# EURÓPAI ADATVÉDELMI BIZTOS

## Az európai adatvédelmi biztos véleménye a vízuminformációs rendszerhez (VIS) a tagállamok belső biztonságért felelős hatóságai, valamint az Europol számára a terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében, konzultációs céllal történő hozzáférésről szóló tanácsi határozati javaslatról (COM(2005) 600 végleges)

(2006/C 97/03)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

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

tekintettel az Európai Unió alapjogi chartájára, 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 45/2001/EK európai parlamenti és tanácsi rendeletre, és különösen annak 41. cikkére,

tekintettel a Bizottságtól 2005. november 29-én kapott, a 45/2001/EK rendelet 28. cikkének (2) bekezdése szerinti véleménykérésre,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

### 1. BEVEZETÉS

#### 1.1. Előzetes megjegyzés

A vízuminformációs rendszerhez (VIS) a tagállamok belső biztonságért felelős hatóságai, valamint az Europol számára a terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében, konzultációs céllal történő hozzáférésről szóló tanácsi határozati javaslatot (a továbbiakban: a javaslat) a Bizottság 2005. november 24-én levélben megküldte az európai adatvédelmi biztos részére. Az európai adatvédelmi biztos ezt a levelet arra irányuló kérelemnek tekinti, hogy a Közösség intézményeit és szerveit – a 45/2001/EK rendelet 28. cikke (2) bekezdésének megfelelően – tanáccsal lássa el. Az európai adatvédelmi biztos szerint ezt a véleményt meg kell említeni a határozat preambulumában.

Az európai adatvédelmi biztos fontosnak tartja, hogy ezzel az érzékeny kérdéssel kapcsolatosan véleményt nyilvánítson, mivel ez a javaslat közvetlenül következik a felügyelete alá tartozó vízuminformációs rendszer (VIS) létrehozásából, amellyel kapcsolatosan 2005. március 23-án véleményt adott ki [1]. Ebben a véleményben már szerepel a bűnüldöző hatóságok általi hozzáférés feltételezése (lásd: alább); a VIS-hez új hozzáférési jogok teremtése – az adatvédelem szempontjából – meghatározó hatást gyakorol a rendszerre. Éppen ezért az ezen javaslattal kapcsolatos véleménynyilvánítás az első vélemény szükségszerű következménye.

#### 1.2. A javaslat fontossága

a) *Összefüggések*

Ezen javaslat nemcsak saját jogán fontos, hanem azért is, mert részét képezi annak a folyamatnak, melynek során a bűnüldöző hatóságok számos információs és azonosító rendszerhez kapnak hozzáférést. Többek között ezt is említi a bel- és igazságügyi együttműködés területén az európai adatbázisok közötti hatékonyság fokozásáról, interoperabilitásuk javításáról és szingergiahatásaikról [2] szóló, 2005. november 24-i bizottsági közlemény, különösen annak 4.6. pontja: *„A terrorizmus és a bűnözés elleni küzdelem célkitűzéseivel összefüggésben a Tanács jelenleg hiányosságként értékeli azt, hogy a belső biztonságért felelős hatóságok nem rendelkeznek hozzáféréssel a VIS adataihoz. Ugyanez elmondható a SIS II bevándorlási, illetve az EURODAC adatairól."*

Éppen ezért lehet ezt a javaslatot a más adatbázisok összefüggésében kifejlesztett hasonló jogi eszközök előfutárának is tekinteni, azon eseteknek a kezdetekben történő meghatározása pedig, amelyekben ez a hozzáférés megadható, kulcsfontosságú.

[1] Az európai adatvédelmi biztos véleménye a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló európai parlamenti és tanácsi rendeletre vonatkozó javaslatról (COM(2004) 835 végleges).

[2] COM(2005) 597 végleges.

b) *A VIS-hez való új hozzáférés hatása*

Az európai adatvédelmi biztos felismeri annak szükségességét, hogy a bűnüldöző hatóságok a terrorista cselekmények vagy egyéb súlyos bűncselekmények elkövetőinek azonosításához a lehető legjobb eszközökkel rendelkezzenek. Annak is tudatában van, hogy a VIS adatai ezen hatóságok számára bizonyos körülmények között lényeges információforrást jelentenek.

Mindazonáltal – bármennyire indokolttá teszi is a terrorizmus elleni küzdelem – messze nem jelentéktelen az első pillérbeli adatbázisokhoz való hozzáférés megadása bűnüldöző szervek számára. Nem szabad elfelejteni, hogy a VIS olyan információs rendszer, amelyet az európai vízumpolitika alkalmazása érdekében, és nem bűnüldöző eszközként fejlesztettek ki. A rutinszerű hozzáférés valóban a célhozkötöttség elvének súlyos megsértését jelentené. Azon utazók magánéletébe való aránytalan beavatkozást jelentene, akik a vízum megszerzése érdekében hozzájárultak adataik feldolgozásához, és akik elvárják, hogy adataik összegyűjtésére, megtekintésére és átadására kizárólag ebből a célból kerüljön sor.

Mivel az információs rendszereket egyedi céllal alakítják ki – az e cél által meghatározott biztosítékokkal, biztonsággal, hozzáférési feltételekkel – az eredetitől eltérő cél érdekében megadott rendszeres hozzáférés nemcsak a célhozkötöttség elvét sértené, hanem a fent említett elemeket is alkalmatlanná vagy elégtelenné tehetné.

Ezen gondolatmenet szerint a rendszer ilyen jelentős mértékű megváltoztatása érvénytelenné tehetné a hatástanulmány eredményét (amely a rendszernek csak az eredeti cél érdekében történő használatát vizsgálta). Ugyanez érvényes az adatvédelmi hatóságok véleményére is. Érvként elhangozhatna, hogy az új javaslat megváltoztatja az általuk elvégzett megfelelőségi elemzések alapjait.

c) *Ezen hozzáférés szigorú korlátozása*

A fenti megjegyzések fényében az európai adatvédelmi biztos hangsúlyozni kívánja, hogy a bűnüldöző hatóságok számára a VIS-hez való hozzáférés csak egyedi körülmények között, eseti alapon adható meg, szigorú biztosítékok mellett. Más szóval: a bűnüldöző szervek számára az adatok megtekintését megfelelő technikai és jogi eszközök révén egyedi esetekre kell korlátozni.

Az európai adatvédelmi biztos ezt már hangsúlyozta a VIS-szel kapcsolatos véleményében: *„Az európai adatvédelmi biztos tudatában van annak, hogy a bűnüldöző szervek érdeklődnek a VIS-hez való hozzáférés számukra történő biztosítása iránt; 2005. március 7-én ilyen értelmű tanácsi következtetések elfogadására került sor. Mivel a VIS célja a közös vízumpolitika javítása, meg kell jegyezni, hogy a bűnüldöző szervek általi rutinszerű hozzáférés nem lenne összhangban e céllal. Míg a 95/46/EK irányelv 13. cikke szerint ilyen hozzáférés eseti alapon, meghatározott körülmények között és megfelelő jogi biztosítékok mellett biztosítható, rendszeres hozzáférés nem engedélyezhető.”*

Következtetésként a legfontosabb követelmények az alábbiak szerint foglalhatóak össze:

– A rendszeres hozzáférés nem adható meg: a határozatnak biztosítania kell, hogy minden alkalommal sor kerül a harmadik pillérbeli hatóságok hozzáférése szükségességének és arányosságának esetenkénti megvizsgálására. Ebben a tekintetben a jogi eszköz pontos megszövegezése rendkívül fontos a szélesebb körű értelmezés lehetőségének kizárása érdekében, ami egyébként rutinszerű hozzáféréshez vezetne.

– A hozzáférés megadása esetén megfelelő biztosítékokat és feltételeket kell elfogadni, ideértve az adatok nemzeti célra történő felhasználására vonatkozó átfogó adatvédelmi rendszert, tekintettel az ezen hozzáférés érzékeny jellegére.

### 1.3. **Kiinduló észrevételek**

Az európai adatvédelmi biztos tudatában van annak, hogy ebben a javasolt eszközben jelentős figyelmet fordítottak az adatvédelemre, elsősorban a hozzáférés egyedi esetekre való korlátozása útján, és kizárólag a súlyos bűncselekmények elleni küzdelem keretében ([1]).

A további pozitív elemek között az európai adatvédelmi biztos külön meg kívánja említeni a következőket:

– a bűncselekmények bizonyos formáira való korlátozás, az Europol-egyezményben említettek szerint;

– a tagállamok azon kötelezettsége, hogy összeállítsák és nyilvánosságra hozzák a hozzáféréssel rendelkező hatóságok jegyzékét;

– a tagállamonként egy központi hozzáférési hely (és az Europol-on belüli szakosodott egység) megléte, lehetővé téve a hozzáférés iránti kérelmek jobb szűrését, valamint a jobb ellenőrzést;

– az adatok további átvitelére vonatkozó szigorú szabályok, a javaslat 8. cikke (5) bekezdése szerint;

– a tagállamok és az Europol azon kötelezettsége, hogy nyilvántartást vezessenek az adatok megtekintéséért felelős személyekről.

## 2. **A JAVASLAT ELEMZÉSE**

### 2.1. **Előzetes megjegyzés**

Hatóságok számára a hozzáférésnek a harmadik pillér alapján való biztosítása érdekében az első pillérbeli VIS-re vonatkozó fő javaslatnak áthidaló záradékot kellene tartalmaznia, amely lényegében meghatározná egy harmadik pillérbeli jogi eszköznek, mint ez a javaslat, a lehetséges tartalmát. Amikor az európai adatvédelmi biztos közzétette a VIS-ről szóló véleményét, ez az áthidaló záradék még nem létezett, és az európai adatvédelmi biztos nem volt abban a helyzetben, hogy arra vonatkozó észrevételt tegyen. Következésképpen valamennyi alábbi észrevételt megfelelő fenntartással teszi az áthidaló záradék tartalma vonatkozásában.

([1]) Ez összhangban van a 2005. márciusi és júliusi tanácsi következtetésekkel, amelyek megkívánják, hogy a VIS-hez való hozzáférést a belső biztonságért felelős hatóságok kapják meg *„a személyes adatok védelmére vonatkozó szabályoknak való szigorú megfelelésre is figyelemmel”*.

### 2.2. **A hozzáférés célja**

A hozzáférés korlátozásának megfelelő biztosítása érdekében fontos a VIS-hez való hozzáférés feltételeinek gondos meghatározása. Üdvözlendő, hogy a javasolt határozat mellett az indokolás és a preambulumbekezdések (lásd: különösen a (7) preambulumbekezdést) nagyon világossá teszik azt a szándékot, miszerint a hozzáférés megadása kizárólag eseti alapon történik.

A javaslat 5. cikkével kapcsolatban – a cikk értelmezése irányának meghatározása érdekében – egy észrevétel tehető.

Az 5. cikk a hozzáférés alkalmazási körét érdemi feltételekhez köti:

b) a konzultáció érdekében való hozzáférés szükséges a terrorcselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy kivizsgálása céljából;

c) a konzultáció érdekében való hozzáférés szükséges egyedi esetekben (…); és

d) kell, hogy tényszerű jelzéseken alapuló ésszerű indoka legyen annak mérlegelésének, hogy a VIS adatainak megtekintése hozzájárul a kérdéses bűncselekmények megelőzéséhez, felderítéséhez vagy kivizsgálásához.

Ezek a feltételek halmozottak, a b) pontban foglalt feltétel inkább a *ratione materiae* alkalmazási kör fogalommeghatározása. Gyakorlatilag ez azt jelenti, hogy a hozzáférést kérelmező hatóságnak a javaslat b) pontjában említettek szerinti súlyos bűncselekményben kell eljárnia; a c) pontban említettek szerinti egyedi esetnek kell fennállnia. Ezen túlmenően a hatóságnak képesnek kell lennie annak bemutatására, hogy abban az egyedi esetben a VIS adatainak megtekintése hozzájárul a d) pontban említett bűncselekmény megelőzéséhez, felderítéséhez vagy kivizsgálásához.

Az 5. cikk ilyen értelmezése mellett is aggodalommal tölti el az európai adatvédelmi biztost a d) pont rugalmas megszövegezése: a „hozzájárul” meglehetősen tág fogalom. Sok olyan eset van, amikor a VIS adatai „hozzájárulhatnának” egy súlyos bűncselekmény megelőzéséhez vagy kivizsgálásához. A VIS adataihoz a célhozkötöttség elvétől való eltérés révén való hozzáférés indokolása érdekében az európai adatvédelmi biztos azt a nézetet képviseli, hogy az ilyen megtekintésnek „jelentős mértékben hozzá kell járulnia” a kérdéses súlyos bűncselekmény megelőzéséhez, felderítéséhez vagy kivizsgálásához, és javasolja az 5. cikk ennek megfelelő módosítását.

A 10. cikk előírja, hogy a nyilvántartásokban fel kell tüntetni a hozzáférés pontos célját. A „pontos célnak” magában kell foglalnia azokat az elemeket, amelyek az 5. cikk d) pontja értelmében szükségessé tették a VIS adatainak megtekintését. Ez segíthet annak biztosításában, hogy a szükségesség tesztjét alkalmazzák a VIS-adatok valamennyi megtekintése esetén, valamint hogy a rutinszerű hozzáférés kockázatát csökkentsék.

### 2.3. **Keresési kulcsok a VIS-adatbázisban**

Az 5. cikk (2) és (3) bekezdése előírja a VIS adataihoz két lépésben való hozzáférést, amelynek értelmében egy adathalmaz csak akkor hozzáférhető, ha az első adathalmaz alapján találat jelent meg. Ez önmagában helyes megközelítés. Ugyanakkor az első adathalmaz nagyon tágnak tűnik. Különösen, az első adathalmaz vonatkozásában azon adatok relevanciáját lehet megkérdőjelezni, amelyeket az 5. cikk (2) bekezdésének e) és i) pontja említ:

– Az „utazás célja” nagyon általános keresési kulcsnak tűnik ahhoz, hogy lehetővé tegye a rendszer adatainak hatékony lekérdezését. Ezen túlmenően magában rejti annak a kockázatát, hogy az utazók besorolása ezen elem alapján történik.

– A „fényképek” tekintetében a fényképek alapján való keresés ekkora adatbázisban korlátozott; az ilyen keresések eredménye a technológia jelenlegi szintjén a hibás megfelelések elfogadhatatlan arányát mutatja. A nem megfelelő azonosítás következményei nagyon komolyak az érintett személy számára.

Éppen ezért az európai adatvédelmi biztos kéri, hogy az 5. cikk (2) bekezdésének e) és i) pontjában említett adatokat hozzáférhető kiegészítő információnak tekintsék, amennyiben az első megtekintés azt mutatja, hogy a rendszerben már vannak adatok, és azokat vigyék át az 5. cikk (3) bekezdésébe.

Alternatív megoldásként a tanácsadó bizottság ezen technológia értékelésének tárgyává tehetné az adatbázisban fényképek alapján való keresést, és az ilyen keresés végrehajtására csak akkor kerülne sor, amikor a technológia kiforrott és eléggé megbízhatónak tekinthető.

### 2.4. **Azon tagállamok tekintetében való alkalmazás, amelyekre a VIS-rendelet nem vonatkozik**

Megtekintés céljából a VIS adataihoz hozzáférhetnek azon tagállamok belső biztonságért felelős hatóságai, amelyek nem részesei a VIS-nek. Ezeknek a szolgálatoknak a megtekintést részes tagállamon keresztül – az 5. cikk (1) bekezdése b)–d) pontjában meghatározott feltételek (azaz eseti alapon való elbírálás) megfelelő tiszteletben tartása mellett – kell elvégezniük, és megfelelően indokolt írásbeli kérelmet kell benyújtaniuk.

Az európai adatvédelmi biztos ki kívánja emelni a megtekintésen kívüli eljárásra vonatkozó néhány feltétel meghatározásának szükségességét. A VIS részes tagállamaira alkalmazandó szabály szerint amennyiben az adatokat a VIS-ből lehívták, azokat a harmadik pillérben alkalmazandó adatvédelemről szóló kerethatározatnak megfelelően kell feldolgozni (lásd: alább). Ugyanezt a feltételt kell alkalmazni azokra a tagállamokra, amelyekre a VIS-rendelet nem vonatkozik, de amelyek a VIS adatait megtekintik. Ugyanezt az indokolást kell alkalmazni a jövőbeni felügyelet érdekében történő nyilvántartás-vezetésre vonatkozóan. Éppen ezért az európai adatvédelmi biztos egy bekezdés felvételét ajánlja a javaslat 6. cikkébe annak érdekében, hogy a határozat 8. és 10. cikke azokra a tagállamokra is alkalmazandó legyen, amelyekre a VIS-rendelet nem vonatkozik.

### 2.5. **Adatvédelmi rendszer**

a) *A harmadik pillérbeli adatvédelemről szóló kerethatározat alkalmazása*

Mivel a belső biztonságért felelős hatóságok általi hozzáférés a VIS céljaihoz képest kivételes, arra egységes adatvédelmi rendszernek kell vonatkoznia, amely biztosítja a VIS-ből lehívott, és a nemzeti hatóságok vagy az Europol által feldolgozott adatok magas szintű védelmét.

A javaslat 8. cikke meghatározza, hogy a javasolt határozat szerint az adatfeldolgozásra a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló tanácsi kerethatározatot (a továbbiakban: a kerethatározat) kell alkalmazni. Az adatvédelem tekintetében ezen javaslatot éppen ezért *lex specialis*-ként kell tekinteni, amely kiegészíti vagy specializálja a *lex generalis*-t (azaz a kerethatározatot). Az adatok továbbítására vonatkozó szabályok például ebben a javaslatban szigorúbbak, és azokat be kell tartani. Ugyanez vonatkozik az adatokhoz való hozzáférés indokaira.

b) *Hatály*

Az európai adatvédelmi biztos üdvözli, hogy a javasolt határozat szerint a kerethatározat adatvédelmi rendszere a személyes adatok valamennyi feldolgozására vonatkozik. Ez azt jelenti, hogy az adatvédelem szintje azonos, bármely hatóság tekinti is meg a VIS adatait.

Mivel a 2. cikk funkcionális kritériumot használ ezen hatóságok meghatározására („a tagállamok terrorcselekmények vagy egyéb súlyos bűncselekmények megelőzéséért, felderítéséért és kivizsgálásáért felelős hatóságai”), ez a meghatározás ugyanúgy vonatkozhat a hírszerző szolgálatokra, mint a bűnüldöző hatóságokra. Következésképpen azokra a hírszerző szolgálatokra, amelyek megtekintik a VIS adatait, elvben ugyanazok az adatvédelmi kötelezettségek vonatkoznak, ami nyilvánvalóan pozitív elem..

Mivel azonban ezen értelmezéssel kapcsolatosan merülhetnek fel kétségek a kerethatározatnak a VIS adataihoz való hozzáférés során a hírszerző szolgálatokra történő alkalmazása vonatkozásában, az európai adatvédelmi biztos más megfogalmazást javasol az alábbiak szerint:

„Azokban az esetekben, amikor a (…) kerethatározat nem alkalmazható, a tagállamok kötelesek az adatvédelemnek legalább olyan szintjét biztosítani, amely megfelel a kerethatározat szerint nyújtott adatvédelmi szintnek”.

c) *Felügyelet*

A 8. cikk szövegezése tekintetében tisztázni kell, hogy az (1) bekezdés a tagállamok területén történő adatfeldolgozásra vonatkozik. A (2) és (3) bekezdés világossá teszi alkalmazásuk hatályát (az Europol és a Bizottság általi adatfeldolgozás), és egyértelművé kell tenni, hogy az (1) bekezdés egy másik hipotézisre vonatkozik.

Az ellenőrzési hatásköröknek a különböző szereplők vonatkozó tevékenységei szerinti megosztása helyénvaló megközelítésnek tűnik. Egy elem azonban hiányzik: az összehangolt megközelítés szükségessége a felügyelet területén. Miként azt az európai adatvédelmi biztosnak a VIS-ről szóló véleménye kijelenti: „*A VIS felügyeletét illetően fontos hangsúlyozni azt is, hogy a nemzeti felügyeleti hatóságok és az európai adatvédelmi biztos tevékenységeit bizonyos mértékig össze kellene hangolni. Valóban szükséges a rendelet harmonizált végrehajtása, illetve a közös problémákkal kapcsolatos közös megközelítés kidolgozása.*

*A [VIS-javaslatban a] 35. cikknek tehát ezért olyan rendelkezést kellene tartalmaznia, amely meghatározza, hogy az európai adatvédelmi biztos legalább évente egyszer megbeszélést hív össze valamennyi nemzeti felügyeleti hatósággal.*”

Ugyanez vonatkozik a VIS-rendszer egyedi használatára (ebben az esetben az Europol közös ellenőrző hatóságának is a részvételével). A felügyeletnek teljes mértékben összhangban kell lennie az „első pillérbeli VIS” felügyeletével, mivel ugyanazon rendszerről van szó. Ezen túlmenően az európai adatvédelmi biztos által összehívott egyeztető megbeszélés, amelyen a felügyeletben érintett valamennyi fél részt vesz, az a modell is, amelyet más átfogó információs rendszerek – mint az Eurodac – felügyelete esetében is választottak.

Az európai adatvédelmi biztos tudatában van annak, hogy a javaslat bizonyos mértékig tartalmazza az egyeztetést, mivel – a javasolt kerethatározat 31. cikke révén létrehozott személyes adatok védelme tekintetében – megemlíti a magánszemélyek védelmével foglalkozó jövőbeni munkacsoport szerepét. Ugyanakkor újra hangsúlyozni kell, hogy magának a felügyeletnek az ellátása nem része a tanácsadó szerv megbízatásának.

Az európai adatvédelmi biztos javasolja egy rendelkezés beillesztését, amely meghatározza, hogy az európai adatvédelmi biztos által az „első pillérbeli VIS” felügyelete keretében összehívott egyeztető megbeszélés hatáskörrel rendelkezik az ezen javaslat alapján feldolgozott adatok vonatkozásában is, és ezért a megbeszélésen az Europol közös ellenőrző hatóságának is képviseltetnie kell magát.

### 2.6. **Önellenőrzés**

A javaslat 12. cikke rendelkezik a VIS felügyeleti rendszereiről. Az európai adatvédelmi biztos azt a nézetet képviseli, hogy ennek a felügyeletnek nemcsak a kibocsátásra, a költséghatékonyságra és szolgáltatások minőségére kell kiterjednie, hanem a jogi követelményeknek való megfelelésre is, különösen az adatvédelem területén. A 12. cikket ennek megfelelően módosítani kell.

A feldolgozás jogszerűségének ezen önellenőrzése érdekében a Bizottságot képessé kell tenni a javaslat 10. cikkével összhangban vezetett nyilvántartások igénybe vételére. Hasonlóképpen, a 10. cikknek rendelkeznie kell arról, hogy ezeket a nyilvántartásokat ne csak az adatvédelem ellenőrzésére és az adatbiztonság biztosítására kelljen tárolni, hanem a VIS önellenőrzésének rendszeres elvégzése céljából is. Az önellenőrzésről szóló jelentések hozzájárulnak az európai adatvédelmi biztos és más felügyelők felügyeleti feladatához, akik jobban ki tudják választani a felügyelet szempontjából elsődleges fontosságú területeket.

3. **KÖVETKEZTETÉSEK**

A fentiek fényében az európai adatvédelmi biztos aláhúzza annak kiemelkedő fontosságát, hogy a belső biztonságért felelős hatóságok és az Europol – kizárólag eseti alapon és szigorú biztosítékok mellett – megkapja a hozzáférést. Ezt a célt a javaslat összességében kielégítő módon megvalósítja, jóllehet néhány, az e véleményben javasolt jobbítás elérhető:

– A VIS-hez az 5. cikk értelmében való hozzáférés feltételéül kell szabni, hogy az adatok megtekintése „jelentős mértékben" hozzájárul a súlyos bűncselekmények megelőzéséhez, felderítéséhez vagy kivizsgálásához, továbbá a 10. cikkben előírt nyilvántartásoknak minden egyes esetben lehetővé kell tenniük e feltétel értékelését.

– Az 5. cikk (2) bekezdésében említett, a VIS-ben található, hozzáférést biztosító két keresési kulcs, nevezetesen az „utazás célja" és a „fényképek" átgondolást igényel, és azokat találat esetén kiegészítő információként kell rendelkezésre bocsátani.

– A megtekintésen túl alkalmazandó adatvédelmi szintnek azonosnak kell lennie, függetlenül attól, hogy milyen hatóság tekinti meg a VIS adatait. A 8. és 10. cikket azon tagállamok tekintetében is alkalmazni kell, amelyekre a VIS-rendelet nem vonatkozik

– A felügyeletet illetően biztosítani kell az egyeztetett megközelítést, tekintettel a VIS-hez való hozzáférés vonatkozásában a javaslatban foglaltakra.

– A felügyeleti rendszerekre vonatkozó rendelkezéseknek biztosítaniuk kell az adatvédelmi követelményeknek való megfelelés önellenőrzését.

Kelt Brüsszelben, 2006. január 20-án.

Peter HUSTINX

*európai adatvédelmi biztos*