A 29. CIKK SZERINTI ADATVÉDELMI MUNKACSOPORT

16/HU
WP 238

1/2016. sz. vélemény az EU–USA adatvédelmi pajzs megfelelőségéről szóló határozattervezetről

Elfogadás időpontja: 2016. április 13.

ÖSSZEFOGLALÓ

2016. február 29-én az Európai Bizottság egy közlemény kiadásával egyidejűleg közzétette a személyes adatok kereskedelmi célú transzatlanti cseréjének új keretrendszerét, az EU–USA adatvédelmi pajzsot (a továbbiakban: adatvédelmi pajzs) alkotó megfelelőségi határozat tervezetét és az ahhoz mellékletként csatolt szövegeket. Az adatvédelmi pajzs célja, hogy felváltsa az előzőleg érvényben lévő, az Európai Unió Bírósága (a továbbiakban: EUB) által a Schrems-ügyben 2015. október 6-án hozott ítéletével érvénytelenített amerikai védett adatkikötőt.

A 95/46/EK irányelv 30. cikke (1) bekezdésének c) pontjának megfelelően a 29. cikk szerinti munkacsoport (a továbbiakban: WP29) értékelte e dokumentumokat abból a célból, hogy véleményt nyilvánítson a megfelelőségi határozat tervezetéről. A WP29 a kereskedelmi szempontokon túlmenően értékelte az adatvédelmi pajzs elveitől való eltérés lehetőségét is nemzetbiztonsági, bűnüldözési, és a közérdek védelmével összefüggő okok esetén.

A WP29 figyelembe vette a 95/46/EK irányelvben meghatározott hatályos uniós adatvédelmi jogi keretet, az Emberi jogok és alapvető szabadságok védelméről szóló egyezmény 8. cikkében, valamint az Európai Unió Alapjogi Chartájának 7. és 8. cikkében foglalt, a magánélet tiszteletben tartásához és az adatvédelemhez fűződő alapvető jogokat. Tekintettel volt továbbá a Charta 47. cikkében foglalt, a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogra, valamint egyes alapvető jogokra vonatkozó ítélkezési gyakorlatra.

Ezen túlmenően az elemzés tükrözi az EUB Schrems-ügyben hozott ítéletének arra vonatkozó indokolását, hogy a Bizottság mekkora mérlegelési jogkörrel rendelkezik a megfelelőségi határozat értékelése terén. Az ellenőrzést és a megfelelőségi követelményeket vizsgálatát szigorúan kell végrehajtani, figyelembe véve a magánélethez és az adatvédelemhez való alapvető jogokat és az adattovábbítások által potenciálisan érintett személyek számát is.

Az adatvédelmi pajzs vizsgálatakor szem előtt kell tartani a jelenlegi nemzetközi körülményeket, például a nagy adathalmazok megjelenését és a megnövekedett biztonsági szükségleteket. A személyes adatok gyűjtésének és használatának hatálya és mértéke drámai mértékben megnövekedett a védett adatkikötőre vonatkozó 2000. évi határozat meghozatala óta. Európai adatvédelmi hatóságok határozottan kiállnak az általuk védett elvek fontossága mellett.

A WP29 mindenek előtt üdvözli az adatvédelmi pajzsnak köszönhető jelentős pozitív változásokat a védett adatkikötőről szóló határozathoz képest. Megjegyzi, hogy a 2014. április 10-i, Reding alelnökhöz intézett levelében kiemelt, a védett kikötő számos hiányosságával már foglalkoztak a tárgyaló felek.

Annak következtében, hogy az adatvédelmi pajzs által biztosított elvek és garanciák a megfelelőségi határozatban és annak mellékleteiben egyaránt szerepelnek, az információk nehezen fellelhetők és időnként ellentmondásosak. Ez hozzájárul ahhoz, hogy az új adatvédelmi keret általában véve nem egyértelmű, valamint megnehezíti a hozzáférhetőséget

az érintettek, a különböző szervezetek és az adatvédelmi hatóságok számára. Hasonlóképpen, a nyelvhasználat nem egyértelmű. A WP29 ezért sürgeti a Bizottságot, hogy tegye azt az Atlanti-óceán mindkét partján érthetővé és világossá.

Az alkalmazandó joggal kapcsolatban a WP29 kiemeli, hogy amennyiben az adatvédelmi pajzs megfelelőségére vonatkozó határozat elfogadása a 95/46/EK irányelv alapján történik, a határozatnak mind hatályát, mind a használt terminológiát illetően összhangban kell lennie az adatvédelemre vonatkozó uniós jogi kerettel. A WP29 megítélése szerint röviddel az általános adatvédelmi rendelet hatálybalépését követően felülvizsgálatot kell végezni annak biztosítása érdekében, hogy a rendelet által nyújtott magasabb adatvédelmi szint a megfelelőségi határozatban és mellékleteiben is érvényesüljön.

Az adatvédelmi pajzs kereskedelmi szempontjai

A WP29 elsődleges célja annak biztosítása, hogy a magánszemélyek részére nyújtott védelem lényegében azonos szinten fenntartható legyen akkor, amikor a személyes adatok kezelése az adatvédelmi pajzs alapján történik. A WP29 – noha nem várja el, hogy az adatvédelmi pajzs pusztán az uniós jogi keret pontos másolata legyen –úgy véli, hogy annak tartalmaznia kell az alapelvek lényegét, és ennek következtében „lényegében megegyező" szintű védelmet kell biztosítania.

Az adatvédelmi pajzs által megvalósított javulás ellenére a WP29 úgy véli, hogy bizonyos alapvető adatvédelmi elvek a megfelelőségi határozatban és mellékleteiben nem tükröződnek úgy, ahogyan azokat az európai jogszabályok megfogalmazzák, vagy pedig a helyettük alkalmazott fogalmak nem megfelelők.

Például az adatmegőrzés elve nem kerül kifejezetten említésre, és azt nem lehet egyértelműen levezetni az adatok sértetlensége és célhoz kötöttség elve jelenlegi megfogalmazásából sem. Ezenkívül nincsen szó a pusztán automatizált feldolgozáson alapuló, automatizált egyedi döntésekkel szemben biztosítandó védelemről. Nem egyértelmű az adatkezelés célhoz kötöttsége elvének alkalmazása sem. Több fontos fogalom használatának egyértelműbbé tétele érdekében a WP29 azt javasolja, hogy az EU és az Egyesült Államok állapodjanak meg egyértelmű fogalmakban, és az adatvédelmi pajzzsal kapcsolatban gyakran felvetődő kérdések (GYFK) közé iktassanak be egy, a fogalmak meghatározását tartalmazó glosszáriumot.

Mivel az adatvédelmi pajzsot az USA-n kívülre irányuló adattovábbításra is használni fogják, a WP29 ragaszkodik ahhoz, hogy az adatvédelmi pajzs keretébe tartozó entitásoktól harmadik országokban található felekhez történő bármely adattovábbítás az adatvédelmi pajzs minden aspektusára (a nemzetbiztonságot is ideértve) kiterjedő azonos védelmet biztosítson, és ne eredményezhessen az uniós adatvédelmi elveknél alacsonyabb, vagy azokat megkerülő adatvédelmi elveket. Az adatvédelmi pajzs keretében harmadik országba irányuló tervezett adattovábbítás esetén az adatvédelmi pajzsban részt vevő valamennyi szervezetet kötelezni kell arra, hogy a továbbítást megelőzően értékelje az adott harmadik ország nemzeti jogrendje szerint az adatátvevőkre vonatkozó, kötelezően alkalmazandó követelményeket. Általában

véve a WP29 megállapítja, hogy az uniós személyes adatok harmadik fél részére történő továbbítása nincs kielégítően szabályozva, különösen az adattovábbítás hatókörét, célhoz kötöttségét, és a megbízott részére történő adattovábbításra vonatkozó biztosítékokat illetően.

Végül, bár a WP29 figyelmét nem kerülte el, hogy az adatvédelmi pajzs kiegészítő jogorvoslati lehetőségeket biztosít a magánszemélyek számára jogaik gyakorlása érdekében, tart attól, hogy az új jogorvoslati mechanizmus a gyakorlatban túl bonyolultnak bizonyulhat, használata az unióbeli magánszemélyek számára túlságosan nehéz lehet, és ezért végeredményben hatástalan lesz. Ezért további pontosításokra van szükség az egyes jogorvoslati eljárásokat illetően; különösen, az uniós adatvédelmi hatóságok – amennyiben készek erre – természetes kapcsolattartási pontként szolgálhatnának az unióbeli magánszemélyek számára a különböző eljárásokban, és eljárhatnának a nevükben.

Eltérések nemzetbiztonsági okokból

Az uniós és harmadik országokbeli hatóságok adatokhoz való hozzáférése tekintetében a WP29 emlékeztet arra az elemzésére, amelyet a releváns alapvető jogokra vonatkozóan végzett a személyes adatok továbbítása során alkalmazott megfigyelési intézkedések által a magánélethez és az adatvédelemhez fűződő alapvető jogokba történő beavatkozás igazolásáról szóló munkadokumentumban (Alapvető európai garanciák) (WP237).

Nagy előrelépést jelent a védett adatkikötőről szóló határozathoz képest, hogy a megfelelőségi határozat tervezete részletesen foglalkozik az adatvédelmi pajzs keretében kezelt adatokhoz nemzetbiztonsági és bűnüldözési célból történő hozzáféréssel. A WP29 elismeri ezt a jelentős lépést, csakúgy, mint az Egyesült Államok kormányzata által a hírszerzési célú adatgyűjtésekre vonatkozó jogszabályok terén felajánlott fokozottabb átláthatóságot (VI. melléklet).

Megjegyzi azonban, hogy az Egyesült Államok Nemzeti Hírszerzés Igazgatója Hivatalának (ODNI) nyilatkozatai nem zárják ki az EU-ból származó személyes adatok tömeges és válogatás nélküli gyűjtésének lehetőségét. A WP29 emlékeztet arra a régóta képviselt álláspontjára, mely szerint a magánszemélyek tömeges és válogatás nélküli megfigyelése a demokratikus társadalmakban soha nem tekinthető arányosnak és feltétlenül szükségesnek – amilyennek a releváns alapjogok által biztosított védelemmel összhangban lennie kell. Ezen túlmenően kulcsfontosságú a megfigyelési programok átfogó felügyelete. A WP29 tudomásul veszi, hogy a terrorizmus elleni küzdelem jegyében egyre inkább előtérbe kerül a tömeges és válogatás nélküli adatgyűjtés. Tekintettel az ennek kapcsán a magánélethez és az adatvédelemhez fűződő alapvető jog védelme vonatkozásban felmerülő aggályokra, a WP29 várakozással tekint az EUB soron következő, a tömeges és válogatás nélküli adatgyűjtéssel kapcsolatos ügyekben meghozandó ítéletei elé.

A jogorvoslat tekintetében a WP29 örvendetesnek tartja az ombudsman intézménye, mint új jogorvoslati mechanizmus bevezetését. Ez jelentős előrelépést jelenthet az unióbeli magánszemélyeket megillető jogok terén az Egyesült Államok hírszerzési tevékenységei vonatkozásában. Azonban aggodalmának ad hangot a tekintetben, hogy ez az új intézmény

nem kellően független és nincs felruházva a feladatai hatékony ellátásához szükséges megfelelő hatáskörökkel annak érdekében, hogy nézeteltérések esetén kielégítő jogorvoslatot garantáljon.

Közös felülvizsgálat

A megfelelőségi határozat tervezetében szereplő éves közös felülvizsgálati mechanizmus kulcsfontosságú tényező az adatvédelmi pajzs általános hitelessége érdekében, és a WP29 nagyra értékeli, hogy ez lehetőséget jelent majd a megfelelőségi határozat felülvizsgálatára. E tekintetben a WP29 tisztában van azzal, hogy nemzeti képviselői teljes mértékben részt vehetnek majd a felülvizsgálati folyamatban, kéri azonban az ezzel kapcsolatos részletek egyértelművé tételét. A feleknek az első felülvizsgálatot megelőzően jó előre meg kell állapodniuk a részletes szabályokról (a felülvizsgálatról készülő jelentést, annak nyilvánosságát és esetleges következményeit, valamint finanszírozását is ideértve).

Következtetés

A WP29 megállapítja, hogy az adatvédelmi pajzs jelentős javulást eredményez a védett adatkikötőről szóló, megsemmisített határozathoz képest. A megfogalmazott aggályokra és a kért pontosításokra tekintettel a WP29 arra kéri a Bizottságot, hogy oszlassa el ezeket az aggályokat, keresse meg a megfelelő megoldásokat, és tegye meg a kért pontosításokat a megfelelőségi határozat tervezetének javítása, valamint annak biztosítása érdekében, hogy az adatvédelmi pajzs által nyújtott védelem az uniós védelemmel valóban egyenértékű legyen.

TARTALOMJEGYZÉK

1. BEVEZETÉS

Az Európai Unió Bíróságának (a továbbiakban: EUB) a Schrems-ügyben 2015. október 6-án hozott ítéletét[1] követően a 29. cikk szerinti munkacsoport (a továbbiakban: WP29) felkérte az Európai Unió (a továbbiakban: EU) tagállamait és a többi uniós intézményt, hogy kezdjenek tárgyalásokat az Egyesült Államok (a továbbiakban: USA) hatóságaival olyan politikai, jogi és technikai megoldások kidolgozása érdekében, amelyek lehetővé teszik, hogy az USA területére történő adattovábbítások az alapvető jogok tiszteletben tartásával menjenek végbe.

Több mint két évig tartó tárgyalásokat követően, 2016. február 2-án az Európai Bizottság és az Egyesült Államok Kereskedelmi Minisztériuma (DoC) politikai megállapodásra jutott *A személyes adatok kereskedelmi célú transzatlanti cseréjének új keretrendszeréről: az EU–USA adatvédelmi pajzsról* (a továbbiakban: adatvédelmi pajzs), melynek célja a korábbi amerikai védett adatkikötő felváltása.

2016. február 29-én a Bizottság közleményt[2] adott ki, valamint közzétette a megfelelőségi határozat-tervezetet és az annak mellékleteit képező szövegeket, amelyek az adatvédelmi pajzsot fogják alkotni. A WP29 a 95/46/EK irányelv (a továbbiakban: az irányelv) 30. cikke (1) bekezdésének c) pontjával összhangban megvizsgálta ezeket a dokumentumokat annak érdekében, hogy a megfelelőségi határozat Bizottság által kidolgozott tervezetére és az ennek alapjául szolgáló, az adatvédelmi pajzs részét képező dokumentumokra vonatkozólag kialakítsa a jelen véleményt. Az értékelés során a WP29 a munkát úgy osztotta meg, hogy külön értékelte az adatvédelmi pajzs kereskedelmi részét, valamint azokat a biztosítékokat, amelyeket az adatvédelmi pajzs elveitől nemzetbiztonsági, bűnüldözési, és a közérdek védelmével összefüggő okból biztosított eltérés esetén kell alkalmazni.

A Schrems-ügyben hozott ítéletet követően a WP29 több megbeszélést tartott az Egyesült Államok kormányának küldöttségeivel és mind az EU-ban, mind az USA-ban működő civil szervezetek képviselőivel, valamint tudományos kutatókkal a Schrems-ügyben hozott ítélet következményeinek felmérése céljából. Az adatvédelmi pajzs értékelés során további megbeszéléseket folytatott az Európai Bizottsággal és az Egyesült Államok kormányának képviselőivel. E megbeszélések alkalmával sor került néhány pontosításra, amelyek szintén figyelembe vételre kerültek a jelen vélemény készítésekor. A WP29 hangsúlyozza, hogy a jelenlegi szakaszban ezek mindössze informális pontosítások, és nem tekinthetők úgy, hogy szerves részét képezik a megfelelőségi határozat tervezetének, mivel még nincsenek írásba foglalva.

Mindazonáltal a WP29 különösen üdvözli, hogy a Kereskedelmi Minisztérium e találkozók során kötelezettséget vállalt arra, hogy az adatvédelmi pajzs alkalmazása során együttműködik az uniós tagállamok nemzeti adatvédelmi hatóságaival, és a weboldalán útmutatást és jogértelmezést tesz közzé az adatvédelmi pajzs alkalmazása tekintetében.

[1] A C-362/14. sz., Maximilian Schrems kontra adatvédelmi biztos ügyben 2015. október 6-án hozott ítélet (a továbbiakban: Schrems-ügyben hozott ítélet).
[2] COM(2016)117 final, 2016. február 29.

1.1. Általános észrevételek

1.1.1. A WP29 értékelésének hatálya

A WP29 mindenekelőtt az Európai Unió tagállamaiban alkalmazandó adatvédelmi keretre volt figyelemmel, ideértve az emberi jogok európai egyezményének (a továbbiakban: EJEE) a magán-és családi élet tiszteletben tartásához való jog védelmét biztosító 8. cikkét, valamint az Európai Unió Alapjogi Chartájának (a továbbiakban: Charta) a magán- és családi élethez tiszteletben tartásához való jog védelmét biztosító 7. cikkét, a személyes adatok védelméhez való jogot tartalmazó 8. cikkét, és a hatékony jogorvoslathoz és tisztességes eljáráshoz való jogot magába foglaló 47. cikkét is. Figyelembe vette továbbá a vonatkozó ítélkezési gyakorlatot, valamint az irányelvben előírt követelményeket.

Az EUB a Schrems-ügyben hozott ítéletében tovább pontosította a harmadik országokra vonatkozó azon követelményt, hogy megfelelő adatvédelmi szintet kötelesek biztosítani. A Bíróság kifejtette, hogy az irányelv rendelkezéseit „a Chartában biztosított alapvető jogok fényében”[3], különösen annak 7. és 8. cikkében foglalt jogokkal összhangban kell értelmezni. Rámutatott arra is, hogy „a «megfelelő védelmi szint» kifejezést úgy kell érteni, mint amely megköveteli, hogy e harmadik ország – belföldi joga, vagy vállalt nemzetközi kötelezettségei alapján – az Unióban a Chartával összefüggésben értelmezett 95/46 irányelv által biztosított védelmi szinttel lényegében azonos védelmi szintet biztosítson ténylegesen az alapvető jogok és szabadságok számára”[4]. A védett adatkikötőről szóló határozat esetében ilyen értékelésre – kellő részletességgel – soha nem került sor. Ezért a WP29 azon követelmény fényében értékelte a megfelelőségi határozat tervezetét, mely szerint az alapvető jogok és szabadságok részére biztosított védelmi szintet oly módon kell elemezni, hogy az az Unióban biztosított védelemmel *lényegében azonos* védelmet biztosítson. A WP29 hangsúlyozza, hogy ez a vélemény a fő aggályokat tartalmazza, a megfelelőségi határozat tervezetének közzététele óta azonban kevés idő telt el, ezért a későbbiekben további problémák merülhetnek fel.

A WP29 álláspontja szerint az EUB azáltal, hogy az irányelv 25. cikkének (6) bekezdésében szereplő „megfelelő” kifejezést a Schrems-ügyben hozott ítéletében „lényegében azonos”-ként definiálta, tovább pontosította megfelelőség fogalmát. A Bíróság hangsúlyozta, hogy a „megfelelő védelmi szint” kifejezést – bár nem követelhető meg, hogy a harmadik ország az uniós jogrendben biztosított védelmi szinttel megegyező védelmi szintet biztosítson –, úgy kell érteni, mint amely megköveteli, hogy e harmadik ország belföldi joga, vagy vállalt nemzetközi kötelezettségei alapján az Unióban a Chartával összefüggésben értelmezett 95/46 irányelv által biztosított védelmi szinttel *lényegében azonos* védelmi szintet biztosítson.

1.1.2. A megfelelőségi határozat-tervezet kereskedelmi részének értékelése

A WP29 a „Személyes adatok továbbítása harmadik országokba: Az európai uniós adatvédelmi irányelv 25. és 26. cikkének alkalmazása” című 12. munkadokumentumában[5]

[3] A Schrems-ügyben hozott ítélet 38. pontja.
[4] A Schrems-ügyben hozott ítélet 73. pontja.
[5] A WP29 1998. július 24-én fogadta el, lásd különösen a 6. oldalt.

már kifejtette, hogyan alkalmazta az alapvető uniós adatvédelmi elveket a személyes adatok harmadik országokba történő továbbítására. A WP29 igyekezett megtalálni azokat a megfelelő biztosítékokat, amelyek az irányelvben foglalt elvekkel azonos szintű védelmet nyújtanak, különösen a célhoz kötöttség, az adatminőség, az arányosság, az átláthatóság, a biztonság, a hozzáférési jogok, a helyesbítés és a tiltakozás joga, az adatmegőrzés, valamint a harmadik fél részére történő adattovábbításra vonatkozó korlátozások tekintetében. A WP29 hasonló módszert alkalmazott az eredeti védett adatkikötőre vonatkozó megfelelőségi határozat értékelésekor kiadott véleményekben[6], valamint a munkacsoport által a Bizottság korábbi alelnökéhez és a jogérvényesülésért felelős uniós biztoshoz, Viviane Redinghez intézett, 2014. április 10-i levélben megfogalmazott ajánlásokban is[7].

1.1.3. A hatóságok hozzáférése tekintetében engedett eltérések és azok biztosítékai

A hatóságok személyes adatokhoz való hozzáférése tekintetében az adatvédelmi pajzs által engedett eltérések értékelése összetett, különösen arra tekintettel, hogy a Snowden-féle adatkiszivárogtatás óta az adatvédelmi hatóságok és a közvélemény fokozott tudatossággal kíséri figyelemmel az amerikai megfigyelési programokat. A munkacsoport elismeri és üdvözli az Egyesült Államok kormányának arra irányuló erőfeszítéseit, hogy növelje a megfigyelési programok átláthatóságát, és arra való készségét, hogy további biztosítékokat illesszen be az adatvédelmi pajzsba. Mindazonáltal a WP29 hangsúlyozza, hogy egy demokratikus társadalomban a magánélethez és az adatok védelméhez való alapjogokba történő bárminemű beavatkozásnak igazolhatónak kell lennie. Az EUB kifogásolta, hogy a védett adatkikötőről szóló határozat nem tartalmazott semmilyen megállapítást azzal kapcsolatban, hogy az Egyesült Államokban léteznek-e olyan szabályok, amelyeket az állam a beavatkozások korlátozása céljából fogadott el, valamint, hogy a határozat nem is utal az ilyen beavatkozásokkal szembeni hatékony jogvédelem meglétére[8].

A WP29 ezért megvizsgálta a jelenlegi egyesült államokbeli jogi keretrendszert és az USA hírszerző ügynökségeinek gyakorlatát, amint azokat a határozattervezet mellékletei tartalmazzák, valamint azt, hogy azok milyen feltételek mellett tesznek lehetővé bármilyen beavatkozás a magánélet tiszteletben tartásához és az adatvédelemhez fűződő – az európai jogi keret szerint védett – alapvető jogokba.

Annak értékelését, hogy egy demokratikus társadalomban bármely beavatkozás igazolható-e, a W29 az európai bíróságok alapvető jogokra vonatkozó ítélkezési gyakorlatának fényében értékelte, amely a hírszerzési tevékenység tekintetében az alábbi négy alapvető garanciát[9] állapítja meg:

A. Az adatkezelésnek a jogszabályokkal összhangban kell történnie, és egyértelmű, pontos és megismerhető szabályokon kell alapulnia: ez azt jelenti, hogy bármely

[6] Lásd: WP62, WP32, WP27, WP23, WP21, WP19, WP15 és WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
[8] A Schrems-ügyben hozott ítélet 87. és 88. pontja.
[9] Az alapvető európai garanciák az EUB és az EJEB ítélkezési gyakorlatán alapulnak, és részletesebben kifejtve a WP29 2016. április 13-án közzétett, WP237. sz. munkadokumentumában találhatók.

ésszerű mértékben tájékozott személynek képesnek kell lennie arra, hogy előre lássa, mi történhet személyes adataival ott, ahová azokat továbbítják;

B. Bizonyítani kell az intézkedés szükségességét és arányosságát az elérni kívánt jogszerű célokra tekintettel: egyensúlyt kell találni a magánszemélyt megillető jogok, illetve azon célkitűzés között, amelynek érdekében az adatok gyűjtése és az azokhoz való hozzáférés történik;

C. Szükséges egy független felügyeleti mechanizmus, amely hatékony és pártatlan: ez lehet bíróság vagy más független szerv is, amennyiben képes megfelelően elvégezni a szükséges ellenőrzéseket;

D. A magánszemélyek számára hatékony jogorvoslati lehetőségeket kell biztosítani; mindenki számára biztosítani kell a jogot, hogy az őt megillető jogokat egy független szerv előtt megvédhesse.

1.2. A megfelelőségi határozat tervezete

A WP29 mindenekelőtt üdvözli, hogy az új megfelelőségi eljárás kevesebb, mint hat hónappal azt követően megindítható, hogy az EUB megsemmisítette a védett adatkikötőről szóló határozatot. Tekintettel arra, hogy az EU és az USA között mekkora adatmennyiség továbbítására kerül sor napi szinten – ami a WP 29 által nem vitatottan az Atlanti-óceán mindkét partján a gazdaság elengedhetetlenül fontos részét képezi – sürgősen egyértelmű jogi helyzetet kell teremteni.

A WP29 azonban sajnálatát fejezi ki amiatt, hogy a Bizottság által közzétett megfelelőségi határozat-tervezet megfelelőségi jelentés formájában nem tartalmazza az Egyesült Államok nemzeti jogának és nemzetközi jogi kötelezettségvállalásainak átfogó értékelését, ahogyan az a múltban hasonló eljárások keretében és az irányelv 25. cikkével összhangban bevett gyakorlat volt. Emiatt a WP29-nek nem volt lehetősége arra, hogy teljes körű elemzést végezzen a tekintetben, hogy az adatvédelmi pajzs milyen jogi környezetben fog működni. Megjegyzi például, hogy a jelenlegi megfelelőségi határozat-tervezet semmiféle megállapítást nem tartalmaz arra vonatkozóan, hogy jelenleg az USA-ban – szövetségi szinten és az egyes államok szintjén egyaránt, és az ágazati jogszabályokat is ideértve – milyen jogszabályok vonatkoznak a magánélet védelmére és az adatok védelmére, sem pedig azon jogszabályokra vonatkozóan, amelyek az állami szervek nem megfigyelési célú adathozzáférését teszik lehetővé. Továbbá nem tisztázott az adatvédelmi pajzs keretében és más meglévő megfelelőségi határozatok, például az EU–USA közötti utas-nyilvántartási adatállományra (PNR) vonatkozó megállapodás és a terrorizmus finanszírozásának felderítését célzó programról szóló megállapodás keretében történő adattovábbítások viszonya sem.

1.2.1. Az uniós adatvédelmi keret, és különösen a 95/46/EK irányelvben foglalt elvek alkalmazási köre

A WP29 emlékeztet rá, hogy az uniós jogi keret, és különösen az irányelv (4. cikk (1) bekezdés) értelmében nemcsak olyan esetben alkalmazandók a tagállami jogszabályok, amikor egy adott tagállam területén letelepedett adatkezelő kezelési műveletet végez, hanem akkor is, amikor az adatkezelő (noha nem az EU területén letelepedett) – különösen

személyes adatok gyűjtése céljából – olyan eszközt alkalmaz, amely az EU területén található. Ennek következtében minden olyan adatkezelésre az uniós tagállami jogszabályokat kell alkalmazni, amelyre az USA-ba történő továbbítást megelőzően, az EU területén letelepedett szervezet tevékenysége keretében, vagy valamely, nem az Unióban letelepedett szervezet által az EU területén található eszköz használatával kerül sor. A WP29 kéri, hogy ez konkrétan szerepeljen a megfelelőségi határozat tervezetében.

Egyértelművé kell tenni, hogy az adattovábbítás pillanatától kezdve az adatvédelmi pajzs elvei alkalmazandók. Ezen túlmenően a WP29 emlékeztet arra, hogy az Európai Unióban letelepedett, és egyesült államokbeli adatfeldolgozókhoz adatokat továbbító adatkezelők az uniós adatvédelmi jogszabályok hatálya alatt maradnak.

1.2.2. Az egyértelműség hiánya az adatvédelmi pajzs részét képező dokumentumokban

Annak következtében, hogy az adatvédelmi pajzs által biztosított elvek és garanciák a megfelelőségi határozatban és annak mellékleteiben egyaránt szerepelnek, az információk nehezen fellelhetők és időnként ellentmondásosak. Ez hozzájárul ahhoz, hogy az új adatvédelmi keret általában véve nem egyértelmű, valamint megnehezíti a hozzáférhetőséget az érintettek, a különböző szervezetek és az adatvédelmi hatóságok számára. Hasonlóképpen, a nyelvhasználat nem egyértelmű. A WP29 ezért sürgeti a Bizottságot, hogy tegye azt az Atlanti-óceán mindkét partján érthetővé és világossá.

A WP29 javasolja, hogy az adatvédelmi pajzs dokumentumaiban előforduló legfontosabb fogalmak egy külön mellékletben kerüljenek meghatározásra. Az adatvédelmi pajzs megfelelőségéről szóló határozatban előírt kötelezettségek azonos és kétértelműségektől mentes értelmezése elengedhetetlen ahhoz, hogy az adatvédelmi pajzs az Atlanti-óceán mindkét partján hatékonyan működjön. Ezért a WP29 aggodalmát fejezi ki amiatt, hogy a számos kereszthivatkozásból és nem egyeztetett megfogalmazásból, valamint a keretdokumentumok bonyolultságából eredően nehézségek fognak felmerülni az adatvédelmi pajzs következetességével, érthetőségével, és alkalmazásának egyértelműségével kapcsolatban.

Ráadásul az adatvédelmi pajzs dokumentumaiban használt terminológia nincs összhangban az uniós adatvédelem területén általában használatos kifejezésekkel. Ez nem feltétlenül jelent problémát mindaddig, amíg egyértelmű, hogy az uniós jogban (és Egyesült Államok jogában) mi az annak megfelelő terminológia. A WP29 azonban sajnálattal jegyzi meg, hogy nem ez a helyzet, és ez a megfelelőségi határozattervezetre is vonatkozik. A „hozzáférés” szó például a megfelelőségi határozattervezet 3. fejezetében olyan értelemben szerepel, amely a személyes adatok gyűjtésére utal, nem pedig arra, hogy valaki lehetőséget kap a már összegyűjtött adatokba betekinteni. A vállalkozások adatokhoz való hozzáférése és a magánszemélyek betekintési joga két külön fogalom, amelyeket nem lenne szabad összekeverni.

A WP29 hangsúlyozza, hogy a terminológiát következetesen kell alkalmazni a dokumentumok egészében, ideértve a megfelelőségi határozattervezetet is. Jelenleg nem ez a helyzet, például a „kezelés” és a „személyes adatok” fogalmak esetében. A II. melléklet

mindkettőt alapvetően jól határozza meg, a dokumentumokban történő alkalmazásuk azonban nem következetes[10].[11]

A WP29 örvendetesnek tartja, hogy a használt fogalmak közül néhánynak a meghatározása szerepel az adatvédelmi pajzsot alkotó dokumentumokban. Nem ez a helyzet azonban számos más fontos kifejezés – például a „megbízott" vagy az „adatfeldolgozó", a „kódolt adatok", „anonimmá tett adatok" és az „unióbeli magánszemély" fogalma – esetében, amelyekre vonatkozóan a WP29 véleménye szerint az Egyesült Államok és az EU által egyaránt elfogadott, egyértelmű fogalommeghatározásokra van szükség annak érdekében, hogy elkerülhető legyen a későbbi zavar mind az adatvédelmi pajzsot használó adatkezelők és adatfeldolgozók, mind a felügyeleti hatóságok és a nyilvánosság körében. Könnyen kivitelezhető megoldás volna egy glosszárium beiktatása az adatvédelmi pajzzsal kapcsolatban gyakran felvetődő kérdések közé.

A WP29 kiemeli az 1. sz. kiegészítő elvet is (II. melléklet, III. szakasz 1. pont), amely az érzékeny adatok kezelését jogos indokok meglétéhez köti azokban az esetekben, amikor a szervezetnek nem kell kifejezett hozzájárulást beszereznie (részvételi záradék esetén). Ezt az 1. sz. kiegészítő elvet lehet úgy érteni, mint amely az EU területén történő adatgyűjtéshez szükséges jogos indokokat részletezi, tekintettel arra, hogy ez a felsorolás hasonló az irányelv 8. cikkében szereplőhöz. A WP29 emlékeztetni kíván arra, hogy az irányelv 8. cikke értelmében az uniós jogszabályok hatálya alá tartozó érzékeny adatok bármilyen kezeléséhez (a gyűjtést és a továbbítást is ideértve) jogos indok fennállása szükséges. Az adatvédelmi pajzsot nem lehet úgy értelmezni, hogy az alternatív jogalapot biztosít az ilyen adatkezeléshez. Például, a WP29 véleménye szerint nem lehetséges, hogy egy egyesült államokbeli szervezet az Egyesült Államok munkajogi törvénye alapján az uniós jog hatálya alá tartozó adatokat gyűjtsön (lásd a II. melléklet, III. szakasz 1.a.v. pontját). Következésképpen a WP hangsúlyozza, hogy az 1. sz. kiegészítő elv bármilyen értelmezése csak oda vezethet, hogy ezt a kiegészítő elvet csak olyan érzékeny adatokra lehet alkalmazni,

[10] Némely szakasz a „kezelés" kifejezés használata helyett pusztán valamilyen adatkezelési műveletek felsorolását tartalmazza. Ez joghézagokat eredményez a védelem terén. Például a II. melléklet III. szakasza 6. pontja f. alpontjának szövege szerint az adatvédelmi pajzs alapelveit csak akkor kellene alkalmazni, amikor a szervezet a kapott adatokat „tárolja, felhasználja, vagy közli" (ami azt jelenti, hogy a „kezelés" kifejezés körébe tartozó egyéb műveletek, például gyűjtés, rögzítés, megváltoztatás, visszakeresés, betekintés, törlés esetében nem). Az adatbiztonság csak személyes információk „létrehozása, fenntartása, felhasználása vagy terjesztése" vonatkozásában lenne kötelező (II. melléklet, II. szakasz 4. pont). Hasonlóképpen, a „személyes adatok" fogalma is csak a „kapott" és „rögzített" adatokat foglalja magában. További példaként említhető a tájékoztatás elve (II. melléklet II. szakasz 1.a.iv. alpont), amely szerint a tanúsítvánnyal rendelkező szervezetek kötelesek tájékoztatni a magánszemélyeket arról, hogy milyen célból „gyűjtenek" adatokat róluk és azokat milyen célra „használják fel". A II. melléklet III. szakaszának 9.a.11. alpontja csak a „továbbított" adatokat említi, vagy azokat, amelyekhez „hozzáférést adtak". Akkor is, ha úgy tűnik, hogy a legtöbb ilyen esetben a szándék nem az alapelvek hatályának korlátozására vagy védelmi joghézagok előidézésére irányul, ez a következetlen terminológia magában hordozza annak kockázatát, hogy ilyen joghézagok keletkeznek. Mivel a „kezelés" fogalmát az alapelvek meghatározzák, a jelenleg meglévő joghézagok elkerülése érdekében elengedhetetlenül fontos annak következetes alkalmazása. Ellenkező esetben túl nagy tér állna rendelkezésre vélhetően nem kívánatos értelmezésekre, ami pedig a határozat szövegének téves értelmezését eredményezheti.

[11] A „személyes adatok" fogalma a II. melléklet I. szakaszának 8.a. pontjában szereplő meghatározás szerint „valamely azonosított vagy azonosítható magánszemélyre vonatkozó adatokat" jelent. Az egyik kiegészítő elv értelmében azonban humánerőforrás-adatokkal kapcsolatban az alapelvek csak akkor alkalmazandók, amikor „azonosított nyilvántartásokat továbbítanak vagy azokhoz férnek hozzá." A WP29 úgy véli, hogy ennek következtében a személyes adatok oly módon történő kezelése válik lehetővé, amely sem az uniós jog szerinti adatvédelmi alapelvekkel, sem a személyes adatoknak az adatvédelmi pajzs szerinti általános fogalmával nem áll összhangban.

amelyeket az EU területén, az irányelv 8. cikkében felsorolt jogos indokok alapján gyűjtöttek, és ezt követően már továbbításra kerültek.

A WP29 végül megjegyzi, nem világos, hogy kik tekinthetők unióbeli magánszemélynek, és ezáltal kik jogosultak az adatvédelmi pajzs által biztosított védelemre: valamennyi uniós polgár, vagy valamennyi, az EU területén tartózkodó személy. Ennek különösen nagy jelentősége van a jogorvoslati joggal kapcsolatban, ideértve az ombudsmani mechanizmus igénybevételének lehetőségét is. A megfelelőségi határozatnak továbbá azzal a kérdéssel is foglalkoznia kellene, hogy az adatvédelmi pajzs milyen mértékben lesz alkalmazandó az EGT-országok és Svájc állampolgáraira / lakosaira. Ezekre az országokra korábban a védett adatkikötő rendszere kiterjedt.

1.2.3. Közös felülvizsgálat és felfüggesztés

A WP29 örvendetesnek tartja, hogy az Európai Bizottság és az USA kormánya megállapodott abban, hogy rendszeresen felülvizsgálja az adatvédelmi pajzs gyakorlati alkalmazását. Ez a közös felülvizsgálat már évek óta ismert gyakorlat az Unión belül adatvédelemmel foglalkozók közösségében, különösen az utas-nyilvántartási adatállomány harmadik országokkal történő cseréjére vonatkozó (PNR) megállapodások és a terrorizmus finanszírozásának felderítését célzó programról szóló (TFTP) megállapodás tekintetében. A WP29 továbbá örvendetesnek tartja, hogy az adatvédelmi hatóságok részéről meghatározatlan számú képviselő részt vehet ezekben a közös felülvizsgálatokban.

A közös felülvizsgálatokkal kapcsolatban az elmúlt években szerzett tapasztalatai alapján a WP29 szeretné világossá tenni: elvárja, hogy az adatvédelmi pajzs közös felülvizsgálata kiterjedtebb legyen, mint amilyen a PNR és TFTP közös felülvizsgálata volt. Különösen fontos, hogy a közös felülvizsgálat ne csak az egyesült államokbeli ügynökségek, szervezetek és a vállalkozások képviselőivel folytatott megbeszélésekre terjedjen ki, hanem az adatvédelmi pajzs egyes elemei tekintetében helyszíni vizsgálatokat is tartalmazzon. Az adatvédelmi hatóságok közös felülvizsgálatban részt vevő képviselői számára lehetőséget kell adni arra, hogy javaslatokat tegyenek ilyen helyszíni vizsgálatokra.

A WP29 úgy véli, hogy a közös felülvizsgálathoz szükséges a megállapítások közös értékelése. Az eddigiekben úgy történt, hogy a közös felülvizsgálatok eredményei egy bizottsági szolgálati dokumentumban kerültek bemutatásra, amelynek előterjesztéséhez nem volt szükség a közös felülvizsgálati csoport Bizottságon kívüli tagjainak jóváhagyására. Az adatvédelmi pajzs esetében a WP29 fontosnak tartja, hogy a vizsgálat eredményeiről készült jelentés valóban közös munkával készülhessen. Alternatív megoldásként megfontolható, hogy az adatvédelmi hatóságok egy különálló közös felülvizsgálati jelentést készítsenek.

A közös felülvizsgálatot illetően a WP29 végezetül a Bizottság azon ígéretére emlékeztet, hogy a WP29 képviselőinél a közös felülvizsgálatok során felmerült költségeket a Bizottság megtéríti. A munkacsoport vélelmezi, hogy ez vonatkozni fog az adatvédelmi pajzs közös felülvizsgálatára is, az adatvédelmi hatóságok legalábbis ésszerű számú képviselője tekintetében.

A WP29 javasolja, hogy legkésőbb három hónappal az adatvédelmi pajzs első közös felülvizsgálatának megkezdése előtt a Bizottság, az Egyesült Államok kormánya valamint a WP29 állapodjon meg a közös felülvizsgálat gyakorlati szabályairól, és ezt foglalja írásba.

1.2.4. Az uniós jogi keret felülvizsgálata

Az adatvédelmi pajzs megfelelőségére vonatkozó határozat az első olyan megfelelőségi határozat, amely az általános adatvédelmi rendeletet szövegéről elvi alapon történt megállapodást követően került megszövegezésre. A WP29 azonban megállapította, hogy az adatvédelmi pajzs még nem tükrözi a jövőbeni helyzetet. Nem kerültek be az adatvédelmi pajzsba például olyan új és fontos fogalmak, mint az adathordozhatósághoz való jog és az adatkezelőkre rótt további kötelezettségek, ideértve az adatvédelmi hatásvizsgálat végzésének kötelezettségét, valamint a beépített és az alapértelmezett adatvédelem elveinek való megfelelés kötelezettségét. A WP29 ezért azt javasolja, hogy az adatvédelmi pajzs felülvizsgálata – csakúgy, mint más meglévő megfelelőségi határozat esetében – röviddel az általános adatvédelmi rendelet hatályba lépése után történjen meg. Kívánatos volna, hogy a végleges megfelelőségi határozat kifejezett utalást tartalmazzon erre a felülvizsgálati eljárásra.

2. A MEGFELELŐSÉGI HATÁROZATTERVEZET KERESKEDELMI RÉSZÉNEK ÉRTÉKELÉSE

2.1. Általános észrevételek

2.1.1. Kedvező változások

A WP29 üdvözli az adatvédelmi pajzs által hozott kedvező változásokat és a tárgyaló felek arra vonatkozó szándékát, hogy megpróbálják orvosolni a védett adatkikötő azon hiányosságait, amelyekre a WP29 felhívta a figyelmet. A védett adatkikötőhöz képest különösen a következő elemek tekintetében figyelhető meg javulás: egyes kulcsfontosságú fogalmak, például a „személyes adatok”, „adatkezelés”, „adatkezelő” fogalmának felvétele a szövegbe, az adatvédelmi pajzsban részt vevő szervezeteket tartalmazó lista felügyeletének biztosítására létrehozott mechanizmusok, és a megfelelőség most már kötelező külső és belső ellenőrzése. Javult a helyzet a hozzáférési elv terén is, és a WP29 megállapítja, hogy most már biztosított a helyesbítés és a törlés joga olyan esetekben, amikor az adatokat az adatvédelmi pajzs alapelveivel össze nem egyeztethető módon használják fel. Ezen túlmenően már egyértelmű az az előírás, hogy a magánszemélyeknek visszaigazolást kell kapniuk arról, hogy adataikat kezelik, és közölni kell velük, hogy mely adatokról van szó.

A WP29 üdvözli a harmadik fél részére történő adattovábbítások esetén alkalmazandó jogi garanciák megerősítését is, valamint a Kereskedelmi Minisztérium és a Szövetségi Kereskedelmi Bizottság (FTC) elkötelezettségét az adatvédelmi pajzsban foglalt kötelezettségek érvényesítésére.

2.1.2. Az adatvédelmi pajzs alkalmazása az adatfeldolgozóként (megbízottként) eljáró szervezetekre

Sajnos nem derül ki egyértelműen, milyen mértékben alkalmazandók az adatvédelmi pajzs alapelvei az EU-ból kizárólag kezelés céljából személyes adatokat fogadó, tanúsítvánnyal rendelkező szervezetekre (a továbbiakban: megbízottak vagy adatfeldolgozók). Bár a II. melléklet III. szakasza 10.a. pontjának rendelkezései említést tesznek a tanúsítvánnyal rendelkező szervezetekhez ilyen célból történő adattovábbításokról – például megemlítik a szerződéskötésre vonatkozó követelményt – semmiféle támpontot nem adnak arra vonatkozólag, hogy az adatvédelmi pajzs alapelvei milyen módon alkalmazandók az adatfeldolgozókra (megbízottakra). Ez egyaránt bizonytalanságot okoz a kezelés céljából személyes adatokat fogadó egyesült államokbeli, tanúsítvánnyal rendelkező szervezetek, és azon uniós vállalkozások számára, amelyek adatokat továbbítanak tanúsítvánnyal rendelkező, adatfeldolgozóként eljáró szervezetekhez, valamint azon magánszemélyek számára is, akiknek az adatait kezelik. Ennek következtében nehezen lesz meghatározható, hogy ténylegesen milyen kötelezettségek terhelik majd az adatvédelmi pajzsban részt vevő, adatfeldolgozói minőségükben eljárva az EU-ból kapott személyes adatokat kezelő szervezeteket. Mindenképpen szükség van ennek tisztázására.

Figyelembe kell venni azt a tényt, hogy az alapelvekben foglalt egyes kötelezettségek nem alkalmazhatók az adatfeldolgozók vonatkozásában, mivel minden esetben az adatkezelő az, aki meghatározza az adatkezelés célját és eszközeit (vö. az „adatkezelő” fogalommeghatározását a II. melléklet I. szakasz 8.c. pontban). Ez az oka annak, hogy az alapelvekben foglalt egyes kötelezettségek, ha azok megbízottként eljáró szervezetekre vonatkoznak, ellentétesek lehetnek az uniós jog által megkövetelt adatkezelési szerződéssel (a II. melléklet III. szakasz 10.a. pontjában említett szerződés). Az adatkezelési szerződés például főszabályként nem engedi meg, hogy az adatfeldolgozó (megbízott) adatokat továbbítson harmadik fél adatkezelő részére, még a II. melléklet II. szakasz 3.a. pontban említett körülmények esetében sem. Harmadik fél megbízott részére történő adattovábbítást csak abban az esetben kellene engedélyezni, ha azt az adatkezelő előzetesen jóváhagyta. Emellett az uniós jog követelményeinek megfelelően az adatfeldolgozó (megbízott) nem lesz képes teljes tájékoztatást adni a magánszemélyek részére, ahogyan azt a tájékoztatás elve célozza (II. melléklet, II. szakasz 1. pont), például amiatt, mert nem ez a szervezet határozza meg az adatkezelés célját.

Ezért alapvető fontosságú annak egyértelművé tétele az alapelvekben, hogy ilyen ellentmondás esetén az adatkezelési szerződés rendelkezései, és különösen az adatokat az EU területéről továbbító szervezet által adott utasítások irányadók. E pontosítás nélkül az alapelveket olyan módon lehetne értelmezni és alkalmazni, ami túl nagymértékű ellenőrzési kapacitást biztosítana az adatvédelmi pajzsban részt vevő megbízottnak, és ennek következtében fennállna az a veszély, hogy az uniós adatátadó megsérti adatkezelői kötelezettségeit, amelyek az uniós jog értelmében akkor terhelik, amikor adatokat továbbít az adatvédelmi pajzsban részt vevő valamely, megbízotti minőségben eljáró szervezetnek. Az egyértelműségnek ez a hiánya továbbá azt a benyomást kelti, hogy az adatfeldolgozó az adatokat ismételten felhasználhatja, ha kívánja.

Ezen túlmenően specifikus szabályokra lenne szükség arra az esetre, amikor egy szervezet adatfeldolgozóként (megbízottként) jár el, annak biztosítása érdekében, hogy az figyelembe veszi az adatkezelő utasításait. Egyértelművé kell tenni, hogy az adatokat pusztán kezelési céllal fogadó egyesült államokbeli szervezetek nem dönthetnek úgy, hogy a saját nevükben kezelik az adatokat. Adatfeldolgozóként eljáró szervezetekre alkalmazandó specifikus szabályok hiányában nehéz meghatározni, hogy az adatfeldolgozó (megbízott) milyen szabályok alapján volna képes öntanúsításra.

2.1.3. Az alapelvek betartására irányuló kötelezettség korlátozása

A II. melléklet I. szakaszának 5. pontja többek között mentességeket határoz meg az alapelvek betartása alól olyan esetekre, amikor az adatvédelmi pajzs hatálya alá tartozó adatokat nemzetbiztonsági[12], közérdekű, vagy bűnüldözési okból használják fel, vagy ha törvény, kormányrendelet, vagy esetjogi döntés ellentétesen rendelkezik, vagy a felhasználásra kifejezett felhatalmazást ad. Anélkül, hogy teljes körűen ismerné az Egyesült Államok jogszabályait mind szövetségi szinten, mind az egyes államok szintjén, a WP29 számára nehézséget okoz e mentesség hatályának értékelése és annak megállapítása, hogy ezek a beavatkozások igazolhatók-e egy demokratikus társadalomban. Alapvetően fontos, hogy az Európai Bizottság a megfelelőségi határozat tervezetében annak értékelését is elvégezze, hogy e mentességek alkalmazása esetén milyen védelmi szint biztosított. A WP29 felhívja a Bizottságot annak biztosítására, hogy az EU tájékoztatást kapjon bármely olyan törvényről vagy kormányrendeletről, amely hatással lehet az alapelvek betartására, akár jelenleg, vagy akkor, amikor új törvény vagy rendelet lép hatályba az USA-ban.

2.1.4. A korlátozott idejű adatmegőrzés elvének hiánya

A korlátozott idejű adatmegőrzés elve (az irányelv 6. cikke (1) bekezdésének e) pontja) az uniós adatvédelmi jog egyik alapelve, amelynek értelmében személyes adatokat csak az adatok gyűjtése vagy további kezelése céljainak eléréséhez szükséges ideig lehet megőrizni.

A WP29 azonban az adatvédelmi pajzsot alkotó dokumentumokban semmilyen utalást nem talált arra vonatkozólag, hogy az adatkezelőknek biztosítaniuk kellene az adatok törlését, amennyiben az azok gyűjtését vagy további kezelését szükségessé tévő ok már nem áll fenn. Következésképpen úgy tűnik, hogy az alapelvek nem írnak elő a tanúsítvánnyal rendelkező szervezetek részére olyan adatmegőrzési határidőt, amely az uniós jogban előírt, korlátozott idejű adatmegőrzés elvéhez hasonló lenne.

Az adatok sértetlensége és célhoz kötöttség elvének szövege (II. melléklet II. szakasz 5. pont) egyáltalán nem tekinthető úgy, mint amely az adatkezelőként eljáró szervezetek részére kötelezővé tenné azon adatok törlését, amelyek az adatgyűjtés céljának megvalósításához vagy további kezelés céljából már nem szükségesek, vagy mint amely a feldolgozóként eljáró szervezetek részére kötelezővé tenné az adatok törlését a szolgáltatási szerződés lejártát követően.

[12] Az adatvédelmi pajzs hatálya alá tartozó személyes adatok nemzetbiztonsági célú felhasználására vonatkozó további észrevételeket a 3. fejezet, bűnüldözési célú felhasználására vonatkozó további észrevételeket pedig a 4. fejezet tartalmaz.

A munkacsoport felhívja a figyelmet arra, hogy az adatvédelmi pajzs hatálya alá tartozó adatokra vonatkozó megőrzési idő korlátozásának hiányában a szervezeteknek lehetőségük lesz olyan hosszú ideig megtartani az adatokat, ameddig kívánják, azt követően is, hogy az adatvédelmi pajzsban való részvételük már megszűnt. Ez nem áll összhangban a korlátozott idejű adatmegőrzés alapvető elvével.

2.1.5. Biztosítékok hiánya joghatásokat keletkeztető, vagy magánszemélyeket jelentős mértékben érintő, automatizált döntések esetében

Az adatvédelmi pajzs semmiféle jogi biztosítékot nem tartalmaz arra az esetre, amikor magánszemélyek vonatkozásában olyan határozatot hoznak, amely rájuk nézve joghatásokat keletkeztet vagy jelentős mértékben érinti őket, és amely kizárólag bizonyos rájuk jellemző személyes szempontok – például munkahelyi teljesítmény, hitelképesség, megbízhatóság, életvitel, stb. – értékelése céljából gyűjtött adatok automatizált kezelésén alapul.

A WP 29 már 12. sz. munkadokumentumában már kiemelte annak szükségességét, hogy a megfelelő szintű védelem biztosítása érdekében jogi garanciákat kell nyújtani a (joghatásokat keletkeztető, vagy a magánszemélyekre jelentős hatással lévő**)** automatizált döntésekkel szemben.

Ez azért is rendkívül fontos, mert a folyamatosan fejlődő technológiáknak köszönhetően egyre több vállalat mérlegeli automatizált döntéshozatali rendszerek alkalmazását, aminek következtében a magánszemélyek helyzete rosszabbodik, hiszen semmilyen jogorvoslati lehetőséggel nem rendelkeznek az ilyen gépesített döntésekkel szemben. Olyan helyzetekben, amikor a pusztán ilyen automatizált rendszerek által generált döntések magánszemélyek jogi helyzetét befolyásolják vagy őket jelentős mértékben érintik (például feketelistára kerülnek és ezáltal jogoktól esnek el), alapvető fontosságú, hogy megfelelő biztosítékok álljanak rendelkezésre, ideértve azt is, hogy az érintetteknek jogukban álljon megismerni a döntéshozatal logikáját és új, nem automatizált döntés hozatalát kérni.

2.1.6. Átmeneti időszak a fennálló kereskedelmi kapcsolatokra tekintettel

Az adatvédelmi pajzs rendelkezése értelmében az adatvédelmi elvek közvetlenül a tanúsítás után már alkalmazandók. Az adatvédelmi pajzs keretrendszerének hatályba lépését követő első két hónap során tanúsító szervezeteknek a harmadik felekkel fennálló bármely kereskedelmi kapcsolataikat a lehető legrövidebb időn belül összhangba kell hozniuk a harmadik fél részére történő adattovábbításokért való elszámoltathatóságra vonatkozó elvvel. Ezt mindenképpen meg kell tenniük legkésőbb kilenc hónappal azt követően, hogy tanúsították az adatvédelmi pajzsban való részvétel feltételeinek való megfelelésüket.

Ez azt jelenti, hogy 2–9 hónappal a tanúsítást követően a meglévő szerződéseket a szükséges mértékben összhangba kell hozni az alapelvekkel. Ezen átmeneti időszak alatt elegendő a tájékoztatás és a választási lehetőség elvét alkalmazni. A WP29 kitart azon álláspontja mellett, miszerint az adatvédelmi pajzs alapján történő adattovábbítás csak attól az időponttól kezdve lehetséges, hogy a szervezet teljes mértékben teljesíteni képes az adatvédelmi pajzs által támasztott valamennyi követelményt. Az a lehetőség, hogy egy átmeneti időszak

folyamán az adattovábbítás úgy történjen, hogy a címzett nem képes maradéktalanul betartani az adatvédelmi pajzs alapelveit, nem tekinthető olyannak, amely megfelel a jogszerű adattovábbítás feltételeinek, következésképpen elfogadhatatlan.

2.2. Konkrét észrevételek

2.2.1. Átláthatóság

a) Általános megjegyzések a tájékoztatás elvével kapcsolatban

A WP29 üdvözli a tájékoztatás elvének keretében meghatározott átfogóbb és részletesebb követelményeket, különösen azt, amely szerint az értesítésnek tartalmaznia kell majd egy, az adatvédelmi pajzsban részt vevő szervezetek listájára vezető linket vagy a listát tartalmazó internetcímet, valamint utalnia kell a magánszemélyek hozzáférési jogára és az alternatív vitarendezési mechanizmusokra[13]. A WP29 javasolja azonban a magánszemélyeket megillető egyéb jogok (a kijavítás és a törlés joga pontatlan vagy az alapelveket sértő kezelés esetén) egyértelműbb megjelenítését.

Az adatvédelmi pajzsot alkotó dokumentumok valóban aggályokat vetnek fel azzal az időponttal kapcsolatban, amikor az adatvédelmi pajzsban részt vevő szervezeteknek tájékoztatniuk kell az érintett magánszemélyt. A II. melléklet II. szakaszának 1. b. pontja úgy rendelkezik, hogy „a tájékoztatást (...) (akkor) kell megadni, az első alkalommal (...) amikor az egyént felkérik arra, hogy a szervezet részére személyes információkat szolgáltasson, vagy azt követően a lehető legrövidebb időn belül, de minden esetben azt megelőzően, hogy a szervezet az ilyen információt más célra használná fel, mint amelyre az adatokat átadó szervezet eredetileg gyűjtötte vagy kezelte őket, vagy mielőtt harmadik félnek azokat először átadná”. A WP29 úgy véli, hogy az adatvédelmi pajzsban részt vevő egyesült államokbeli szervezetek gyakran nem közvetlenül az érintettől gyűjtenek adatokat, ezért a tájékoztatásnak abban az időpontban kellene megtörténnie, amikor a pajzsban részt vevő szervezet rögzíti az adatokat.

A WP29 megjegyzi, hogy a követelmények tényleges teljesítésének értékelését – a tájékoztatás elvére és az adatvédelmi politikára figyelemmel – az adatvédelmi pajzs első éves felülvizsgálatakor kellene elvégezni.

b) Az adatvédelmi politika nyilvános elérhetősége

A WP29 üdvözli, hogy konkréttá vált: a Kereskedelmi Minisztérium ellenőrizni fogja, hogy a nyilvános weboldallal rendelkező vállalatok közzétették-e adatvédelmi politikáikat ezen a weboldalon, vagy, ha nem rendelkeznek nyilvános weboldallal, hol tették hozzáférhetővé a nyilvánosság számára adatvédelmi politikáikat[14].

[13] II. melléklet II. szakasz 1. pont; A WP29 a COM(2103)847 közleményben tett második bizottsági ajánlásra is utal, valamint a WP29 Reding alelnökhöz intézett 2014. április 10-i levelére, különösen az „Átláthatóság” cím alatt szereplő 4. pontra.

[14] Lásd az Európai Bizottság COM(2013)847 sz. közleményében szereplő első ajánlást, és a WP29 Reding alelnökhöz intézett 2014. április 10-i levelét, különösen az „Átláthatóság” cím alatti 3. pontot.

c) Az adatfeldolgozókkal kötött szerződésekben szereplő adatvédelmi feltételek közzététele

Az adatvédelmi pajzs arra vonatkozó előírásai között, hogy az adatvédelmi pajzsban részt vevő szervezetek milyen feltételekkel továbbíthatnak adatokat a feldolgozókhoz (megbízottakhoz), szerepel az a követelmény, mely szerint az öntanúsított vállalatoknak „az adott megbízottal kötött szerződésük megfelelő adatvédelmi rendelkezéseinek összefoglalását vagy egy reprezentatív példányát kérésre át kell adniuk a Minisztériumnak" (lásd a II. melléklet II. szakaszának 3.b.v. pontját). A munkacsoport üdvözli ezt az átláthatósági követelményt a Kereskedelmi Minisztérium javára.

2.2.2. Választási lehetőség

Az adatvédelmi pajzs kívülmaradási jogot („opt-out") biztosít a személyes adatok harmadik fél részére történő átadása vagy lényegesen eltérő célra történő felhasználása tekintetében[15] (II. melléklet III. szakasz 2. pont). Ezen kívül a magánszemélyeknek bármikor kívülmaradási joggal élhetnek a személyes adatok közvetlen üzletszerzés céljából történő felhasználásával szemben (II. melléklet III. szakasz 12.a. pont)[16].
Semmilyen részlet nem derül ki arról, hogy a közvetlen üzletszerzés célú felhasználás esetkörét kivéve a kívülmaradási joggal hogyan és mikor lehet élni. A WP29 úgy véli, hogy az adatvédelmi pajzsban nem lehet elegendő az e jog létezésére történő egyszerű utalás, hanem *személyre szabott* lehetőséget kell biztosítani arra, hogy az érintettek a személyes adatok harmadik fél részére történő átadását vagy újbóli felhasználását *megelőzően* gyakorolhassák ezt a jogukat.

Ezen túlmenően a WP29 kiemeli, hogy az adatvédelmi pajzsnak biztosítania kellene egy olyan (az érintett személyes helyzetéből eredő kényszerítő ok miatt indokolt) általános kifogásolási jogot, amelynek alapján az érintett magánszemély, bármikor, amikor egyéni helyzetéből eredő kényszerítő ok ezt szükségessé teszi, kérhetné a rá vonatkozó adatok kezelésének abbahagyását[17]. A WP29 nyomatékosan javasolja, hogy a megfelelőségi határozat tervezetéből világosan tűnjön ki, hogy a kifogásolási jognak minden pillanatban fenn kell állnia, valamint, hogy ilyen kifogás nem kizárólag az adatok közvetlen üzletszerzési célra történő felhasználásával szemben emelhető[18].

A WP29 attól tart, hogy zavart és jogbizonytalanságot fog eredményezni, ha nincs egyértelműen meghatározva, mi tekintendő „lényegesen eltérő" célnak. Egyértelművé kell tenni, hogy a választási lehetőség elvét semmiképpen nem lehet a célhoz kötöttség elvének megkerülésére használni[19]. Csak akkor kellene alkalmazhatónak lennie, amikor a cél jelentősen eltérő, de még mindig összeegyeztethető, tekintve, hogy az összeegyeztethetetlen adatkezelés tilos (II. melléklet II. szakasz 5.a. pont). Egyértelművé kell tenni, hogy a

[15] A 14.c.I számú kiegészítő elv biztosítja a klinikai kísérletből való kilépés jogát, amely a kifogásolási jognak vagy a beleegyezés visszavonásához való jognak feleltethető meg.
[16] Ez azonos azzal, amit a védett adatkikötő rendszere biztosított (12. GYFK), és e tekintetben semmilyen változás nem történt.

[18] Lásd a WP29 Reding alelnökhöz intézett levelét, „A választási lehetőség elve" cím alatt.
[19] A választási lehetőség elve alapján engedélyezett nem összeegyeztethető további kezelésre konkrét példa található a 9.b.i. sz. kiegészítő elv alatt (a WP 29 erre vonatkozó észrevételét lásd a humánerőforrás -adatokra vonatkozó pontban).

kívülmaradás jogának alkalmazása nem teszi lehetővé a szervezet számára az összeegyeztethetetlen célból történő adatkezelést. Ezért a WP29 a szóhasználat harmonizálását javasolja egyetlen és meghatározott jelentésű kifejezés használata által (például „lényegesen eltérő, de összeegyeztethető cél").

Hasznos lenne tisztázni, hogy az uniós jog hatálya alá tartozik-e a más céllal történő adatkezelésről vagy az információk harmadik fél számára történő átadásáról való döntés. Ebben az esetben a szokásos uniós jogi feltételek (például a nem összeegyeztethető célból történő kezelés tilalma, az adatkezelés jogszerű indoka, és a magánszemély tájékoztatására irányuló kötelezettség) közvetlenül alkalmazandók, azokra az egyesült államokbeli szervezetekre is, amelyek az uniós jog hatálya alá tartoznak. A gyakorlatban ez azt jelenti, hogy az ilyen döntést hozó uniós adatátadónak kell majd biztosítania a kezelés uniós jog szerinti átláthatóságát és jogszerűségét. Ezért a választási lehetőség elve csak abban az esetben lesz alkalmazandó, ha a döntést kizárólag az adatvédelmi pajzsban részt vevő olyan egyesült államokbeli szervezet hozza, amely nem tartozik az uniós jog hatálya alá.

2.2.3. Adattovábbítás harmadik fél részére

a) Alkalmazási kör

A WP29 aggodalmának ad hangot azokkal a helyzetekkel kapcsolatban, amikor az adatvédelmi pajzsban részt vevő egyesült államokbeli tanúsított szervezet a személyes adatokat harmadik országbeli címzettnek továbbítja.

Az adatvédelmi pajzsot nem lehet csupán olyan eszköznek tekinteni, amelynek révén uniós adatokat továbbítanak az Unióból az Egyesült Államokba, hanem azt az USA-ból harmadik országokba irányuló adattovábbításra is használni fogják. A harmadik országokba irányuló adattovábbításra vonatkozó rendelkezések ezért az adatvédelmi pajzs fontos elemét jelentik, amelyeknek elegendő garanciát és megfelelő védelmi szintet kell biztosítaniuk abban az esetben, amikor az adatokat az USA területén kívülre, harmadik országba továbbítják. Különösen problematikus területek e tekintetben a nemzetbiztonság és a bűnüldözés.

Az adatvédelmi pajzs keretében az adattovábbítás elszámoltathatósága elvének alkalmazása nem korlátozódik azokra az adatkezelő címzettekre, adatfeldolgozókra vagy megbízottakra, amelyek az USA-ban letelepedettek. Ezért a harmadik országokba irányuló adattovábbítás akkor is történhetne az adatvédelmi pajzs keretében, ha az adott harmadik ország jogszabályai lehetővé teszik a személyes adatokhoz való nyilvános hozzáférést, például megfigyelési célból. Ez azzal a kockázattal jár, hogy az uniós adatok esetében az alapvető jogok védelme igazolatlan sérelmet szenvedhet.

Harmadik országba irányuló bármely adattovábbítás esetén az adatvédelmi pajzsban részt vevő valamennyi szervezetet kötelezni kellene arra, hogy a továbbítást megelőzően értékelje az adott harmadik ország nemzeti jogszabályai által az adatátvevőkre előírt, kötelezően alkalmazandó követelményeket. Ha megállapításra kerül az adatvédelmi pajzs által előírt garanciákat, kötelezettségeket és védelmi szintet érintő, jelentősen káros hatás kockázata, az

adatvédelmi pajzsban részt vevő, adatfeldolgozóként (megbízottként) eljáró egyesült államokbeli szervezetnek haladéktalanul értesítenie kell az uniós adatkezelőt, mielőtt bármilyen adattovábbítást végezne. Ebben az esetben az adatátadó jogosult az adattovábbítást felfüggeszteni és/vagy a szerződést felbontani. Amikor ilyen jelentősen káros hatás kockázata fennáll, az adatvédelmi pajzsban résztvevő, adatkezelőként eljáró szervezet számára nem volna szabad engedélyezni az adattovábbítást, mivel ez a kockázat veszélyeztetné arra irányuló kötelezettségének teljesítését, hogy adattovábbítás esetén ugyanolyan szintű védelmet biztosítson, mint amilyet az alapelvek nyújtanak (lásd a II. melléklet, II. szakaszának 3.a. pontját).

Hasonlóképpen, harmadik ország jogszabályainak olyan változása esetén, amely valószínűsíthetően jelentős káros hatást gyakorolna az adatvédelmi pajzs által előírt garanciákra, kötelezettségekre és védelmi szintre, az adatvédelmi pajzsban részt vevő, adatfeldolgozóként (megbízottként) eljáró egyesült államokbeli szervezetet – az adatvédelmi pajzs által – kötelezni kellene arra, hogy amint e a jogszabályváltozásról tudomást szerez, haladéktalanul értesítse róla az adatátadót. Ebben az esetben az adatátadó jogosult felfüggeszteni az adattovábbítást és/vagy a szerződést felbontani. Ennek megfelelően ilyen esetben az adatvédelmi pajzsban részt vevő, adatkezelőként eljáró szervezet számára nem lehetne engedélyezni, hogy harmadik országba történő továbbítást végezzen, tekintettel arra, hogy az alapelvek által nyújtott védelemmel azonos szintű védelmet kell biztosítania (lásd a II. szakasz II. mellékletének 3.a. pontját).

A WP29 emlékeztet arra az álláspontjára, mely szerint, ha az uniós adatkezelő még az USA-ba irányuló adattovábbítás megtörténte előtt tudomást szerez harmadik fél részére, az USA-n kívülre tervezett adattovábbításról, vagy ha az adatkezelő is felelős a harmadik országba történő továbbítást engedélyező döntésért, az adattovábbítást az Unióból az USA területén kívüli, harmadik országba történő közvetlen továbbításnak kell tekinteni. Ez azt jelenti, hogy az irányelv 25. és 26. cikke alkalmazandó, nem pedig az adatvédelmi pajzs harmadik fél részére történő adattovábbításra vonatkozó elve.

b) Az adatvédelmi pajzsban résztvevő szervezettől harmadik fél adatkezelő részére történő adattovábbítás

A WP29 örvendetesnek tartja annak a kötelezettségnek az előírását, mely szerint szerződéseket kell kötni (II. melléklet II. szakasz 3.a. pont) annak biztosítása érdekében, hogy a harmadik fél adatkezelő legalább ugyanolyan szintű adatvédelmet biztosítson, mint amilyet az adatvédelmi pajzs alapelvei megkövetelnek. A cél annak biztosítása, hogy a személyes adatok továbbra is megfelelő védelemben részesüljenek, azt követően is, hogy harmadik országba továbbították őket. A WP29-nek azonban van néhány észrevétele a javasolt feltételekkel kapcsolatban.

<u>A célhoz kötöttség elvére történő hivatkozás hiánya</u>

A WP29 a célhoz kötöttség elvére (II. melléklet II. szakasz 5.pont) történő egyértelmű hivatkozás beillesztését javasolja a harmadik fél adatkezelő részére történő adattovábbítás

feltételei közé (II. melléklet II. szakasz 3.a. pont). Ez egyértelművé tenné, hogy az adattovábbításra nem kerülhet sor akkor, ha a harmadik fél adatkezelő az adatkezelést összeegyeztethetetlen célból végzi.

Mentesség a szerződéskötési kötelezettség alól adatkezelők közötti, csoporton belüli adattovábbítás esetén

Az adatkezelők közötti, csoporton belüli adattovábbítások mentesülnek a szerződéskötési kötelezettség alól. Az adatvédelmi pajzs elvei szerint ilyen esetben a személyes adatok védelmének folytonosságát kötelező erejű vállalati szabályok vagy „más csoporton belüli eszközök (pl. megfelelőségi vagy ellenőrzési programok)" biztosíthatják (II. melléklet III. szakasz 10.b. pont). A WP29 úgy ítéli meg, hogy a „más csoporton belüli eszközökre" történő utalás nem garantálja a csoport többi tagjának jogilag kötelező erejű kötelezettségvállalását. Mivel a WP29 és az uniós jogszabályok is általában azt támogatják[20], hogy a csoporton belüli továbbításokat kötelező érvényű kötelezettségvállalások alapján kell végezni, fontos elkerülni, hogy az adatvédelmi pajzsot e követelmények megkerülésére használják. A WP29 emlékeztet arra, hogy azokat az USA-ból harmadik országokba irányuló adattovábbításokat, amelyek már az USA-ba irányuló adattovábbítás megtörténte előtt tervben vannak, vagy amelyek uniós adatkezelővel közös adatkezelés alatt állnak[21], az EU-ból az USA területén kívüli harmadik országba irányuló közvetlen adattovábbításnak kell tekinteni, és ezért alkalmazni kell rájuk az irányelv 25. és 26. cikkét.

c) Az adatvédelmi pajzsban résztvevő szervezet által harmadik személy adatfeldolgozó fél (megbízott) részére történő adattovábbítások

A WP29 örvendetesnek tartja, hogy a címzett szervezetek adatfeldolgozóként (megbízottként) történő elfogadásához most már kötelező a harmadik országokba irányuló adattovábbításra vonatkozó szerződést kötni, függetlenül attól, hogy azok részt vesznek-e az adatvédelmi pajzsban, vagy más megfelelőségi ténymegállapítás szerinti megoldást vesznek-e igénybe. A WP29 üdvözli a harmadik országokba irányuló adattovábbításokra vonatkozó kiegészítő biztosítékok előírását is (a II. melléklet II. szakasz 3.a.i., 3.a.iii., 3.a.iv., 3.a.v. és 7.d. pontja). Az utolsó pont (II. melléklet II. szakasz 7.d. pont) a felelősség fennmaradását érinti abban az esetben, amikor az adatokat megbízottnak adják át. Úgy tűnik azonban, hogy ez a garancia nem alkalmazandó abban az esetben, ha egy szervezet úgy döntött, adatvédelmi hatósággal működik együtt (lásd a II. melléklet III. szakasz 5.a. pont vége). A WP29 nem érti, hogy mi az oka ennek a mentességnek, és úgy ítéli meg, hogy a felelősségnek ilyen esetben is fenn kell állnia.

A célhoz kötöttség elvére történő hivatkozás hiánya

A WP29 megjegyzi, hogy a harmadik fél részére történő adattovábbításért való elszámoltathatóság elve (II. melléklet, II. szakasz 3. pont) kifejti, hogy személyes adatok

[20] Az általános adatvédelmi rendeletet szintén kiemeli a kötelező erejű és érvényesíthető kötelezettségvállalások szükségességét, a használt eszközöktől (kötelező erejű vállalati szabályok, szerződéses feltételek, magatartási kódexek vagy tanúsítványok) függetlenül.
[21] Például humánerőforrás-adatok.

megbízottként eljáró harmadik fél számára csak korlátozott és meghatározott célokra továbbíthatók, de azt kifejezetten nem írja elő, hogy e korlátozott és meghatározott céloknak összeegyeztethetőknek kell lenniük az adatgyűjtés eredeti céljával, valamint az adatkezelő utasításaival. Nagyobb egyértelműségre van szükség e tekintetben. A WP29 ezért annak biztosítását javasolja, hogy a megfelelőségi határozat több részletet közöljön, például a célhoz kötöttség elvére (II. melléklet, II.5.) történő egyértelmű hivatkozás beillesztése által. A célhoz kötöttség elve szerint a harmadik fél részére történő adattovábbítás elve keretében (a kívülmaradás elve mellett) nem megengedett az adatok összeegyeztethetetlen célból történő kezelése (a hozzáférhetővé tételt is ideértve).

További kötelezettségek előírása szükséges az adatvédelmi pajzsban résztvevő, adatfeldolgozóként (megbízottként) eljáró szervezetek vonatkozásában, amikor azok más adatfeldolgozóként (megbízottként) eljáró harmadik országbeli szervezetek részére továbbítanak adatokat

Az adatvédelmi pajzsban résztvevő szervezet megbízottként (például valamely uniós adatkezelő nevében) történő eljárására vonatkozó egyértelmű szabályok hiánya joghézag létére utal, és megakadályozhatja az uniós adatkezelőt abban, hogy ellenőrzést tudjon gyakorolni. Az uniós adatkezelőtől megbízotti minőségben adatokat fogadó, az adatvédelmi pajzsban résztvevő szervezet köteles betartani az uniós adatkezelőtől kapott utasításokat. Ennek kifejezetten szerepelnie kellene az alapelvekben annak biztosítása érdekében, hogy az utasítások be nem tartása ne csak a szerződés megszegését jelentse (II. melléklet III. szakasz 10.a.ii. pont), hanem az adatvédelmi pajzs alapelveinek megsértését is.

Az adatkezelő számára átláthatóvá és előzetes hozzájárulásától függővé kell tenni annak lehetőségét, hogy az adatvédelmi pajzsban résztvevő, megbízottként eljáró szervezet a későbbiekben egy harmadik országbeli megbízotthoz fogja továbbítani az adatokat. Ezért egyértelműen ki kell jelenteni, hogy a megbízott által az uniós adatkezelővel kötött szerződés (10. GYFK a „17. cikk szerinti szerződésre" való hivatkozás) dönti el, hogy megengedett-e az adatok harmadik országba történő továbbítása[22].

A harmadik országbeli megbízottak részére történő adattovábbításra vonatkozó jelenlegi feltételek azon a vélelmen alapulnak, hogy az adatvédelmi pajzsban résztvevő szervezet adatkezelőként jár el, és ezért saját maga tud dönteni egy harmadik országbeli megbízott lehetséges beavatkozásáról. Erre azonban nem szabadna hogy lehetőség legyen akkor, amikor az adatvédelmi pajzsban résztvevő szervezet megbízottként jár el. Ellenkező esetben az uniós adatkezelő elveszti ellenőrzési lehetőségeit.

Az adatkezelő számára elérhetővé kell tenni a harmadik fél megbízottal kötött szerződés adatvédelmi rendelkezéseit, és ezeknek legalább olyan védelmi szintet kell biztosítaniuk, mint amilyet az adatkezelővel kötött szerződés rendelkezései biztosítanak

[22] Lásd a WP29 Reding alelnökhöz intézett 2014. április 10-i levelét, a „Harmadik országba történő továbbítás" címet viselő 4. pontot.

2.2.4. Az adatok sértetlensége és célhoz kötöttség

a) Arányosság

A WP29 egy csekélyebb jelentőségű kérdésben utal Reding alelnökhöz intézett levelére, amelyben rámutatott, hogy „a személyes adatok kezelése még a tájékoztatás és a választási lehetőség elvének szigorú betartása mellett is lehet aránytalan az érintett személy vagy a társadalom érdekeivel, jogaival és szabadságaival összevetve. Az arányosság és az ésszerűség elvét az adatkezelés minden szakaszában tiszteletben kell tartani, és a tájékoztatás és választási lehetőség elvének kiegészítéseként kell alkalmazni”[23].

Az adatvédelmi pajzs (II. melléklet II. szakasz 5.a. pont) kimondja, hogy a személyes adatoknak olyan információkra kell korlátozódniuk, amelyek a kezelés célja szempontjából relevánsak. A WP29 azt szeretné, ha ez a szövegrész a végleges megfelelőségi határozatban módosításra kerülne, ugyanis az a puszta tény, hogy az adatoknak az adatkezelés célja szempontjából relevánsnak kell lenniük, nem teszi arányossá a kezelést. Annak érdekében, hogy megfeleljen az arányosság elvének, a kezelésnek azokra az adatokra kell korlátozódnia, amelyek az adott kezelés céljára tekintettel szükségesek.

b) Pontosság

Az adatok sértetlensége és a célhoz kötöttség elve (II. melléklet II. szakasz 5. pont) kimondja továbbá: „A szervezetnek az ilyen célokhoz szükséges mértékben megfelelő lépéseket kell tennie annak biztosítására, hogy a személyes adatok a tervezett felhasználás szempontjából megbízhatók, pontosak, teljesek és naprakészek legyenek”. A WP29 megjegyzi, hogy ez pontosan ugyanaz a megfogalmazás, mint amely a védett adatkikötőre vonatkozó megállapodásban szerepel. A WP29 kételkedik abban, hogy az „ilyen célokhoz szükséges mértékben” kifejezésre szükség van a szövegben, mivel véleménye szerint az adatok pontosságának nem szabad az adatkezelés céljától függenie. A WP29 előnyösebbnek tartaná, ha ez az összekapcsolás nem szerepelne a végleges megfelelőségi határozatban.

c) Célhoz kötöttség

Amikor az Európai Unióban letelepedett adatkezelő személyes adatokat továbbít egyesült államokbeli szervezet számára, az adatátadónak kifejezett tájékoztatást kell nyújtania az egyesült államokbeli szervezetnek arról, hogy az adatokat eredetileg milyen célra gyűjtötték. Ez elengedhetetlen annak megállapításához, hogy a továbbítást követően a cél változott-e, ezáltal szükségessé vált-e a tájékoztatás elvének és a választási lehetőség elvének alkalmazása, valamint hozzájárulna a kockázat és a felelősség megosztásához.

Az adatok sértetlensége és a célhoz kötöttség elve (II. melléklet II. szakasz 5. pont) értelmében a szervezet nem kezelhet személyes adatot a gyűjtés céljaival vagy a magánszemély által a későbbiekben engedélyezett célokkal összeegyeztethetetlen módon. A választási lehetőség elve (II. melléklet, II. szakasz 2. pont) azonban lehetőséget ad egy

[23] Lásd a WP29 Reding alelnökhöz intézett 2014. április 10-i levelének 8. pontját.

érzékeny adatok (például az érintett személy orvosi kezelésére vagy egészségi állapotára, faji vagy etnikai hovatartozására, politikai véleményére, vallási vagy világnézeti meggyőződésére, szakszervezeti tagságára, vagy a szexuális életére vonatkozó információk, vagy bűnügyi nyilvántartására vonatkozó adatok) „használatára" vonatkozó részvételi záradék olyan célból történő alkalmazására, amely lényegesen eltér az adatgyűjtés eredeti céljaitól vagy a magánszemély által a későbbiekben engedélyezett céloktól. Ez a részvételi záradék nem szükséges az 1.a. sz. kiegészítő elvben (II. melléklet III. szakasz 1.a. pont) említett helyzetekben. A nem érzékeny személyes adatok tekintetében kívülmaradási rendszer áll rendelkezésre.

A WP29 felhívja a figyelmet arra, hogy a célhoz kötöttség elvének hatálya eltérő a tájékoztatás, a választási lehetőség, valamint adatok sértetlensége és célhoz kötöttség elve alapján. Valójában az „összeegyeztethetetlen cél" és a „lényegesen eltérő cél" kifejezések úgy szerepelnek ugyanabban a szövegben, hogy egyik sincs egyértelműen definiálva[24].

A WP29 komolyan aggályosnak tartja, hogy e következetlenség miatt esetleg nagyon nehezen lesz összeegyeztethető az adatok sértetlensége és célhoz kötöttség elve (II. melléklet, II. szakasz 5. pont) a választási lehetőség elvével (II. melléklet, II. szakasz 2. pont), mivel az egyik elv azt mondja ki, hogy az adatok nem kezelhetők az adatgyűjtés eredeti céljával összeegyeztethetetlen módon, a másik viszont kívülmaradási mechanizmust biztosít abban az esetben, ha az adatok kezelése az eredeti céltól lényegesen eltérő célból történik.

Ezért a választási lehetőség elve értelmezhető úgy, hogy az megengedi a nem összeegyeztethető további kezelést[25]. A WP29 álláspontja szerint világosan ki kell tűnnie a szövegből, hogy nem engedélyezhető a szervezetek számára a lényegesen eltérő célból történő adatkezelés, ha ez a cél a célhoz kötöttség elve alapján összeegyeztethetetlennek minősül. Más szóval, egyértelművé kell tenni, hogy a választási lehetőség elve nem jelent a célhoz kötöttség elve alóli mentességet.

Minden esetre, ha a további kezelés összeegyeztethetőnek tekinthető, a tájékoztatás és választás elve szintén alkalmazandó.

2.2.5. Újságírói kivételek

A személyes adatok kezelése tekintetében érvényesülő újságírói kivételekre a 2. sz. kiegészítő elv vonatkozik (II. melléklet III. szakasz 2. pont). E rendelkezések a szólásszabadság egyesült államokbeli alkotmányos védelmét tükrözik. Ezért az adatvédelmi pajzsot alkotó dokumentumok szerint „korábban közzétett anyagban talált, médiaarchívumból terjesztett személyes adatokra az adatvédelmi pajzs elveinek követelményei nem vonatkoznak" (II. melléklet III. szakasz 2.b. pont). Úgy tűnik, hogy ez a mentesség bármely adatkezelő vagy

[24] A WP29 rámutatott, hogy egyéb kifejezések is előfordulnak: „felhasználás nem összeegyeztethető" (II. melléklet III. szakasz 14.b.ii. pont), „használhatja fel különböző célokra" (II. melléklet III. szakasz. 9b.i. pont) „t más célra használná fel, mint amelyre az adatokat átadó szervezet eredetileg gyűjtötte" (II. melléklet II. szakasz 1.b. pont). Az egyértelműségnek ez a hiánya oda vezethet, hogy nem állnak rendelkezésre megfelelő garanciák a célhoz kötöttség elve tekintetében.

[25] Lásd a választási lehetőség elve témakörében tett észrevételt is. A WP29 úgy véli, az a tény, hogy a harmadik fél részére történő adattovábbításra vonatkozó szabályok (II. melléklet II. szakasz 3. pont) csak a választási lehetőség elvére utalnak, és a célhoz kötöttség elvére nem, növeli az ilyen értelmezés veszélyét.

adatfeldolgozó által végzett minden további kezelésre kiterjed, vagyis nem korlátozódik az újságírói célból történő továbbkezelésre. A WP29 – amint azt már Reding alelnökhöz intézett, 2014. április 10-i levelében is kifejtette – szívesebben látott volna egy korlátozottabb megközelítést az újságírói kivételekkel kapcsolatban, amely közelebb áll ahhoz, ahogyan ezt az elvet az EU-ban alkalmazzák, valamint összhangban van a Google Spain ügyben hozott ítéletet követően a keresőmotorok által kiadott találatok törlésének jogával[26].

2.2.5. Az érintettek betekintési, helyesbítési és törlési joga

Az adatvédelmi pajzs értelmében a magánszemélyeknek joguk van *visszaigazolást* kapni arról, hogy a szervezet kezeli-e az adataikat, valamint joguk van ahhoz, hogy *közöljék velük* az ilyen adatokat (II. melléklet III. szakasz 8.a.i. pont). Mindemellett meglehetősen enyhe a szervezetek arra való kötelezése, hogy válaszolniuk kell a magánszemélyek azon kérdéseire, hogy mi az adatkezeléss célja, melyek az érintett személyesadat-kategóriák, és melyek a címzettek vagy a címzettek azon kategóriái, akik felé az adatokat továbbítják. A WP29 úgy véli, hogy az érintettekkel közlendő részleteket a főszövegben kellene felsorolni, és nem pusztán egy lábjegyzetben, és azokat egyértelmű kötelességként kellene azokat megfogalmazni (a II. melléklet III. szakasz 8.a.i.1. ponthoz kapcsolódóan).

A 8. kiegészítő elv szerint „hozzáférés biztosítása csak azon a szinten szükséges, ahogyan a szervezet tárolja a személyes információt (II. melléklet III. szakasz 8d.ii. pont)". Ezt a szabály nem szabadna megszorítóan értelmezni, tehát úgy, hogy főszabály szerint akkor kell hozzáférést biztosítani, amikor a szervezet a személyes adatokat nem pusztán tárolja, hanem kezeli azokat. Ezért a hozzáférési jog hatékonyságának érdekében fontos egyértelművé tenni, hogy a „tárol" kifejezés jelentése „kezelés", a II. melléklet I. szakasz 8.b. pontjában szereplő fogalommeghatározás értelmében Ennek a szabálynak az alkalmazását az adatvédelmi pajzs közös felülvizsgálata alkalmával alaposan vizsgálni kell.

Továbbra is aggodalomra ad okot a kivételek listája a II. melléklet III. szakasza 8.e (i) pontjában, amely hasonló a védett adatkikötő 8. GYFK-ban szereplő listához, és amely az egyensúlyt inkább a szervezetek érdekei felé tolja el. Ezzel összefüggésben az alább felsorolt indokok fennállása esetén a magánszemély nem férhet hozzá a saját személyes adataihoz: „törvényes vagy más szakmai kiváltság vagy kötelezettség megsértése" (II. melléklet III. szakasz 8.e.3. pont), „munkavállalói biztonsági vizsgálatok vagy panaszeljárások, vagy a munkavállalói utánpótlás-tervezéssel és vállalkozás-átszervezésekkel kapcsolatos eljárások hátrányos befolyásolása" (II. melléklet III. szakasz 8.e.4. pont), és „a biztos irányítással összefüggő folyamatos ellenőrzéssel, felülvizsgálattal vagy szabályozó funkciókkal összefüggésben vagy a szervezet részvételével a jövőben vagy jelenleg folyamatban levő tárgyalások során szükséges titkosság hátrányos befolyásolása" (II. melléklet III. szakasz 8.e.5. pont). Ezen indokok a II. melléklet III. szakaszának 8.c. pontjában szereplő, a bizalmas üzleti információk esetén alkalmazható általános eltérésen felül léteznek. Emiatt a fent felsorolt helyzetekben a magánszemélyeknek egyáltalán nincs lehetőségük a saját adataikhoz

[26] A C-131/12. sz., Google Spain kontra Agencia Española de Protección de Datos és Mario Costeja González ügyben 2014. május 13-án hozott ítélet.

hozzáférni, mivel nem biztosított a magánszemélyek és a szervezetek jogainak és érdekeinek egyensúlya, és ezáltal nem megoldott a hozzáférés iránti igények kérdése.

A WP29 felhívja a figyelmet arra, hogy a magánszemélyek számára a saját adataikhoz történő hozzáféréshez való jogát a Charta 8. cikkének (2) bekezdése biztosítja. Bár ez nem abszolút jog, alapvető jelentőséggel bír a személyes adatok védelméhez való jog szempontjából, mivel megkönnyíti az érintettek számára egyéb jogaik, például az adatok helyesbítéséhez és törléséhez való joguk gyakorlását.

Az adatok helyesbítéséhez és törléséhez való jog tekintetében a WP29 örvendetesnek tartja a védett adatkikötőre vonatkozó alapelvekhez képest elért jelentős javulást, feltéve, ha ezek a jogok nem kizárólag azokban az esetekben biztosítottak, amikor az adatok pontatlanok, hanem akkor is, amikor a kezelés az alapelvekbe ütköző módon történt (II. melléklet II. szakasz 6. pont).

2.2.6. Jogorvoslat, végrehajtás és betudhatóság (jogorvoslati mechanizmusok)

a) Az unióbeli magánszemélyeket megillető jogorvoslati jog hatékony gyakorlása

A WP29 méltányolja az Egyesült Államok hatóságainak a jogorvoslati mechanizmus különböző szintjei tekintetében megnyilvánuló elkötelezettségét. Figyelembe véve azonban, hogy e jogorvoslati rendszer bonyolult és nem elég egyértelmű, a WP29 attól tart, hogy a gyakorlatban ez veszélyeztetheti az érintettek tényleges joggyakorlását. A WP29 felhívja a figyelmet arra, hogy az unióbeli magánszemélyek által igénybe vehető jogorvoslati eszközök mennyiségével szemben a jogorvoslati mechanizmus minősége kell, hogy elsőbbséget élvezzen. Aggodalomra ad okot az is, hogy a legtöbb – ha nem az összes – jogorvoslati mechanizmus olyan eljárásokat tartalmaz, amelyeket az Egyesült Államokban kell folytatni, megnehezítve ezáltal, hogy az uniós adatvédelmi hatóságok nyomon kövessék az eljárást.

Valóban az a helyzet, hogy az adatvédelmi pajzs által biztosított jogorvoslati mechanizmus első körben arra a lehetőségre összpontosít, hogy az érintettek „jogaik védelme érdekében az egyesült államokbeli öntanúsított vállalkozással való közvetlen kapcsolatfelvétel révén indíthatnak eljárást az adatvédelmi elvek be nem tartása miatt”[27]. Továbbá, a szervezeteknek ki kell jelölniük egy független vitarendezési testületet az egyéni panaszok kivizsgálására és rendezésére. A WP29 üdvözli azt a tényt, hogy ennek megszervezése nem fog költségeket eredményezni a magánszemélyek számára.

Alternatív lehetőségként a panaszokat közvetlenül a Szövetségi Kereskedelmi Bizottsághoz lehet benyújtani, annak ellenére, hogy az FTC-nek nem kötelessége, hogy panaszokkal foglalkozzon. Az adatvédelmi hatóságok is élhetnek panasszal, a Kereskedelmi Minisztérium pedig vállalta, hogy felülvizsgálja azokat, és mindent megtesz a panaszok elintézésének elősegítése érdekében (I. melléklet), a Szövetségi Kereskedelmi Bizottság pedig „elsőbbségi elbírálást” biztosít e panaszok esetében (II. melléklet III. szakasz 7.e. pont). A panaszok FTC

[27] Európai Bizottság, a megfelelőségi határozat tervezete, (43). preambulumbekezdés.

általi rangsorolása azonban nem jelent biztosítékot az érintettek számára a tekintetben, hogy foglalkoznak majd a panaszukkal.

Végső eszközként a magánszemélyek kötelező érvényű választottbírósági eljárást kezdeményezhetnek. A választottbírói testület székhelye az Egyesült Államokban lesz, és határozatainak felülvizsgálatára egyesült államokbeli bíróságoknak lesz hatásköre.

Az adatvédelmi pajzs azt is lehetővé teszi a szervezetek számára, hogy az uniós adatvédelmi hatóságokkal történő együttműködést válassza (II. melléklet III. szakasz 5. pont). Sőt, a munkaviszonnyal összefüggésben gyűjtött humánerőforrás-adatok esetében ez kötelező (II. melléklet III. szakasz 9.d.ii. pont). Ebben az esetben alternatív vitarendezés (AVR) nem alkalmazható (II. melléklet III. szakasz 5.a. pont). Az adatvédelmi pajzs nem határozza meg egyértelműen, hogy a gyakorlatban hogyan fog történni az uniós adatvédelmi hatóságokkal való együttműködés. Különösen az nem egyértelmű, hogy minden üggyel a választottbírói testület fog-e foglalkozni, vagy az egyes ügyeket különböző testületek fogják-e kezelni.

A WP29 úgy véli, hogy az adatvédelmi hatóságoknak a panaszok kezelésével kapcsolatos hatásköre tekintetében a megfelelőségi határozatnak részletesebbnek kell lennie. Úgy tűnik, ez a hatáskör a szervezet minősítésétől függ, nem világos azonban, hogy milyen módon.

Amikor a szervezet uniós adatkezelő nevében közvetítőként jár el, a magánszemélyeknek minden esetben lehetőségük lesz arra, hogy panaszt nyújtsanak be az illetékes uniós adatvédelmi hatósághoz. Hasonló lesz a helyzet a humánerőforrás- és egyéb kereskedelmi adatok kezelése esetében.

Amikor az adatvédelmi pajzsban résztvevő szervezetek adatkezelőként járnak el, a panaszok elbírálására illetékes adatvédelmi hatóság hatásköre az uniós jog hatálya alá tartozó kezeléssel kapcsolatos panaszokra fog korlátozódni (uniós adatkezelő felelősségi körébe tartozó kezelés – ideértve az egyesült államokbeli szervezetekkel közösen végzett adatkezelést is – vagy amikor az adatvédelmi pajzsban részt vevő szervezet közvetlenül az uniós jog hatálya alatt áll, például azáltal, hogy az EU területén található eszközt használ). Azokra az adatkezelésekre azonban, amelyeket csak az Egyesült Államok joga alapján végeznek, kizárólag az adatvédelmi pajzs mechanizmusát kell majd alkalmazni. A nyelvi akadályok és az Egyesült Államok jogrendszerére vonatkozó ismeretek hiányának leküzdése érdekében hasznos lehetne, ha az uniós adatvédelmi hatóságok felhatalmazást kapnának arra, hogy közvetítőként járjanak el a magánszemélyek panaszainak benyújtásakor, vagy segítsék őket az egyesült államokbeli szervezetekkel szembeni AVR eljárások során, vagy, ha ezt indokoltnak tartják, az egyesült államokbeli hatóságokkal való egyeztetések során.

A WP29 kiemeli, hogy az adatvédelmi pajzsban leírt mechanizmus nem követi a korábbi ajánlást, amely szerint az unióbeli magánszemélyeknek „lehetőségük kell, hogy legyen arra, hogy kártérítési követeléseiket áthozzák az Európai Unió területére”, valamint „biztosítani kell számukra a jogot, hogy keresetet nyújtsanak be az illetékes uniós bírósághoz.”[28]

[28] Lásd a WP29 Reding alelnökhöz intézett 2014. április 10-i levelét

Örvendetes lenne, ha az adatvédelmi pajzsban résztvevő szervezetek belefoglalnának egy ilyen lehetőséget az adatvédelmi politikáikba.

A hatékonyság biztosítása érdekében a WP29 azt ajánlja, hogy a rendszer lehetőség szerint engedje meg, hogy az uniós adatvédelmi hatóságok képviseljék az érintetteket, és helyettük eljárjanak vagy közvetítőként lépjenek fel. Más megoldásként, tartalmazzon specifikus joghatósági záradékokat, amelyek alapján az érintetteknek lehetőségük van jogaikat Európában gyakorolni.

b) Választottbírósági eljárás

A választottbírósági eljárások szabályozása még nem végleges, ami megnehezíti a WP29 általi értékelést. Mivel úgy tűnik, a választottbírósági eljárás az Egyesült Államok joga alapján nyer majd szabályozást, és az eljárási nyelv kizárólag az angol lesz, az uniós adatvédelmi hatóságok valószínűleg felhatalmazást kívánnak majd kapni arra, hogy segítsék a magánszemélyeket a folyamatban.

Ezen túlmenően, a választottbírósági eljárás azért került bevezetésre, mert semmilyen biztosíték nem volt arra, hogy a panaszokkal foglalkozni fognak, ugyanis a Szövetségi Kereskedelmi Bizottság nem köteles minden panaszt kivizsgálni. A WP29 felhívja a figyelmet arra, hogy amennyiben az unióbeli magánszemélyek úgy érzik, hogy jogi képviselő segítségére szorulnak, ennek költségeit saját maguknak kell viselniük. Ez visszatarthatja őket attól, hogy panaszaikat választottbírósági eljárás keretében nyújtsák be.

c) Felügyelet, végrehajtás és a jogorvoslati mechanizmusok hatékonysága

<u>Az adatvédelmi pajzsban való részvétel feltételei</u>

Az EUB szerint „az öntanúsítási rendszer […] megbízhatósága lényegében azon hatékony felderítési és felügyeleti mechanizmusok bevezetésén alapul, amelyek a gyakorlatban lehetővé teszik az alapvető jogok […] védelmét biztosító szabályok esetleges megsértésének azonosítását és szankcionálását.”[29]

A WP29 megjegyzi, úgy tűnik, hogy az adatvédelmi pajzs vonatkozásában a Kereskedelmi Minisztérium szerepe a tanúsítási eljárásban pusztán a benyújtott dokumentáció teljességének ellenőrzésére korlátozódik. Bár a WP29 elismeri, hogy az öntanúsítás nem követeli meg az adatvédelmi politikák végrehajtásának szisztematikus előzetes ellenőrzését, a Kereskedelmi Minisztériumnak legalább azt mindenképpen ellenőriznie kellene, hogy az az adatvédelmi politikák valamennyi adatvédelmi alapelvet tartalmazzák-e. A megfelelőségi határozat tervezete említést tesz ilyen kötelezettségvállalásról, a Kereskedelmi Minisztérium leveléből azonban nem lehet ezt egyértelműen megállapítani.[30]

Az adatvédelmi pajzs alapelveinek megsértése hosszú ideig észrevétlen maradhat, és lehetséges, hogy arra csak azt követően derül fény, hogy az érintett alapvető jogai súlyosan,

[29] Az EUB Schrems-ügyben hozott ítéletének 81. pontja.
[30] Európai Bizottság, a megfelelőségi határozat tervezetének (34.) preambulumbekezdése.

esetleg jóvátehetetlenül sérültek. Ezért ez a megközelítés sértheti az elővigyázatosság európai elvét.

Az adatvédelmi pajzs lista által biztosított átláthatóság, és a listáról eltávolított szervezetek nyilvántartása

Az átláthatóság tekintetében jelentős javulás történt az érintett javára. Az új adatvédelmi pajzs lista az összes, a Kereskedelmi Minisztériumnál öntanúsított szervezet feltüntetésén kívül tartalmazni fogja valamennyi olyan szervezet nyilvántartását is, amelyet eltávolítottak adatvédelmi pajzs listáról, a törlés indokával együtt[31]. A Kereskedelmi Minisztérium adatvédelmi pajzzsal kapcsolatos honlapja erőteljesebben fog a célközönségre összpontosítani oly módon, hogy megkönnyíti a szervezet öntanúsításában szereplő információk típusának, valamint a benne szereplő információkra vonatkozó adatvédelmi politikának az ellenőrzését, és a szervezet által az elvek betartásának ellenőrzésére alkalmazott módszer ellenőrzését[32]. A WP29 üdvözli, hogy konkréttá vált: a Kereskedelmi Minisztérium ellenőrizni fogja, hogy a nyilvános weboldallal rendelkező vállalatok közzétették-e adatvédelmi politikáikat ezen a weboldalon, vagy, ha nem rendelkeznek nyilvános weboldallal, hol tették a nyilvánosság számára hozzáférhetővé az adatvédelmi politikáikat[33]. A dokumentumok informatívabbak az adatvédelmi politika tartalmával kapcsolatban is[34].

A WP29 megítélése szerint probléma merülhet fel, ha egy szervezet, amely már szerepel az adatvédelmi pajzs listán, később kiterjeszti a tanúsítását más adatkategóriákra is. Ezekben az esetekben a lista nem fogja tükrözni a különböző adatkategóriák esetében az elvek különböző alkalmazási időszakait. Ez azzal a kockázattal jár, hogy az unióbeli magánszemélyek és vállalkozások nem tudják teljes körűen értékelni, hogy egy konkrét adatsorra valóban alkalmazandók-e az adatvédelmi pajzs elvei, és ha igen, mikortól. E hiányosságok elkerülése érdekében a munkacsoport azt ajánlja, hogy a szervezeteknek az adatvédelmi pajzs listában való nyilvántartásában minden személyesadat-kategória vonatkozásában egyenként szerepeljen az öntanúsítás hatálybalépésének dátuma.

A WP29 üdvözli azt a tényt, hogy a Kereskedelmi Minisztérium nyilvántartást fog vezetni azokról a szervezetekről, amelyeket töröltek az adatvédelmi pajzs listáról, valamint, hogy ez a nyilvántartás tartalmazni fog egy arra vonatkozó magyarázatot, hogy e szervezetek részére már nem biztosítottak az adatvédelmi pajzs előnyök, de kötelesek továbbra is alkalmazni az elveket az abban az időszakban kapott személyes adatok vonatkozásában, amikor az adatvédelmi pajzs céljából tanúsított szervezetként működtek, mindaddig, amíg ezeket az adatokat megőrzik. (I. melléklet, 3. oldal). Tekintettel azonban arra, hogy az adatvédelmi pajzs listájáról eltávolított egyes szervezetek úgy is dönthetnek, hogy visszaküldik vagy törlik

[31] I. melléklet 5. o., és II. melléklet II. szakasz 1. pont; A WP29 utal a COM(2103)847 sz. közleményben szereplő negyedik bizottsági ajánlásra is, valamint a WP29 Reding alelnökhöz intézett 2014. április 10-i levelére, különösen annak „Átláthatóság" címet viselő szakasz 5. pontjára.
[32] I. mellékletet, 8. o. A WP29 utal Reding alelnökhöz intézett 2014. április 10-i levelére, különösen annak „Átláthatóság" címet viselő szakasz 2. pontjára.
[33] I. melléklet 3. és 4. o. A WP29 utal a COM(2103)847 sz. közleményben szereplő első bizottsági ajánlásra is, valamint a WP29 Reding alelnökhöz intézett 2014. április 10-i levelére, különösen annak „Átláthatóság" címet viselő szakasza 3. pontjára.
[34] I. melléklet 5. és 6. o. és II. melléklet III. szakasz 6. pont

a keret alapján megkapott személyes adatokat, más szervezetek viszont megtartják a pajzs keretében kapott adatokat, fontos e tekintetben a magánszemélyek számára jobb átláthatóságot biztosítani. Ezért a Kereskedelmi Minisztérium által a vállalatokról vezetett nyilvántartásban szerepelnie kell, hogy az adott szervezet továbbra is megtartja-e az adatvédelmi pajzs keretében kapott személyes adatokat, vagy pedig visszaküldte vagy törölte azokat. Ha a szervezet továbbra is megtartja az ilyen adatokat, a nyilvántartásban egyértelműen fel kell tüntetni, hogy a szervezet az ilyen adatok vonatkozásában továbbra is köteles alkalmazni az elveket.

A Kereskedelmi Minisztérium által vezetett nyilvántartásban annak is szerepelnie kell, hogy új adattovábbítások tekintetében e szervezetek részére már nem biztosítottak az adatvédelmi pajzs előnyök, ami azt jelenti, hogy ezek a szervezetek az elvek keretében már nem jogosultak az EU-ból származó személyes adatokat fogadni.

Ellenőrzési eljárások

Annak ellenőrzése érdekében, hogy a gyakorlatban hatékony-e az öntanúsítás, a szervezetek önellenőrzést végezhetnek, vagy külső megfelelőségi felülvizsgálatnak vethetik alá magukat. A WP29 sajnálatát fejezi ki amiatt, hogy a munkavállalók képzése csak abban az esetben kötelező, amikor a szervezet az önellenőrzés lehetősége mellett dönt (II. melléklet III. szakasz 7.c. pont). Úgy tűnik továbbá, az arra vonatkozó ellenőrzés, hogy egy adott szervezet adatvédelmi politikája pontos, átfogó, jól látható módon bemutatott, teljes mértékben végrehajtott és hozzáférhető-e, csak abban az esetben kötelező, amikor a szervezet a belső felülvizsgálat (önellenőrzés) mellett dönt, valamint, hogy a külső mechanizmus általi felülvizsgálat kizárólag arra terjed ki, hogy a szervezet az adatvédelmi politikájának megfelelően működik-e.

A posteriori

A WP29 örvendetesnek tartja, hogy az FTC a és a Kereskedelmi Minisztérium vizsgálati jogkörrel van felruházva. A WP29 megállapítja továbbá, hogy a Kereskedelmi Minisztériumnak lehetősége lesz hivatalból vizsgálatokat indítani, különösen kérdőívek kiküldése által. Azonban a WP29 biztosítani szeretné, hogy ez a megközelítés elegendő ahhoz, hogy teljesüljön az EUB által megfogalmazott követelmény a jogsértések hatékony felderítési és felügyeleti mechanizmusaira vonatkozóan. Valójában a WP29-nek továbbra is kérdései vannak a tekintetben, hogy az egyesült államokbeli bűnüldöző hatóságok pontosan milyen hatáskörrel rendelkeznek arra, hogy az öntanúsító szervezetek helyiségeiben helyszíni vizsgálatokat folytassanak az adatvédelmi pajzs megsértésének kivizsgálása céljából, hogy az Egyesült Államok területén miképpen lehet egy uniós hatóság határozatának végrehajthatóvá nyilvánítása iránti eljárást folytatni, valamint, hogy az adatvédelmi pajzs keretében alkalmazható szankciók a gyakorlatban megfelelő visszatartó erővel bírnak-e.

2.2.7. Humánerőforrás-adatok kezelése

Alkalmazási kör

A 9. kiegészítő elv (II. melléklet III. szakasz 9. pont) a (korábbi vagy jelenlegi) munkavállalókról a munkaviszonnyal kapcsolatban gyűjtött személyes információkra alkalmazandó. A 9. kiegészítő elv a. pontjának ii. alpontja értelmében az adatvédelmi pajzs elvei csak „egyedileg azonosított vagy azonosítható adatok továbbítása vagy azokhoz való hozzáférés esetén” alkalmazandók. Ez az „azonosított adatok” kifejezés nincs összhangban a „személyes adatok” fogalmának a II. melléklet I. 8. pontjának aalpontjában szereplő meghatározásával, amely az „azonosított vagy azonosítható egyénre vonatkozó adatok” megfogalmazást tartalmazza, így nem áll összhangban az irányelv szerinti fogalommeghatározással[35].

[35] Amint a WP29 korábban már kiemelte, a fogalomnak a „továbbított vagy hozzáférhetővé tett adatokra” történő korlátozása szintén nem áll összhangban a „kezelés” kifejezéssel (II. melléklet I. szakasz 8.b. pont).

A 9. kiegészítő elv a. pont ii. alpontja leszögezi, hogy az „összesített foglalkoztatási adatokra és a személyes adatokat nem tartalmazó vagy név nélküli adatok felhasználására támaszkodó statisztikai jelentés adatvédelmi aggályokra nem ad okot". Ez az állítás a WP29 által kiadott több véleménynek ellentmond. A WP29 hangsúlyozni kívánja, hogy az összesített adatok újraazonosíthatók, és ezért személyes adatnak kell tekinteni őket[36].

[36] Lásd a 4/2007. sz. véleményt a személyes adatok fogalmáról, és az 5/2014. sz. véleményt az anonimizálási technikákról.

Tájékoztatás, választási lehetőség és célhoz kötöttség

A 9. kiegészítő elv b. pontjának i. alpontja példát hoz a tájékoztatás és választási lehetőség elv olyan esetekben történő alkalmazására, amikor a humánerőforrás-adatokat más célra használják fel. A példa olyan esetre vonatkozik, amikor valamely egyesült államokbeli szervezet „munkaviszonyon keresztül összegyűjtött személyes információt nem munkaviszonnyal összefüggő célokra – például marketingértesítésekre – szándékozik felhasználni". Ebben az esetben a cél megváltoztatása azzal a feltétellel megengedett, hogy be kell tartani a tájékoztatás és választási lehetőség elvét. A WP29 szerint a humánerőforrás-adatok értékesítési célból történő további kezelését a legtöbb esetben összeegyeztethetetlen célnak kell tekinteni, ezért az ellentétes a célhoz kötöttség elvével (II. melléklet, II. szakasz 5.a. pont). Továbbá a WP29 úgy véli, hogy a választási lehetőség elve nem jelenthet megfelelő alapot arra, hogy a munkavállaló egy munkaviszonnyal összefüggésben a cél megváltoztatásához „hozzájáruljon" (kívülmaradás), tekintve, hogy egy ilyen kontextusban a hozzájárulás esetleg nem teljesen önkéntes.

A WP29 határozottan kétli, hogy megfelelne az OECD adatvédelmi iránymutatásnak, hogy az adatvédelmi pajzs az adatok egyéb célra történő további felhasználásának feltételeként főként a választási lehetőség elvére összpontosít, mivel nincs megfelelő biztosíték arra, hogy ezt a kívülmaradási mechanizmust az összeegyeztethetetlen célból történő további kezelés esetében is igénybe lehetne venni. A 9. kiegészítő elv b. pontjának iv. alpontja széleskörű és kifejezett mentességet nyújt a tájékoztatás és választási lehetőség elv alkalmazása alól, „olyan mértékben és arra az időtartamra, amely annak érdekében szükséges, hogy a szervezet lehetőségei ne csorbuljanak az előléptetések, kinevezések vagy más hasonló foglalkoztatási döntések meghozatala során". Először is, a humánerőforrás-adatok ilyen célokra történő felhasználását már az adatgyűjtéskor kifejezetten közölni kellene. Továbbá, a „más hasonló foglalkoztatási döntések" megfogalmazás túl homályos és túl tág. Az lesz a következménye, hogy a humánerőforrás-adatok teljesen kikerülnek a tájékoztatás és választási lehetőség elv alkalmazási köréből azokban az esetekben, amikor a kezelésük a munkaviszony keretében történik. A fogalom annyira tág, hogy nem teszi lehetővé annak értékelését, hogy a jövőbeni felhasználás összeegyeztethető-e az eredeti céllal. A WP29 e kivétel törlését javasolja.

Hozzáférési jog

A 9. kiegészítő elv e. pontjának i. alpontja mentességet nyújt a hozzáférési elv alkalmazása alól is, vagy a humánerőforrás-adatok harmadik fél adatkezelőjével történő szerződéskötés kötelezettsége alól, ha a személyes adatok ilyen továbbítása munkavállalók kis létszámú csoportját érinti, és alkalmi, a foglalkoztatással összefüggő operatív intézkedéshez – például repülőjegy- vagy hotelszoba-foglaláshoz, vagy biztosításkötéshez – kapcsolódik, feltéve, hogy teljesülnek a tájékoztatás és a választási lehetőség elvének követelményei. A WP29 semmilyen ésszerű indokot nem lát az ilyen mentesség igazolására, és ennek az alpontnak a törlését javasolja.

2.2.8. Gyógyszeripari és gyógyászati termékek

Alkalmazási kör

Az adatvédelmi pajzs úgy rendelkezik, hogy kódolt adatoknak gyógyszeripari és orvostechnikai termékekkel összefüggésben az Európai Unióból az Egyesült Államokba történő továbbítása nem minősül az adatvédelmi pajzs hatálya alá tartozó adattovábbításnak (II. melléklet III. szakasz 14.g.i. alpont). Azonban az uniós adatvédelmi jogban viszont a kódolt adatok továbbítása védelmet élvez. A gyakorlatban ez azt jelenti, hogy az adatvédelmi pajzs nem terjedhet ki az ilyen továbbításokra. A WP29 arra kéri az Európai Bizottságot, kifejezetten írja elő, hogy a megfelelőségi határozat-tervezet hatálya a gyógyszeripari és orvostechnikai termékekkel összefüggő kódolt adatok továbbítására nem fog kiterjedni, valamint, hogy ennek következtében ezekre a továbbításokra olyan más biztosítékok kell, hogy vonatkozzanak, mint például az általános szerződési feltételek (a továbbiakban: ÁSZF), vagy a kötelező erejű vállalati szabályok. A WP29 azt javasolja, hogy ezt tisztázni lehetne a végleges megfelelőségi határozatban.

Adattovábbítás szabályozási és felügyeleti célokra (II. melléklet III. szakasz 14.d. pont)

A WP29 aggasztónak tartja, hogy e rendelkezések értelmében olyan személyes adatok, amelyek orvosi tartalmuk miatt a legtöbb esetben érzékeny adatok, továbbíthatók az Egyesült Államok szabályozó hatóságainak. Mivel az adatvédelmi pajzs rendeltetése a magánszervezetek közötti adattovábbítás, úgy tűnik, hogy egy állami szervezet, például valamely egyesült államokbeli szabályozó hatóság, nem jogosult az adatvédelmi pajzs keretében történő öntanúsításra, ami felveti a megfelelő adatvédelem kérdését az ilyen továbbításokkal kapcsolatban. Ha szabályozási célból ilyen továbbításokat kell végrehajtani, megfelelő intézkedéseket kell hozni annak garantálása érdekében, hogy biztosított legyen az unióbeli érintettek alapvető jogainak folyamatos védelme. A WP29 kiemeli azt a tényt, hogy a megfelelőségi határozat tervezete ezzel a kérdéssel kapcsolatban semmilyen útmutatást nem tartalmaz. A WP29 ezért semmilyen garanciával nem rendelkezik a tekintetben, hogy az unióbeli érintettek érzékeny adatai ebben az összefüggésben hatékony védelmet fognak élvezni.

A WP29 továbbá nem érti, hogy a „marketing” célból történő felhasználás miért szerepel példaként a jövőbeni tudományos kutatás céljából történő kezelések felsorolásában. Ugyancsak nem világos, hogy a vállalkozások telephelyei részére és a más kutatók részére történő továbbítás (II. melléklet III. szakasz 14.d. pont) miért a „Adattovábbítás szabályozási vagy felügyeleti célokra” cím alatt szerepel. Ezeket a kérdéseket a végleges megfelelőségi határozatban tisztázni kell.

Termékbiztonság, a hatékonyság ellenőrzése (a kormányzati ügynökségek részére történő jelentéstételt is ideértve), és a bizonyos gyógyszereket vagy orvostechnikai eszközöket használó betegek nyomon követése

Az adatvédelmi pajzs mentességet nyújt a tájékoztatás, választási lehetőség, harmadik fél részére történő adattovábbítás valamint a hozzáférés elvei alól annyiban, amennyiben az adott elv betartása megfelelőségi vagy szabályozási követelményeket sértene. A megfelelőségi határozat tervezete nem tartalmaz útmutatást arra a helyzetre vonatkozóan, amikor az adatvédelmi elvek betartása megfelelőségi vagy szabályozási követelményeket sértene. Ha a WP29 azt esetleg méltányolja is, hogy egyes kormányzati vizsgálatok igazolhatják a tájékoztatás és a hozzáférés elveinek korlátozott érvényesülését a vizsgálat védelme érdekében, olyan okot nem lát, amely igazolhatná ilyen széles körű mentességek engedélyezését azokban az esetekben, amikor az adatkezelést a magánszektorhoz tartozó szervezet vagy harmadik fél végzi. Például, tekintettel arra, hogy a betegek kezelése egyre inkább egyénre szabottan történik, elfogadhatatlan az adatvédelmi elvek alóli ilyen széles körű mentesség nyújtása bizonyos gyógyszereket vagy orvostechnikai eszközöket használó betegek nyomon követése esetén, mivel ez a fajta ellátás általánossá fog válni. Ez akkor is érvényes, amikor a gyógyszeripari vállalkozások termékbiztonsági és a hatékonyságellenőrzési célból használnak fel adatokat (új gyógyszerek tesztelése vagy értékesítése).

2.2.9. Nyilvánosan hozzáférhető információk

Aggodalomra ad okot a hozzáférés iránti jog alóli kivétel a nagyközönség számára elérhető és nyilvános nyilvántartásban szereplő információk esetében (II. melléklet III. szakasz 15. d. és e. pont), amennyiben a magánszemélyek – annak érdekében, hogy képesek legyenek ellenőrizni az adataik kezelését a hozzáférési joguk gyakorlása keretében tudni akarják, hogy egy adott adatkezelő kezel-e rájuk vonatkozó adatokat, és mely adatok ezek. A WP több alkalommal leszögezte, hogy az uniós jog értelmében az érintetteknek mindig joguk van az adataikhoz hozzáférni, és joguk van ahhoz, hogy szükség esetén az adatok helyesbítését vagy törlését igényeljék, ha a kezelés jogszerűtlen volt, vagy ha a személyes adatok hiányosak vagy pontatlanok, függetlenül attól, hogy azok közzétételre kerültek-e[37]. Ha a magánszemély hozzáférés iránti kérelmét visszautasítanák, azon az alapon, hogy az adatok nyilvános forrásokból, vagy nyilvánosan elérhető nyilvántartásokból származnak, a magánszemély nem lenne képes az adatok pontosságának, valamint annak ellenőrzésére, hogy azok közzététele jogszerű volt-e egyáltalán.

Ennek ellenére az adatvédelmi pajzs mentesíti a nyilvánosan elérhető nyilvántartásokból származó és a nyilvánosan elérhető információkat a tájékoztatás, választási lehetőség, a hozzáférés, és a harmadik fél részére történő adattovábbításért való elszámoltathatóság elvei alól (II. melléklet II. szakasz 15.b. pont). Ezek a mentességek túlságosan széles körűnek tűnnek az irányelvhez képest, és aggodalomra adnak okot, mivel hátrányosan befolyásolják többek között a magánszemélyek lehetőségét arra, hogy adataik pontosságát ellenőrizzék, és korlátozzák azok terjesztését.

[37] Lásd WP20., 4. o.

2.3. Következtetés

A WP29 elismeri, hogy az Egyesült Államok hatóságai és az Európai Bizottság jelentős javulást idéztek elő a két kontinens közötti adattovábbítások kereskedelmi vonatkozásait illetően. A fenti elemzésre figyelemmel azonban a WP29 úgy véli, hogy az adatvédelmi pajzs kereskedelmi része több ponton további tisztázásra szorul. Aggodalomra ad okot például, hogy nem történik kifejezett említés az adatmegőrzés elvéről. A WP29-nek ezért komoly kétségei vannak azzal kapcsolatban, hogy az adatvédelmi pajzs a gyakorlatban az uniós adatvédelemmel lényegében azonos szintű védelmet tud biztosítani.

A megfelelőségi határozatban tovább kell pontosítani a célhoz kötöttség és a választási lehetőség elvét. Továbbra is fennáll a joghézagok kockázata több elv vonatkozásában, különösen a harmadik személyek számára történő adattovábbítással, a panaszkezelési mechanizmussal, és a HR vagy a gyógyszerészeti adatok kezelésével kapcsolatban. Jobban ki kell dolgozni továbbá, hogy az adatvédelmi pajzs elvek milyen módon alkalmazandók az adatfeldolgozókra (meghatalmazottakra), és különös figyelmet kell fordítani arra, hogy a használt terminológia egyértelmű és ellentmondásoktól mentes legyen.

3. A MEGFELELŐSÉGI HATÁROZAT-TERVEZETBEN SZEREPLŐ NEMZETBIZTONSÁGI GARANCIÁK ÉRTÉKELÉSE

3.1. Az Egyesült Államok nemzetbiztonsági hatóságaira vonatkozóan alkalmazandó biztosítékok és korlátozások

A magánélethez és az adatvédelemhez fűződő alapvető jogok korlátozhatók, feltéve, hogy a korlátozás egy demokratikus társadalom normái szerint igazolható. Ez azt jelenti, hogy az adatvédelmi elvek nem abszolút érvényűek, és azok alkalmazásától el lehet térni, de csak akkor, ha érvényesülnek az irányadó (minimális) biztosítékok. Az adatvédelem javítására irányuló célkitűzéssel összhangban a szervezeteknek törekedniük kell az elvek maradéktalan és átlátható alkalmazására, ideértve azt is, hogy adatvédelmi politikájukban jelezniük kell, hogy az USA jogszabályai hol engednek rendszeres kivételeket az adatvédelmi elvek alkalmazása alól. Ugyanezen okból, ahol az elvek és/vagy az Egyesült Államok jogszabályai választási lehetőséget engednek, a szervezetektől elvárják a magasabb szintű védelem választását, ahol lehetséges.

A II. melléklet I. szakaszának 5. pontja szerint „az elvek betartása az alábbiak szerint korlátozható: a) a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítéséhez szükséges mértékben; b) törvény, kormányrendelet vagy az ítélkezési gyakorlat által, amelyek az elvekkel ellentétes kötelezettségeket vagy kifejezett felhatalmazásokat hoznak létre, feltéve, hogy az ilyen felhatalmazás gyakorlása során a szervezet bizonyítani tudja, hogy az elvek nemteljesítése az ilyen felhatalmazás által támogatott törvényes érdekek teljesítéséhez szükséges mértékre korlátozódik; vagy c) ha az irányelv vagy a tagállami jogszabályok hatálya kivételeket vagy eltéréseket tesz lehetővé, feltéve, hogy az ilyen kivételeket vagy eltéréseket összehasonlítható esetekben alkalmazzák.”

A kérdés az, hogy a II. mellékletben szereplő eltérések igazolhatók-e egy demokratikus társadalomban. Az adatvédelmi pajzsra vonatkozó megfelelőségi határozat tervezete szerint a Bizottság azt állapította meg, hogy „az Egyesült Államokban léteznek olyan szabályok, amelyeknek az a célja, hogy a szóban forgó törvényes cél eléréséhez feltétlenül szükséges mértékűre korlátozzanak bármely nemzetbiztonsági célú beavatkozást azon személyek alapvető jogaiba, akiknek a személyes adatait az EU–USA adatvédelmi pajzs keretében az Unióból az Egyesült Államokba továbbították."[38]

A jelen vélemény 1.2. szakaszában ismertetett keretet használatával, az USA hatóságainak nyilatkozataira és a Bizottság megállapításaira figyelemmel, a WP29 értékelte az USA jelenleg hatályos jogszabályait és hírszerzési ügynökségeinek jelenlegi gyakorlatát, valamint azokat a feltételeket, amelyek mellett a jogszabályok lehetővé teszik a magánélethez és az adatvédelemhez fűződő alapvető jogok bármilyen olyan korlátozását, ami az uniós jogi keret által biztosított védelmi szintnek megfelelő védelmi szintet károsan befolyásolná. Ez az értékelés a 28. sz. elnöki politikai irányelven (a továbbiakban: PDD-28), a 12333. számú elnöki rendeleten (a továbbiakban: EO12333), valamint azokon a különböző jogalapokon alapul, amelyeket a külföldi hírszerzői tevékenységről szóló törvény (a továbbiakban: FISA) (104., 402., 215., 501., és 702. szakasz) hozott létre. A WP29 az adatvédelmi pajzs VI. mellékletére támaszkodott, amely a nemzeti hírszerzés igazgatójának hivatala (ODNI) által készített, az USA nemzetbiztonsági hatóságaira vonatkozó biztosítékokról és korlátozásokról szóló levelet tartalmazza, és a jelfelderítési adatok gyűjtési tevékenységével kapcsolatban az Európai Bizottsággal közölt információkat foglalja össze.

3.2. A-biztosíték – Az adatkezelésnek a jogszabályokkal összhangban, és egyértelmű, pontos és megismerhető szabályok alapján kell történnie

Az uniós jog értelmében bármely korlátozás csak a jogszabályokkal összhangban, kidolgozott politikák és eljárások alapján történhet, valamint kellően egyértelműnek és megismerhetőnek kell lennie (az egyes országok számára biztosított mozgástér keretein belül) ahhoz, hogy a polgárok megfelelően tisztában legyenek azzal, hogy a hatóságok milyen körülmények között és milyen feltételekkel foganatosíthatnak megfigyelési intézkedéseket.[39]

A WP29 megjegyzi, hogy a jelfelderítési adatok gyűjtésére irányuló tevékenység megismerhető jogi keret alapján történik. A VI. mellékletben említett összes jogszabály (PDD-28, FISA, USA FREEDOM törvény, FOIA) elérhető online a közvélemény részére (az

[38] A 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló bizottsági határozat tervezete, (75) preambulumbekezdés.

[39] Az EJEB Zakharov-ügyben hozott ítéletének 247. pontja; „A Bíróság korábban már megállapította, hogy a jogszabály »előreláthatóságának« követelménye nem azt jelenti, hogy az államnak olyan jogszabályi rendelkezéseket kell hoznia, amelyek részletesen felsorolják az összes olyan magatartást, amelynek következtében egy magánszemélyre vonatkozóan, »nemzetbiztonsági« okokból titkos megfigyelést kell elrendelni. A nemzetbiztonsági fenyegetések a téma jellegénél fogva többfélék lehetnek, és adott esetben nehéz lehet előre jelezni vagy meghatározni azokat (lásd a fent hivatkozott Kennedy-ítélet 159. pontját). A Bíróság ugyanakkor azt is hangsúlyozta, hogy alapvető jogokat érintő ügyekben a demokratikus társadalmak egyik alapelvével, az Egyezményben szentesített jogállamiság elvével ellentétes volna a végrehajtó hatalmat szuverén hatáskörben megnyilvánuló mérlegelési jogkörrel felruházni a nemzetbiztonság tekintetében. Ebből kifolyólag az illetékes hatóságokra ruházott ilyen mérlegelési jogkör határait jogszabályban kell meghatározni, a gyakorlásának módját pedig kellően egyértelműen kell megfogalmazni, szem előtt tartva, hogy a kérdéses intézkedés célja az, hogy a magánszemély részére az önkényes beavatkozással szemben védelmet nyújtson".

USA-n kívül és belül is). A VI. melléklet tartalmazza az irányadó jogszabályok összefoglalását az adatgyűjtésre vonatkozó korlátozások, az adatok megőrzésére és terjesztésére vonatkozó korlátozások, a megfelelés és felügyelet, az átláthatóság és a jogorvoslati lehetőségek tekintetében. Az Egyesült Államoknak a hírszerzésre vonatkozó jogszabályi keretét egy sor különböző dokumentum alkotja, ezek között olyan különálló ügynökségi jelentések, szakpolitikák és eljárásrendek, amelyeket elemezni kell annak jobb megértése érdekében, hogyan történik egyes tevékenységek végzése elméletileg és a gyakorlatban. E tekintetben a WP29 néhány olyan kérdésre összpontosított, amelyeket döntő fontosságúnak tekint.

3.2.1. A 12333. számú elnöki rendelet és a 28. sz. elnöki politikai irányelv

Az EO12333 hatálya igen széleskörű: főszabály szerint bármilyen külföldi hírszerzési célú adatgyűjtés az elnök mérlegelése alapján és a rendelet szerint történhet. Ezzel szemben felvetődött az az ellenérv, hogy a FISA bevezetése óta az EO12333 csak az USA területén kívül történő adatgyűjtésre alkalmazható. A WP29 megjegyzi, hogy az EO12333 nem tartalmaz túl sok részletet annak területi hatályával kapcsolatban, azzal kapcsolatban, hogy milyen mértékben történhet az adatok gyűjtése, megőrzése vagy további terjesztése, és melyek azok a bűncselekmények, amelyek esetében megfigyelés alkalmazható, valamint, hogy milyen típusú információkat lehet gyűjteni vagy felhasználni.

A 28. sz. elnöki politikai irányelv (PPD-28) fő rendeltetése a WP29 értelmezése szerint az, hogy meghatározza a személyes adatok gyűjtésének és kezelésének korlátait, függetlenül attól, hogy milyen megfigyelési programot használtak vagy honnan származnak az adatok.

A PPD-28 az Egyesült Államok elnöke által kibocsátott irányelv, amely meghatározza azokat az elvi követelményeket, amelyek teljesülése mellett a jelfelderítési adatok gyűjtésére irányuló tevékenység engedélyezhető és végezhető, azonban a PPD-28 nem az adatgyűjtés jogalapja. A PPD-28 azáltal hatékony, hogy a hírszerzési testületek számára előírja azokat az elveket, amelyeket e testületeknek az adatvédelmi politikájukban és eljárásaikban alkalmazniuk kell. Az irányelv a jelfelderítési adatok gyűjtésére irányuló tevékenységekre alkalmazandó, tekintet nélkül arra, hogy az adatgyűjtéskor az adatok hol találhatók, az USA területén, vagy azon kívül. Ebből kifolyólag a jelfelderítési célból gyűjtött adatokra akkor is alkalmazandó, amikor ezeket az adatokat az EU-ból az USA-ba továbbítják.

A PPD-28 előírja különösen, hogy a jelfelderítési tevékenységnek a lehető legcélzottabbnak kell lennie[40]. Az adatok felhasználása tekintetében meghatározza az adatminimalizációs eljárásokat (ideértve az adatok megőrzésére és terjesztésére vonatkozó feltételeket is), az adatbiztonságra, és a jogosult személyzet általi hozzáférésre irányuló eljárást (nevezetesen a visszaélés és a nem megfelelő használat kockázatát csökkentő biztosítékokra vonatkozó szabályokat), rendelkezik az adatminőségről és a felügyelet szabályairól. Ezeket a garanciákat

[40] „A jelfelderítési tevékenységnek a lehető legcélzottabbnak kell lennie. Annak meghatározásakor, hogy kell-e jelfelderítési adatokat gyűjteni, az Egyesült Államoknak figyelembe kell vennie egyéb információk elérhetőségét, ideértve a diplomáciai vagy állami forrásokat is. az adatgyűjtésben ezeknek az ésszerű és megvalósítható eszközöknek kell prioritást biztosítania." (1.d. szakasz)).

az érintett állampolgárságától függetlenül, tehát az amerikai és a nem amerikai személyekre is.

Az adatoknak az USA-ba történő továbbítása során a PPD-28 által előírt biztosítékok szintén alkalmazandók. A VI. melléklet tartalmazza az ODNI kötelezettségvállalását arra vonatkozólag, hogy amennyiben az USA hírszerző közössége az Atlanti óceánt átszelő kábelekről gyűjtene adatokat, „arra is vonatkoznának az itt ismertetett korlátozások és biztosítékok, beleértve a PPD-28 követelményeit is”[41]. A WP29 rámutat, hogy továbbra sincs kialakult ítélkezési gyakorlat az elektronikus kommunikáció megszerzésének jogszerűségére vonatkozóan olyan esetekben, amikor azt másik ország végezné. Mindenesetre, az USA nem erősíti meg és nem cáfolja, hogy kábeles adatszerzést alkalmaz hírszerzési adatgyűjtési módszerként.

A „jelfelderítési tevékenység” fogalmát sem a PPD-28, sem más releváns dokumentum nem határozza meg.

3.2.2. A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény (FISA)

Általánosan elmondható, hogy a FISA szövege egyértelműbbnek és pontosabbnak tűnik. Több rendelkezésének a PPD-28 fényében történő értelmezése, és így azok gyakorlati alkalmazása azonban nagymértékben a különféle ügynökségek általi végrehajtás függvénye. Bár még nem áll rendelkezésre teljes értékelés az új biztosítékok alkalmazására vonatkozóan, amerikai küldöttek arról tájékoztatták a WP29 képviselőit, hogy a PPD-28 szerinti biztosítékok végrehajtása valóban befejeződött, és hasonlóan megtörtént a hírszerzési szervezetek körében is.

Pontosabban, az 501. szakasz viszonylag egyértelmű a tekintetben, hogy milyenfajta hírszerzési műveletek végzésére lehet utasítást adni: „bármely tárgyi bizonyíték (többek között könyvek, nyilvántartások, iratok, dokumentumok és egyéb tárgyak) beszerzésére”. Meg kell jegyezni azonban, az a tény, hogy a „tárgyi bizonyíték” fogalma magában foglal „egyéb tárgyakat”, e felhatalmazás hatályát meglehetősen kiszélesíti.

A 702. szakasz, amely külföldi hírszerzési információ beszerzése céljából lehetővé teszi az adatgyűjtést olyan nem amerikai személyektől, akikről megalapozottan feltételezhető, hogy az Egyesült Államokon kívül tartózkodnak[42], nem biztosít ugyanolyan részletességet, mint az 501. szakasz. Hatályát illetően a 702. szakasz az USA-ban letelepedett elektronikus kommunikációs szolgáltatókra alkalmazandó az Egyesült Államokon kívül tartózkodó személyekre vonatkozó külföldi hírszerzési információk gyűjtése céljából. A „külföldi hírszerzési információ” fogalommeghatározása tág. Ez magában foglalja többek között „a külföldi hatalomra vagy külföldi területre vonatkozó olyan információkat, amelyek az

[41] Adatvédelmi pajzs VI. melléklet, a Nemzeti Hírszerzés Igazgatója Hivatalának (ODNI) az egyesült államokbeli nemzetbiztonsági hatóságokkal kapcsolatban alkalmazandó biztosítékokra és korlátozásokra vonatkozó levele, 2. o.
[42] 50 U.S. Code §1881a (D)(1).

Egyesült Államok külpolitikájának alakításával összefüggenek”[43], ami némileg bizonytalanná teszi, hogy a gyakorlatban milyen típusú információk gyűjthetők.

A FISA alkalmazása – ideértve meghatározott kiválasztási kritériumok alkalmazási körét és használatát is – továbbra is homályos és zavaros, annak ellenére, hogy egyes dokumentumok, a Kongresszusnak küldött jelentések, és az adatvédelmi és polgári szabadságjogi felügyelő tanács (a továbbiakban: PCLOB) felügyeleti jelentéseinek titkosságát feloldották. A PCLOB jelentése[44] utal meghatározott kiválasztási kritériumok használatára („kiválasztási feltétel”), a WP29 értelmezése szerint azonban ez nem áll összhangban a célzottá tételre vonatkozó, a 702. szakasz szerinti szabályokkal[45]. Általánosan megismerhető szabályokban nem szerepelnek, amennyire a WP29 meg tudta állapítani.

3.2.3. Következtetés

Összességében a WP29 megállapítja, hogy a hírszerzési tevékenységekre vonatkozó kapcsolódó szövegek elérhetők az interneten, és az USA hatóságai több fontos lépést tettek az átláthatóság érdekében.

A WP29 megállapítja, hogy 2013 óta számos dokumentum került közzétételre, például politikák, eljárások, FISC-határozatok és egyéb dokumentumok, amelyek titkosítását feloldották. Ezen túlmenően a PCLOB fontos jelentéseket tett közzé a 702. szakasz és az USA FREEDOM törvény alapján végzett tevékenységekről. Hasonló jelentés várható az EO12333 alapján végzett tevékenységekről.

Számos olyan jogalkotási melléklet, amely megvilágíthatja az elnöki rendelet az Egyesült Államok területén kívüli egyénekre gyakorolt hatásait , valamint az alkalmazható biztosítékokat, titkosításra került, ennek következtében nem hozzáférhető a nyilvánosság, vagy azon magánszemélyek számára, akikre a rendelet alkalmazása hatással lehet. Amikor a dokumentumok titkosítását feloldották, azok már csak korlátozott értékkel és információval bírnak a hírszerzési tevékenységekkel kapcsolatban.

A Snowden-féle adatkiszivárogtatást követően az EO12333 működésének megvilágítására – különösen PPD-28 elfogadása révén – tett erőfeszítések ellenére az EO12333 jelenlegi gyakorlati alkalmazása továbbra sem világos. A WP29 megállapítja, hogy az adatvédelmi pajzs VI. melléklete nem tartalmaz részletes információkat az EO12333 működésével kapcsolatban.

Jóllehet a WP29 örvendetesnek tartja a PPD-28 által bevezetett korlátozásokat, nehéz megállapítani, hogy kellően előre láthatóak-e az USA megfigyelésekre vonatkozó jogszabályai, vagyis, hogy tartalmaznak-e „megfelelő információ[ka]t arra vonatkozóan, hogy a hatóságok milyen körülmények között és milyen feltételekkel jogosultak ilyen intézkedések alkalmazására”, tekintettel arra, hogy további pontosítások – ideértve az EO12333-ra vonatkozó PCLOB-jelentést is – még nem érkeztek.

[43] 50 U.S. Code § 1801 (e) (2).
[44] A PCLOB jelentése a FISA 702. szakasza szerint működtetett megfigyelési programról, 32. o.
[45] 50 U.S. Code § 1881a(D).

3.3. B-biztosíték – Bizonyítani kell az elérni kívánt törvényes cél szükségességét és arányosságát

3.3.1. A 28. elnöki politikai irányelv

A PPD-28 korlátozásokat vezetett be a tekintetben, hogy milyen célokra lehet személyes adatokat felhasználni, milyen feltételekkel lehet azokat terjeszteni, és kihat a jelfelderítési adatok gyűjtésére, függetlenül attól, hogy az melyik jogalap alapján történik.

Különösen, a PPD-28 1. szakasza előírja, hogy az Egyesült Államok jelfelderítési tevékenységének minden esetben a „lehető legcélzottabbnak" kell lennie. E korlátozást elismerve, ugyanakkor nehéz eldönteni, hogy a „lehető legcélzottabb" azt jelenti-e, hogy minden adatgyűjtés szükséges és arányos.

A PPD-28 elismeri, hogy a nagy mennyiségű adatgyűjtés továbbra is megengedett „az új vagy kialakuló veszélyek és más létfontosságú nemzetbiztonsági információk azonosítása érdekében, amelyek gyakran el vannak rejtve a modern globális kommunikáció hatalmas és összetett rendszerében".[46] A WP29 megállapítja, hogy a „« tömegesen »gyűjtött jelfelderítés nagy mennyiségű jelfelderítési adat engedélyezett gyűjtését jelenti, ami műszaki vagy operatív megfontolások miatt diszkriminánsok (például konkrét azonosítók, kiválasztási feltételek stb.) használata nélkül történik".

A PPD-28 a felhasználási cél tekintetében korlátozza a tömegesen gyűjtött jelfelderítési adatok használatát. Tömeges adatgyűjtés hat célból végezhető, ezek közé tartozik a terrorizmus és egyéb súlyos (nemzetközi) bűncselekmények elleni küzdelem. A WP29 elemzése arra enged következtetni, hogy a célok behatárolása meglehetősen (és esetleg túlzottan) tág ahhoz, hogy célzottnak lehessen tekinteni.

A PPD-28 nem szüntette meg a személyes adatok tömeges, válogatás nélküli gyűjtésének lehetőségét, és továbbra sem világos, hogy az ilyen adatgyűjtést milyen mértékben lehet végezni, és továbbra is lehetséges, hogy széles körben. E tekintetben a WP29 megjegyzi, a VI. mellékletben az ODNI azt állítja, hogy „az internetes kommunikációra vonatkozó minden olyan tömeges adatgyűjtési tevékenység, amelyet az USA hírszerző közössége jelfelderítésen keresztül végez, csak az internet kis részén történik"[47], és ezért kívánatosnak tartaná további bizonyítékok szolgáltatását átláthatósági intézkedések révén.

3.3.2. A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény (FISA)

A FISA 215. és 702. szakasza szerinti adatminimalizációs eljárások annak érdekében kerültek bevezetésre, hogy az amerikai magánszemélyeket megvédjék az adataikhoz való erőteljes

[46] PPD-28 2. szakasz, adatvédelmi pajzs VI. melléklet, a nemzeti hírszerzés igazgatója irodájának (ODNI) levele az USA nemzetbiztonsági hatóságaira vonatkozó biztosítékokról és korlátozásokról, 3. o.

[47] Adatvédelmi pajzs VI. melléklet, a nemzeti hírszerzés igazgatója irodájának (ODNI) levele az USA nemzetbiztonsági hatóságaira vonatkozó biztosítékokról és korlátozásokról, 4. o.; A WP29 e tekintetben emlékeztet az EU-USA eseti munkacsoport uniós társelnökeinek adatvédelmi megállapításairól szóló jelentésre, mely szerint „a kommunikációs adatok igen kis hányadát teszik ki a globális internetforgalomnak", mivel a „annak túlnyomó többségét nagy volumenű streaming és letöltés alkotja, például televíziós sorozatok, filmek és sportközvetítések" (a jelentés 3.1.2. pontja)44

kormányzati hozzáféréstől. Ezek a korlátozások külföldiek esetében hivatalosan nem alkalmazandók, annak ellenére, hogy az Egyesült Államok kormányzati tisztviselői a WP29 képviselőivel tartott nyilvános és magánjellegű találkozókon többször kijelentették, hogy az adatminimalizációs eljárások alkalmazási körét azok hatályba lépése óta a gyakorlatban kiterjesztették minden személyre, állampolgárságtól vagy szokásos tartózkodási helytől függetlenül.

A 702. szakasz pontosítja, hogy az engedélyezett információszerzést „olyan módon kell lefolytatni, amely összhangban van az Egyesült Államok Alkotmányának Negyedik Kiegészítésével, amely az adatgyűjtést az indokolt kutatás elvének megfelelő mértékre korlátozza. E tekintetben nincs különbségtétel az egyesült államokbeli illetve a nem egyesült államokbeli vállalkozások között". Más szóval, amennyiben a negyedik kiegészítés az USA-ban gyűjtött valamennyi adatra vonatkozna, az USA-ban történő „tömeges" adatgyűjtés „indokolatlan", és ezért alkotmányellenes lenne.

A WP29 üdvözli a PCLOB-jelentés azon megállapítását, mely szerint „a gyakorlatban a « nem egyesült államokbeli személyek » is részesülnek azon hozzáférési és adatmegőrzési korlátozások előnyeiből, amelyeket a különböző ügynökségek eljárásai a minimalizálás és/vagy a célzottság érdekében megkövetelnek, tekintettel arra, hogy költséges és nehéz volna az az egyesült államokbeli személyekre vonatkozó személyes adatokat egy nagy adatkészletben azonosítani és onnan eltávolítani, ami azt jelenti, hogy jellemzően a teljes adatkészletet a magasabb szintű egyesült államokbeli adatvédelmi normáknak megfelelően kezelik".

A WP29 megállapítja továbbá, hogy a PCLOB megállapítása szerint „a program nem a kommunikáció tömeges gyűjtése révén működik". Az ODNI által 2014-ben kibocsátott statisztikai átláthatósági jelentés alátámasztja ezt a megállapítást. Emellett, a PCLOB-jelentés szerint a megfigyelés célját „kiválasztási feltételek", például e-mail cím vagy telefonszámát alkalmazásával határozzák meg[48].

A célzottá tételre vonatkozó megfelelő, nyilvánosan elérhető jogszabályok azonban nem tartalmaznak ilyen célzott szabályokat, és mindössze arra irányulnak, hogy megakadályozzák az Egyesült Államok állampolgárainak vagy az Egyesült Államokban élő személyeknek a célba vételét. Továbbá azok az előnyök, amelyek a PCLOB szerint a nem egyesült államokbeli személyekre alkalmazandók, a gyakorlatban jogilag nem kötelező erejűek, vagy nem törvény írta elő őket, mivel a célzottá tételre vonatkozó rendelkezésre álló jogi szabályozás ilyen célzott szabályokat nem tartalmaz, és mindössze arra irányul, hogy megakadályozza az Egyesült Államok állampolgárainak vagy az egyesült Államokban élő személyeknek a célba vételét.

A WP29 továbbá emlékeztet arra, hogy a 702. szakasz alkalmazásában személy nemcsak természetes személy lehet, hanem csoport, szervezet, szövetség, közjogi szervezet, vagy a külföldi hatalom is. Ezenkívül az a tény, hogy a gyűjtést „az adatszerzés külföldi hírszerzési

[48] A PCLOB jelentése a FISA 702. szakasza szerint működtetett megfigyelési programról, 32. o.

információk megszerzésére irányuló, jelentős célja” igazolja, némi bizonytalanságot eredményez annak célját és szükségességét illetően. A WP29 mindazonáltal üdvözli a VI. mellékletben szereplő azon információt, amely szerint 2014-ben mintegy 90000 magánszemély volt a 702. szakasz alapján célszemély[49]. Az adatvédelmi pajzs első felülvizsgálata lehetőséget biztosít majd a célzottá tételre vonatkozó szabályok létezését alátámasztó további bizonyítékok bemutatására.

Mindeddig nem áll rendelkezésre egyértelmű ítélkezési gyakorlat a tömeges és válogatás nélküli adatgyűjtés és a személyes adatok ezt követő, bűnüldözési célú használata vonatkozásában, ideértve azt a kérdést is, hogy milyen körülmények között van lehetőség a személyes adatok ilyen módon történő gyűjtésére és felhasználására. Az EUB ezt a kérdést várhatóan legalább bizonyos mértékben tárgyalni fogja 2016 folyamán, mind az egyesített Tele2 Sverige AB kontra Post- och telestyrelsen és Secretary of State for the Home Department kontra Davis és társai ügyekben[50], mind az utas-nyilvántartási adatállományról (PNR) Kanadával kötött megállapodás érvényessége tekintetében adandó tanácsadó véleménye keretében.[51] Addig is, a WP29 emlékeztet arra, hogy következetesen úgy vélte, a tömeges és válogatás nélküli adatgyűjtés semmilyen körülmények között nem tekinthető arányosnak[52].

3.3.3. Következtetés

A PPD-28-at követően bevezetett korlátozások ellenére a WP29 kétségei, különös tekintettel az adatgyűjtés arányosságára, továbbra is fennállnak. Először is, vannak arra utaló jelek, hogy az Egyesült Államok továbbra is gyűjt adatokat tömegesen és válogatás nélkül, vagy legalábbis nem zárja ki, hogy a jövőben tehet ilyet. A WP29 következetesen úgy ítélte meg, hogy az ilyen adatgyűjtés nincs összhangban az uniós joggal, és ezért nem fogadható el.

Másodszor, a WP29 megjegyzi, hogy a célzott, vagy a „lehető legcélzottabb” adatkezelést szintén lehet tömegesnek tekinthető. Jelenleg az EUB előtt eljárások folynak arra vonatkozólag, hogy az ilyen tömeges adatgyűjtés megengedhető legyen-e vagy sem. Ezért a WP29 nem ad végleges értékelést a célzott, de tömeges adatkezelés jogszerűségéről. Hangsúlyozza azonban, hogy amennyiben a célzott, de tömeges adatkezelés megengedett lenne, a célzottá tételre vonatkozó elveket alkalmazni kell mind az adatok gyűjtésére, mind azt követő használatára, és azokat nem lehet csak az adatok használatára korlátozni. A megfelelőségi határozat tervezetét mindenképpen egyértelművé kell tenni a PPD-28-ban említett hat céllal kapcsolatban, amelyek esetében megengedett a „tömeges” adatgyűjtés. A WP29 ebben a szakaszban nincs meggyőződve arról, ezek a célok kellően korlátozottak ahhoz, hogy biztosítható legyen, hogy az adatgyűjtés valóban a szükséges és arányos mértékre korlátozódik.

[49] VI. melléklet, 11. oldal.
[50] EUB, C-203/15. és C-698/15. sz. egyesített ügyek
[51] EUB, A-1/15. sz. ügy
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_hu.pdf

3.4. C-biztosíték – Független felügyeleti mechanizmus kialakítása

Az Egyesült Államokban nem egyetlen, szövetségi szintű felügyeleti szerv látja el a hírszerzési és megfigyelési programok magánéleti és adatvédelmi vonatkozásainak felügyeletét. Az Egyesült Államok hírszerzési tevékenységeit ehelyett egy többszintű folyamat keretében felügyelik, mely belső és külső felügyeleti elemekre választható szét. A WP29 elismeri, hogy az Egyesült Államok felügyeleti szerveinek jelentéstételi gyakorlata igen részletes és jórészt nyilvános.

3.4.1. Belső felügyelet

Valamennyi hírszerzési és biztonsági ügynökség rendelkezik az adott ügynökségre vonatkozó jogi szabályok betartását biztosító munkatársakkal, így főellenőrökkel (*Inspectors-General*), akik elsődleges feladata az ügynökségi munka jogszabályoknak – többek között, de nem kizárólag a magánéletről és adatvédelemről szóló törvényeknek – való általános megfelelését vizsgálni. A főellenőri tisztség törvény által létrehozott poszt, a főellenőröket – szenátusi jóváhagyásukat követően – kivétel nélkül az Egyesült Államok elnöke nevezi ki (illetve fogja rövidesen kinevezni), ami egyfelől szervezeti függetlenségüket hivatott biztosítani, másfelől pedig, hogy jelentés tegyenek a Kongresszusnak. A WP29 úgy véli, hogy a főellenőrök ennek alapján valószínűleg megfelelnek az EUB és az Emberi Jogok Európai Bírósága (EJEB) meghatározása szerinti szervezeti függetlenségnek, legalábbis amikortól az új kinevezési eljárás mindegyikükre vonatkozik. Egyelőre azonban továbbra is aggályos azon főellenőrök helyzete, akiket még mindig az általuk felügyelt ügynökség igazgatója jelöl ki.

A főellenőrnek módjában áll ajánlásokat tenni, melyeket ezt követően továbbíthatnak az Igazságügyi Minisztériumnak és a PCLOB-nak, sőt akár még a kongresszusi bizottságnak is, amely előírhatja az ajánlások végrehajtását. A főellenőr által megállapított jogsértések orvosolhatók szervezeten belüli, illetve szakpolitikai intézkedésekkel, és azokról jelentést tesznek a Kongresszusnak. A főellenőri hatáskör egyebek között ellenőrzések és vizsgálatok lefolytatására is kiterjed.

A WP 29 jelzi, hogy a főellenőri jelentés nyilvánosságra hozatala megtagadható, a főellenőri jelentéstétel pedig abban az esetben, ha a vizsgálat tárgyát minősített információk képezik, megakadályozható. A jelentések mindazonáltal kivétel nélkül kongresszusi felügyelet alá tartoznak, ami komoly biztosítéknak számít, még akkor is, ha külön jogorvoslatra nem ad lehetőséget.

Valamennyi ügynökség kötelékében megtalálhatók az adatvédelemi és polgári szabadságjogi tisztviselők, akik a kötelező, saját jelentéstételi rendszerrel a kongresszusi felügyeletben működnek közre.

A jelenlegi belső felügyeleti mechanizmusok összességében eléggé szilárdnak tekinthetők, de ahhoz, hogy a magánélet védelméhez és az adatvédelemhez való alapjogokba történő beavatkozás igazolható legyen, teljesen független felügyelet szükséges. A WP29 szerint továbbá – amellett, hogy megbecsüli és elismeri az adatvédelmi és polgári szabadságjogi,

különböző tisztviselők által végzett munkát – nem vonható le az a következtetés, hogy függetlenségük tekintetében e tisztviselők megfelelnének a független felügyelőkkel szemben támasztott követelménynek.

3.4.2. Külső felügyelet

A külső felügyeletet több különböző mechanizmus alkotja: a FISA-Bíróság (a továbbiakban: FISC) által a 501. és 702. szakasz alapján biztosított bírósági felügyelet, a kongresszusi hírszerzési vizsgálóbizottságok felügyeleti tevékenysége, valamint a PCLOB által ellátott feladatok.

A WP29 emlékeztet arra, hogy ideális esetben – miként azt az EUB és az EJEB is kimondta – a független és pártatlan eljárás szavatolása érdekében a felügyeletnek bírói hatáskörbe kell tartoznia. A FISC-eljárás egészen a legutóbbi időkig *ex parte* eljárásként működött, amelynek keretében az érintett egyének nemcsak meghallgatási lehetőséget nem kaptak, de magáról az ügyről sem volt tudomásuk. Jóllehet a FISC-eljárás a mai napig megtartotta *ex parte* jellegét, az USA FREEDOM törvény (az Egyesült Államok szabadságjogokról szóló törvénye) elfogadása nyomán a FISC esetében bevezették az *amicus curiae* intézményének alkalmazását. Bár az *amicus curiae* feladataik ellátása során független szereplőként járnak el, az intézmény létrehozásának hátterében nem az állt, hogy konkrét, az ügyben esetlegesen érintett egyének védelmében lépjenek fel.

Az USA Freedom törvénnyel létrehozott *amicus curiae-csoport* feladata a jelentősebb peres ügyek anyagának összefoglalása a FISC számára. A Bíróság öt, megfelelő biztonsági tanúsítvánnyal rendelkező ügyvédet választott ki, akik technikai tanácsokkal szolgálnak, részt vesznek a FISC-meghallgatásokon és összefoglalják a peres ügyek anyagait, továbbá érveket sorakoztatnak fel a magánélet tiszteletben tartásához való jog, illetve a polgári jogok szempontjából egy adott ügy érdemi kérdései kapcsán. Erre azonban kizárólag jelentősebb ügyekben vagy új jogi kérdések felmerülésekor kerül sor.[53]

A 215. szakasz szinte teljes egészében *ex-ante* (de nem *ex-post*) bírósági felügyelet tárgyát képezi abból adódóan, hogy a 215. szakasz alapján adatgyűjtést végző programokat kivétel nélkül jóvá kell hagynia a FISC-nek. A PCLOB-jelentés szerint „a FISA e hagyományos elektronikus felügyeleti keretétől a 702. szakasz mind az alkalmazott normák, mind a FISC egyénenkénti döntéseinek mellőzése tekintetében eltér. A törvény értelmében a legfőbb ügyész és a nemzeti hírszerzés igazgatója – anélkül, hogy a FISC számára pontosan megadná a célba vett nem egyesült államokbeli személyt – külföldi hírszerzési információk megszerzése érdekében éves tanúsítványokkal engedélyezi a célba vételét azon nem egyesült államokbeli személyeknek, akikről megalapozottan feltételezhető, hogy az Egyesült Államokon kívül tartózkodnak. [...] Emellett olyan előírás sincs, mely szerint a kormány köteles bizonyítani annak megalapozottságát, hogy a 702. szakasz célpontja külföldi hatalom

[53] Freedom törvény: IV. Cím – Bírósági reformok a külföldi hírszerzői tevékenység megfigyelésével összefüggésben, 401. szakasz (*Freedom Act TITLE IV--FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS Sec. 401.*). Az *amicus curiae* kijelölése

vagy külföldi hatalom ügynöke, ami pedig a hagyományos FISA szerint követelmény lenne."[54]

A kongresszusi vizsgálóbizottságok a hírszerzési tevékenységek jóváhagyásával – mindenekelőtt pedig a költségvetés megszavazásával – ugyancsak ellátnak felügyeleti feladatokat. A Szenátus és a Képviselőház hírszerzési bizottságait a hírszerzési tevékenységekről minősített összefoglalók útján tájékoztatják. E bizottságoknak a legfőbb ügyész hathavonta köteles jelentést tenni a FISA elektronikus megfigyelési tevékenységéről. A WP29 számára továbbra sem egyértelmű, hogy e feleknek milyen mértékben áll módjukban megvitatni az egyének – különösképpen a nem egyesült államokbeli személyek – személyes adatainak kezelését.

A PCLOB a végrehajtó hatalmi ágnak az Egyesült Államok kormányán belüli független része, amelynek két alapvető feladata: 1) az [amerikai] nemzet terrorizmussal szembeni védelme érdekében hozott végrehajtó hatalmi intézkedések felülvizsgálata és elemzése a szóban forgó intézkedések, illetve a magánélet tiszteletben tartásához való jog és a polgári szabadságjogok védelmének szükségessége közötti egyensúly érdekében, valamint 2) annak érvényre juttatása, hogy a nemzet terrorizmussal szembeni védelmét szolgáló jogszabályok, rendeletek és szakpolitikák kialakítása és végrehajtása során a szabadságjogi megfontolások kellő figyelmet kapjanak. A WP29 megjegyzi, hogy a PCLOB jogszerű bizonyítási cselekményben való közreműködésre kötelező határozathozatali jogkörrel rendelkezik, és minősített adatokhoz is hozzáférhet. Feladatai emellett még a programok eredményességének ellenőrzésére is kiterjednek. Felügyeleti feladatát nem előzetesen, hanem utólagosan látja el. A PCLOB immár tanúbizonyságot tett független jogköréről, amikor az Egyesült Államok elnöke által képviselttől eltérő véleményt fogalmazott meg jogi kérdések kapcsán. Konkrétan: jogszerűtlennek találta a 215. szakasz szerinti telefon metaadat programot, amelyről azt is megállapította, hogy mivel zavarkeltést célzó támadásokra nincs bizonyíték, eredménytelen programnak minősül. A PCLOB továbbá egy évig tanulmányozta a 702. szakasz szerinti programot, amelyet jogszerű és egyértelműen törvény által előírt programnak talált, a 702. szakaszról pedig kijelentette, hogy a terrorizmussal összefüggő problémák esetében is igen hatékony eszköznek bizonyult. Végezetül: az átláthatósági követelmény kapcsán végzett munkája eredményeként úgy találta, hogy a minősített tényeket számos esetben indokolatlanul nyilvánították minősítetté. Az értesülések szerint a PCLOB a közeljövőben jelentésben fog beszámolni a PPD-28 végrehajtásáról. Ezzel összefüggésben azt az álláspontot képviseli, hogy a külföldi személyekre vonatkozó információk megőrzésére önmagában nem szolgáltat kellő alapot az a tény, hogy a szóban forgó személy külföldi.

A WP29 végezetül megjegyzi, hogy az EO12333 a megfigyelési programjaira vonatkozóan sem bírósági felülvizsgálatot, sem pedig felügyeleti vagy jogorvoslati mechanizmust nem tartalmaz.

[54] A FISA 702. szakasza szerint működtetett megfigyelési programról szóló PCLOB-jelentés 24. és 25. oldala.

3.4.3. Következtetés

A megfelelőségi határozat tervezetéből kitűnik, hogy az Egyesült Államokban többszintű, belső és külső felügyeleti mechanizmusokat egyaránt tartalmazó megközelítést alkalmaznak. Jóllehet a felügyeleti mechanizmusok működése áttekinthetetlennek tűnhet, a WP29 elégedett azzal, hogy – összességében – elegendő belső felügyeleti mechanizmus áll rendelkezésre. A WP29 mindazonáltal aggályosnak tartja, hogy az EO12333 alapján indított megfigyelési programokat nem felügyelik kellő mértékben.

A WP29 megjegyzi, hogy a FISC-eljárások nem kontradiktórius jellege kapcsán megfogalmazott korábbi bírálatára csak részben jelent megoldást az – egyének magánélete és polgárjogi védelmének előmozdítását szolgáló – *amicus curiae* intézményének bevezetése. A FISC mindazonáltal a nem egyesült államokbeli célszemélyek tekintetében nem szolgál hatékony bírósági felügyelettel. Ezen túlmenően – miként arra a PCLOB is rámutatott[55] – továbbra is aggályos, hogy a FISC képes-e hatékony módon értékelni a célzottá tételre, illetve adatminimalizációra vonatkozó eljárásokat.

3.5. D-biztosíték – Hatékony jogorvoslati lehetőségek biztosítása az egyének számára

3.5.1. Bírósági jogorvoslatok

3.5.1.1. A kereshetőségi jog követelménye

A bírósági jogorvoslatok egyesült államokbeli rendszerének részét képezi egy lényeges korlátozás: az Egyesült Államok alkotmánya az egyének számára követelményként előírja kereshetőségi joguk bizonyítását: „feltétel a felpereseket ért kár bekövezte, vagy hogy a közvetlen kár vagy sérelem be fog következni, és hogy e sérelem orvosolható legyen. Nem lehet keresetet benyújtani szövetségi szinten pusztán azon alapon, hogy az egyén vagy csoport elégedetlen a kormány intézkedésével vagy törvényével.”[56] Az ilyen jellegű követelményt a jelek szerint érvényteleníti, hogy a megfigyelt egyéneket még az intézkedések megszűntetése után sem értesítik. Az EUB és az EJEB több alkalommal is kimondta, hogy az egyéneknek lehetőséget kell biztosítani közigazgatási és bírósági jogorvoslatra. A Zakharov-ügyben hozott ítéletében az EJEB megerősítette, hogy az ítélkezési gyakorlat alapján minden olyan személynek joga van bírósághoz fordulni, aki jogos okkal feltételezi, hogy alapvető jogaiba beavatkoznak.[57]

Az Egyesült Államokon kívül tartózkodó külföldiek ráadásul – az Egyesült Államok Legfelsőbb Bíróságának ítélkezési gyakorlata szerint[58] – az Egyesült Államokban nem részesülnek teljes alkotmányos védelemben. Különösen igaz ez a negyedik alkotmánykiegészítés tekintetében, amely az egyesült államok állampolgárait – a nem egyesült államokbeli személyeket viszont nem – védi az indokolatlan kutatások és

[55] A FISA 702. szakasza szerint működtetett megfigyelési programról szóló PCLOB-jelentés 11. oldala.
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper kontra Amnesty International USA.
[57] Az EJEB Zakharov-ügyben hozott ítéletének 171. pontja.
[58] Egyesült Államok kontra Verdugo–Urquidez, 264–266. o.

letartóztatásokkal szemben, és amelyre a magánélet tiszteletben tartásához való egyesült államokbeli jog jórészben épül. A nem az Egyesült Államokban élő uniós polgárokra, illetve más európai személyekre a negyedik alkotmánykiegészítés biztosította védelem egyszerűen nem terjed ki[59].

A bírósági jogorvoslatról szóló törvény korlátozott alkalmazása (ami egyrészt érdemben érhető tetten, hiszen a nemzetbiztonságra nem terjed ki, másrészt pedig azon személyek szempontjából, akiknek módjában áll hivatkozni a törvényre) miatt, továbbá a kivételek széles köre és a bírósági jogorvoslatról szóló törvény majdani hatálya alá tartozó ügynökségekkel kapcsolatos jogbizonytalanság miatt nem teljesíti a követelményt, miszerint a nemzetbiztonsági hírszerzési megfigyelésekben érintett egyének teljes köre számára biztosítani kell a hatékony jogorvoslati mechanizmus igénybevételének lehetőségét.

3.5.1.2. A 28. sz. elnöki irányelv

A WP29 megjegyzi, hogy a PPD-28 abból adódóan, hogy mindössze irányelvi szabályozás, nem keletkeztethet jogokat az egyének számára. Jogok ugyanis kizárólag jogszabályokkal határozhatók meg. Az egyének következésképp a PPD-28 biztosítékainak állítólagos megsértésére hivatkozva nem fordulhatnak bírósághoz.

3.5.1.3. A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény

A jogellenes megfigyelések kapcsán a FISA kínál bizonyos jogorvoslati lehetőségeket az egyének számára. A FISA kimondja, hogy „a külföldi hatalmon vagy külföldi hatalom ügynökén kívüli olyan sértett személy [...], aki elektronikus megfigyelés alatt állt, vagy akiről egy ilyen személy elektronikus megfigyelésével szerzett információkat e cím 1809. szakaszát megsértve nyilvánosságra hozzák vagy felhasználják, keresetindítási jogosultsággal rendelkezik az említett jogsértést elkövetett személlyel vagy személyekkel szemben”. Ez mindazonáltal kifejezetten kizárja a külföldi hatalmat, illetve a külföldi hatalom ügynökét, akire az intézkedés vonatkozott. Mindamellett – amint az már említésre került – a felperesnek bizonyítania kell kereshetőségi jogát, ami viszont gyakorlatilag lehetetlen.

Az USA Freedom törvény létrehozta a FISA-Bíróság mellett működő *Amicus Curiae* tanácsadó testületet, mely a jelentősebb új jogi értelmezések kapcsán szolgál (nem kötelező jellegű) tanácsokkal. Feladata ugyanakkor a pártatlan tanácsadás, nem pedig az, hogy konkrét egyéni felkérésre eljárjon az adott egyén érdekeinek védelmében.

3.5.2. Közigazgatási jogorvoslatok

3.5.2.1. Főellenőrök (Inspectors-General)

Egy másik jogorvoslati lehetőségként a főellenőrökhöz is benyújtható panasz. A főellenőrök azonban nem kötelesek foglalkozni minden egyes panasszal: meghallgatáshoz való jog ugyan nem áll fenn, de a főellenőrök rendelkeznek mérlegelési jogkörrel. A főellenőrök emellett

[59] Az uniós társelnökök jelentésének 2. szakasza.

olyan jogsértésekről is jelentést tehetnek, amelyek esetében az információk minősítését feloldották. Amennyiben az egyén feltételezése szerint a jelentésben foglaltak érintik személyét, akkor a jogsértés megállapítására hivatkozva bírósághoz fordulhat.

3.5.2.2. Az információhoz való szabad hozzáférésről szóló törvény

Valamennyi személynek lehetőségében áll, hogy az információhoz való szabad hozzáférésről szóló törvény (*Freedom of Information Act – FOIA*) alapján kérelmezze az információhoz való szabad hozzáférést. Az Egyesült Államok kormánya szerint FOIA-kérelmet az ügynökségi nyilvántartási adatok egyszerű kikérésével általában bárki – függetlenül attól, hogy az Egyesült Államok állampolgára vagy sem – benyújthat. Ez az egyénre vonatkozóan nyilvántartott adatokra is igaz, jóllehet ilyenkor a személyazonosságot igazolni kell. Abban az esetben azonban, ha az információt nemzetbiztonság-védelmi okokból minősített adattá nyilvánították, a FOIA-kérelmet valószínűleg valamely kivétel alapján elutasítják: az ügynökségek nem kötelesek hozzáférést biztosítani a minősített adatokhoz, még abban az esetben sem, ha a kérelmet benyújtó egyénre vonatkozó információkról van szó. A folyamatban lévő bűnügyi nyomozásokra vonatkozó információk teljes köre a FOIA-kérelmek hatályán kívül esik. Végezetül pedig: a WP29 úgy látja, hogy a FOIA-kérelem nem biztosít jogot arra, hogy az adatkezelés jogszerűségének ellenőrzését független hatóság végezze el.

3.5.3. Az adatvédelmi pajzs ombudsmanja

3.5.3.1. Az ombudsmani mechanizmus kialakítása

Az adatvédelmi pajzs új mechanizmust vezet be, amely lehetőséget biztosít az „uniós egyének” számára, hogy az adatvédelmi pajzs újonnan létrehozott ombudsmani hivatalhoz nyújtsák be az „Egyesült Államok jelfelderítésével” kapcsolatos kérelmeiket. Az ombudsmani tisztséget – miként az a John Kerry külügyminiszter 2016. február 22-én kelt leveléhez mellékletként csatolt feljegyzésben is szerepel – C. Novelli miniszterhelyettes fogja betölteni. E feladatkörét a miniszterhelyettes a PPD-28 4d. szakaszával létrehozott „nemzetközi informatikai diplomácia főkoordinátora” tisztsége mellett látja majd el. Mind a levél, mind pedig a feljegyzés nyomatékosítja, hogy a miniszterhelyettes a külügyminiszter közvetlen alárendeltje, és független a hírszerzési közösségtől.

Miként azt a feljegyzés kifejti, az adatvédelmi pajzs ombudsmanja – elnevezése ellenére – nem kizárólag azokkal a kérelmekkel fog foglalkozni, amelyek az EU-ból az Egyesült Államokba az adatvédelmi pajzs keretében továbbított adatokhoz történő nemzetbiztonsági hozzáférésére vonatkozóan nyújtottak be, hanem (a feljegyzés 2. lábjegyzetében meghatározottak szerint) azokkal is, amelyek esetében általános szerződési feltételek, kötelező erejű vállalati szabályok, (a 95/46/EK irányelv 26. cikke szerinti) eltérések vagy „esetleges jövőbeli eltérések” alapján továbbították az adatokat.

A mechanizmus működési modellje a következőképpen foglalható össze: az uniós egyének benyújtják kérelmüket a nemzetbiztonsági szolgálatok felett felügyeleti hatáskörrel

rendelkező tagállami szervhez vagy – későbbi létrehozása vagy kijelölése esetén – az uniós egyének központosított panaszkezelő szervéhez. A kérelmet az ombudsmanhoz továbbító hatóságnak először is ellenőriznie kell, hogy a levél 3. szakaszának b) pontjában meghatározottak alapján[60] a kérelem teljes-e. Azt követően, hogy a kérelmet továbbították az adatvédelmi pajzs ombudsmanjához, és a kérelemről megállapítást nyert, hogy megfelel a 3. szakasz b) pontjában előírtaknak, az adatvédelmi pajzs ombudsmanja megküldi válaszát, amellyel egyben véglegesen megerősíti, hogy „.i. a panaszt megfelelően kivizsgálták, és ii. az Egyesült Államok jogszabályai, alapszabályai, végrehajtási rendeletei, elnöki irányelvei és hivatali politikái, amelyek a nemzeti hírszerzés igazgatójának hivatala (*Office of the Director of National Intelligence – ODNI*) levélben leírt korlátozásokról és biztosítékokról rendelkeznek, teljesültek, vagy nemteljesülés esetén a nemteljesülést orvosolták”.[61] A válasz maga „nem erősíti meg és nem is cáfolja, hogy az egyén megfigyelés célpontja volt, és az adatvédelmi pajzs ombudsman nem erősíti meg az alkalmazott konkrét jogorvoslatot”.[62] Az ombudsmani vizsgálat lefolytatásának mikéntje kapcsán a levél kifejti, hogy az adatvédelmi pajzs ombudsmanja „szorosan együttműködik az Egyesült Államok más kormánytisztviselőivel – köztük a megfelelő független felügyeleti szervekkel”[63], közelebbről pedig, hogy „koordinálni fogja tevékenységét [...] az ODNI-val, az Igazságügyi Minisztériummal és szükség szerint az Egyesült Államok nemzetbiztonságával foglalkozó más minisztériumokkal és hivatalokkal, valamint főellenőrökkel, az információhoz való szabad hozzáférésről szóló törvényért felelős tisztviselőkkel és a polgári szabadságjogi és adatvédelmi tisztviselőkkel”[64]. A tevékenységek szóban forgó összehangolásának lehetővé kell tennie, hogy az adatvédelmi pajzs ombudsmanja olyan választ küldhessen, amely a fent leírtaknak megfelelő megerősítést tartalmaz.

3.5.3.2. Az új ombudsmani mechanizmus értékelése

A munkacsoport méltányolja az Európai Bizottság és az Egyesült Államok eddigi, az Egyesült Államok megfigyelési tevékenységeivel kapcsolatos jogorvoslati lehetőségek bővítését célzó új mechanizmus bevezetésére irányuló törekvéseit. A munkacsoport tisztában van azzal, hogy a mechanizmus értékelése – abból adódóan, hogy a jelfelderítés és a nemzetbiztonság szempontjából a mechanizmus a nemzetközi kapcsolatok terén új fejleménynek számít – különösen lényeges.

---

[60] b) Az EU egyéni panaszkezelő szerve biztosítja az alábbi intézkedéseknek megfelelően, hogy a kérelem hiánytalan:
i. Az egyén azonosítása és annak ellenőrzése, hogy az egyén a saját nevében jár el, és nem egy kormányzati vagy kormányközi szervezet képviselője.
ii. Annak biztosítása, hogy a kérelmet írásban nyújtják be, és a kérelem tartalmazza az alábbi alapvető információkat:
• a kérelem alapját képező bármely információ,
• kért információ vagy jogorvoslat jellege,
• az Egyesült Államok vélelmezetten érintett jogi személyei, ha vannak ilyenek, és
• a kért információ vagy jogorvoslat elérése érdekében foganatosított egyéb intézkedések és az ilyen intézkedésekre kapott válaszok.
iii. Annak ellenőrzése, hogy a kérelem olyan adatokra vonatkozik, amelyekről alapos indokkal feltételezhető, hogy az EU-ból az Egyesült Államokba továbbították az adatvédelmi pajzs, az általános szerződési feltételek, a kötelező erejű vállalati szabályok, eltérések vagy esetleges jövőbeli eltérések keretében.
iv. Annak a kezdeti meghatározása, hogy a kérelem nem komolytalan, zaklató vagy rosszhiszemű.
[61] Az adatvédelmi pajzs III. melléklete 4. szakaszának e) pontja.
[62] Az adatvédelmi pajzs III. melléklete 4. szakaszának e) pontja.
[63] Az adatvédelmi pajzs III. melléklete 2. szakaszának a) pontja.
[64] Az adatvédelmi pajzs III. melléklete 2. szakaszának a) pontja.

E szakasz a WP29 arra vonatkozó értékelését hivatott bemutatni, hogy az adatvédelmi pajzs ombudsmani mechanizmusának létrehozása miként illeszkedik az egyének jogorvoslat iránti kereseti lehetőségeinek Chartában, valamint az EJEB és az európai bíróságok ítélkezési gyakorlatában meghatározott követelményeihez.

3.5.3.3. Elegendő az ombudsmani mechanizmus létrehozása önmagában?

Mindenekelőtt azt a kérdést kell megválaszolni, hogy az ombudsmani mechanizmus létrehívása legalább azokban az esetekben összeegyeztethetőnek tekinthető-e a Charta 47. cikkével – amely egyébiránt pártatlan bíróság előtti hatékony jogorvoslatot ír elő[65] –, amikor egyéb alternatíva nem áll rendelkezésre a hatékony jogorvoslatra. E kérdés azért fontos, mert a Schrems-ügyben hozott ítélet mértékadó 95. pontjában az EUB a Charta 47. cikkére hivatkozik, mégpedig oly módon, hogy semmiféle támpontot nem ad arra vonatkozóan, hogy a 47. cikk módosításokkal lenne értelmezendő a megfigyelési intézkedésekkel összefüggésben. Éppen ellenkezőleg: az EUB a Kadi II-ügyben hozott ítéletében[66] már alkalmazta – mind a nemzeti, mind pedig a nemzetközi biztonsággal összefüggésben – a 47. cikket megfigyelési intézkedésekre[67].

Az EJEB ítélkezési gyakorlata alapján mindazonáltal teljesen egyértelmű, hogy a rendes bíróságok előtti jogorvoslat nem feltétele annak, hogy a megfigyelési rendszerek megfeleljenek a 8. cikknek (és az EJEE 13. cikkének).[68] Ehelyett a Bíróság a 8. cikkel összefüggésben kialakított gyakorlata szerint az egyéb hatóságok előtti jogorvoslat – a megfigyelési tevékenységek szükséges biztosítékaként – adott esetben szintén szabályszerű. Az EJEB mindamellett szigorú elvárásokat támaszt a hatékony jogorvoslati fórumként működő egyéb hatóságokkal szemben azzal, hogy e hatóságokat illetően kimondja: azok „függetlenek a megfigyelést végző hatóságoktól, egyúttal a hatékony és folyamatos ellenőrzéshez kellő jogkörökkel és hatáskörrel vannak felruházva”[69].

A Kennedy-ügyben, illetve a Klass-ügyben hozott ítéleteivel az EJEB részletesebb iránymutatással szolgált arról, hogy mit is takarnak ezen elvárások a titkosszolgálati megfigyelések azon eseteiben, amikor az érintetteket nem értesítik adataik kezeléséről. Az EJEB mindkét ítéletében megállapította, hogy a hatóságok függetlenek, különösképpen a megfigyelést végző szervektől, de az összes többi hatóság utasításaitól[70] is. Pontosabban: a Kennedy-ügyben a Bíróság egy olyan független és pártatlan hatóságot hagyott jóvá, amely

[65] A „Magyarázatok az Alapjogi Chartához” című dokumentum ezenkívül kimondja, hogy a 47. cikket úgy kell értelmezni, mint amely biztosítja a bíróság előtti hatékony jogorvoslathoz való jogot (Magyarázatok az Alapjogi Chartához, Magyarázat a 47. cikkhez [2007/C 303/02]).
[66] A Bíróság C-584/10. P., C-593/10. P. és C-595/10. P. sz., Európai Bizottság és Egyesült Királyság kontra Kadi egyesített ügyekben 2013. július 18-án hozott ítélete.
[67] A Kadi II-ügyben hozott ítélet 97. és 100. pontja: az uniós bíróságok valamennyi uniós jogi aktus – beleértve a Biztonsági Tanácsnak az Egyesült Nemzetek Alapokmánya VII. fejezete alapján elfogadott határozatainak végrehajtására irányuló jogi aktusokat is – jogszerűségét felülvizsgálják (a VII. fejezet a béke veszélyeztetése, a béke megszegése és a támadó cselekmények estében követendő eljárást tárgyalja).
[68] Az EJEE 13. cikke kötelezettségként írja elő a tagállamok számára, hogy „[b]árkinek, akinek [...] jogait és szabadságait megsértették, joga van ahhoz, hogy a hazai hatóság előtt a jogsérelem hatékony orvoslását kérje”. E hatóságnak – miként azt a Klass-ügyben hozott ítéletének 56. és 67. pontjában az EJEB kimondta – nem kell feltétlenül igazságügyi hatóságnak lennie.
[69] A Klass-ügyben hozott ítélet 56. és 67. pontja.
[70] Az EJEB Klass-ügyben hozott ítéletének 21. és 53. pontja.

eljárási szabályzatát maga fogadta el, és amelynek tagjai az ítélet meghozatalakor, vagy a korábbiakban felsőbb bírói feladatokat láttak el, illetve tapasztalt jogászok voltak[71].

A hatóságok mindkét ítélet esetében valamennyi releváns információhoz – így a lezárt anyagokhoz is – hozzáfértek az egyének által benyújtott panaszok vizsgálata alkalmával. Végezetül: mindkét hatóság rendelkezett jogkörrel ahhoz, hogy orvosolja a meg nem felelést.[72]

Azon kérdésen túlmenően, hogy igazságszolgáltatási fórumnak tekinthető-e az ombudsmani mechanizmus, a Charta 47. cikke második bekezdésének alkalmazása felvet egy további problémát, hiszen „törvény által [...] létrehozott" igazságszolgáltatási fórumot ír elő követelményként, márpedig az vitatható, hogy az új mechanizmus működését ismertető feljegyzés „törvénynek" tekinthető.

Ebből adódóan a munkacsoport – a lényegi azonosság elvét szem előtt tartva – nem azt vizsgálta, hogy az ombudsman törvény által létrehozott igazságszolgáltatási fórumnak tekinthető-e hivatalosan, hanem úgy döntött, hogy azoknak a konkrét követelményeknek az ítélkezési gyakorlatbeli finom eltéréseit tanulmányozza részletesebben, amelyeknek teljesülniük kell ahhoz, hogy a „jogorvoslatot" és a „törvényi kártérítést" a Charta 7., 8. és 47. cikke, valamint az EJEE 8. (és 13.) cikke szerinti alapvető jogokkal összhangban állónak lehessen tekintetni. A munkacsoport ily módon az új mechanizmus hatályának további elemzését az alábbi kritériumokra összpontosítja: a kérelem ombudsmanhoz történő benyújtására és a válaszadásra vonatkozó követelmény (a továbbiakban: kereshetőségi jog), az ombudsman függetlensége, vizsgálati hatásköréből adódó hozzáférés a szükséges anyagokhoz (a minősített dokumentumokat is ideértve), segítségkérés más ügynökségektől, végezetül pedig a meg nem felelés orvoslására irányuló jogköre.

3.5.3.4. Az ombudsmani mechanizmus hatálya

Az ombudsmani mechanizmus igénybevételét illetően a WP29 meglátása szerint az adatvédelmi pajzsba beépített biztosítékoknak az uniós jogalanyok teljes körét le kell fedniük. Az állampolgárságon alapuló megkülönböztetés elfogadhatatlan lenne, különösképpen amiatt, hogy az alapjogok az Unióban nemcsak az uniós útlevéllel rendelkezőkre, hanem minden személyre érvényesek. A III. melléklet az „uniós egyén" (*EU individual*) kifejezést használja, de anélkül, hogy részletesebben meghatározná e kör tagjait. A munkacsoport sajnálatosnak tartja e tisztázatlan pontot és javasolja a fogalom egyértelműsítését, mégpedig oly módon, hogy valamennyi uniós jogalanynak jogában álljon igénybe venni az ombudsmani mechanizmust kérelme – feljegyzésben foglalt feltételek szerinti – feldolgozása tekintetében. A Bizottságnak és az Egyesült Államoknak foglalkoznia kell továbbá azzal is, hogy az adatvédelmi pajzs hatálya milyen mértékben lesz alkalmazandó az EGT-országok és Svájc állampolgáraira / lakosaira, akikre korábban kiterjedt a védett adatkikötő rendszere.

[71] A G-10 Bizottság (az ítélet meghozatalának időpontjában) három tagot számlál, az elnöki tisztséget pedig kizárólag bírói hivatal betöltésére jogosult személy töltheti be (Klass-ügy 21. és 53. pontja).
[72] Az EJEB Kennedy-ügyben hozott ítéletének 167. pontja, a Klass-ügyben hozott ítélet 21. és 53. pontja.

Az ombudsmani mechanizmus alkalmazási területével kapcsolatban a WP29 felhívja a figyelmet néhány homályos pontra. Jóllehet a feljegyzés alapján az ombudsman feladatköre kiterjed az uniós jog értelmében felhasználható összes átviteli eszközzel – az EU-ból az Egyesült Államokba – továbbított adatok nemzetbiztonsággal kapcsolatos kezelése iránti kérelmekre, a feljegyzés azt is világosan leszögezi, hogy a mechanizmus létrehozása a „jelfelderítés tekintetében" történik. Ez utóbbi kifejezés azt sugallja, hogy a hatály kizárólag azon adattovábbításokra terjed ki, amelyek esetében az adatgyűjtésre jelfelderítési eszközökkel kerül sor, ami felveti a kérdést, hogy – például – a FISA alapján végzett adatgyűjtés „jelfelderítésnek" minősül-e. Úgy tűnik, hogy a 702. szakasz esetében erről van szó, miként azt az ODNI nyilatkozata[73] is kifejti (10. oldal). A WP29 mindazonáltal sajnálatát fejezi ki, hogy a „jelfelderítés" kifejezés e kontextusban olyan bizonytalanságot eredményez, amely elkerülhető lett volna.

A munkacsoport – szintén ebből adódóan – arra a megállapításra jutott, hogy a bűnüldöző hatóságok hozzáférésével kapcsolatos kérelmeket az ombudsmani mechanizmus nem vizsgálja.[74] Ha ez igaz, akkor továbbra sem egyértelmű, hogy bizonyos ügynökségek – nevezetesen a CIA – kérelmeire alkalmazandó-e a mechanizmus.

3.5.3.5. Kereshetőségi jog és a kérelmezési eljárás

Az Egyesült Államokban igen nehéz rendes bíróság előtt jogi eljárást indítani az Egyesült Államok kormánya által hozott megfigyelési intézkedésekkel szemben. A munkacsoport tisztában van azzal, hogy a hírszerzési ügyekkel összefüggésben az Egyesült Államok Legfelsőbb Bírósága nem ismeri el a kereshetőségi jogot abban az esetben, ha a felperes nem tudja bizonyítani személye kapcsán a konkrét, pontosan meghatározott és tényleges károsodást vagy a károsodás veszélyét[75]. E tekintetben az ombudsmani mechanizmus létrehozása fontos lépésnek számít, hiszen lehetőséget teremt egyfajta jogorvoslatra, amely máskülönben nem is létezne. A munkacsoport tehát üdvözli a 3. szakasz c) pontjában szereplő pontosítást. E szakasz alapján az új mechanizmus esetében a kérelmezéshez nem kell bizonyítani, hogy a kérelmező adatihoz ténylegesen hozzáfértek jelfelderítési tevékenység keretében.

A munkacsoport lényegében egyetért a panaszosok azonosításának ombudsmani mechanizmus szerinti eljárásával. Teljesen logikus, hogy az azonosítást – az EU–USA TFTP2 megállapodás hozzáférési mechanizmusához hasonlóan – uniós terülten végezzék el. A munkacsoport számára viszont nem világos, hogy az Unión belüli ellenőrzést miért a nemzetbiztonsági szolgálatok felügyeletéért felelős tagállami szervek feladata lenne elvégezni. Először is: az Európai Unióról szóló szerződés 4. cikkének (2) bekezdése alapján valószínűtlennek tűnik, hogy az Európai Bizottságnak módjában áll e szerveket olyan feladatokkal megbízni, amelyek egyértelműen tagállami hatáskörbe tartoznak.

[73] Az adatvédelmi pajzs VI. melléklete, 10. o.
[74] Az ombudsmani mechanizmus létrehozásáról szóló feljegyzés, 1. o.
[75] Clapper kontra Amnesty International USA, 568 U.S. ___ (2013) II.10. o.

Továbbá a nemzetbiztonsági szolgálatok felügyeletére létrehozott tagállami mechanizmusok ráadásul igen változatos képet mutatnak, így a megfelelő hatóságok szerepvállalása az állampolgárok szempontjából jelentősen ronthatja a rendszer eredményes működését a tagállamokban. Erre lehet példa, ha a nemzetbiztonsági szolgálatok felügyeletét több hatóság látja el és az egyén számára nehézséget okoz megállapítani, hogy ügyében melyik hatóság jogosult eljárni, vagy ha az alkalmazandó nemzeti jogi normák nem teszik lehetővé az egyének számára, hogy a hatáskörrel rendelkező felügyeleti hatósággal kapcsolatba lépjenek, vagy ha e hatóságok kialakításuknál fogva nem alkalmasak a megfelelőségi határozat tervezetében rájuk bízott feladatok ellátására[76]. Tekintettel az adatvédelmi hatóságoknak az adatvédelmi pajzs alkalmazásában és felügyeletében játszott, valamint a TFTP2 megállapodás keretében betöltött hasonló szerepére, megfelelőbbnek tűnik, ha a szóban forgó feladatot a tagállamok nemzeti adatvédelmi hatóságai látják el. A munkacsoport hangsúlyozza, hogy valószínűtlennek tartja, hogy az adatvédelmi pajzs ombudsmanja előtti eljárások részeként minősített adatok kezelésére is sor fog kerülni, hiszen mindössze „teljesült" vagy „nem teljesült, de a nemteljesülést orvosolták" válasz adható.

3.5.3.6. Függetlenség

A külügyminiszter nyilatkozataiból egyértelműen kiderül, hogy az ombudsmani tisztséget az Egyesült Államok Külügyminisztériumának egyik miniszterhelyettese fogja betölteni. Magát a személyt az elnök nevezi ki és a Szenátus erősíti meg tisztségében. Az ombudsman feladatköre – annak adott személyhez rendelésén túlmenően – nem igényel további megerősítést. A miniszterhelyettest, aki ombudsmani tisztségében a külügyminiszter irányítása alá tartozik, az Egyesült Államok elnöke nevezi ki és az Egyesült Államok Szenátusa erősíti meg miniszterhelyettesi posztjában. Miként azt a levél és a feljegyzés is kiemeli, az ombudsman „független az Egyesült Államok hírszerzési közösségétől". A WP29 mindazonáltal megkérdőjelezi, hogy valóban a legmegfelelőbb minisztérium alá rendelték-e az ombudsmani tisztséget. Az ombudsmani feladatkör eredményes ellátásához egyfelől a jelek szerint bizonyos mértékben ismerni kell és át kell látni a hírszerzési szervek működését, másfelől viszont az ombudsmannak kellő távolságot kell tartania e szervektől, hogy függetlenként járhasson el.

Az ombudsman tekintetében az adatvédelmi pajzs nem állapít meg külön felmentési kritériumokat. A munkacsoport ennélfogva úgy látja, hogy az ombudsman e tisztségéből történő felmentésére ugyanazon eljárás alkalmazandó, mint az Egyesült Államok Külügyminisztériumában betöltött miniszterhelyettesi posztjából való felmentésére, ami potenciálisan alááshatja az ombudsman függetlenségét.

Az Egyesült Államok Külügyminisztériumának kötelékéhez tartozó miniszterhelyettes ombudsmani kinevezése a függetlenség szempontjából jellegét illetően nyilvánvalóan különbözik az egyének jogorvoslata tekintetében hatáskörrel rendelkező rendes bíróságok joghatóságának megállapításától. A kérdés tehát voltaképp az, hogy az ombudsman azon egyéb független felügyeleti testületek függetlenségéhez mérhető függetlenséggel rendelkezik-

[76] Néhány tagállamban például az egyének kizárólag a legfelsőbb bíróságtól kérelmezhetik a nemzetbiztonsági szolgálatok birtokában lévő információkhoz való hozzáférést.

e, amelyek megfelelőségét már megerősítették. A megfigyelési ügyek terén mindenekelőtt az egyesült királyságbeli nyomozati szervekkel foglalkozó bíróság (*Investigatory Powers Tribunal – IPT*) és a németországi G-10 bizottság tekintendő ilyen jellegű testületnek.

Amennyiben a válasz igen, akkor a „független" testületre ruházott jogkörök elemzéséhez további vizsgálatok szükségesek.

3.5.3.7. Vizsgálati hatáskörök

A Charta 47. cikke kapcsán az EUB megállapította a Kadi II-ügyben, hogy az „[megköveteli], hogy az érintett megismerhesse a rá vonatkozóan hozott határozat alapjául szolgáló indokokat – akár magának a határozatnak a szövege, akár ezen indokok kérésére történő közlése alapján –, az illetékes bíróság azon hatáskörének sérelme nélkül, hogy a szóban forgó hatóságtól megkövetelje azok közlését annak érdekében, hogy lehetővé tegye számára jogai lehető legjobb feltételek mellett történő védelmét"[77]. Az uniós bíróság feladata, hogy meggyőződjön arról, hogy az említett határozat kellően biztos ténybeli alappal rendelkezik.[78] Az EUB egyértelműen kimondja, hogy – legalábbis az uniós bírósággal szemben – „nem hivatkozható [az] információk vagy bizonyítékok titkos vagy bizalmas jellege"[79]. A munkacsoport ennélfogva arra a következtetésre jutott, hogy az EUB követelményei abban az esetben teljesülnek, ha az intézkedések végrehajtását alátámasztó indokokra vonatkozó információk és bizonyítékok ombudsman felé történő továbbítása kötelező[80].

Egyelőre nem világos, hogy az ombudsman milyen dimenziójú vizsgálati hatáskörrel rendelkezne. E kérdésre sem a Bizottság határozattervezete, sem pedig az Egyesült Államok Külügyminisztériumától kapott III. melléklet nem ad teljesen egyértelmű választ. Amennyire a munkacsoport meg tudja ítélni, az ombudsman számára elegendő információt kell rendelkezésre bocsátani ahhoz, hogy egyfelől eldönthesse a biztonsági szolgálatok adatkezelési műveleteiről, hogy azokat a jogszabályok betartásával hajtják-e végre vagy sem, másfelől pedig, hogy az utóbbi esetben megbizonyosodhasson arról, hogy orvosolták a megfelelés megsértését. Ugyanakkor arra sem a Külügyminisztérium levele, sem pedig a Bizottság határozattervezete nem tér ki, hogy az ombudsman közvetlenül hozzáférhet-e majd a kérdéses személyről tárolt adatokhoz – amivel módjában állna az önálló vizsgálat lefolytatására – vagy kénytelen kizárólag az Egyesült Államok más kormánytisztviselőinek jelentéseire hagyatkozva ellátni feladatait.

3.5.3.8. Jogorvoslati jogkörök

A feljegyzésben foglaltak alapján meglehetősen homályos, hogy az ombudsman milyen módon rendelheti el a megfelelés megsértésének orvosolást. Figyelembe véve a vizsgálati hatáskört övező bizonytalanságot, még kevésbé világos, hogy az ombudsman mint olyan milyen mértékben lesz ténylegesen képes utasítást adni a megfelelés megsértésének

[77] A Kadi II-ügyben hozott ítélet 100. pontja.
78 A Kadi II-ügyben hozott ítélet 119. pontja.
79 A Kadi II-ügyben hozott ítélet 125. pontja.
[80] A Kadi II-ügyben hozott ítélet 122. pontja, jóllehet az érintett hatóság nem köteles az intézkedések alapjául szolgáló indokokra vonatkozó összes információt és bizonyítékot átadni.

orvoslására, és hogy ez milyen eredménnyel fog járni. Jelentheti ez azt esetleg, hogy a megfelelés megsértésével (vagyis jogellenesen) beszerzett adatok további eljárások során nem használhatók fel és azokat törölni kell?

A munkacsoport emellett úgy látja, hogy az ombudsmani „határozatok" elleni fellebbezésre vagy azok felülvizsgálatára az adatvédelmi pajzs semmiféle lehetőséget nem biztosít.

Végezetül pedig, ami az ombudsman panaszosnak címzett – a panasz ombudsmani kivizsgálását követően küldött – válaszát illeti, az ombudsman azt nem fedheti fel, ha a hírszerzési szervek jogellenesen jártak el. A válasz minden esetben ugyanaz lesz, és nem fog konkrétumokat tartalmazni. A Kadi II-ügyben az EUB kimondta, hogy bár az EUMSZ 296. cikke nem követeli meg, hogy részletesen válaszolni kelljen, az illetékes hatóság (felügyelő testületként) minden körülmények között köteles tiszteletben tartani az indoklási kötelezettséget[81].

3.5.4. Következtetés

A WP29 szerint továbbra is aggodalomra ad okot az egyének esetében a hatékony jogorvoslat kérdése. Először is: a megfelelőségi határozat tervezete adós marad az egyértelmű válasszal, hogy az egyének milyen helyzetekben és feltételek mellett indíthatnak jogaik megállapítására irányuló keresetet.

A WP29 ténylegesen elismeri és üdvözli az ombudsmani tisztséggel létrehozott alternatív jogorvoslati mechanizmus bevezetését, ami az Európai Unió és a harmadik országok közötti kapcsolatok szempontjából példa nélkül álló fejleménynek számít. Amellett, hogy az „uniós egyének" fogalmát a már említetteknek megfelelően tisztázni kell, a mechanizmussal egy további lehetőség vált számukra elérhetővé ahhoz, hogy az Egyesült Államok kormányához forduljanak jogorvoslatért annak biztosítására, hogy a felperesek személyes adatait az Egyesült Államok joga szerint kezeljék.

A WP29 ugyanakkor az ombudsmani mechanizmust – a Charta 47. cikke szerinti független bíróságra vonatkozó előírásai alapján, valamint az EUB és az EJEB megfigyelési esetekre vonatkozó ítélkezési gyakorlatában megállapított követelmények alapján – értékelve komoly hiányosságokat azonosított. Először is kérdéses, hogy az ombudsman (formailag és teljes mértékben) függetlennek tekinthető-e, különösképpen annak fényében, hogy a politikai kinevezettek felmentése viszonylag egyszerű. Másodszor: továbbra is aggályokat vetnek fel azon ombudsmani jogosítványok, amelyek a hatékony és folyamatos ellenőrzést hivatottak szolgálni. A III. mellékletben szereplő információk alapján a WP29 számára nem állapítható meg egyértelműen, hogy az ombudsman bármikor közvetlenül hozzáférhet-e a saját értékelésének elvégzéséhez szükséges összes információhoz, aktához és informatikai rendszerhez, ahogy az sem, hogy ténylegesen kötelezheti-e a megbízott hírszerzési ügynökségeket arra, hogy hagyjanak fel a megfelelést sértő adatkezelésekkel, kiváltképpen, ha az álláspontok eltérnek az adatkezelés jogszerűsége tekintetében. Az ombudsman

[81] A Kadi II-ügyben hozott ítélet 116. pontja.

helyzetének és jogkörének további pontosításával a WP29 aggályai valószínűleg eloszlathatók.

3.6. Záró megjegyzések az Egyesült Államok nemzetbiztonsági hatóságainak működésére vonatkozó biztosítékokhoz és korlátozásokhoz

A WP29 mindenekelőtt elismerését fejezi ki a Bizottságnak és az Egyesült Államok hatóságainak eddigi, arra irányuló erőfeszítéseikért, hogy átláthatóbbá tegyék az Egyesült Államok megfigyelési programjainak az adatvédelmi pajzs keretében – vagy éppenséggel bármely más adattovábbítási eszközzel – továbbított adatokra esetlegesen kifejtett hatását. A Snowden-féle első, 2013. júniusi adatkiszivárogtatás óta komoly lépések történtek. Ennek ellenére a WP29 megítélése szerint továbbra is vannak még aggodalomra okot adó kérdések. Az adatvédelmi pajzsból következő jogok és kötelezettségek mindenképpen további magyarázatokat és pontosításokat igényelnek.

A WP29 szerint a két legjelentősebb aggály, hogy az Egyesült Államok hatóságai nem zárkóznak el teljesen a tömeges és válogatás nélküli adatgyűjtéstől, valamint hogy az ombudsman jogkörének és helyzetének részletes szabályozása még várat magára. Emellett a nemzeti adatvédelmi hatóságoknak, nem pedig a hírszerzési ügynökségek felügyeletét ellátó szerveknek kell hatáskörrel rendelkezniük, hogy egyének nevében eljárást indítsanak az ombudsman előtt. Ezen túlmenően a WP29, jóllehet kifejezetten értékeli az adatvédelmi hatóságok aggályainak eloszlatására irányuló igyekezetet, szerencsésnek tartaná további biztosítékok bevezetését annak szavatolására, hogy az Egyesült Államok megfigyelési programjainak bármely esetleges beavatkozása szükséges a demokratikus társadalmakban.

4. AZ ADATVÉDELMI PAJZS BŰNÜLDÖZÉSI BIZTOSÍTÉKAINAK ÉRTÉKELÉSE

4.1. Bevezetés

A személyes adatokhoz bűnüldözési célokból való nyilvános hozzáféréssel kapcsolatosan a WP29 megjegyzi, hogy az adatvédelmi pajzs II. mellékletének adatvédelmi elvei között olyan eltérés szerepel, amely azonos a védett adatkikötőre vonatkozó elvekkel. Az eltérés általános jellegét ezért megőrizték, ami azt jelenti, hogy az új adatvédelmi pajzs alapelvek „a nemzetbiztonságra, a közérdekre vagy a bűnüldözésre vonatkozó [egyesült államokbeli követelmények vagy nemzeti jogszabályok] alapján” lehetővé teszik azon személyek alapvető jogaiba való beavatkozást, akik személyes adatait az EU-ból az Egyesült Államokba továbbítják[82].

A védett adatkikötőről szóló határozattal kapcsolatosan a Schrems-ügyben a Bíróság által megfogalmazott fő kritika az volt, hogy az „nem tartalmaz semmilyen megállapítást azzal kapcsolatban, hogy az Egyesült Államokban léteznek azon személyek alapvető jogaiba való esetleges beavatkozások korlátozására irányuló állami szabályok, akiknek az adatait az Unióból az Egyesült Államokba továbbítják”.

[82] A Schrems-ügyben hozott ítélet 87. pontja.

A WP29 ezért üdvözli az Egyesült Államok kormányának arra irányuló erőfeszítését, hogy több tájékoztatást nyújtson az adatvédelmi pajzs keretében bűnüldözési célokra továbbított személyes adatokba való beavatkozásra vonatkozó jogi keretre vonatkozóan, ideértve az alkalmazandó korlátozásokat és biztosítékokat is. Mindazonáltal a munkacsoport a nyilvános hozzáférés kérdésköre kapcsán hangsúlyozza annak szem előtt tartását, hogy egy demokratikus társadalomban a magánélethez és az adatok védelméhez való alapjogokba történő bárminemű beavatkozásnak igazolhatónak kell lennie. A WP29 ezért elemezte az adatvédelmi pajzs bűnüldözési biztosítékait, az e vélemény 1.2. szakaszában meghatározott keret alkalmazásával.

4.2. Az alapvető európai garanciák alkalmazása a bűnüldöző hatóságoknak a vállalatok által tárolt adatokhoz való hozzáférésére

4.2.1. A bűnüldöző hatóságok személyes adatokhoz való hozzáférésének a jogszabályokkal összhangban kell megvalósulnia, és egyértelmű, pontos és megismerhető szabályokon kell alapulnia

Az adatvédelmi pajzs VII. melléklete tartalmazza az Egyesült Államok Igazságügyi Minisztériumának levelét , amely „rövid áttekintést nyújt az Egyesült Államokban a kereskedelmi adatok és más vállalati információk bűnüldözési vagy közérdekű (polgári és közigazgatási) célú beszerzésére használt elsődleges nyomozati eszközökről, ideértve az ezekben a hatáskörökben meghatározott betekintési korlátokat”.

A VII. mellékletben említett valamennyi eljárás közvetlenül az Egyesült Államok alkotmányából (a negyedik alkotmánykiegészítésből), anyagi és eljárásjogi jogszabályból, vagy az Igazságügyi Minisztérium iránymutatásaiból és szakpolitikáiból ered. Ugyanakkor a VII. melléklet nem hivatkozik kifejezetten valamennyi jogszabályra, amely ezen eljárásokról rendelkezik, hanem maguknak az eljárásoknak a rövid leírására összpontosít. A VII. melléklet megemlíti továbbá, hogy „vannak más, az adott ágazaton és a birtokukban lévő adatok típusán alapuló jogalapok is a közigazgatási hivatalok adatkéréseinek vitatására”, és több nem kimerítő példát sorol fel, így a banktitokról szóló törvényt, a méltányos hitelminősítésről szóló törvényt, a pénzügyi adatok védelméről szóló törvényt.

A WP29 megjegyzi, hogy a jogszabályok, eljárások és szakpolitikák kerete széttagolt, és a hozzáférésre vonatkozó adott kérelemmel kapcsolatban alkalmazandó jogalap a kért adatok jellegétől, a cég típusától, a jogi eljárások jellegétől (büntetőjogi, közigazgatási, más közérdekhez kapcsolódó), továbbá a hozzáférést igénylő szervezet jellegétől függ.

Mivel az adatvédelmi pajzs keretében továbbítható adatok tekintetében a bűnüldöző hatóságok hozzáférését korlátozó valamennyi alkalmazandó szabály az alkotmányon, jogszabályon és az Igazságügyi Minisztérium átlátható szakpolitikáin alapul, e szabályok hozzáférhetőségének vélelmét a WP29 figyelembe vette. Ugyanakkor a szabályok egyértelműségét és pontosságát minden egyes eljárás egyedi típusa és hozzáférési kérelem esetében külön lehet csak értékelni. A WP29 ezért sajnálattal jegyzi meg, hogy az

adatvédelmi pajzs VII. mellékletében rendelkezésre álló adatok és a határozattervezet megállapításai alapján jelenleg ilyen értékelés nem végezhető.

4.2.2. Bizonyítani kell az intézkedés szükségességét és arányosságát az elérni kívánt jogszerű célokra tekintettel

A WP29 megjegyzi, hogy az adatokhoz való bűnüldözési célú hozzáférésre irányuló kérelmet jogszerű cél érdekében tettnek lehet tekinteni. Például az EJEE 8. cikkének (2) bekezdése elfogadja a magánélet védelméhez való jog gyakorlásába való hatósági beavatkozást, amikor „az (...) a nemzetbiztonság, (...) zavargás vagy bűncselekmény megelőzése (...) érdekében szükséges". Ugyanakkor az ilyen beavatkozások csak akkor elfogadhatóak, ha szükségesek és arányosak[83].

Az EUB állandó ítélkezési gyakorlatának megfelelően az arányosság elve a magánélethez és a személyes adatok védelméhez való jogokba való beavatkozást javasló jogalkotási intézkedésektől elvárja, hogy azok „alkalmasak legyenek a *szóban forgó szabályozás* által kitűzött jogszerű célok elérésére, és ne haladják meg az e célok eléréséhez szükséges mértéket"[84] (utólagos kiemelés). Ezért a szükségesség és arányosság értékelése mindig a jogalkotás által tervezett konkrét intézkedésekkel kapcsolatosan végzendő el.

Az Egyesült Államok kormánya a VII. mellékletben meghatározza, hogy a szövetségi ügyészek és a szövetségi nyomozó ügynökök „többféle típusú kötelező bírósági eljáráson keresztül kérhetik vállalati dokumentumok és más adatok kiadását, beleértve az esküdtszék által kibocsátott bizonyításfelvételben vagy a tárgyaláson való közreműködésre vagy kötelező vádesküdtszéki parancsokat, bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat és házkutatási parancsokat, és a „szövetségi bűnügyi lehallgatási és hívásrögzítési hatáskörök szerint" más kommunikációkhoz is hozzáférhet[85]. Ezen túlmenően a polgári és szabályozó feladatkörrel felruházott hivatalok bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat adhatnak ki vállalatoknak „üzleti adatok, elektronikusan tárolt információk vagy más ingóságok tárgyában"[86]. A VII. melléklet ezen túlmenően meghatározza, hogy e bírósági eljárásokat általában véve arra használják, hogy információkat szerezzenek be „vállalkozásoktól" az Egyesült Államokban, függetlenül attól, hogy azok az adatvédelmi pajzs keretében tanúsított szervezetek-e vagy sem, továbbá „tekintet nélkül az érintett állampolgárságára". Vagyis úgy tűnik, hogy e védelmek alanyai a szervezetek, nem pedig maguk a magánszemélyek.

A VII. mellékleten túl a határozattervezet – amely az adatvédelmi pajzs alapelveire épül – a Bizottság megállapításait is tartalmazza az Egyesült Államokban olyan szabályok fennállásáról, amelyek az azon személyek alapvető jogaiba való beavatkozást korlátozták,

[83] Lásd az alapvető európai garanciákra vonatkozó munkadokumentum 7–9. oldalát. A szükségesség és az arányosság fogalmának általános értékelésére lásd a WP28 1/2014. számú véleményét a szükségesség és az arányosság fogalmának alkalmazásáról és az adatvédelemről a bűnüldözési ágazatban, 2014. február 27.
[84] A Digital Rights Ireland ügyben hozott ítélet 46. pontja, valamint az ott hivatkozott ítélkezési gyakorlat.
[85] VII. melléklet, 2. oldal.
[86] VII. melléklet, 4. oldal.

akik személyes adatait az adatvédelmi pajzs keretében az EU-ból az Egyesült Államokba továbbítják.

A határozattervezet megállapításai elsősorban az Egyesült Államok negyedik alkotmánykiegészítése értelmében alkalmazandó korlátozásokra és biztosítékokra hivatkoznak, amelyek szerint a bűnüldöző hatóságok általi kutatáshoz és lefoglaláshoz főszabály szerint „valószínű indokon" alapuló bírósági parancs szükséges[87]. A megállapítások hivatkoznak arra a tényre is, hogy azon kivételes esetekben, amikor a parancs követelménye nem alkalmazandó, a bűnüldözés ésszerűségi vizsgálat alá tartozik[88].

Ugyanakkor a megállapítások alapján nem egyértelmű, hogy e biztosítékok miként alkalmazandók nem egyesült államokbeli személyekre. A határozattervezet kifejezetten elismeri egy preambulumbekezdésben, hogy „a negyedik alkotmánykiegészítésbe foglalt jog nem terjed ki azokra a nem amerikai személyekre, akik nem az Egyesült Államokban laknak"[89]. Ezen túlmenően a határozattervezet azonos bekezdéseiben az áll, hogy „az utóbbiak mindazonáltal közvetetten hozzájutnak annak védelmi normáihoz, mivel a személyes adatok [a bűnüldözési megkereséseseket fogadó] amerikai vállalatok birtokában vannak". A munkacsoport ugyanakkor sajnálattal jegyzi meg, hogy ez a megállapítás nem hivatkozik jogi forrásra, sem az anyagi jogban, sem az ítélkezési gyakorlatban.

Összegezve a WP29 megjegyzi, hogy az Egyesült Államokban bűnüldözési vagy közérdekbeli célokból – ideértve az hozzáférési korlátozásokat és biztosítékokat is – a vállalkozásoktól beszerzendő kereskedelmi adatok és más nyilvántartott információk beszerzésére használt nyomozási eszközök rendszere összetett intézkedésekből áll. A rendelkezésre álló információk alapján ezt a rendszert jelenleg nem lehet általánosságban értékelni. Az egyes konkrét esetekben egyedi értékelésre van szükség annak érdekében, hogy a magánélethez és adatvédelemhez fűződő alapvető jogokkal kapcsolatos bűnüldözési célú nyomozati intézkedések szükségességét és arányosságát ténylegesen értékelni lehessen.

4.2.3. Független felügyeleti mechanizmus kialakítása

A WP29 megjegyzi, hogy a VII. melléklet által leírt legtöbb eljárás előfeltételezi egy bírósági határozat meglétét a hatóságoknak az adatokhoz való hozzáférését megelőzően (pl. hívásrögzítésre és lehallgatásra vonatkozó bírósági végzések, a szövetségi lehallgatási törvény szerinti megfigyelésre szóló bírósági végzések, házkutatási parancsok – 41. szabály). Ugyanakkor úgy tűnik, hogy nem mindegyikhez szükséges bíróság előzetes részvétele. Például polgári és szabályozó feladatkörrel felruházott hivatalok „bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat adhatnak ki"[90]. Ilyen esetekben fennáll az idézés ésszerűségével kapcsolatos utólagos bírósági ellenőrzés lehetősége, mivel a

[87] A megfelelőségi határozattervezet (107) preambulumbekezdése.
[88] Az adatvédelmi pajzs (107) preambulumbekezdése.
[89] A megfelelőségi határozattervezet (108) preambulumbekezdése.
[90] VII. melléklet, 4. oldal.

bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat címzettje bíróságon vitathatja az adott határozat végrehajtását[91].

A rendelkezésre álló információk alapján a WP29 megjegyzi, hogy a bűnüldöző hatóságok által az Egyesült Államokbeli cégek által tárolt adatokhoz való hozzáférés vonatkozásában szemlátomást meglehetősen erős, független felügyeleti mechanizmus létezik.

4.2.4. A magánszemélyek számára hatékony jogorvoslati lehetőségeket kell biztosítani

Ahogy az korábban említésre került, „a negyedik alkotmánykiegészítésbe foglalt jog nem terjed ki azokra a nem amerikai személyekre, akik nem az Egyesült Államokban laknak"[92]. Ez azt jelenti, hogy egy nem egyesült államokbeli személy nem vitathatná bíróságon a negyedik alkotmánykiegészítés felhívásával a parancsokat vagy bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat. A megfelelőségi határozat tervezete meghatározza, hogy a nem egyesült államokbeli személyek közvetetten élvezik a bűnüldözési célból megkeresett személyes adatokat tároló egyesült államokbeli cégeknek biztosított védelmet. A munkacsoport ugyanakkor megjegyzi, hogy ha még ez a védelem hatékony is, nem jelenti azt, hogy a magánszemélyeknek hatékony jogorvoslatok állnak rendelkezésére, mivel ebben az esetben a hatékony jogorvoslathoz való jog alanya szemlátomást a hozzáférés végett megkeresett cég, nem pedig az a magánszemély, akinek az adatairól szó van.

A VII. melléklet nem tartalmaz további információt a jogszabályokból fakadó lehetséges jogorvoslatokra vonatkozóan, amelyek a nem egyesült államokbeli személyek rendelkezésére állnak, amikor a hatóságok vagy cégek jogszerűtlenül biztosítanak vagy szereznek hozzáférést adataik tartalmához.

A munkacsoport üdvözli azt a tényt, hogy a közelmúltban elfogadott, a bírósági jogorvoslatról szóló törvény[93] a nem egyesült államokbeli személyek részére is jogorvoslathoz való jogokról rendelkezik. Ezek a jogok ugyanakkor egyértelműen meghatározott jogcímekre korlátozottak: a kijavításhoz és az adatokhoz való hozzáféréshez, továbbá az ügyvédi díjakra való jog, amikor egy „kijelölt szövetségi hivatal vagy egység" megtagadja az adatok módosítását vagy az ilyen adatokhoz való hozzáférést, és a polgári jogi jogorvoslatokhoz való jogot az adatok „szándékos" közzétételével kapcsolatos esetekben.

Ezen túlmenően a határozattervezet vonatkozó preambulumbekezdéseinek lábjegyzeteiben feltüntetett egyesült államokbeli ítélkezési gyakorlat – különösen a City of Ontario kontra Quon[94], a Maryland kontra King[95] és a Samson kontra California[96] ügyekben – nem releváns annak értékeléséhez, hogy egy nem egyesült államokbeli személy keresetet nyújthat-e be bíróságra a magánéletével kapcsolatos beavatkozás jogszerűségének vitatása érdekében[97].

[91] VII. melléklet, 4. oldal.
[92] A megfelelőségi határozattervezet (108) preambulumbekezdése.
[93] A bírósági jogorvoslatról szóló 2015. évi törvény, H.R. 1428.
[94] *City of Ontario, Cal. kontra Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland kontra King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson kontra California*, 547 U.S. 843, 848 (2006).
[97] Az *Ontario kontra Quon* ügyben a bíróság megállapította, hogy Ontario városa nem sértette meg alkalmazottainak a negyedik alkotmánykiegészítésben biztosított jogait, mivel a város hozzáférése a szóban forgó alkalmazott magánjellegű

Valamennyi ügy egyesült államokbeli személyek magánélethez való jogával kapcsolatos, és mindegyik az Egyesült Államok Legfelsőbb Bíróságának olyan határozatait tartalmazza, amelyek valójában a negyedik alkotmánykiegészítés alkalmazását korlátozzák.

Összegezve a WP29 elismeri és üdvözli a bírósági jogorvoslatról szóló törvény elfogadását, de kétségei vannak a tekintetben, hogy a hatékony jogorvoslatok valóban az egyes érintettek rendelkezésére állnak-e.

4.3. Záró megjegyzések

A WP29 üdvözli és elismeri az Egyesült Államok kormányának arra irányuló erőfeszítését, hogy az EU–USA adatvédelmi pajzs keretében bűnüldözési célokra továbbított személyes adatokba való beavatkozásra vonatkozó jogi keretre vonatkozóan több tájékoztatást nyújtson, ideértve az alkalmazandó korlátozásokat és biztosítékokat.

WP29 megjegyzi, hogy az Egyesült Államokban a bűnüldöző hatóságok nyomozási eszközeinek rendszere – ideértve az alkalmazandó korlátozásokat és biztosítékokat is – széles körű és összetett, az adatvédelmi pajzsban szereplő információ pedig csekély. A munkacsoport ezért sajnálja, hogy a korlátozott (vagyis az adatvédelmi pajzs VII. mellékletében és a határozattervezet megállapításaiban szereplő) információ alapján jelenleg nem tud átfogó értékelést nyújtani az alkalmazandó szabályok hozzáférhetőségéről, előreláthatóságáról, valamint szükségességéről és arányosságáról. A WP29-nek az e véleményében az adatvédelmi pajzzsal kapcsolatosan tett más megállapításaitól függetlenül egy ilyen értékelés az adatvédelmi pajzs éves felülvizsgálatának részét képezheti.

A bűnüldöző hatóságok hozzáférését illetően a WP29 megjegyzi, hogy szemlátomást meglehetősen erős, független felügyeleti mechanizmus létezik erre nézve. Ezen túlmenően a munkacsoport üdvözli a bírósági jogorvoslatról szóló törvény elfogadását, amely bírósági jogorvoslathoz való jogokat biztosít a nem egyesült államokbeli személyeknek. Ugyanakkor a WP29 felhívja a figyelmet arra, hogy e jogok korlátozott jellegűek. Azon megállapításon túl, hogy egy nem egyesült államokbeli személy nem vitathatná a parancsokat vagy bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat bíróság előtt a negyedik alkotmánymódosítás felhívásával, aggályok maradnak arra nézve is, hogy ténylegesen rendelkezésre állnak-e hatékony jogorvoslatok az egyedi érintettek számára a bűnüldözés területén.

5. KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK

A WP29 először is üdvözli a tényt, hogy a védett adatkikötőről szóló határozat érvénytelenítését követő öt hónapon belül előterjesztettek egy új megfelelőségi

---

üzeneteinek tartalmához ésszerű volt, mivel jogszerű munkához kapcsolódó cél motiválta és hatóköre nem volt túlzott mértékű. A *Samson kontra California* ügyben a bíróság megállapította, hogy „a negyedik alkotmánykiegészítés nem tiltja meg egy rendőr számára egy feltételesen szabadlábra helyezett személy gyanú nélküli átkutatásának elvégzését”. A *Maryland kontra King* ügyben a bíróság megállapította, hogy amikor a rendőrök valószínű indok alapján egy súlyos bűncselekménnyel gyanúsítható személyt letartóztatnak és a rendőrségre viszik, hogy őrizetbe vegyék, a letartóztatott személytől szájüregéből DNS-mintát vesznek és azt elemzik, az az ujjnyomatvételhez és a fényképkészítéshez hasonló jogszerű rendőrségi nyilvántartásba vételi eljárás, amely a negyedik alkotmánykiegészítés keretében ésszerűnek minősül.

határozattervezetet, amely a korábbi mechanizmushoz képest számos előrelépést tartalmaz. A munkacsoport különösen nagyra értékeli a két adatvédelmi pajzs lista bevezetése által nyújtott fokozott átláthatóságot, amelyek a Kereskedelmi Minisztérium honlapján találhatók: az egyik lista az adatvédelmi pajzsban részt vevő szervezetek nyilvántartása, a másik pedig azon szervezeteké, amelyek korábban részt vettek az adatvédelmi pajzsban, de immár nem. A munkacsoport szintén örömmel üdvözli az adatvédelmi pajzs keretében – akár nemzetbiztonsági, akár bűnüldözési célokból – továbbított adatokhoz való nyilvános hozzáféréssel kapcsolatos fokozott átláthatóságot. Végül a WP29 nagy örömmel fogadta, hogy az Egyesült Államokba történő valamennyi adattovábbítás azonos védelmet élvez majd: nincs olyan konkrét jogi rendelkezés, amelyik egyik eszköznek a másikkal szemben előnyt biztosítana.

5.1. Három aggályos pont

Ugyanakkor három fő aggályos pont áll fenn továbbra is, amelyeket a WP29 álláspontja szerint kezelni kell.

Az első az, hogy a megfelelőségi határozattervezetben használt nyelv nem kötelezi a szervezeteket az adatok törlésére, amennyiben azokra már nincs szükség. Az uniós adatvédelmi jog alapvető eleme annak biztosítása, hogy az adatokat nem tárolják tovább, mint ameddig az az adatgyűjtés céljának eléréséhez szükséges. Másodszor, a WP29 úgy értelmezi a VI. mellékletet, hogy az Egyesült Államok kormánya nem zárja ki teljes körűen a tömeges és válogatás nélküli adatgyűjtés folytatását. A WP29 következetesen azon az álláspontón van, hogy az ilyen adatgyűjtés jogosulatlan beavatkozás a magánszemélyek alapvető jogaiba. A harmadik aggályos pont az ombudsmani mechanizmus bevezetésével kapcsolatos. Bár a munkacsoport üdvözli ez a példa nélküli lépést, amely további jogorvoslati lehetőséges és felülvizsgálati mechanizmust hoz létre a magánszemélyek számára, fennáll az aggály arra nézve, hogy az ombudsman elégséges jogkörrel rendelkezik-e a hatékony működéshez. Legalább az ombudsman hatásköreit és helyzetét kell egyértelműsíteni annak érdekében, hogy kimutatható legyen a szerep tényleges függetlensége, és hatékony jogorvoslatot tudjon biztosítani a nem megfelelő adatkezeléssel szemben.

5.2. Ajánlott egyértelműsítések

A fent említett pontokon túlmenően a WP29 ezen véleményben több pontot jelzett, ahol a megfelelőségi határozat további egyértelműsítése szükséges. A legfontosabb e tekintetben annak biztosítása, hogy az adatvédelmi pajzsban használt alapvető adatvédelmi fogalmakat egységesen határozzák meg és alkalmazzák. Jelenleg nem ez a helyzet. A munkacsoport üdvözölné, ha az adatvédelmi pajzzsal kapcsolatos gyakori kérdések közé beiktatnák az ideális esetben az EU és az USA közötti egyeztetéssel összeállított fogalmak meghatározását tartalmazó glosszáriumot. A WP29 megállapítja továbbá, hogy az uniós személyes adatok harmadik fél részére történő továbbítása nincs kielégítően szabályozva, különösen az adattovábbítás hatókörét, célhoz kötöttségét, és a megbízott részére történő adattovábbításra vonatkozó biztosítékokat illetően. Aggályos a bűnüldöző hatóságok által az adatvédelmi pajzs adataihoz való hozzáférés, különösen a jogalkotás előreláthatósága, az Egyesült Államok

bűnüldöző rendszerének szövetségi és állami szinten egyaránt kiterjedt és összetett jellege, valamint a megfelelőségi határozatban szereplő információk korlátozott volta miatt.

Az adatvédelmi pajzs az első megfelelőségi határozat, amelyet azóta készítettek, hogy a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló rendelet szövegtervezeteiről elvi egyetértés született. A magánszemélyek számára nyújtott adatvédelem szintjének számos előrelépése mégsem tükröződik az adatvédelmi pajzsban. A WP29 ezért azt javasolja, hogy e megfelelőségi határozat, valamint a más harmadik országok számára kibocsátott megfelelőségi határozatok felülvizsgálatára nem sokkal azt követően sort kell keríteni, hogy a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló rendelet hatályba lép.

A WP29 utolsó itt kiemelendő ajánlása a közös felülvizsgálatra vonatkozik. A munkacsoport üdvözli azt a tényt, hogy az adatvédelmi pajzs megfelelőségi határozatát valóban éves szinten felülvizsgálják majd, az adatvédelmi hatóságok és más érdekelt felek széles körű részvétele mellett. A munkacsoport javasolja a közös felülvizsgálatok elemeiről az első felülvizsgálatot jóval megelőzően történő megállapodást, ideértve a felülvizsgálati jelentés összeállítását és közzétételét.