenységek gyakorlása során történik. A személyes adatok SIS II-ben történő feldolgozása a közösségi jog hatálya alá esik.”

Ennek gyakorlati okai vannak: valójában roppantul nehéz lenne – már ami a Bizottságot illeti – meghatározni, hogy az adatok feldolgozása az első vagy harmadik pillérre vonatkozó jogszabályok keretében történik.

Továbbá a SIS II vonatkozásában egyetlen jogi eszköz alkalmazása a Bizottság összes tevékenységére nem csak gyakorlati szemszögből célszerűbb, hanem a következetességet is szolgálja (biztosítva – a rendelettervezet 21. preambulumbekezdése szerint – „a személyes adatok feldolgozása tekintetében az egyének alapvető jogainak és szabadságainak védelmére vonatkozó szabályok következetes és egységes alkalmazását”). Ennek megfelelően az Európai Adatvédelmi Biztos üdvözli, hogy a Bizottság elismeri, hogy a 45/2001 számú rendelet a Bizottság valamennyi SIS II-ben történő adatfeldolgozási tevékenységére vonatkozik.

2.2.3. *A tagállamokra vonatkozó szabályozás*

A tagállamokat illetően a helyzet bonyolultabb. A rendeletjavaslat alkalmazásában a személyes adatok feldolgozását maga a rendeletjavaslat, valamint a 95/46/EK irányelv szabályozza. A rendeletjavaslat (14) preambulumbekezdésének értelmezése teljesen egyértelművé teszi, hogy az irányelvet *lex generalis*-nak, míg a SIS II rendeletet *lex specialis*-nak kell tekinteni. Ez számos, a későbbiekben kifejtendő következménnyel jár.

A határozati javaslatot illetően hivatkozásul szolgáló adatvédelmi jogi eszköz (*lex generalis*) a 108. számú egyezmény, amely az első és a harmadik pillérbeli adatvédelmi rendszerek között néhány ponton lényeges különbségtételt tesz lehetővé.

2.2.4. *Az adatvédelem szintjére gyakorolt hatás*

Az adatvédelem ezen felépítésére vonatkozó általános megjegyzésként az Európai Adatvédelmi Biztos az alábbiakat hangsúlyozza:

– A rendeletjavaslatnak a 95/46/EK irányelv *lex specialis*-aként (és hasonlóképpen, a határozati javaslatnak a 108. számú egyezmény *lex specialis*-aként) történő alkalmazása soha nem vezethet az irányelvben vagy az egyezményben biztosított adatvédelem szintjének felhígításához. Az Európai Adatvédelmi Biztos ebből a célból ajánlásokat fog kiadni (lásd például a jogorvoslathoz való jogot).

[1] (COM(2005) 475 végleges)

– A jogi eszközök együttes alkalmazása ugyanígy nem eredményezheti a Schengeni Egyezmény jelenlegi rendelkezései által szavatolt adatvédelmi szint csökkenését (lásd például alább a 95/46/EK irányelv 13. cikkével kapcsolatos megjegyzéseket).

– A közösségi jogi szabályozás keretében bármennyire szükséges is a két különböző eszköz alkalmazása, ez nem vezethet az érintett személyek adataira vonatkozó védelmi szintek közötti indokolatlan eltérésekhez attól függően, hogy milyen típusú, rájuk vonatkozó adatok feldolgozására kerül sor. Ezt, amennyire lehet, el kell kerülni. Az alábbi ajánlások a következetesség lehető legnagyobb mértékű javítását szorgalmazzák (lásd például a nemzeti ellenőrző hatóságok hatásköreit).

– A jogi keret annyira bonyolult, hogy a gyakorlati alkalmazás során nagy valószínűséggel bizonyos zavarhoz vezethet. Egyes esetekben nehéz átlátni, hogy a *lex generalis* és a *lex specialis* miként viszonyulnak egymáshoz, ezért a javaslatokban ezt célszerű lenne tisztázni. Ezen túlmenően ebben a bonyolult jogi környezetben a schengeni közös ellenőrző hatóságnak a SIS II javasolt jogalapjáról szóló, 2005. szeptember 27-i véleményében felvetett, a SIS II-vel összefüggő összes létező jog felsorolását, valamint az alkalmazandó jogszabályok egyértelmű hierarchiáját tartalmazó útmutató kidolgozására vonatkozó javaslat rendkívül hasznos.

Következésképp jelen vélemény az érintettek szükséges jogbiztonságának szavatolása érdekében a magas szintű adatvédelem, következetesség és egyértelműség biztosítását szorgalmazza.

2.2.5. *A kerethatározat-tervezet hatása a harmadik pillérbeli adatvédelemre*

A SIS II határozattervezet adatvédelmi hivatkozási eszközéül szolgáló 108. számú egyezményt a harmadik pillérben az adatvédelemről szóló kerethatározat váltja fel. [1] Erről ugyan nem történik említés a javaslatban, de a javasolt kerethatározatból következik. A kerethatározat 34. cikkének (2) bekezdése ugyanis kimondja, hogy „minden, az egyének személyes adataik gépi feldolgozása során való védelméről szóló, 1981. január 28-i 108. számú európa tanácsi egyezményre való hivatkozás az ezen kerethatározatra történő hivatkozásként értelmezendő". Az Európai Adatvédelmi Biztos az elkövetkező hetekben véleményt fog kiadni a kerethatározatról, és jelen véleményben a kerethatározat tartalmát nem fogja részletesen elemezni. Ugyanakkor valahányszor a kerethatározat alkalmazása valószínűleg jelentős hatással lesz a SIS II adatvédelmi szabályrendszerre, erre mindannyiszor kitérünk.

2.2.6. *A 95/46/EK irányelv 13. cikkének és a 108. számú egyezmény 9. cikkének alkalmazása*

A 95/46/EK irányelv 13. cikke és a 108. számú egyezmény 9. cikke arról rendelkezik, hogy a tagállamok jogszabályokat fogadhatnak el az általuk biztosított jogok és kötelezettségek körének korlátozására, amennyiben a korlátozásra más, jelentős érdekek védelme érdekében van szükség (például nemzetbiztonság, honvédelem, közbiztonság) [2].

A rendeletjavaslat és a határozati javaslat preambulumbekezdései egyaránt megemlítik, hogy ezzel a lehetőséggel a tagállamok a javaslatok nemzeti szintű végrehajtása során élhetnek. Ebben az esetben kettős feltételrendszernek kell megfelelni: a 95/46/EK irányelv 13. cikke alkalmazásának összhangban kell lennie az emberi jogokról szóló európai egyezmény 8. cikkével és nem szabad a jelenlegi adatvédelmi szabályrendszer gyengüléséhez vezetnie.

Ez a SIS II esetében még sarkalatosabb kérdés, tekintettel arra, hogy a rendszernek kiszámíthatónak kell lennie. Mivel a tagállamok megosztják egymással az adatokat, lehetővé kell tenni, hogy kellő bizonyosságot lehessen szerezni arról, hogy nemzeti szinten miként dolgozzák fel azokat.

Ebben a tekintetben különösen egy aggályos pont van, mégpedig az, amikor a javaslatok a jelenlegi adatvédelmi szint csökkenéséhez vezetnének. A Schengeni Egyezmény 102. cikke olyan rendszerről rendelkezik, amelyben az adatok felhasználása még nemzeti szinten is szigorúan szabályozva és korlátozva van („Az (1)–(4) bekezdésnek nem megfelelő adatfelhasználás minden Szerződő Fél jogszabályai értelmében rendeltetésellenes felhasználásnak minősül."). Ugyanakkor mind a 95/46/EK irányelv, mind a 108. számú egyezmény tartalmaz olyan rendelkezést, amelynek értelmében többek között a célhoz kötöttség elve alóli kivételek kerülhetnek be a nemzeti szabályozásba. Amennyiben ez megtörténik, ez eltávolodást jelentene a Schengeni Egyezményben rögzített jelenlegi rendszertől, amelyben a nemzeti szabályozás nem térhet el a célhoz kötött és rendeltetésszerű adatfeldolgozás alapelvétől.

A kerethatározat elfogadása ezt az észrevételt nem módosítaná: a probléma sokkal inkább a szigorú célhoz kötöttségi elv fenntartása a SIS II adatok feldolgozása során, mintsem annak szavatolása, hogy az adatokat a kerethatározattal összhangban dolgozzák fel.

[1] A Schengeni Egyezmény általános adatvédelmi rendszerét is felváltja (a Schengeni Egyezmény 126–130. cikke) Ez a rendszer a SIS-re nem alkalmazandó.

[2] Az a tagállam, amely él ezzel a jogokat korlátozó lehetőséggel, ezt csak – miként már említettük – az emberi jogokról szóló európai egyezmény 8. cikkével összhangban teheti meg.

Az Európai Adatvédelmi Biztos azt javasolja, hogy a SIS II javaslatokba (konkrétan a rendeletjavaslat 21. cikkébe, valamint a határozati javaslat 40. cikkébe) vegyenek bele egy, a Schengeni Egyezmény jelenlegi 102. cikke (4) bekezdésével azonos célú rendelkezést, amely korlátozza a tagállamok lehetőségét, hogy az adatok olyan felhasználására vonatkozó rendelkezéseket hozzanak, amely a SIS II szövegekben nem szerepel. Egy másik lehetőség az, hogy a határozati javaslat és a rendeletjavaslat kifejezett korlátozást írjon elő az irányelv 13. cikkének vagy az egyezmény 9. cikkének értelmében megengedhető kivételek körére oly módon, hogy például rögzíti, hogy a tagállamok csak a hozzáférési és a tájékoztatási jogot korlátozhatják, az adatminőség elvét nem.

3. **CÉLOK**

A két dokumentum 1. cikkének értelmében („A SIS II létesítése és általános célkitűzése") a SIS II „annak lehetővé tétele érdekében [jön létre], hogy a hatáskörrel rendelkező tagállami hatóságok a személyekkel és tárgyakkal kapcsolatos ellenőrzés céljából információt cserélhessenek", és ez „hozzá fog járulni a tagállamok közötti belső határok ellenőrzése nélküli térség magas biztonsági szintjének fenntartásához".

A SIS II céljait meglehetősen tágan fogalmazták meg; a fent említett rendelkezések önmagukban nem jelzik pontosan, hogy e célkitűzés mit fed (e célkitűzés alatt mit kell érteni).

Úgy tűnik, hogy a SIS II célkitűzése sokkal tágabb, mint a jelenlegi SIS-nek a Schengeni Egyezmény 92. cikkében rögzített célkitűzése, amely konkrétan hivatkozott a „(…) határellenőrzések, és más, az országon belül végzett rendőrségi és vámellenőrzések céljából kiadott figyelmeztető jelzésekre (…), továbbá (a 96. cikk szerinti figyelmeztető jelzésekkel kapcsolatban) a vízumok és tartózkodási engedélyek kiadása, valamint az idegenrendészeti jogszabályok alkalmazása céljából a személyekre és tárgyakra vonatkozó figyelmeztető jelzésekre (…)".

Ez a tágabb cél abból is ered, hogy a SIS II-höz új funkciókat és hozzáféréseket rendeltek, amelyek nem annyira a személyekkel és tárgyakkal kapcsolatos ellenőrzések eredeti célkitűzésébe, hanem inkább egy nyomozati eszköz keretébe illenek. Különösen kiemelendő, hogy olyan hatóságok kapnának hozzáférést, amelyek a SIS II adatokat saját céljaikra, nem pedig a SIS II céljainak megvalósítására használnák (lásd alább); a figyelmeztető jelzések összekapcsolása általános lesz, ami pedig a rendőrségi nyomozati eszközök tipikus jellemzője.

Kérdések merülnek fel továbbá a következő években kifejlesztendő biometrikus keresőprogrammal kapcsolatban, amely egy ellenőrző rendszer igényein túlmutató kereséseket tesz lehetővé.

Következésképp a javaslatok hatálya a jelenlegi keretnél sokkal kiterjedtebb. Ez további biztosítékokat követel meg. Ebben a tekintetben az Európai Adatvédelmi Biztos elemzése nem magára az 1. cikkben foglalt széles fogalom-meghatározásra, hanem inkább a SIS II funkcióira és egyéb összetevőire fog összpontosítani.

4. **JELENTŐS VÁLTOZÁSOK A SIS II-BEN**

E fejezet először a SIS II által bevezetett új elemekre, konkrétan a biometrikus adatokra, a gépjármű nyilvántartásért felelős hatóságok általi hozzáférés új koncepciójára – különös tekintettel az Europol és az Eurojust általi hozzáférésre –, a figyelmeztető jelzések összekapcsolására, valamint a különböző hatóságoknak a bevándorlási adatokhoz való hozzáférésére összpontosít.

4.1. **Biometrikus azonosítók**

A SIS II javaslatok egy olyan új adatkategória feldolgozásának lehetőségét vezetik be, amely külön figyelmet érdemel: ezek a biometrikus adatok. Miként azt az Európai Adatvédelmi Biztosnak a vízuminformációs rendszer létrehozásáról szóló véleménye ([1]) hangsúlyozza, a biometrikus adatok természeténél fogva érzékeny jellege a SIS II javaslatokban nem szereplő külön biztosítékokat igényel.

Általános megjegyzésként elmondható, hogy az uniós méretű információs rendszerekben (VIS, EURODAC, vezetői engedélyek információs rendszere, stb.) tárolt biometrikus adatok felhasználásának tendenciája kitartóan növekszik, de ehhez nem társul az ezzel járó kockázatok és a megkövetelt biztosítékok gondos mérlegelése.

Az alaposabb mérlegelés ezen szükségességét az adatvédelmi biztosok Montreux-i nemzetközi konferenciája által a közelmúltban a biometrikus azonosítókról kiadott állásfoglalása is kiemelte ([2]). A szabványok kidolgozásának hozzáadott értékével kapcsolatosan a mai napig csak a rendszerek közötti egyre fokozódó interoperabilitásra került a hangsúly, és nem a biometrikus adatok minőségének javítására.

([1]) Az európai adatvédelmi biztos 2005. március 23-i véleménye a Vízuminformációs Rendszerről (VIS) és a rövid idejű tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló európai parlamenti és tanácsi rendeletre vonatkozó javaslatról, 3.4.2. pont

([2]) Az adatvédelmi és a magánéletért felelős biztosok 27. nemzetközi konferenciája, Montreux, 2005. szeptember 16., Állásfoglalás a biometrikus azonosítóknak az útlevelekben, személyazonosító igazolványokban és útiokmányokban történő felhasználásáról

Célszerű lenne az ilyen adatok sajátosságával összefüggő közös kötelezettségek vagy követelmények, valamint ezek bevezetése közös módszerének felállítása. E közös követelmények különösen a következő elemekből állhatnának (aminek szükségességét a SIS II javaslatok szemléltetik):

– **Célzott hatásvizsgálat:** Hangsúlyozni kell, hogy a javaslatokat nem vetették alá a biometrikus azonosítók felhasználására vonatkozó hatásvizsgálatnak ([1])

– **A nyilvántartásba vételi folyamat kiemelése:** Hiányoznak a biometrikus adatok forrására és gyűjtésük miként jére vonatkozó részletek. A nyilvántartásba vételi folyamat a biometrikus azonosítás átfogó folyamatának kritikus pontja, amelyet – mivel a folyamat végeredményét, azaz a téves elutasítási arány vagy a téves elfogadási arány szintjét közvetlenül befolyásolni fogja – nem lehet csupán mellékletekkel vagy további alcsoporti tárgyalások útján meghatározni.

– **A pontossági szint hangsúlyozása:** A javaslatban az azonosításra szolgáló biometrikus adatok felhasználásának (egy a többel való összehasonlítás) egy „biometrikus kereső-program" jövőbeni bevezetéseként történő bemutatása még kritikusabb, ugyanis e folyamat eredményei pontatlanabbak, mint az adatok eredetiségvizsgálat vagy ellenőrzés céljára történő felhasználása (egy az eggyel való összehasonlítás). A biometrikus azonosítás ezért nem lehet egyedüli azonosítási mód vagy a további információkhoz való hozzáférés egyedüli kulcsa.

– **Tartalékeljárás:** Könnyen hozzáférhető tartalékeljárásokat kell bevezetni az esetlegesen rosszul azonosított személyek méltóságának tiszteletben tartása, valamit annak érdekében, hogy a rendszer hiányosságainak terhe ne rájuk háruljon.

A biometrikus adatok megfelelő előzetes értékelés nélküli felhasználása a biometrikus azonosítók megbízhatóságának túlbecsléséről is árulkodik. A biometrikus adatok „élő", időben változó adatok; az adatbázisban tárolt minták csak egy dinamikus elemről készült pillanatfelvételt jelentenek. Ez utóbbi állandósága nem abszolút, és ellenőrzést igényel. A biometrikus azonosítók pontossága – mivel soha nem abszolút jellegűek – mindig más elemek fényében vizsgálandó.

([1]) A vizsgálat a „Biometria a határokon: a társadalomra gyakorolt hatás értékelése" című tanulmányban foglalt úgynevezett biometrikus bölcsesség hét pillérén alapulhatna, IPTS, DG-JRC, EUR 21585 EN, 1.2. rész, 32. o.

Ha a biometrikus bizonyítékoknak fokozottabb vagy túlbecsült szerepet tulajdonítanak, a SIS II adatok nyomozati célú lehetséges felhasználása – miként ezt múltbeli esetek is bizonyítják ([2]) – súlyos veszélyekkel jár az érintettekre nézve.

A javaslatoknak ezért el kell ismerniük és tudatosítaniuk kell az azonosítási célú biometriában rejlő reális lehetőségeket.

4.2. **Hozzáférés a SIS II adatokhoz**

4.2.1. *Új hozzáférés-kép*

Minden egyes figyelmeztető jelzéshez meghatározásra kerülnek a SIS adatokhoz hozzáféréssel rendelkező hatóságok. A SIS adatokhoz való hozzáférés biztosításához elvileg kettős feltételrendszert alkalmaznak: hozzáférést a SIS általános céljainak és minden egyes figyelmeztető jelzés konkrét céljának teljes mértékben megfelelő hatóságok kaphatnak.

Ez a figyelmeztető jelzéseknek a rendeletjavaslatban, valamint a határozati javaslatban található fogalom-meghatározásából következik (mindkét eszköz 3. cikke (1a.) bekezdése: *„figyelmeztető jelzés": a SIS II-be bevitt adatok halmaza, amely a hatáskörrel rendelkező hatóságok számára lehetővé teszi, hogy egy meghozandó egyedi intézkedésre tekintettel egy személyt vagy tárgyat azonosítsanak.*) A határozati javaslat 39. cikkének (3) bekezdése megerősíti ezt a szemléletet azzal, hogy kimondja: *„az (1) bekezdésben említett adatokat csak személyek azonosítására lehet felhasználni az e határozattal összhangban foganatosítandó egyedi intézkedés végrehajtása érdekében*". Ebben a tekintetben a SIS II még mindig egy találat/nincs találat rendszer jellegzetességeit hordozza, amely minden egyes figyelmeztető jelzést egy konkrét célhoz rendel (átadás, beléptetés megtagadása, …).

A SIS adatokhoz hozzáféréssel rendelkező hatóságok ezen adatokat ténylegesen korlátozottan használhatják fel, mivel elvileg csak egy egyedi intézkedés végrehajtása céljából férhetnek hozzájuk.

Ugyanakkor egyes, az új javaslatokban szereplő hozzáférések nincsenek összhangban ezzel a logikával, ugyanis a hatóság tájékoztatását célozzák és nem azt, hogy lehetővé tegyék a hatóság számára egy adott személy azonosítását és a figyelmeztető jelzésben előírt intézkedés foganatosítását.

([2]) 2004 júniusában egy portlandi (US) ügyvéd két hétre börtönbe került, mert ujjlenyomatát az FBI-nak sikerült egy, a madridi bombamerénylet után (a detonátort tartalmazó műanyag zacskón) talált ujjlenyomattal azonosítania. Végül kiderült, hogy az összehasonlítási folyamatba hiba csúszott, ami téves értelmezéshez vezetett.

Konkrétabban ez az alábbiakat érinti:

– a menekültügyi hatóságok hozzáférése a bevándorlási adatokhoz;

– a menekültstátusz megadásáért felelős hatóságok hozzáférése a bevándorlási adatokhoz;

– az Europol hozzáférése a kiadatásra, leplezett megfigyelésre és a lefoglalandó ellopott okmányokra vonatkozó figyelmeztető jelzésekhez;

– az Eurojust hozzáférése a kiadatási és helymeghatározási adatokhoz.

A SIS II adatok viszonylatában mindezen hatóságok ugyanazokkal a jellemzőkkel bírnak:

nem foganatosíthatják a figyelmeztető jelzések fogalommeghatározásában említett egyedi intézkedést. A hozzáférés a saját céljaikat szolgáló infomációforrásként van biztosítva a számukra.

Még ezen hatóságok esetében is különbséget kell tenni azok között, amelyek saját céljaikra, de konkrét célból rendelkeznek hozzáféréssel, valamint azok között (ezek konkrétan az Europol és az Eurojust), amelyek számára a hozzáférés célja egyáltalán nincs pontosan körülhatárolva. A menekültügyi hatóságok például konkrét célból rendelkeznek hozzáféréssel, még akkor is, ha ez nem a figyelmeztető jelzésben említett cél. A bevándorlási adatokhoz „annak meghatározása céljából [férhetnek hozzá], hogy egy menedékjogot kérelmező személy jogellenesen tartózkodott-e egy másik tagállamban.” Az Europol és az Eurojust viszont bizonyos figyelmeztető jelzés kategóriákban szereplő olyan adatokhoz fér hozzá, „amelyek feladataik elvégzéséhez szükségesek”.

Összefoglalásképpen a SIS II adatokhoz történő hozzáférés három esetben biztosított:

– a figyelmeztető jelzés végrehajtása céljából történő hozzáférés;

– a SIS II céljától eltérő, de a javaslatokban jól körülírt célból történő hozzáférés;

– a SIS II céljaitól eltérő, de nem pontosan körülhatárolt célból történő hozzáférés;

Az Európai Adatvédelmi Biztos azon a véleményen van, hogy minél általánosabb a hozzáférés célja, a bevezetendő biztosítékoknak annál szigorúbbaknak kell lenniük. Az általános biztosítékokat az alábbiakban részletezzük; majd az Europol és az Eurojust sajátos helyzetével foglalkozunk.

4.2.2. *A hozzáférés biztosításának feltételei*

1. Hozzáférés minden esetben csak akkor biztosítható, ha ez a SIS II általános céljaival összeegyeztethető és annak jogalapjával összhangban van.

   Ez a gyakorlatban azt jelenti, hogy a rendeletjavaslat értelmében a bevándorlási adatokhoz való hozzáférésnek a schengeni vívmányok részét képező, a személyek mozgásához kapcsolódó politikák végrehajtását kell támogatniuk.

   A határozat által rögzített figyelmeztető jelzésekhez való hozzáférés ugyanígy a büntetőügyekben folytatott rendőrségi és igazságügyi operatív együttműködés támogatását célozza.

   Ebben a tekintetben az Európai Adatvédelmi Biztos felhívja a figyelmet a járművek forgalmi engedélyének kiadásáért felelős szolgálatoknak a SIS II-höz való hozzáférésével kapcsolatos fejezetre (lásd alább a 4.6. pontot).

2. A SIS II adatokhoz való hozzáférés szükségességét bizonyítani kell, valamint azt is, hogy más, kisebb sérelmet okozó eszközökkel lehetetlen vagy nagyon nehéz beszerezni az adatokat. Ezt indoklás formájában kellett volna megtenni, amelynek hiánya, mint már mondottuk, felettébb sajnálatos.

3. Az adatok felhasználását kifejezetten és megszorító módon kell meg határozni.

   Például a menekültügyi hatóságok „annak meghatározása céljából férhetnek hozzá a bevándorlási adatokhoz, hogy egy menedékjogot kérelmező személy jogellenesen tartózkodott-e egy másik tagállamban”. Az Europol és az Eurojust viszont hozzáfér bizonyos figyelmeztető jelzés kategóriákban szereplő olyan adatokhoz, „amelyek feladataik elvégzéséhez szükségesek”: ez nem eléggé részletes körülhatárolás (lásd alább).

4. A hozzáférés feltételeit jól meg kell határozni és korlátozni kell. E szervezeteken belül különösen csak azok a szolgálatok kaphatnak a SIS II adatokhoz hozzáférést, amelyeknek az adatokkal foglalkozniuk kell. Ezt, a határozati javaslat 40. cikkében és a rendeletjavaslat 21. cikkének (2) bekezdésében rögzített kötelezettséget a nemzeti hatóságok azon kötelezettségével kell kiegészíteni, hogy kötelesek naprakész jegyzéket vezetni a SIS II adatokhoz hozzáférési jogosultsággal rendelkező személyekről. Az Europolra és az Eurojustra ugyanennek kell vonatkoznia.

5. Az, hogy ezen hatóságok hozzáféréssel rendelkeznek a SIS II adatokhoz, soha nem képezhet jogalapot ahhoz, hogy a rendszerbe olyan adatokat vigyenek be, vagy a rendszerben olyan adatokat tároljanak, amelyek nem célravezetők azon konkrét figyelmeztető jelzés szempontjából, amelynek a részét képezik. A rendszert új adatkategóriákkal nem lehet bővíteni, mivel ezek más információs rendszerek céljait szolgálnák. A határozati javaslat 39. cikke például arról rendelkezik, hogy a figyelmeztető jelzésekbe vigyenek be a kibocsátó hatóságra vonatkozó adatokat. Ezen adatok egy intézkedés (letartóztatás, megfigyelés, …) foganatosításához nem szükségesek, és bevezetésük egyedüli oka valószínűleg az lenne, hogy az Europol vagy az Eurojust ezeket hasznosíthatná. Ezen adatok feldolgozásának jogosultságát egyértelműen indokolni kell.

6. Az adatok megőrzési idejét akkor, ha ahhoz a célhoz, amelyhez az adatokat bevitték, nem szükséges, nem lehet meghosszabbítani. Ez azt jelenti, hogy még ha az Europol vagy az Eurojust hozzáfér is ezen adatokhoz, a rendszerben történő tartásukra ez nem teremt elegendő jogalapot (például ha egy körözött személyt már kiadtak, az adatokat törölni kell, még akkor is, ha ezek az Europol számára hasznosak lehetnének.) Itt megint alapos ellenőrzésre van szükség annak szavatolásához, hogy ezt a nemzeti hatóságok alkalmazzák.

4.2.3. *Az Europol és az Eurojust hozzáférése*

a) *A hozzáférés jogalapja*

Az Europol és az Eurojust bizonyos SIS adatokhoz való hozzáférése már a 2005. február 24-i tanácsi határozatba történő bevezetésük előtt vita tárgyát képezte ([1]). E két szervezet az összes, a saját céljaikra hozzáféréssel rendelkező hatóság közül a legtágabb értelemben vett hozzáférést élvezi. Jóllehet ezen adatok felhasználását a határozat XII. fejezete leírja, a hozzáférés elsődleges biztosításának jogalapja nincs kellőképp kifejtve. Ez a megállapítás annak figyelembevételével, hogy az Europol és az Eurojust feladatai idővel valószínűleg változnak, még inkább érvényes.

Az Európai Adatvédelmi Biztos arra ösztönzi a Bizottságot, hogy pontosan határozza meg, mely feladatok elvégzéséhez lenne indokolt az Europol és az Eurojust hozzáférése.

b) *Adatkorlátozás*

A Europol és az Eurojust „gyűjtögető akcióinak” elkerülése, valamint annak szavatolása érdekében, hogy csak a „feladataik elvégzéséhez szükséges” adatokhoz férjenek hozzá, a schengeni közös ellenőrző hatóság a SIS II javaslatokról szóló 2005. szeptember 27-i véleményében azt javasolta, hogy az Europol és az Eurojust személyes adatokhoz való hozzáférését azon személyekre korlátozzák, akiknek a neve az adatállományaikban már szerepel. Ez szavatolná, hogy csak az ezen személyekre vonatkozó releváns figyelmeztető jelzésekbe kapnak betekintést. Az Európai Adatvédelmi Biztos támogatja ezt az ajánlást.

c) *Biztonsági vetületek*

Az Európai Adatvédelmi Biztos üdvözli az Europol és az Eurojust által végzett valamennyi összekötött művelet naplózásának kötelezettségét, valamint a rendszer részei másolásának vagy letöltésének tilalmát.

A határozati javaslat 56. cikke az Europol és az Eurojust számára „egy-kettő” hozzáférési pontot irányoz elő. Bármennyire érthető is, hogy egy tagállam – hatáskörrel rendelkező hatóságainak decentralizált helyzete miatt – egynél több hozzáférési pontra tartana igényt, az Europol és az Eurojust jogállása és tevékenysége ezt a kérést nem indokolja. Ezen túlmenően azt is hangsúlyozni kell, hogy biztonsági szempontból a hozzáférési pontok szaporodása növeli a visszaélés kockázatát, ezért ezt következetesebb elemekkel kellene pontosan indokolni. Ezért meggyőző érvrendszer hiányában az Európai Adatvédelmi Biztos azt javasolja, hogy az Europol és az Eurojust számára csak egy hozzáférési pontot biztosítsanak.

4.3. **A figyelmeztető jelzések összekapcsolása**

A rendelet 26. cikke és a határozat 46. cikke úgy rendelkezik, hogy a tagállamok nemzeti jogszabályaikkal összhangban két vagy több figyelmeztető jelzés közötti összeköttetés létesítése céljából kapcsolatot létesíthetnek a figyelmeztető jelzések között.

Jóllehet a figyelmeztető jelzések közötti kapcsolatok ellenőrzés céljára bizonyosan hasznosak lehetnek (például egy autótolvajra kiadott elfogatóparancsot összekapcsolhatnak egy ellopott járművel), a figyelmeztető jelzések közötti kapcsolatok bevezetése a rendőrségi nyomozati eszközök rendkívül tipikus jellemzője.

A figyelmeztető jelzések összekapcsolása jelentős hatással lehet az érintett személy jogaira, mivel az adott személy „értékelése” ezentúl nem csupán a rá vonatkozó adatok alapján, hanem az illető más személyekkel való lehetséges társítása alapján történik. Azokat a személyeket, akiknek az adatait bűnözők vagy körözött személyek adataival kapcsolják össze, valószínűleg nagyobb gyanakvással kezelik, mint másokat. A figyelmeztető jelzések összekapcsolása ezen túlmenően a SIS vizsgálati jogköreinek kiterjesztését is jelenti, mivel lehetővé teszi az állítólagos bűnszövetkezetek vagy -hálózatok nyilvántartását (ha például az illegális bevándorlók adatait embercsempészek adataival kapcsolják össze). Végezetül, mivel a kapcsolatok létrehozását a nemzeti jogszabályok teremtik meg, ennek lehetséges következménye az, hogy az egyik tagállamban törvényellenes kapcsolatok a másik tagállamban létrejöhetnek, és ezáltal „törvényellenes” adatok kerülnek be a rendszerbe.

([1]) A Tanács 2005. február 24-i 2005/211/IB határozata néhány új funkciónak – többek között a terrorizmus elleni küzdelemnek – a Schengeni Információs Rendszerbe történő bevezetéséről, HL L 68., 2005.3.15., 44. o.

A Tanács 2004. június 14-i, a SIS II funkcionális követelményeiről szóló következtetéseiben megállapította, hogy minden egyes kapcsolatnak egyértelmű operatív követelménnyel kell rendelkeznie, világosan meghatározott összeköttetésen kell alapulnia és meg kell felelnie az arányosság követelményének. Ezen túlmenően nem érintheti a hozzáférési jogokat. Mindenesetre mivel a figyelmeztető jelzések összekapcsolása feldolgozási műveletnek minősül, meg kell felelnie a 95/46/EK irányelvet végrehajtó nemzeti jogszabályoknak, és/vagy a 108. számú egyezménynek.

A javaslatok megismétlik, hogy a kapcsolatok megléte nem módosíthatja a hozzáférési jogokat (ugyanis egyébként olyan adatokhoz való hozzáférést tenne lehetővé, amelyek feldolgozása a nemzeti jogszabályok értelmében, az irányelv 6. cikkének megsértésével, nem lenne jogszerű).

Az Európai Adatvédelmi Biztos hangsúlyozza a rendeletjavaslat 26. cikke és a határozati javaslat 46. cikke megszorító értelmezésének fontosságát: az egyik mód ennek biztosítására annak egyértelművé tétele, hogy a bizonyos adatkategóriákhoz hozzáférési joggal nem rendelkező hatóságok nemcsak, hogy nem férhetnek hozzá az e kategóriákba tartozó adatokhoz, hanem e kapcsolatok létezéséről még nem is tudhatnak. Amikor a kapcsolt adatokhoz nincs hozzáférési jog, a kapcsolatok megjelenítését lehetetlenné kell tenni.

Ezen túlmenően az Európai Adatvédelmi Biztos azt szeretné, ha konzultálnának vele a fentiek biztosításához szükséges technikai intézkedésekről.

4.4. **A belépés megtagadása céljából kiadott figyelmeztető jelzés**

4.4.1. *A bevezetés jogalapja*

A „harmadik országbeli állampolgárokra vonatkozó beléptetési tilalmat elrendelő figyelmeztető jelzések” (a rendelet 15. cikke) használata jelentős hatással bír a személyes szabadságokra: az e rendelkezés értelmében megjelölt személy több éven keresztül nem léphet be a schengeni térségbe. A megjelölt személyek számát figyelembe véve eddig ez volt a leggyakoribb figyelmeztető jelzés. Tekintve a figyelmeztető jelzés következményeit és az érintett személyek számát, nagy körültekintésre van szükség a figyelmeztető jelzés koncepciójának és végrehajtásának tekintetében is. Bár a fentiek a többi figyelmeztető jelzésre is igazak, az Európai Adatvédelmi Biztos külön fejezetet fog szentelni ennek a figyelmeztető jelzésnek, mert ez külön problémákat vet fel a bevezetésének jogalapját illetően.

Az új beléptetési tilalmat elrendelő figyelmeztető jelzés javulást mutat a jelenlegi helyzethez képest, de még mindig nem teljes mértékben kielégítő, mert főként olyan jogi eszközökön alapul, amelyeket még nem fogadtak el, sőt még nem is javasoltak.

A javulások az adatfelvétel jogalapjának pontosabb meghatározásában rejlenek. A Schengeni Egyezmény jelenlegi megszövegezése olyan helyzethez vezetett, hogy jelentős különbségek állnak fenn a tagállamok között az egyezmény 96. cikke alapján megjelölt személyek száma tekintetében. A Schengeni Közös Ellenőrző Hatóság átfogó tanulmányt [1] készített a témáról, és azt az ajánlást tette, hogy „a politikai döntéshozóknak mérlegelniük kell a figyelmeztető jelzések kiadása okainak harmonizálását a különböző schengeni államokban”.

A javasolt 15. cikk megfogalmazása részletesebb, ami üdvözlendő.

Ezen túlmenően a 15. cikk (2) bekezdése felsorolja azokat az eseteket, amelyekben egy személyt nem lehet megjelölni, mivel különböző jogállásoknak megfelelően jogszerűen tartózkodik valamely tagállam területén. Bár a fentiek következnek a jelenlegi Schengeni Egyezményből, a gyakorlat azt mutatta, hogy ennek a mechanizmusnak az alkalmazása tagállamonként különböző volt. Ezért a pontosítás pozitív elem.

Ugyanakkor ezt a rendelkezést is komoly kritikák érték, mivel jelentős részben egy még el nem fogadott szövegen alapul, nevezetesen a visszatérésről szóló irányelven.

A SIS II-re vonatkozó javaslatok elfogadása óta a Bizottság (2005. szeptember 1-jén) javaslatot tett egy „a tagállamokban illegálisan tartózkodó harmadik országbeli állampolgárok visszatérésére vonatkozó közös szabályokról és eljárásokról szóló irányelvre”, de amíg a szöveg nem végleges, addig nem lehet az adatok rendszerbe történő bevitele érvényes jogalapjának tekinteni. Ez különösen az emberi jogokról szóló európai egyezmény 8. cikkét sérti, mivel az egyének magánéletébe történő beavatkozást – egyebek mellett – világos és bárki számára hozzáférhető jogszabályoknak kell alátámasztaniuk.

Ezért az Európai Adatvédelmi Biztos arra ösztönzi a Bizottságot, hogy vagy vonja vissza ezt a rendelkezést, vagy oly módon fogalmazza át, hogy az meglévő jogszabályokon alapulva tegye lehetővé az egyének számára azon intézkedések pontos azonosítását, amelyeket a hatóságok velük szemben hozhatnak.

4.4.2. *A 15. cikkben foglalt figyelmeztető jelzésekhez való hozzáférés*

A 18. cikk meghatározza, mely hatóságok férhetnek hozzá ezekhez a figyelmeztető jelzésekhez és milyen célokból. A 18. cikk (1) és (2) bekezdése meghatározza, mely hatóságok férhetnek hozzá a visszatérési irányelv alapján kiadott figyelmeztető jelzésekhez. A fent megfogalmazott észrevételek vonatkoznak erre a helyzetre is.

[1] A Schengeni Közös Ellenőrző Hatóság jelentése a 96.cikkben foglalt figyelmeztető jelzéseknek a Schengeni Információs Rendszerben való használatával kapcsolatos vizsgálatról, Brüsszel, 2005. június 20.

A rendeletjavaslat 18. cikkének (3) bekezdése olyan irányelv alapján biztosít hozzáférést a menekültstátusz megadásáért felelős hatóságok számára, amelyet még nem is javasoltak. Rendelkezésre álló szöveg hiányában az Európai Adatvédelmi Biztos megismétli a fenti észrevételeket.

4.4.3. *A 15. cikkben foglalt figyelmeztető jelzések megőrzési ideje*

A figyelmeztető jelzést a 20. cikknek megfelelően nem lehet a (kiutasítási vagy kitoloncolási) határozatban lefektetett, a beléptetés megtagadására vonatkozó időnél hosszabb ideig megőrizni. Ez megfelel az adatvédelmi szabályoknak. Ezenkívül a figyelmeztető jelzést öt év elteltével automatikusan törlik, hacsak az adatot a SIS II-be bevivő tagállam másképpen nem határoz.

Megfelelő nemzeti szintű ellenőrzésnek kell biztosítania, hogy nem kerül sor a megőrzési idő indokolatlan, automatikus meghosszabbítására, és hogy a tagállamok az ötéves határidő előtt törlik az adatot, amennyiben a beléptetés megtagadására vonatkozó idő ennél rövidebb.

4.5. **Megőrzési idő**

Bár a figyelmeztető jelzések megőrzésére vonatkozó elv változatlan marad (a figyelmeztető jelzést általában törölni kell a SIS II-ből, mihelyt a figyelmeztető jelzés által kért intézkedést végrehajtották), a javaslatoknak az lesz a következményük, hogy a figyelmeztető jelzések megőrzésének ideje rendszerint meghosszabbodik.

A Schengeni Egyezmény úgy rendelkezett, hogy az adatok megőrzésének szükségességét a bevitelüket követően legfeljebb három éven belül (leplezett megfigyelés céljából bevitt adatok esetében egy éven belül) felül kell vizsgálni. Az új javaslatok automatikus adattörlést irányoznak elő (amely ellen a kiadó tagállam ellentmondással élhet), a bevándorlással kapcsolatos adatok esetében 5 évvel a bevitelük után, a letartóztatásokkal, az eltűnt személyekkel és az igazságügyi eljárás lefolytatása érdekében körözött személyekkel kapcsolatos adatok esetében 10 évvel a bevitelük után, a leplezett megfigyelés alá helyezendő személyekkel kapcsolatos adatok estében pedig 3 évvel a bevitelük után.

Bár a tagállamok a figyelmeztető jelzés céljának elérését követően törölni fogják az adatokat, itt a maximális megőrzési idő jelentős növeléséről (a legtöbb esetben megháromszorozásáról) van szó, amelyet a Bizottság semmilyen módon sem indokol. A bevándorlásra vonatkozó adatokkal kapcsolatban feltételezhető, hogy az 5 éves időszak a visszatérésről szóló irányelvben javasolt beléptetési tilalom időtartamával van összefüggésben. A többi esetben az Európai Adatvédelmi Biztos tudomása szerint nincs olyan ok, amely indokolná a hosszabbítást.

Az adatok SIS-be történő bevitelének jelentős hatásai lehetnek az érintett személyek életére. Ez különösen a leplezett megfigyelés vagy célzott ellenőrzés céljából személyekre kiadott figyelmeztető jelzések esetében ad okot aggodalomra, mivel ezeket a figyelmeztető jelzéseket gyanú alapján is ki lehet adni.

Az Európai Adatvédelmi Biztos komoly indokot szeretne látni az adatmegőrzési idő meghosszabbítására. Amennyiben nincs meggyőző indok, azt javasolja, hogy a megőrzési időket a jelenlegi időtartamra csökkentsék, különösen a leplezett megfigyelés és a célzott ellenőrzés céljából kiadott figyelmeztető jelzések esetében.

4.6. **A járművek forgalmi engedélyének kiadásáért felelős hatóságok hozzáférése**

A fő probléma itt egy igen megkérdőjelezhető jogalapválasztásában rejlik. A Bizottság nem jár el meggyőző módon, amikor egy, az első pillérhez tartozó „közlekedési” jogalapot választ egy olyan intézkedéshez, amely a bűnmegelőzés és bűnüldözés (lopott gépjármű-kereskedelem) céljából hozzáférést biztosít a közigazgatási hatóságok számára a SIS-hez. A SIS II-höz való hozzáférés meggyőző indoklása és szilárd jogalapja szükségességének részletezésére e vélemény 4.2.2 pontjában már sor került.

Az Európai Adatvédelmi Biztos a Schengeni Közös Ellenőrző Hatóság e tárgyban tett észrevételeire hivatkozik, amelyeket a SIS II javasolt jogalapjáról szóló véleményében tett. Különösen a Schengeni Közös Ellenőrző Hatóság azon javaslatát kell figyelembe venni, amelynek értelmében a javasolt határozatot oly módon kell módosítani, hogy ezt a hozzáférést is belefoglalják.

5. A BIZOTTSÁG ÉS A TAGÁLLAMOK SZEREPE

A SIS II-vel kapcsolatos felelősségek világos meghatározása és kiosztása elsődleges fontosságú, nem csak a rendszer problémamentes működése, de az ellenőrzés szempontjából is. A felügyeleti hatáskörök kiosztása a felelősségek meghatározásából fog következni, itt tehát maximális pontosságra kell törekedni.

5.1. **A Bizottság szerepe**

Az Európai Adatvédelmi Biztos üdvözli mindkét javaslat III. fejezetét, amely meghatározza a Bizottság SIS II-vel kapcsolatos szerepét és hatásköreit (mint az „operatív irányítás” szerepét). Ez a meghatározás nem szerepel a VIS-javaslatban. Ugyanakkor önmagában ez a fejezet nem definiálja kimerítő módon a Bizottság szerepét. Valójában, ahogyan az már e vélemény 9. fejezetében is szerepel, a Bizottság a komitológiai eljáráson keresztül a rendszer végrehajtásában és irányításában is részt vesz.

Adatvédelmi szempontból a Bizottságnak van egy, a VIS és az Eurodac rendszer esetében már elfogadott szerepe, nevezetesen az operatív irányítás. A Bizottságnak a rendszer fejlesztésében és fenntartásában játszott fő szerepe mellett ezt sajátos adatkezelői szerepnek kell tekinteni. Amint az Európai Adatvédelmi Biztos a VIS-ről szóló véleményében már kifejtette, ez a szerep túlmutat az adatfeldolgozó szerepén, de korlátozottabb az adatkezelő szerepénél, mert a Bizottság nem fér hozzá a SIS II-ben feldolgozott adatokhoz.

Mivel a SIS II olyan összetett rendszerekre épül, amelyek közül néhány kialakulóban lévő technológiákat használ, az Európai Adatvédelmi Biztos ragaszkodik ahhoz, hogy megerősítsék a Bizottság hatáskörét a rendszereknek a biztonság és az adatvédelem terén rendelkezésre álló legjobb technológiák segítségével történő naprakésszé tételében.

A javaslatok 12. cikkét ki kell tehát egészíteni azzal, hogy a Bizottságnak rendszeresen javasolnia kell az ezen a területen rendelkezésre álló legmodernebb technológiák alkalmazását, amelyek növelik az adatvédelem és a biztonság szintjét, valamint megkönnyítik az ezen adatokhoz hozzáférő nemzeti hatóságok helyzetét.

5.2. **A tagállamok szerepe**

A tagállamok helyzete nem teljesen világos, mivel nehéz megállapítani, mely hatóság(ok) lesz(nek) az adatkezelő(k).

A javaslatok meghatározzák a SIS II nemzeti hivatal szerepét (az illetékes hatóságok SIS II-höz való hozzáférésének biztosítása), valamint a SIRENE hatóságok szerepét (a kiegészítő információk cseréjének biztosítása). A tagállamoknak biztosítaniuk kell továbbá a „nemzeti rendszereik" működését és biztonságát. Nem világos, hogy ez utóbbi a fent említett hatóságok valamelyikének hatáskörébe tartozik-e. Mindenesetre ebben a tekintetben pontosításra van szükség.

Adatvédelmi szempontból a Bizottságot és a tagállamokat közösen kell adatkezelőknek tekinteni, ahol mindkettőnek megvannak a maga felelősségei. Egyedül ezen egymást kiegészítő feladatok elismerésén keresztül lehet biztosítani, hogy a SIS II tevékenységének ne legyenek felügyelet nélküli területei.

6. **AZ ÉRINTETTEK JOGAI**

6.1. **Tájékoztatás**

6.1.1. *A javasolt rendelet*

A rendeletjavaslat 28. cikke tartalmazza az érintett tájékoztatáshoz való jogát, amely alapvetően a 95/46 irányelv 10. cikkéből következik. Ez üdvözlendő változás a jelenlegi helyzethez képest, mivel az Egyezmény nem tartalmazza kifejezetten a tájékoztatáshoz való jogot. Az alábbi pontokon ugyanakkor lehetne javítani.

Néhány információt még hozzá kellene adni a listához, ez hozzájárulna az érintettel szembeni méltányos bánásmód biztosításához ([1]). Az információnak tartalmaznia kellene az adatmegőrzés időtartamát, a figyelmeztető jelzést kiadó határozattal kapcsolatos felülvizsgálati kérelem vagy a határozat elleni fellebbezés benyújtásához való jog meglétét (egyes esetekben lásd a rendeletjavaslat 15. cikkének (3) bekezdését), az adatvédelmi hatóság segítségnyújtása igénybevételének lehetőségét, valamint a jogorvoslat lehetőségét.

A rendeletjavaslat nem tartalmazza, hogy az információt mikor kell átadni az érintettnek. Ez lehetetlenné teheti, hogy az érintett élni tudjon jogaival. Ezen jogok hatékonyságának biztosítása érdekében a rendeletnek tartalmaznia kellene, hogy a figyelmeztető jelzést kiadó hatóságtól függően pontosan mikor kell az információt megosztani az érintettel.

Praktikus megoldás lenne, ha a figyelmeztető jelzéssel kapcsolatos információkat elsőként az azt indokoló határozatban adnák meg: vagy bírósági vagy közigazgatási határozatban, amely a közrendet (…) fenyegető veszélyen alapul, vagy visszautazási tilalommal kísért kitoloncolási vagy kiutasítási határozatban. Ezt a rendelet 28. cikkében kellene lefektetni.

6.1.2. *A javasolt határozat*

A határozat 50. cikke kimondja, hogy az információt az érintett kérésére adják ki, és meghatározza az információátadás megtagadásának lehetséges indokait. Figyelembe véve az adatok természetét és feldolgozásuk módját érthető, hogy ezt a jogot bizonyos mértékben korlátozzák.

Ugyanakkor a tájékoztatáshoz való jognak nem lehet feltétele az érintett kérelme (ebben az esetben inkább a hozzáférés iránti kérelem meghatározásáról lenne szó). Feltételezhető, hogy az információ iránti „kérelem" szükségességét azok az esetek indokolták, amelyekben az érintettet nem lehet tájékoztatni, mivel tartózkodási helye ismeretlen.

A kérdés megoldása lenne, ha kivételt biztosítanának a tájékoztatáshoz való jog alól azokban az esetekben, amikor az információnyújtás lehetetlen vagy aránytalanul nagy erőfeszítést igényel. A határozat 50. cikkét ennek megfelelően kell módosítani.

([1]) Ezzel kapcsolatban lásd az Európai Adatvédelmi Biztosnak a vízuminformációs rendszer létrehozásáról szóló véleménye 3.10.1. pontját.

Ez a megoldás összhangban lenne a harmadik pillérben folyó adatvédelemről szóló kerethatározat-tervezet alkalmazásával is.

6.2. **Hozzáférés**

Mind a rendeletjavaslat, mind a határozati javaslat határidőt állapít meg a hozzáférés iránti kérelem megválaszolásához, ami előrelépést jelent. Ugyanakkor mivel a hozzáférési jog gyakorlására vonatkozó eljárást nemzeti szinten szabályozzák, felmerül a kérdés, hogy a javaslatokban meghatározott határidők hogyan viszonyulnak a már létező eljárásokhoz, különösen, ha az adott tagállamok rövidebb határidőt szabtak meg a hozzáférés iránti kérelem megválaszolására. Világossá kell tenni, hogy az érintett számára kedvezőbb határidőket kell alkalmazni.

6.2.1. *A javasolt rendelet*

Érdemes megjegyezni, hogy a hozzáférési jognak a Schengeni Egyezményben jelenleg meglévő korlátozásai („megtagadják az információk közlését, ha ez a figyelmeztető jelzéssel kapcsolatos jogszerű feladatok végrehajtása vagy harmadik személyek jogainak és szabadságainak védelme érdekében szükséges") nem szerepelnek a rendeletjavaslatban.

Ugyanakkor ez valószínűleg a 95/46/EK irányelv alkalmazhatóságából ered, mivel az (a 13. cikkében) kimondja, hogy a nemzeti jogszabályokban lehetőség van kivételek alkalmazására. Mindenesetre rá kell mutatni, hogy a 13. cikknek a hozzáférési jog korlátozása céljából a nemzeti jogszabályokban történő alkalmazása csak korlátozott esetekben fog megfelelni az emberi jogokról szóló európai egyezmény 8. cikkének.

6.2.2. *A javasolt határozat*

A határozati javaslat megtartja a hozzáférési jognak a Schengeni Egyezményben meghatározott korlátozását. A kerethatározat-javaslat lényegében a hozzáférési jog ugyanazon korlátozásait tartalmazza; e jogi eszköz elfogadása tehát nem eredményez jelentős változást ebben a tekintetben.

Mivel a bűnüldözési adatokhoz való hozzáférés több tagállamban „közvetetten" történik (azaz a nemzeti adatvédelmi hatóságon keresztül), hasznos lenne meghatározni, hogy a hozzáférési jog gyakorlása során az adatvédelmi hatóságoknak kötelező aktívan együttműködniük.

6.3. **A figyelmeztető jelzés kiadásáról szóló határozat felülvizsgálatához és az ellene történő fellebbezéshez való jog**

A rendelet 15. cikkének (3) bekezdése biztosítja a jogot ahhoz, hogy amennyiben a figyelmeztető jelzést elrendelő határozatot közigazgatási hatóság hozta, az érintett kérheti annak igazságügyi hatóság általi felülvizsgálatát vagy az igazságügyi hatósághoz fellebbezést nyújthat be. Ez a jelenlegi Schengeni Egyezményhez képest üdvözlendő javulást jelent.

Ez még inkább kihangsúlyozza az érintett teljes és időben történő tájékoztatásának szükségességét, amint az a fenti 6.1. pontban már említésre került: a tájékoztatás nélkül az új jog elvi vívmány maradna.

6.4. **Jogorvoslat**

A rendeletjavaslat 30. cikke és a határozati javaslat 52. cikke rendelkezik arról, hogy az érintett jogosult keresetet indítani vagy panaszt tenni az adott tagállam bíróságai előtt, ha nem biztosították számára az adatokhoz való hozzáférés vagy az adathelyesbítési, illetve -törlési jogát, valamint az információkéréshez vagy kártérítéshez való jogát.

A megfogalmazás („valamely tagállam területén tartózkodó bármely személy") azt sugallja, hogy a panaszosnak fizikai értelemben a tagállam területén kell tartózkodnia ahhoz, hogy keresetet nyújthasson be a bíróságokhoz. Ez a területi korlátozás indokolatlan és adott esetben hatástalanná teheti a jogorvoslathoz való jogot, mivel a panaszos igen gyakran pontosan azért nyújt be keresetet, mert megtagadják tőle a schengeni területre való belépést. Ezen túlmenően ami a rendeletjavaslatot illeti, mivel az irányelv a *lex generalis*, annak 22. cikkét kell figyelembe venni; ez pedig kimondja, hogy tartózkodási helyétől függetlenül „mindenkinek" joga van jogorvoslathoz. A kerethatározat-javaslat sem tartalmaz területi korlátozást. Az Európai Adatvédelmi Biztos a 30. és 52. cikkben szereplő területi korlátozás elhagyását javasolja.

7. ELLENŐRZÉS

7.1. **Bevezető megjegyzés: felelősségmegosztás**

A javaslatok hatáskörüknek megfelelően megosztják az ellenőrzési feladatokat a nemzeti ellenőrző hatóságok ([1]) és az Európai Adatvédelmi Biztos között. Ez összhangban áll a javaslatoknak a SIS II működésére és használatára alkalmazandó joggal és felelősségekkel kapcsolatos megközelítésével, valamint a hatékony ellenőrzés szükségességével.

Az Európai Adatvédelmi Biztos ezért üdvözli a rendeletjavaslat 31. cikkében és a határozati javaslat 53. cikkében foglalt ezen megközelítést. Ugyanakkor a feladatok jobb megértése és pontosítása érdekében az Európai Adatvédelmi Biztos azt javasolja, hogy a cikkeket több rendelkezésre bontsák, amelyek mindegyike az ellenőrzés valamely szintjét érintené, amint azt a VIS-ről szóló javaslatban is tették.

([1]) Az Europol és az Eurojust ellenőrző hatóságai is érintve vannak, de kisebb mértékben.

7.2. **A nemzeti adatvédelmi hatóságok által végzett ellenőrzés**

A rendeletjavaslat 31. cikkének és a határozati javaslat 53. cikkének megfelelően valamennyi tagállamnak biztosítania kell, hogy a SIS II-ben található személyes adatok feldolgozásának jogszerűségét egy független hatóság ellenőrizze.

A határozati javaslat 53. cikke biztosítja azt a jogot, mely szerint a személyek kérhetik az ellenőrző hatóságtól, hogy az ellenőrizze a velük kapcsolatos adatok feldolgozásának jogszerűségét. Hasonló rendelkezést a rendeletjavaslat nem tartalmaz, mivel *lex generalis*-ként az irányelv alkalmazandó. Úgy kell tehát tekinteni, hogy a nemzeti adatvédelmi hatóságok a SIS II-vel kapcsolatban is gyakorolhatják a 95/46/EK irányelv 28. cikkében rájuk ruházott hatásköröket, beleértve a feldolgozott adatok jogszerűségének ellenőrzését is. A rendelet 31. cikkének (1) bekezdése a hatóságok feladatának pontosítása, és nem tekinthető ezen hatáskörök korlátozásának. A hatáskörök elismerését a rendeletjavaslat szövegében világossá kell tenni.

A határozati javaslat több feladatot tulajdonít a nemzeti ellenőrző hatóságoknak, mivel más a *lex generalis*-a. Ugyanakkor nem ésszerű egy olyan helyzet, amelyben az ellenőrző hatóságoknak a feldolgozott adatok kategóriájától függően különböző feladataik és hatásköreik vannak, és gyakorlati megvalósítása is igen nehéz. Ezt a helyzetet tehát el kell kerülni, vagy úgy, hogy a határozati javaslat szövegében is ugyanazokkal a hatáskörökkel ruházzák fel ezeket a hatóságokat, vagy úgy, hogy egy másik, az adatvédelmi hatóságoknak több hatáskört biztosító *lex generalis*-ra (nevezetesen a harmadik pillérben folyó adatvédelemről szóló kerethatározatra) hivatkoznak.

7.3. **Az Európai Adatvédelmi Biztos által végzett ellenőrzés**

Az Európai Adatvédelmi Biztos ellenőrzi, hogy a Bizottság adatfeldolgozási tevékenységei a javaslatoknak megfelelően folynak-e. Az Európai Adatvédelmi Biztosnak hasonlóképpen képesnek kell lennie a 45/2001 rendeletben meghatározott hatáskörei gyakorlására, figyelembe véve ugyanakkor azt a tényt, hogy a Bizottság hatáskörei magukkal az adatokkal kapcsolatban korlátozottak.

Hasznos még megjegyezni, hogy a 45/2001 rendelet 46. cikkének f) pontja értelmében az Európai Adatvédelmi Biztos „együttműködik a nemzeti felügyelő hatóságokkal olyan mértékben, amilyen mértékben erre e hatóságoknak saját feladatkörük ellátásához szükségük van”. A tagállamokkal való együttműködés a SIS II ellenőrzése során nem csak a javaslatokból, de a 45/2001 rendeletből is következik.

7.4. **Közös ellenőrzés**

A javaslatok azt is elismerik, hogy szükség van a különböző érintett hatóságok ellenőrző tevékenységének összehangolására. A rendeletjavaslat 31. cikke és a határozati javaslat 53. cikke kimondja, hogy „a nemzeti ellenőrző hatóságok és az Európai Adatvédelmi Biztos aktívan együttműködnek. Az Európai Adatvédelmi Biztos e célból évente legalább egyszer ülést hív össze.”

Az Európai Adatvédelmi Biztos üdvözli ezt a javaslatot, amely lényegében tartalmazza az ellenőrzéssel nemzeti és európai szinten megbízott hatóságok közötti – alapvető fontosságú – együttműködés kialakításához szükséges valamennyi elemet. Hangsúlyozni kell, hogy a javaslatok évi legalább egy ülésről rendelkeznek, de ezt valóban minimumnak kell tekinteni.

A rendelkezéseket (a rendeletjavaslat 31. cikke és a határozati javaslat 53.cikke) ugyanakkor az összehangolás tartalmának tekintetében pontosítani lehetne. A jelenlegi közös ellenőrző hatóság hatásköre kiterjed az Egyezménnyel kapcsolatos értelmezésbeli vagy alkalmazásbeli nehézségek vizsgálatára, a független ellenőrzés vagy a hozzáférési jog gyakorlása során felmerülő problémák kivizsgálására, valamint a meglévő problémák közös megoldásához összehangolt javaslatok kidolgozására.

Az új javaslatok nem vezethetnek a közös ellenőrzés jelenlegi alkalmazási körének csökkentéséhez. Amennyiben nem kérdéses, hogy az adatvédelmi hatóságok a SIS II-vel kapcsolatban gyakorolhatják azokat az ellenőrzési hatásköröket, amelyekkel az irányelv felruházta őket, az e hatóságok közötti együttműködés a SIS II ellenőrzésének több szempontját is magában foglalhatja, beleértve a jelenlegi közös ellenőrző hatóság által a Schengeni Egyezmény 115. cikke alapján végzett feladatokat.

Hasznos lenne ugyanakkor, ha a teljes világosság kedvéért ezt kifejezetten megemlítenék a javaslatokban.

8. **BIZTONSÁG**

A SIS II optimális biztonsági szintjének kialakítása és fenntartása alapvető követelmény az adatbázisban tárolt személyes adatok megfelelő védelmének biztosítása szempontjából. A megfelelő védelmi szint elérése érdekében megfelelő biztosítékokat kell bevezetni a rendszer infrastruktúrájával és az érintett személyekkel kapcsolatos lehetséges kockázatok kezelésére. Erre a javaslat több része kitér, és e kérdésben még némi javítás szükséges.

A javaslat 10. és 13. cikke több intézkedést is tartalmaz az adatbiztonság érdekében, és meghatározza, mely visszaéléseket kell megelőzni. Az Európai Adatvédelmi Biztos üdvözli, hogy a biztonsági intézkedések rendszeres (ön)ellenőrzésére vonatkozó rendelkezéseket illesztettek ezekbe a cikkekbe.

Ugyanakkor a határozati javaslat 59. cikkének és a rendeletjavaslat 34. cikkének – melyek az ellenőrzésre és az értékelésre vonatkoznak – nem csak az eredmény, a költséghatékonyság és a szolgáltatásminőség szempontjaira kell kiterjedniük, hanem a jogi követelményeknek való megfelelésre is, különösen az adatvédelem területén. Az Európai Adatvédelmi Biztos ezért azt javasolja, hogy ezen cikkek alkalmazási körét terjesszék ki az eljárások jogszerűségének ellenőrzésére és az azokkal kapcsolatos jelentéstételre.

Ezen túlmenően a határozati javaslat 10. cikke (1) bekezdésének f) pontja vagy 18. cikke és a rendeletjavaslat 17. cikke – amelyek az adatokhoz való hozzáféréshez kellően felhatalmazott személyzetre vonatkoznak – kiegészítéseként meg kell határozni, hogy a tagállamoknak (valamint az Europol-nak és az Eurojust-nak) biztosítaniuk kell a pontos felhasználói profilok rendelkezésre állását (amelyeket ellenőrzés céljából a nemzetközi ellenőrző hatóságok rendelkezésére kell bocsátani). A felhasználói profilokon kívül a tagállamoknak létre kell hozniuk a felhasználók személyazonosságát tartalmazó teljes listát, és ezeket folyamatosan frissíteniük kell. Ugyanez vonatkozik értelemszerűen a Bizottságra is.

Ezeket a biztonsági intézkedéseket ellenőrzési és szervezési biztosítékok egészítik ki. A javaslatok 14. cikke felsorolja mindazokat a feltételeket és célokat, amelyek alapján valamennyi adatfeldolgozási műveletről nyilvántartást kell vezetni. Ezeket a nyilvántartásokat nemcsak az adatvédelem ellenőrzésére és az adatbiztonság biztosítására tárolják, hanem a SIS II 40. cikkben előírt rendszeres önellenőrzésének megerősítéséhez is. Ezek az önellenőrzési jelentések elősegítik a felügyeleti hatóságok feladatainak hatékony végrehajtását, amelyek ily módon be tudják azonosítani a leggyengébb pontokat, és saját önellenőrzésük során ezekre tudnak összpontosítani.

Amint a vélemény korábbi részében már említésre került, a rendszerhez való hozzáférési pontok megtöbbszörözésének szükségességét körültekintően indokolni kell, mivel az automatikusan megnöveli a visszaélések veszélyét. A javaslatok 4. cikke (1) bekezdése b) pontjának következésképpen elő kell írnia a második hozzáférési pont szükségességének konkrét bizonyítását.

A javaslatok nem indokolják világosan a központi rendszer nemzeti szintű másolatainak szükségességét, és komoly aggodalmat keltenek a rendszer egészének veszélyességi szintje és biztonsága tekintetében, mint például az alábbiak:

– a másolatok többszöröződése megnöveli a visszaélések veszélyét (különösen az új típusú adatok, mint például a biometrikus adatok jelenlétét is figyelembe véve);

– a másolatok által érintett adatok nincsenek pontosan meghatározva;

– a 9. cikkben foglalt, pontossággal, minőséggel és rendelkezésre állással kapcsolatos követelmények komoly technikai kihívást jelentenek, és ezáltal a rendelkezésre álló technológia fejlődésének megfelelően megnöveli a költségeket;

– a másolatok nemzeti hatóságok általi ellenőrzése további emberi és anyagi erőforrásokat követelhet meg, amelyek elképzelhető, hogy nem minden esetben állnak rendelkezésre.

Figyelemmel a kockázatokra az Európai Adatvédelmi Biztos sem a nemzeti másolatok szükségességéről (tekintetbe véve a rendelkezésre álló technológiákat), sem az azok használatából eredő többletértékről nincs meggyőződve. Azt javasolja, hogy töröljék annak lehetőségét, hogy a tagállamok nemzeti másolatokat használjanak.

Ha azonban mégis nemzeti másolatokat készítenek, az Európai Adatvédelmi Biztos emlékeztet, hogy nemzeti használatuk során a célhoz kötöttség elvét következetesen kell alkalmazni. A nemzeti másolatot hasonlóképpen kizárólag a központi adatbázison keresztül lehet kérni.

A személyes adatok feldolgozásának jogszerűsége az adatbiztonság és az adatsértetlenség szigorú betartásán alapul. Az Európai Adatvédelmi Biztos hatékony módon ellenőrizni fogja ezeket a folyamatokat, amennyiben az adatbiztonságon kívül az adatok sértetlenségét is ellenőrizheti a rendelkezésre álló naplókon keresztül. A 14. cikk (6) bekezdését ki kell tehát egészíteni az „adatsértetlenséggel”.

9. **KOMITOLÓGIA**

A javaslatok több olyan esetben is komitológiai eljárást írnak elő, ahol a SIS II végrehajtásával vagy irányításával kapcsolatos technológiai jellegű döntésre van szükség. Ahogyan a VIS-ről szóló véleményben hasonló okokból már szerepel, ezek a döntések jelentős hatással lesznek a célhoz kötöttség és az arányosság elvének megfelelő alkalmazására.

Az Európai Adatvédelmi Biztos figyelmeztet arra, hogy az adatvédelemre lényeges hatást gyakorló döntéseket – mint például az adatokhoz való hozzáférésre és az adatok bevitelére, a kiegészítő információk cseréjére, az adatok minőségére és figyelmeztető jelzések közötti összeegyeztethetőségre, a nemzeti másolatok technikai megfelelőségére, stb. vonatkozó döntéseket – rendelet vagy határozat formájában kell meghozni, lehetőleg az együttdöntési eljárás alkalmazásán keresztül ([1]).

([1]) Ezzel kapcsolatban lásd még az Európai Adatvédelmi Biztosnak a vízuminformációs rendszerről szóló véleménye 3.12. pontját és az Európai Adatvédelmi Biztosnak az elektronikus hírközlési közszolgáltatások nyújtásával összefüggésben feldolgozott adatok megőrzéséről szóló irányelvjavaslatról szóló, 2005. szeptember 26-án kiadott véleményének 60. pontját.

Az adatvédelemre hatással levő egyéb esetekben az Európai Adatvédelmi Biztosnak lehetőséget kell biztosítani, hogy véleményt nyilvánítson a bizottságok általi választásokról.

Az Európai Adatvédelmi Biztos tanácsadói szerepét a határozat 60. és 61. cikkében, valamint a rendelet 35. cikkében rögzíteni kell.

A figyelmeztető jelzések összekapcsolására vonatkozó technikai szabályok konkrét esetében (a rendelet 26. és a határozat 46. cikke) a komitológia egy eltérő módjának (tanácsadó a határozat esetében és szabályozó a rendelet esetében) szükségessége további magyarázatra szorul.

10. **INTEROPERABILITÁS**

Mivel a Bizottságnak a kialakulóban lévő uniós rendszerek interoperabilitásáról szóló közleménye még mindig nem készült el, a tervezett, de még meg nem határozott szervi együttműködés többletértékét nehéz megfelelően értékelni.

Ezzel összefüggésben az Európai Adatvédelmi Biztos hivatkozni kíván a terrorizmus elleni küzdelemről szóló 2004. március 25-i tanácsi nyilatkozatra, amelyben a Bizottság felkérést kap arra, hogy javaslatokat nyújtson be az információs rendszerek (SIS, VIS és Eurodac) közötti interoperabilitás és szinergiák erősítése érdekében. Hivatkozni kíván továbbá a jelenleg folyó tárgyalásokra is, amelyek arról szólnak, hogy a jövőben mely szervezetet bízzák meg a nagy rendszerek irányításával (lásd e vélemény 3.8. pontját is).

Az Európai Adatvédelmi Biztos a vízuminformációs rendszerről szóló véleményében már megállapította, hogy az interoperabilitás kritikus és rendkívül fontos követelménye az olyan összetett informatikai rendszerek hatékony működésének, mint a SIS II. Az interoperabilitás lehetővé teszi az összköltségek következetes csökkentését, valamint a heterogén elemek természetes feltorlódásának elkerülését.

– Az e politika valamennyi alkotóelemére ugyanazon eljárási szabály bevezetésén keresztül az interoperabilitás hozzájárulhat azon célkitűzés eléréséhez, hogy egy olyan területen tartsák fenn a biztonság magas szintjét, amelyben a tagállamok között nincs belső határellenőrzés. Rendkívül fontos ugyanakkor megkülönböztetni az interoperabilitás két szintjét:

  – Az uniós tagállamok közötti interoperabilitás mindenképpen kívánatos; a valamely tagállam hatóságai által küldött figyelmeztető jelzéseknek ugyanis interoperábilisnak kell lenniük a bármely más tagállam által küldött figyelmeztető jelzésekkel.

  – Ennél sokkal inkább megkérdőjelezhető a különböző célokból vagy harmadik országok rendszereivel kiépített rendszerek közötti interoperabilitás.

A rendszer céljainak körülhatárolására és a „funkcióbeli csúszások” megelőzésére használt, rendelkezésre álló biztosítékok között a különböző technológiai szabványok használata hozzájárulhat ehhez az elhatároláshoz. Továbbá a két különböző rendszer közötti interakció bármely formáját szigorúan dokumentálni kellene. Az interoperabilitás nem teremthet olyan helyzetet, amelyben egy hatóság, amely nem jogosult bizonyos adatokhoz való hozzáférésre vagy az adatok használatára, egy másik információs rendszeren keresztül hozzáférést szerezhet. Amennyire az a javaslatokból kiolvasható, úgy tűnik például, hogy a SIS II működésének első éveiben nem fog automatikus ujjlenyomat-azonosító rendszer (AFIS) rendelkezésre állni; csak egy jövőbeni biometrikus keresőprogramra való utalás található bennük. Amennyiben felmerül annak lehetősége, hogy más uniós rendszerek AFIS-át használják, azt az ilyen szervi együttműködés által megkövetelt biztosítékok használata mellett világosan dokumentálni kell.

Az Európai Adatvédelmi Biztos ismételten hangsúlyozni kívánja, hogy a rendszerek interoperabilitásának végrehajtása nem sértheti a célhoz kötöttség elvét, és hogy minden, e témával kapcsolatos javaslatot be kell nyújtani hozzá.

11. **A KÖVETKEZTETÉSEK ÖSSZEFOGLALÁSA**

11.1. **Általános szempontok**

1. Az Európai Adatvédelmi Biztos üdvözli a javaslatok számos vonatkozását, amelyek a jelenlegi helyzethez képest néhány ponton javulást jelentenek. Elismeri, hogy az adatvédelemre vonatkozó rendelkezéseket általában véve nagy körültekintéssel dolgozták ki.

2. Az Európai Adatvédelmi Biztos hangsúlyozza, hogy az összetett új jogi szabályozásnak

   – biztosítania kell az adatvédelem magas szintjét,

   – kiszámíthatónak kell lennie a polgárok és az adatokat használó hatóságok számára,

   – következetesnek kell lennie a különböző (első vagy harmadik pillérbeli) keretek között történő alkalmazása során.

3. Másfelől az olyan új elemeknek a SIS II-höz való hozzáadását, amelyek megnövelhetik a rendszer befolyását az egyének életére, a véleményben leírt szigorúbb biztosítékok alkalmazása mellett kell végrehajtani. Itt különösen az alábbiakra kell gondolni:

– A SIS II-höz való hozzáférést nem lehet meggyőző indoklás nélkül új hatóságok számára biztosítani. A hozzáférést a lehetőségekhez mérten korlátozni kell mind az elérhető adatok, mind a felhatalmazott személyek tekintetében.

– A figyelmeztető jelzések közötti összekapcsolások sosem vezethetnek – még közvetve sem – a hozzáférési jogok megváltoztatásához.

– El nem fogadott jogszabályok nem tekinthetők a SIS II-be való adatbevitel (a beléptetés megtagadása céljából kiadott figyelmeztető jelzés) érvényes jogalapjának.

– A járművek forgalmi engedélyének kiadásáért felelős hatóságok hozzáférésének jogalapját felül kell vizsgálni, mivel ez a hozzáférés alapvetően a bűnözés elleni küzdelmet szolgálja.

– Az Európai Adatvédelmi Biztos elismeri, hogy a biometrikus adatok használata javítja a rendszer működését és segíti a személyazonossággal való visszaélés áldozatait. Ugyanakkor úgy tűnik, hogy bevezetésük hatásait nem gondolták át kellőképpen, valamint ezen adatok megbízhatóságát is túlbecsülték.

11.2. **Egyedi megjegyzések**

1. Az Európai Adatvédelmi Biztos üdvözli, hogy a Bizottság elismerte, a 45/2001 rendeletet kell alkalmazni minden, a SIS II-ben általa végzett adatfeldolgozási tevékenység során, mivel ez hozzájárul az egyének alapvető jogainak és szabadságainak védelmére vonatkozó szabályok következetes és egységes alkalmazásához a személyes adatok feldolgozása tekintetében.

2. A szigorú célhoz kötöttség nemzeti szintű biztosítása érdekében az Európai Adatvédelmi Biztos azt javasolja, hogy a SIS II javaslatokba (konkrétan a rendeletjavaslat 21. cikkébe, valamint a határozati javaslat 40. cikkébe) vegyenek bele egy, a Schengeni Egyezmény jelenlegi 102. cikke (4) bekezdésével azonos célú rendelkezést, amely korlátozza a tagállamok lehetőségét, hogy az adatok olyan felhasználására vonatkozó rendelkezéseket hozzanak, amely a SIS II szövegekben nem szerepel.

3. Amikor egy hatóságnak hozzáférést biztosítanak a SIS II-höz, az alábbi szigorú feltételeket kell alkalmazni:

– A hozzáférésnek összeegyeztethetőnek kell lennie a SIS II általános céljaival és összhangban kell lennie annak jogalapjával.

– A SIS II-höz való hozzáférés szükségességét bizonyítani kell.

– Az adatok felhasználását kifejezetten és korlátozó módon meg kell határozni.

– A hozzáférés feltételeit meg kell határozni és korlátozni kell. Naprakész listát kell készíteni a SIS II-höz való hozzáférésre feljogosított személyekről, az Europol és az Eurojust tekintetében is.

– Az, hogy ezen hatóságok hozzáféréssel rendelkeznek a SIS II adatokhoz, soha nem képezhet jogalapot ahhoz, hogy a rendszerbe olyan adatokat vigyenek be, vagy a rendszerben olyan adatokat tároljanak, amelyek nem célravezetőek azon konkrét figyelmeztető jelzés szempontjából, amelynek a részét képezik.

– Az adatmegőrzés időtartamát nem lehet meghosszabbítani, amennyiben ez nem szükséges azon cél eléréséhez, amely miatt az adatot bevitték.

4. Az Európai Adatvédelmi Biztos arra ösztönzi a Bizottságot, hogy az Europol és az Eurojust konkrét esetében pontosan határozza meg, mely feladatok elvégzéséhez indokolt a hozzáférés. Az Europol és az Eurojust általi hozzáférést továbbá azon személyek adataira kell korlátozni, akiknek a neve ezen szervezetek anyagaiban már szerepel. Javasolt, hogy az Europol és az Eurojust számára csak egy hozzáférési pontot biztosítsanak.

5. A beléptetés megtagadása céljából kiadott figyelmeztető jelzések tekintetében a még el nem fogadott jogszabályokon alapuló rendelkezéseket vagy törölni kell, vagy oly módon kell őket – a már meglévő jogszabályok alapján – újrafogalmazni, hogy az érintett személyeknek lehetőségük legyen megtudni, hogy a hatóságok milyen intézkedéseket hozhatnak velük kapcsolatban.

6. Az adatmegőrzési időszakot megfelelő komoly indok nélkül meghosszabbították. Amennyiben nincs meggyőző indok, a megőrzési időket – különösen a leplezett figyelés és a célzott ellenőrzés céljából kiadott figyelmeztető jelzések esetében – a jelenlegi időtartamra kell csökkenteni.

7. A Bizottság szerepe az operatív irányítás. A Bizottságnak a rendszer fejlesztésében és fenntartásában játszott fő szerepe mellett ezt sajátos adatkezelői szerepnek kell tekinteni. Ez a szerep túlmutat az adatfeldolgozó szerepén, de korlátozottabb egy rendes adatkezelő szerepénél, mert a Bizottság nem fér hozzá a SIS II-ben feldolgozott adatokhoz.

   A javaslatok 12. cikkét ki kell egészíteni azzal, hogy e szerepének keretében a Bizottságnak rendszeresen javasolnia kell az ezen a területen rendelkezésre álló legmodernebb technológiák alkalmazását, amelyek növelik az adatvédelem és a biztonság szintjét.

8. A tagállamok szerepét illetően pontosítani kell, hogy mely hatóságok töltenek be adatkezelői funkciókat.

9. Az érintett tájékoztatására vonatkozóan az alábbiakat kell figyelembe venni:

   – A rendeletjavaslatban a következő néhány információval kell kiegészíteni a listát: az adatmegőrzés időtartama, a figyelmeztető jelzést kiadó határozattal kapcsolatos felülvizsgálati kérelem vagy a határozat elleni fellebbezés benyújtásához való jog megléte, az adatvédelmi hatóság segítségnyújtása igénybevételének lehetősége, valamint a jogorvoslat lehetősége.

     A tájékoztatás időpontjával kapcsolatosan kötelezővé kell tenni, hogy a figyelmeztető jelzéssel kapcsolatos információkat elsőként az azt indokoló határozatban adják meg.

   – A határozati javaslat 50. cikkét oly módon kell módosítani, hogy a tájékoztatáshoz való jog gyakorlásához az érintettnek ne kelljen kérelmet benyújtania.

10. A hozzáférés iránti kérelem megválaszolásának határidejével kapcsolatban már önmagában az a tény is üdvözlendő, hogy a javaslatok határidőket szabnak meg. Amennyiben a nemzeti jogszabályok szintén meghatároznak határidőket, világossá kell tenni, hogy az érintett számára kedvezőbb határidőket kell alkalmazni.

    Ezen túlmenően hasznos lenne meghatározni, hogy a hozzáférési jog gyakorlása során az adatvédelmi hatóságoknak kötelező aktívan együttműködniük.

11. A jogorvoslathoz való jogot illetően az Európai Adatvédelmi Biztos a 30. és 52. cikkben található területi korlátozás elhagyását javasolja.

12. A nemzeti adatvédelmi hatóságok hatáskörét illetően az alábbiakat kell figyelembe venni:

    – a rendeletben: úgy kell tekinteni, hogy a SIS II-vel kapcsolatban minden, a 95/46/EK irányelv 28. cikkében rájuk ruházott hatáskört gyakorolhatják; ezt a rendeletjavaslat szövegében pontosítani kell.

    – a határozati javaslatban: az ellenőrző hatóságokat ugyanazokkal a hatáskörökkel kell felruházni, mint a rendeletben/irányelvben.

13. Az Európai Adatvédelmi Biztos hatáskörével kapcsolatban a következőket kell figyelembe venni: az Európai Adatvédelmi Biztosnak képesnek kell lennie a 45/2001 rendeletben meghatározott hatáskörei gyakorlására, figyelembe véve ugyanakkor azt a tényt, hogy a Bizottság hatáskörei magukkal az adatokkal kapcsolatban korlátozottak.

14. Az összehangolt ellenőrzésre vonatkozóan a következőket kell tekintetbe venni: a javaslatok azt is elismerik, hogy szükség van a különböző érintett hatóságok ellenőrző tevékenységének összehangolására. Az Európai Adatvédelmi Biztos üdvözli azt a tényt, hogy a javaslatok lényegében tartalmazzák az ellenőrzéssel nemzeti és európai szinten megbízott hatóságok közötti együttműködés kialakításához szükséges valamennyi elemet. A rendelkezéseket (a rendeletjavaslat 31. cikke és a határozati javaslat 53. cikke) ugyanakkor az összehangolás tartalmának tekintetében pontosítani lehetne.

15. A javaslat 10. és 13. cikke számos, az adatbiztonsággal kapcsolatos intézkedést tartalmaz; a biztonsági intézkedések rendszeres (ön)ellenőrzésére vonatkozó rendelkezések beillesztése üdvözlendő.

    – Ugyanakkor a határozati javaslat 59. cikkének és a rendeletjavaslat 34. cikkének – melyek az ellenőrzésre és az értékelésre vonatkoznak – nem csak az eredmény, a költséghatékonyság és a szolgáltatásminőség szempontjaira kell kiterjedniük, hanem a jogi követelményeknek való megfelelésre is, különösen az adatvédelem területén. Ezeket a rendelkezéseket ennek megfelelően módosítani kell.

    – Ezen túlmenően a határozati javaslat 10. cikke (1) bekezdésének f) pontja vagy 18. cikke és a rendeletjavaslat 17. cikke kiegészítéseként meg kell határozni, hogy a tagállamoknak, az Europol-nak és az Eurojustnak biztosítaniuk kell a pontos felhasználói profilok rendelkezésre állását (amelyeket ellenőrzés céljából a nemzetközi ellenőrző hatóságok rendelkezésére kell bocsátani). A felhasználói profilokon kívül a tagállamoknak létre kell hozniuk a felhasználók személyazonosságát tartalmazó teljes listát, és ezeket folyamatosan frissíteniük kell. Ugyanez vonatkozik a Bizottságra is.

    – A személyes adatok feldolgozásának jogszerűsége az adatbiztonság és az adatsértetlenség szigorú betartásán alapul. Az Európai Adatvédelmi Biztost fel kell hatalmazni arra, hogy a rendelkezésre álló naplókon keresztül az adatbiztonságon kívül az adatok sértetlenségét is ellenőrizhesse. A 14. cikk (6) bekezdését ki kell tehát egészíteni az „adatsértetlenséggel”.

16. A nemzeti másolatok használata további kockázatokat rejthet magában. Az Európai Adatvédelmi Biztos nincs meggyőződve sem a nemzeti másolatok szükségességéről (tekintetbe véve a rendelkezésre álló technológiákat), sem az azok használatából eredő többletértékről. Azt javasolja, hogy kerüljék, vagy legalább jelentősen korlátozzák a tagállamok azon lehetőségét, hogy nemzeti másolatokat használjanak. Ha azonban mégis nemzeti másolatokat készítenek, akkor nemzeti használatuk során a szigorú célhoz kötöttségi elvet kell alkalmazni. A nemzeti másolatból adatot kizárólag a központi adatbázishoz hasonlóan lehet kérni.

17. A komitológiával kapcsolatban az alábbiakra kell figyelmet fordítani: az adatvédelemre lényeges hatást gyakorló döntéseket rendelet vagy határozat formájában kell meghozni, lehetőleg az együttdöntési eljárás alkalmazásán keresztül. Azokon a területeken, ahol a komitológiai eljárást alkalmazzák, az Európai Adatvédelmi Biztos tanácsadói szerepét rögzíteni kell a határozat 60. és 61. cikkében, valamint a rendelet 35. cikkében.

18. A rendszerek interoperabilitásának végrehajtása nem sértheti a célhoz kötöttség elvét, és minden e témával kapcsolatos javaslatot be kell nyújtani az Európai Adatvédelmi Biztosnak.

Kelt Brüsszelben, 2005. október 19-én.

Peter HUSTINX

Európai Adatvédelmi Biztos