A 29. CIKK SZERINTI ADATVÉDELMI MUNKACSOPORT

18/HU

WP 254 rev.01

A 29. cikk alapján létrehozott munkacsoport

Megfelelőségi referencia

Elfogadás időpontja: 2017. november 28.

A legutóbbi felülvizsgálat és elfogadás időpontja: 2018. február 6.

Bevezetés

Az uniós adatvédelmi hatóságok munkacsoportja[1] (a továbbiakban: WP29) korábban közzétette a személyes adatok harmadik országokba történő továbbításáról szóló munkadokumentumot (a továbbiakban: WP12)[2]. Mivel az irányelvet felváltotta az általános uniós adatvédelmi rendelet (a továbbiakban: GDPR)[3], a WP29 felülvizsgálja a korábbi iránymutatását, a WP12-t, hogy az új jogszabály és az Európai Unió Bírósága (a továbbiakban: EUB) újabb ítélkezési gyakorlatának[4] fényében módosítsa azt.

Ez a munkadokumentum a WP12 első fejezetét kívánja módosítani, amely a harmadik ország, az adott harmadik ország valamely területe vagy egy vagy több meghatározott ágazata vagy a nemzetközi szervezetek (a továbbiakban: „harmadik országok vagy nemzetközi szervezetek") megfelelő adatvédelmi szintjének központi kérdésével foglalkozik. A következő években a GDPR alkalmazása során szerzett gyakorlati tapasztalatok alapján a dokumentum felülvizsgálatára és szükség esetén módosítására rendszeresen sor fog kerülni. A WP12 2. (*A 108. egyezményt ratifikáló országokra vonatkozó megközelítés alkalmazása*) és 3. (*Az ágazati önszabályozásra vonatkozó megközelítés alkalmazása*) fejezetének felülvizsgálata a későbbiekben fog megtörténni.

Ez a munkadokumentum kizárólag a megfelelőségi határozatokra fókuszál, amelyek az Európai Bizottságnak a GDPR 45. cikke alapján elfogadott végrehajtási jogi aktusai[5]. A személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítása egyéb szempontjainak vizsgálatára későbbi munkadokumentumokban kerül sor, amelyeket külön teszünk közzé (kötelező erejű vállalati szabályok, eltérések).

Ez a dokumentum a GDPR alapján kíván iránymutatást nyújtani az Európai Bizottságnak és a WP29-nek a harmadik országok és nemzetközi szervezetek adatvédelmi szintjének értékelése során azzal, hogy meghatározza azokat az alapvető adatvédelmi elveket, amelyeknek az uniós jogi kerettel való lényegi azonosság biztosítása érdekében szerepelniük kell a harmadik ország jogi keretében vagy a nemzetközi szervezet szabályaiban. Ezenkívül segítséget nyújthat azoknak a harmadik országoknak és nemzetközi szervezeteknek, amelyek el akarják érni a megfelelő szintet. Az ebben a munkadokumentumban meghatározott elvek azonban nem közvetlenül az adatkezelőket vagy az adatfeldolgozókat célozzák.

A dokumentum négy fejezetből áll:

1. fejezet: Néhány általános információ a megfelelőség fogalmával kapcsolatban

2. fejezet: A megfelelőségre vonatkozó megállapítások eljárásjogi vonatkozásai a GDPR szerint

3. fejezet: Általános adatvédelmi elvek. Ez a fejezet azokat az alapvető általános adatvédelmi elveket tartalmazza, amelyek szükségesek annak biztosításához, hogy az adott harmadik ország vagy nemzetközi szervezet adatvédelmi szintje lényegében egyenértékű legyen az uniós jogszabályok által meghatározott szinttel.

4. fejezet: A bűnüldözői és nemzetbiztonsági szervek hozzáférésére vonatkozó lényeges garanciák az alapvető jogokba való beavatkozás korlátozása érdekében. Ez a fejezet az EUB által a Schrems-ügyben hozott 2015. évi ítélet és a WP29 2016-ban elfogadott, lényeges garanciákról szóló munkadokumentuma alapján meghatározott, a bűnüldözői és nemzetbiztonsági szervek hozzáférésére vonatkozó lényeges garanciákat tartalmazza.

---

[1] A 95/46/EK uniós adatvédelmi irányelv 29. cikke szerint jött létre.

[2] WP12, „Munkadokumentum: Személyes adatok továbbítása harmadik országokba: Az európai uniós adatvédelmi irányelv 25. és 26. cikkének alkalmazása", amelyet a munkacsoport 1998. július 24-én fogadott el.

[3] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg).

[4] Beleértve a C-362/14. sz., Maximillian Schrems kontra adatvédelmi biztos ügyben 2015. október 6-án hozott ítéletet.

[5] A végrehajtási jogi aktusokkal kapcsolatos további információkat lásd a GDPR 45. cikkének (3) bekezdésében és 93. cikkének (2) bekezdésében.

1. fejezet: Néhány általános információ a megfelelőség fogalmával kapcsolatban

A GDPR 45. cikkének (1) bekezdése meghatározza azt az elvet, amely szerint a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha a harmadik ország, a harmadik ország valamely területe vagy egy vagy több meghatározott ágazata vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít.

A már a 95/46/EK irányelv alapján is létező, „megfelelő adatvédelmi szintre" vonatkozó elvet az EUB továbbfejlesztette. Itt fontos emlékeztetni arra a normára, amelyet az EUB a Schrems-ítéletben határozott meg, azaz, hogy bár a harmadik országban az „*adatvédelem szintjének*" az EU-n belül biztosított szinttel „*lényegében azonosnak" kell lennie, „azok az eszközök, amelyeket a harmadik ország az ilyen védelmi szint biztosításához e tekintetben igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket (...) az Unióban alkalmaznak,"*[6]*. Ennek értelmében a cél nem az uniós jogszabályok pontról pontra történő lemásolása, hanem a jogszabályok lényegi – alapvető követelményeinek kialakítása.*

Az Európai Bizottság által hozott megfelelőségi határozatok célja, hogy a tagállamokra nézve kötelező hatállyal[7], hivatalosan is megerősítsék, hogy az adott harmadik ország vagy nemzetközi szervezet adatvédelmi szintje lényegében megegyezik az Európai Unió adatvédelmi szintjével[8]. A megfelelőség az érintettek számára biztosított jogok és az adatok kezelését végzők vagy az adatkezelést felügyelők és az ellenőrzést gyakorló független szervezetek számára előírt kötelezettségek kombinációjával érhető el. Az adatvédelmi szabályok azonban csak akkor hatékonyak, ha a gyakorlatban is kikényszeríthetők és betarthatók. Ezért a szabályok hatékonyságának biztosítása érdekében nem csupán a harmadik országokba vagy nemzetközi szervezetek részére továbbított személyes adatokra vonatkozó szabályok tartalmát kell figyelembe venni, hanem a bevezetett rendszert is. A hatékony végrehajtási mechanizmusok elengedhetetlenek az adatvédelmi szabályok hatékonysága szempontjából.

A GDPR 45. cikkének (2) bekezdése meghatározza azokat az elemeket, amelyeket az Európai Bizottságnak figyelembe kell vennie az adott harmadik ország vagy nemzetközi szervezet adatvédelmi szintje megfelelőségének értékelése során.

A Bizottságnak például figyelembe kell vennie a jogállamiságot, az emberi jogok és alapvető szabadságok betartását, a vonatkozó jogszabályokat, az egy vagy több független felügyeleti hatóság meglétét és tényleges működését, valamint a harmadik ország vagy nemzetközi szervezet nemzetközi kötelezettségvállalásait.

Ezért egyértelmű, hogy a megfelelő védelem érdemi elemzésének két alapvető elemből kell állnia: a hatályos szabályok tartalmának és az azok hatékony alkalmazását biztosító eszközök vizsgálatából. Az Európai Bizottság feladata rendszeresen ellenőrizni, hogy a bevezetett szabályok a gyakorlatban is hatékonyak-e.

Az „alapvető" „tartalmi" adatvédelmi elvek és az „eljárási/végrehajtási" követelmények, amelyek a védelem megfelelőségének minimumkövetelményei, az Európai Unió Alapjogi Chartáján és a GDPR-en alapulnak. Figyelembe kell venni továbbá az egyéb nemzetközi adatvédelmi szerződéseket is, például a 108. egyezményt[9].

Figyelmet kell fordítani az állami hatóságok személyes adatokhoz való hozzáférésének jogi keretére is. Ezzel kapcsolatban a megfigyelésre vonatkozó garanciákról szóló 237. sz. munkadokumentumban (azaz a lényeges garanciákról szóló dokumentumban)[10] található további iránymutatás.

---

[6] A C-362/14. sz., Maximillian Schrems kontra adatvédelmi biztos ügyben 2015. október 6-án hozott ítélet 73–74. pontja;

[7] Az EUMSZ 288. cikkének (2) bekezdése.

[8] A C-362/14. sz., Maximillian Schrems kontra adatvédelmi biztos ügyben 2015. október 6-án hozott ítélet 52. pontja;

[9] A GDPR (105) preambulumbekezdése.

[10] 01/2016. sz. munkadokumentum a személyes adatok kezelése során a megfigyelési intézkedéseken keresztül a magánélettel és az adatvédelemmel kapcsolatos alapvető jogokba történő beavatkozás indoklásáról (lényeges európai garanciák), 16/EN WP 237, 2016. április 13.

A harmadik ország adatvédelemmel és magánélettel kapcsolatos általános rendelkezései nem elegendők. Épp ellenkezőleg, az adatvédelemhez való jog gyakorlati szempontból releváns aspektusaira vonatkozó konkrét igényeket célzó, kifejezett rendelkezéseket kell bevezetni a harmadik ország vagy nemzetközi szervezet jogi keretébe. Ezeknek a rendelkezéseknek kikényszeríthetőnek kell lenniük.

2. fejezet: A megfelelőségre vonatkozó megállapítások eljárásjogi vonatkozásai a GDPR szerint

Annak érdekében, hogy az Európai Adatvédelmi Testület eleget tegyen a GDPR 70. cikkének (1) bekezdésének s) pontjában meghatározott, Európai Bizottság számára nyújtott tanácsadói feladatoknak, az Európai Adatvédelmi Testület rendelkezésére kell bocsátani a releváns dokumentációt, beleértve az Európai Bizottság kapcsolódó levelezését és megállapításait. Összetett jogi keret esetén a dokumentáció magában foglalja a harmadik ország vagy nemzetközi szervezet adatvédelmi szintjéről szóló jelentést is. Az Európai Bizottság által rendelkezésre bocsátott tájékoztatásnak minden esetben teljes körűnek kell lennie, és lehetővé kell tennie az Európai Adatvédelmi Testület számára, hogy elvégezze a harmadik ország adatvédelmi szintjével kapcsolatos saját értékelését. Az Európai Adatvédelmi Testület megfelelő időn belül véleményt ad ki az Európai Bizottság megállapításairól, és adott esetben azonosítja a megfelelőségi keret hiányosságait. Az Európai Adatvédelmi Testület továbbá törekszik arra, hogy az esetleges hiányosságokkal kapcsolatban módosításokat vagy kiegészítéseket javasoljon.

A GDPR 45. cikkének (4) bekezdésével összhangban az Európai Bizottság feladata, hogy folyamatosan figyelemmel kísérje azon fejleményeket, amelyek érinthetik a megfelelőségi határozatok végrehajtását.

A GDPR 45. cikkének (3) bekezdése előírja, hogy rendszeresen, legalább négyévente felülvizsgálatot kell végezni. Ez azonban általános időkeret, amelyet a megfelelőségi határozattal az adott harmadik országhoz vagy nemzetközi szervezethez kell igazítani. Az adott körülményektől függően rövidebb felülvizsgálati ciklust is elő lehet írni. Ezenkívül bizonyos incidensek vagy az adott harmadik ország vagy nemzetközi szervezet jogi keretével kapcsolatos egyéb információk vagy változások is előidézhetik az ütemterv előtti felülvizsgálat szükségességét. Célszerű továbbá a teljesen új megfelelőségi határozat első felülvizsgálatát minél hamarabb elvégezni, majd az eredménytől függően fokozatosan módosítani a felülvizsgálati ciklust.

Mivel az Európai Adatvédelmi Testület feladata, hogy az Európai Bizottság rendelkezésére bocsássa a véleményét arról, ha a harmadik ország, a harmadik ország valamely területe vagy meghatározott ágazata vagy valamely nemzetközi szervezet már nem biztosítja a megfelelő adatvédelmi szintet, az Európai Adatvédelmi Testületnek megfelelő időben meg kell kapnia az érdemi információkat az adott harmadik ország vagy nemzetközi szervezet kapcsolódó fejleményeinek Bizottság általi nyomon követéséről. Ennek értelmében az Európai Adatvédelmi Testületet az adott harmadik országban vagy nemzetközi szervezetnél végzett, valamennyi felülvizsgálati folyamatról és felülvizsgálati kiküldetésről tájékoztatni kell. Az Európai Adatvédelmi Testület örömmel venné, ha meghívást kapna a felülvizsgálati folyamatokon és felülvizsgálati kiküldetéseken való részvételre.

Szintén fontos megjegyezni, hogy a GDPR 45. cikkének (5) bekezdésével összhangban az Európai Bizottságnak joga van ahhoz, hogy a megfelelőségi határozatokat hatályon kívül helyezze, módosítsa vagy felfüggessze. A hatályon kívül helyezésre, módosításra vagy felfüggesztésre irányuló eljárásokban értelemszerűen részt kell vennie az Európai Adatvédelmi Testületnek is a 70. cikk (1) bekezdésének s) pontja alapján történő véleménykérésen keresztül.

Ahogyan a GDPR 58. cikkének (5) bekezdése elismeri, valamint az EUB Schrems-ügyben hozott ítéletével összhangban az adatvédelmi hatóságoknak képesnek kell lenniük arra, hogy jogi eljárást kezdeményezzenek, ha a megfelelőségi határozat ellen benyújtott panaszt megalapozottnak ítélik: *„A nemzeti jogalkotó feladata, hogy előírja azon jogorvoslati lehetőségeket, amelyek lehetővé teszik az érintett nemzeti felügyeleti hatóság számára, hogy a nemzeti bíróságok előtt az általa megalapozottnak talált kifogásokra hivatkozzon annak érdekében, hogy amennyiben az utóbbiak*

osztják e hatóságnak a bizottsági határozat érvényessége tekintetében fennálló kétségeit, előzetes döntéshozatali eljárást kezdeményezhessenek e határozat érvényességének vizsgálata céljából”[11].

[11] A C-362/14. sz., Maximillian Schrems kontra adatvédelmi biztos ügyben 2015. október 6-án hozott ítélet 65. pontja.

3. fejezet: Általános adatvédelmi elvek annak biztosítása érdekében, hogy az adott harmadik ország, annak bármely területe vagy egy vagy több meghatározott ágazata vagy az adott nemzetközi szervezet adatvédelmi szintje lényegében megegyezzen az uniós jogszabályok által biztosított szinttel

Az adott harmadik ország vagy nemzetközi szervezet rendszerének az alábbi alapvető tartalommal és eljárási/végrehajtási adatvédelmi elvekkel és mechanizmusokkal kell rendelkeznie:

A. <u>Tartalmi elvek:</u>

1) Fogalmak

Alapvető adatvédelmi elképzeléseket és/vagy elveket kell kialakítani. Ezeknek nem kell a GDPR terminológiáját tükrözniük, azonban meg kell felelniük az európai adatvédelmi jogszabályokban megfogalmazott kifejezéseknek. A GDPR például az alábbi fontos kifejezéseket használja: „személyes adatok”, „a személyes adatok kezelése”, „adatkezelő”, „adatfeldolgozó”, „címzett” és „érzékeny adatok”.

2) A jogos célokból végzett jogszerű és tisztességes adatkezelés alapjai

Az adatokat jogszerűen, tisztességesen és jogos célból kell kezelni.

A jogszerű, tisztességes és jogos célból végzett személyesadat-kezelés jogalapjait kellően egyértelműen kell meghatározni. Az európai jogi keret számos jogszerű jogalapot ismer el, beleértve például a nemzeti jog rendelkezéseit, az érintett hozzájárulását, a szerződés teljesítését vagy az adatkezelő vagy harmadik fél jogos érdekeit, amelyek nem írják felül az érintett érdekeit.

3) A célhoz kötöttség elve

Az adatokat konkrét célból kell kezelni, és később csak olyan mértékben lehet használni, amely nem inkompatibilis az adatkezelés céljával.

4) Az adatminőség és az arányosság elve

az adatoknak pontosnak, és szükség esetén naprakésznek kell lenniük. Az adatoknak a feldolgozási célokhoz képest megfelelőnek és relevánsnak kell lenniük, és azokkal arányban kell állniuk.

5) Az adatmegőrzés elve

Az adatokat általános szabályként csak az adatkezelés céljai érdekében feltétlenül szükséges ideig lehet megőrizni.

6) A biztonság és a titoktartás elve

A személyes adatokat kezelő jogi személyeknek biztosítaniuk kell, hogy a személyes adatok kezelésére a személyes adatok biztonságát garantáló módon kerüljön sor, beleértve a jogosulatlan vagy jogszabályellenes adatkezelés, valamint a véletlenszerű elvesztés, megsemmisítés vagy károsodás elleni védelmet a megfelelő technikai és szervezési intézkedések alkalmazásával. A biztonsági szint tervezésénél figyelembe kell venni a legmodernebb technikákat és a kapcsolódó költségeket.

7) Az átláthatóság elve

Minden érintettet egyértelmű, könnyen hozzáférhető, tömör, átlátható és érthető módon kell tájékoztatni a személyes adatai kezelésének főbb elemeiről. A tájékoztatásnak ki kell térnie az adatkezelés céljára, az adatkezelő személyére, az érintett számára elérhető jogokra, valamint egyéb információkra, amennyiben azok a tisztességes eljárás biztosítása érdekében szükségesek. Bizonyos körülmények között a tájékoztatáshoz való jog alól vannak kivételek, például a büntetőeljárások, nemzetbiztonsági kérdések, a bírói függetlenség és az igazságügyi eljárások vagy egyéb fontos, közérdekű célok védelme érdekében, mint a GDPR 23. cikkében foglaltak esetében.

8) A hozzáféréshez, helyesbítéshez, törléshez és tiltakozáshoz való jog

Az érintett számára biztosítani kell, hogy megerősítést tudjon szerezni arról, hogy személyes adatait kezelik-e vagy nem, valamint hogy hozzáférjen a személyes adataihoz, beleértve a kezelt személyes adatairól készült másolat megszerzésének lehetőségét.

Az érintett számára biztosítani kell, hogy adatai helyesbítését tudja kérni a meghatározott okokból, például ha azok nem pontosak vagy nem teljesek, valamint hogy személyes adatai törlését tudja kérni, ha például az adatkezelés már nem szükséges vagy nem jogszerű.

Az érintettnek biztosítani kell azt is, hogy a helyzetével kapcsolatos kényszerítő erejű indokok alapján bármikor tiltakozni tudjon a személyes adatai kezelése ellen a harmadik ország jogi keretében meghatározott feltételek függvényében. A GDPR-ben például ezen feltételek közé tartozik, ha az adatkezelés a közérdek érdekében végzett feladat teljesítése, az adatkezelőre ruházott közhatalmi jogosítványok gyakorlása vagy az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítése érdekében szükséges.

E jogok gyakorlása nem lehet aránytalanul megterhelő az érintett számára. E jogok bizonyos esetben korlátozottak lehetnek, például a büntetőeljárások, nemzetbiztonsági kérdések, a bírói függetlenség és az igazságügyi eljárások vagy egyéb fontos, közérdekű célok védelme érdekében, mint a GDPR 23. cikkében foglaltak esetében.

9) Az újbóli adattovábbítás korlátozása

A személyes adatoknak az eredeti adattovábbítás elsődleges címzettje általi újbóli továbbítása kizárólag akkor lehet engedélyezett, ha a további címzettekre (azaz az újbóli adattovábbítás címzettjeire) olyan szabályok (beleértve a szerződéses szabályokat) vonatkoznak, amelyek megfelelő adatvédelmi szintet biztosítanak, és követik az adatkezelő nevében végzett adatkezelésre vonatkozó utasításokat. Az adattovábbítással érintett természetes személyek védelmének szintjét az újbóli adattovábbítás nem csökkentheti. Az EU-ból továbbított adatok első címzettje felelős azért, hogy megfelelőségi határozat hiányában meggyőződjön az újbóli adattovábbításra vonatkozó megfelelő garanciák előírásáról. Ezekre az újbóli adattovábbításokra kizárólag korlátozott és meghatározott célokból kerülhet sor, és kizárólag abban az esetben, ha az adatkezelésnek van jogalapja.

B. <u>Példák az egyes adatkezelési típusokra alkalmazandó további tartalmi elvekre:</u>

1) Speciális adatkategóriák

Speciális adatkategóriák esetén külön garanciákat kell bevezetni[12]. Ezeknek a kategóriáknak meg kell felelniük a GDPR 9. és 10. cikkében foglaltaknak. Ezt a védelmet az adatkezelésre vonatkozó szigorúbb követelményeken keresztül kell biztosítani, mint az érintettnek az adatkezeléshez való kifejezett hozzájárulása vagy további biztonsági intézkedések révén.

[12] Ezeket a különleges kategóriákat a GDPR (10) preambulumbekezdése „érzékeny adatokként” említi.

2) Közvetlen üzletszerzés

Ha az adatok kezelésére közvetlen üzletszerzési célokból kerül sor, az érintettnek bármikor képesnek kell lennie az ilyen típusú adatkezelés elleni tiltakozásra további költségek nélkül.

3) Automatizált döntéshozatal és profilalkotás

A kizárólag automatizált adatkezelésen (egyedi ügyekben történő automatizált döntéshozatal), beleértve a profilalkotást is, alapuló döntésekre, amelyek az érintettre nézve jogi vagy egyéb jelentős következménnyel járnak, kizárólag a harmadik ország jogi keretében meghatározott, bizonyos körülmények között kerülhet sor. Az európai jogi keretben ezen feltételek közé tartozik például az érintett kifejezett hozzájárulásának szükségessége vagy a döntés szerződés megkötéséhez való szükségessége. Ha a döntés nem felel meg a harmadik országi jogi keretében lefektetett feltételeknek, az érintettnek joga van ahhoz, hogy kivonja magát az automatizált döntéshozatal alól. A harmadik ország jogszabályainak minden esetben biztosítania kell a szükséges garanciákat, beleértve a döntéshozatal mögött rejlő okokkal és az alkalmazott logikával kapcsolatos tájékoztatáshoz, a pontatlan vagy nem teljes információk helyesbítéséhez, valamint a helytelen tényálláson alapuló döntéshozatal ellen tiltakozáshoz való jogot.

C. <u>Az eljárási és végrehajtási mechanizmusok:</u>

Bár azok az eszközök, amelyeket az adott harmadik ország a megfelelő adatvédelmi szint biztosítása érdekében alkalmaz, eltérhetnek az Európai Unión belül alkalmazott eszközöktől[13], az európai rendszerrel összhangban lévő rendszereket az alábbi elemek meglétének kell jellemeznie:

1) Illetékes független felügyeleti hatóság

A harmadik országban lennie kell egy vagy több független felügyeleti hatóságnak, amely az adatvédelmi és magánélet védelmét célzó rendelkezéseknek való megfelelés nyomon követéséért és biztosításáért felelős. A felügyeleti hatóságnak teljesen függetlenül és pártatlanul kell eljárnia kötelességei teljesítése és jogkörei gyakorlása során, és e tekintetben nem kérhet és nem fogadhat el utasításokat. Ezzel kapcsolatban az adatvédelmi jogoknak való megfelelés és a tájékoztatás előmozdításának biztosítása érdekében a felügyeleti hatóság számára biztosítani kell minden szükséges és elérhető jogot és hatáskört. Nem szabad megfeledkezni a felügyeleti hatóság személyzetéről és költségvetéséről sem. A felügyeleti hatóságnak képesnek kell lennie arra, hogy saját kezdeményezésére vizsgálatokat folytasson.

2) Az adatvédelmi rendszernek a szabályok betartásának jó szintjét kell biztosítania

A harmadik ország rendszerének az adatkezelők és az ő nevükben adatokat kezelő jogi személyek magas szintű elszámoltathatóságát és kötelezettségeik, feladataik és felelősségeik ismeretét, valamint az érintetti jogok és az azok gyakorlására irányuló eszközök érintettek általi ismeretét kell biztosítania. A hatékony és elrettentő hatású szankciók fontos szerepet játszhatnak a szabályok betartásának biztosításában, éppen úgy, mint a hatóságok, ellenőrök vagy független adatvédelmi tisztviselők közvetlen ellenőrzései.

3) Elszámoltathatóság

[13] A C-362/14. sz., Maximillian Schrems kontra adatvédelmi biztos ügyben 2015. október 6-án hozott ítélet 74. pontja.

A harmadik ország adatvédelmi jogi keretének a jogszabályoknak való megfelelésre és annak az illetékes adatvédelmi hatóság felé történő igazolására kell kötelezni az adatkezelőket és/vagy a nevükben adatokat kezelő jogi személyeket. Ezek az intézkedések magukban foglalhatják például az adatvédelmi hatásvizsgálatokat, az adatkezelési tevékenységekről készített nyilvántartások vagy naplófájlok megfelelő ideig történő megőrzését, adatvédelmi tisztviselő kinevezését vagy a beépített és alapértelmezett adatvédelmet.

4) Az adatvédelmi rendszernek támogatást és segítséget kell nyújtania az érintetteknek a jogaik és a megfelelő jogorvoslati mechanizmusok gyakorlása során

Az érintett jogainak gyors és hatékony, valamint túlzott költségek nélküli gyakorlása és a megfelelés biztosítása érdekében az érintettnek képesnek kell lennie arra, hogy jogorvoslatot vegyen igénybe. Ehhez olyan felügyeleti mechanizmusokat kell bevezetni, amelyek lehetővé teszik a panaszok független vizsgálatát és az adatvédelmi és magánélethez való jogok megsértésének feltárását és gyakorlati szankcionálását.

A szabályok be nem tartása esetén az érintett számára hatékony közigazgatási és igazságügyi jogorvoslatot kell biztosítani, beleértve a jogszerűtlen személyesadat-kezelés eredményeként felmerülő károk megtérítését. Ez olyan kulcsfontosságú elem, amelynek adott esetben kártérítések megfizettetését és szankciók elrendelését lehetővé tevő, független, bíróság előtti vitarendezési vagy választottbíráskodási rendszert kell tartalmaznia.

4. fejezet: A bűnüldözői és nemzetbiztonsági szervek hozzáférésére vonatkozó lényeges garanciák a harmadik országokban az alapvető jogokba való beavatkozás korlátozása érdekében

A védelmi szint megfelelőségének értékelésekor a 45. cikk (2) bekezdésének a) pontja alapján a Bizottságnak az alábbiakat kell figyelembe vennie: „*a vonatkozó általános és ágazati jogszabályok, köztük a közbiztonságra, a védelemre, valamint a nemzetbiztonságra vonatkozó és a büntetőjogi rendelkezések, a közhatalmi szerveknek a személyes adatokhoz való hozzáférését szabályozó rendelkezések, valamint e jogszabályok végrehajtása (...)".*

A Schrems-ügyben hozott ítéletben az EUB megjegyezte, 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/EK irányelv által biztosított védelmi szinttel lényegében azonos védelmi szintet biztosítson ténylegesen az alapvető jogok és szabadságok számára*". Jóllehet azok az eszközök, amelyeket a harmadik ország e tekintetben igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket az Európai Unióban alkalmaznak, ezen eszközöknek a gyakorlatban mégis hatékonynak kell lenniük[14].

E tekintetben a Bíróság kritikus módon megjegyezte, hogy a minimum mentesítési szabályra vonatkozó korábbi határozat „*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, e beavatkozásokat az állami szervek megengedik, amennyiben azok jogszerű célokat követnek, mint például a nemzetbiztonság*".

A WP29 a 2016. április 13-i, WP237. sz. véleményében azonosította azokat a lényeges garanciákat, amelyek tükrözik az EUB és az emberi jogok európai egyezményének joggyakorlatát a megfigyelés terén. Míg a WP237. sz. véleményben foglalt ajánlások továbbra is érvényesek, és figyelembe kell venni őket a harmadik ország megfigyelés terén való megfelelőségének értékelésekor, e garanciák alkalmazása eltérhet a bűnüldözési szervek és a nemzetbiztonsági szervek adatokhoz való hozzáférésének tekintetében. A megfelelőség érdekében azonban minden harmadik országnak be kell tartania ezt a négy garanciát az adatokhoz való hozzáférés esetében, akár nemzetbiztonsági, akár bűnüldözési célokról van szó:

1) **Az adatkezelésnek egyértelmű, pontos és hozzáférhető szabályokon kell alapulnia (jogalap)**

2) **Bizonyítani kell az intézkedés szükségességét és arányosságát az elérni kívánt jogszerű célokra tekintettel**

3) **Az adatkezelést független felügyelet alá kell vonni**

4) **A magánszemélyek számára hatékony jogorvoslati lehetőségeket kell biztosítani**

[14] A C-362/14. sz., Maximillian Schrems kontra adatvédelmi biztos ügyben 2015. október 6-án hozott ítélet 74. pontja.