Ajánlások

01/2021 ajánlás a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv szerinti megfelelőségi referenciáról

Elfogadás időpontja: 2021. február 2.

Verziótörténet

1.1.verzió	2021. július 6.	Formázási módosítás
1.0. verzió	2021. február 2.	Az ajánlások elfogadása

Tartalomjegyzék

Az Európai Adatvédelmi Testület

Tekintettel a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelv[1] 51. cikke (1) bekezdésének b) pontjára,

tekintettel eljárási szabályzatának 12. és 22. cikkére,

ELFOGADTA A KÖVETKEZŐ AJÁNLÁST:

1. BEVEZETÉS

1. A 29. cikk alapján létrehozott (WP 29) munkacsoport közzétett egy munkadokumentumot[2] az általános adatvédelmi rendelet (GDPR)[3] szerinti megfelelőségi referenciáról. Az Európai Adatvédelmi Testület első plenáris ülésén jóváhagyta ezt a munkadokumentumot.

2. Amint azt a Lisszaboni Szerződéshez csatolt 21. nyilatkozat is kimondja, az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikke alapján a büntetőügyekben folytatott igazságügyi együttműködés és a rendőrségi együttműködés területén – e területek sajátos természetéből adódóan – a személyes adatok védelmére és az ilyen adatok szabad áramlására vonatkozó különleges szabályok válhatnak szükségessé.

3. Az uniós jogalkotó ennek alapján fogadta el az (EU) 2016/680 irányelvet (a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet, a továbbiakban: irányelv), amely szabályokat állapít meg a természetes személyek védelmére a személyes adatoknak az illetékes hatóságok által a **bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása – így többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése – céljából** végzett kezelése tekintetében.

4. Az irányelv ebben az összefüggésben meghatározza a személyes adatok harmadik országnak vagy nemzetközi szervezetnek történő továbbítását lehetővé tevő indokokat. Az ilyen adattovábbítás egyik indoka az Európai Bizottság azon határozata, amely szerint a szóban forgó harmadik ország vagy nemzetközi szervezet megfelelő védelmi szintet biztosít.

[1] HL L 119., 2016.5.4., 89. o.
[2] A 29. cikk szerinti (WP 29) munkacsoport által 2017. november 28-án elfogadott, legutóbb 2018. február 6-án felülvizsgált és elfogadott WP254.rev01 dokumentum. Ez a WP12 munkadokumentumnak a „Személyes adatok továbbítása harmadik országokba: Az európai uniós adatvédelmi irányelv 25. és 26. cikkének alkalmazása” című I. fejezetét frissíti, amelyet a WP 29 munkacsoport 1998. július 24-én fogadott el.
[3] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 26.) 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), HL L 119., 2016.5.4., 1. o.

5. A megfelelőségi referenciáról szóló WP254.rev01 munkadokumentum célja az, hogy iránymutatást nyújtson az Európai Bizottságnak a GDPR szerinti, harmadik országokban és nemzetközi szervezetekben biztosított adatvédelem szintjéről, e dokumentum célja pedig az, hogy az irányelvhez nyújtson hasonló iránymutatást. Ebben az összefüggésben megállapítja azokat az alapvető adatvédelmi elveket, amelyeknek egy harmadik országban vagy nemzetközi szervezetben jelen kell lenniük annak érdekében, hogy az irányelv alkalmazási körén belül lényegi egyenértékűséget biztosítsanak az uniós kerettel (azaz a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelésénél). Ezenkívül segítséget jelenthet azoknak a harmadik országoknak és nemzetközi szervezeteknek is, amelyek el szeretnék érni a megfelelőséget.

6. Ez a dokumentum kizárólag a megfelelőségi határozatokra összpontosul. Ezek az Európai Bizottság végrehajtási jogi aktusai a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv 36. cikkének (3) bekezdése értelmében.

2. A MEGFELELŐSÉG FOGALMA

7. Az irányelv meghatározza a személyes adatok harmadik országoknak és nemzetközi szervezeteknek történő továbbítására vonatkozó szabályokat addig a mértékig, ameddig az ilyen adattovábbítás a hatálya alá tartozik. A személyes adatok nemzetközi továbbításának szabályait az irányelv V. fejezete, különösen 35–39. cikke tartalmazza.

8. Az irányelv 36. cikke szerint személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha a harmadik ország, annak valamely területe vagy egy vagy több meghatározott ágazata, vagy az említett nemzetközi szervezet megfelelő védelmi szintet biztosít. Az Európai Unió Bíróságának (a továbbiakban: Bíróság) ítélkezési gyakorlatából[4] az következik, hogy ezt a rendelkezést az irányelvnek „A személyes adatok továbbítására vonatkozó általános elvek” című 35. cikkével összefüggésben kell értelmezni, amely kimondja, hogy „[az irányelv V. fejezetének] valamennyi rendelkezését alkalmazni kell annak biztosítása érdekében, hogy a természetes személy számára ebben az irányelvben garantált védelem szintje ne sérüljön”.

9. Amennyiben az Európai Bizottság úgy határozott, hogy a megfelelő szintű védelem biztosított, a személyes adatoknak az adott harmadik ország, terület, ágazat vagy nemzetközi szervezet számára való továbbítására külön engedély nélkül sor kerülhet, kivéve, ha egy másik tagállamnak, amelytől az adatokat megszerezték, az irányelv 35. és 36. cikkében, valamint (66) preambulumbekezdésében előírtak szerint engedélyeznie kell az adattovábbítást. Ettől függetlenül továbbra is szükséges, hogy az adatok kezelésénél az érintett tagállami hatóságok megfeleljenek az (EU) 2016/680 irányelv alapján elfogadott nemzeti rendelkezéseknek.

[4] A Bíróság 2020. július 16-i ítélete, Data Protection Commissioner kontra Facebook Ireland Limited és Maximillian Schrems (Schrems II. ügy), C-311/18, ECLI:EU:C:2020:559, 92. pont.

10. A „megfelelő védelmi szint” fogalmát, amely már a 95/46/EK irányelv[5] és a 2008/977/IB tanácsi kerethatározat[6] alapján is létezett, a Bíróság ezzel összefüggésben – és nemrég a GDPR keretében is – továbbfejlesztette.

11. Amint azt a Bíróság megállapította, míg a harmadik országban a védelem szintjének lényegében egyenértékűnek kell lennie az EU-ban biztosított védelmi szinttel, „azok az eszközök, amelyeket a harmadik ország az ilyen védelmi szint biztosításához e tekintetben igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket az Unióban alkalmaznak”, de „ezen eszközöknek a gyakorlatban mégis hatékonynak kell lenniük”[7]. A megfelelőségi normánál ezért nem követelmény, hogy pontról pontra tükrözze az uniós jogszabályokat, viszont meg kell határoznia az említett jogszabály lényegi alapkövetelményeit.

12. Ebben az összefüggésben a Bíróság azt is egyértelművé tette, hogy a bizottsági megfelelőségi határozatoknak tartalmazniuk kellene megállapításokat azzal kapcsolatban, hogy a harmadik országban léteznek-e azon személyek alapvető jogaiba való esetleges beavatkozásokat korlátozó állami szabályok, akiknek az adatait az Unióból a harmadik országba továbbítják, és e beavatkozásokat az állami szerveknek *megengedik-e*, amennyiben azok jogszerű célokat követnek, mint például a nemzetbiztonság[8].

13. Az Európai Bizottság megfelelőségi határozatainak célja, hogy a tagállamokra[9] és azok illetékes adatvédelmi hatóságaira[10] nézve kötelező erővel formálisan megerősítsék, hogy a harmadik országban vagy nemzetközi szervezetben az adatvédelem szintje lényegében egyenértékű az Európai Unió adatvédelmi szintjével. A harmadik országnak olyan garanciákat kell vállalnia, amelyek megfelelő – az Unión belül biztosítottal lényegében egyenértékű – védelmi szintet biztosítanak, különösen amikor egy vagy több konkrét ágazatban történik az adatkezelés[11].

14. 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 nemcsak a harmadik országnak vagy nemzetközi szervezetnek továbbított személyes adatokra vonatkozó szabályok tartalmát kell figyelembe venni, hanem az ilyen szabályok eredményességét biztosító rendszert is. A hatékony végrehajtási mechanizmusok kiemelkedő fontosságúak az adatvédelmi szabályok eredményessége szempontjából[12].

---

[5] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (HL L 281., 1995.11.23., 31. o.).
[6] A Tanács 2008/977/IB kerethatározata (2008. november 27.) a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről (HL L 350., 2008.12.30., 60. o.).
[7] A Bíróság 2015. október 6-i ítélete, Maximillian Schrems kontra Data Protection Commissioner (Schrems I. ügy), C-362/14, ECLI:EU:C:2015:650, 73. és 74. pont.
[8] Schrems I. ügy, 88. pont.
[9] Az EUMSZ 288. cikke.
[10] Schrems I. ügy, 52. pont.
[11] Az irányelv (67) preambulumbekezdése.
[12] Schrems I ügy, 72–74. pont és a Bíróság 2017. július 26-i 1/15. sz. véleménye a Kanada és az Európai Unió közötti megállapodás tervezetéről, ECLI:EU:C:2017:592 (1/15. sz. vélemény), 134. pont: „A személyes adatok védelméhez való e jog megköveteli többek között, hogy a személyes adatoknak az Unióból valamely harmadik országba történő továbbítása esetén érvényesüljön az alapvető szabadságok és jogok tekintetében az uniós jog által biztosított magas szintű védelem folytonossága. Még ha az ilyen szintű védelem biztosítására irányuló eszközök különbözhetnek is azoktól, amelyeket az uniós jogból eredő követelmények tiszteletben tartásának biztosítása érdekében az Unión belül kialakítottak, ezen eszközöknek a gyakorlatban akkor is hatékonynak kell lenniük ahhoz, hogy az Unióban biztosított védelemmel lényegében egyenértékű védelmet biztosítsanak.

3. A MEGFELELŐSÉGI MEGÁLLAPÍTÁSOK ELJÁRÁSI VONATKOZÁSAI AZ IRÁNYELV SZERINT

15. Ahhoz, hogy az irányelv 51. cikke (1) bekezdésének g) pontjában meghatározott, Európai Bizottság számára nyújtott tanácsadói feladatoknak eleget tehessen, az Európai Adatvédelmi Testületnek meg kell kapnia a teljes releváns dokumentációt, közte az Európai Bizottság kapcsolódó levelezését és megállapításait is. Feltétlenül szükséges, hogy minden releváns dokumentumot angolra fordítva és kellő időben előre eljuttassanak az Európai Adatvédelmi Testülethez annak érdekében, hogy a megfelelőségi határozatok végleges elfogadása előtt tájékozott és hasznos megbeszéléseket lehessen folytatni. Ha a jogi keret összetett, ennek magában kell foglalnia a harmadik ország vagy nemzetközi szervezet adatvédelmi szintjéről készített jelentést is. Az Európai Bizottság által rendelkezésre bocsátott tájékoztatásnak minden esetben teljes körűnek kell lennie, és lehetővé kell tennie az Európai Adatvédelmi Testületnek, hogy a harmadik ország vagy nemzetközi szervezet adatvédelmi szintjéről készült bizottsági elemzést értékelje.

16. Az Európai Adatvédelmi Testület megfelelő időn belül véleményt ad az Európai Bizottság megállapításairól, amely adott esetben azonosítja a megfelelőségi keret hiányosságait, és szükség esetén lehetséges ajánlásokat ad.

17. Az irányelv 36. cikkének (4) bekezdésével összhangban az Európai Bizottság feladata, hogy folyamatosan figyelemmel kísérje azon fejleményeket, amelyek érinthetik a megfelelőségi határozatok végrehajtását.

18. Az irányelv 36. cikkének (3) bekezdése előírja, hogy rendszeresen, legalább négyévente felülvizsgálatot kell végezni. Ez azonban egy általános időkeret, amelyet a megfelelőségi határozattal kell az adott harmadik országhoz vagy nemzetközi szervezethez igazítani. Az adott körülményektől függően rövidebb felülvizsgálati ciklust is elő lehet írni. Ezen kívül bizonyos incidensek, vagy a szóban forgó harmadik ország vagy nemzetközi szervezet jogi keretével kapcsolatos más információk vagy azok változásai szintén szükségessé tehetik az eredetileg tervezettnél korábbi felülvizsgálatot. Egy teljesen új megfelelőségi határozatnál célszerű továbbá az első felülvizsgálatot minél hamarabb elvégezni, majd az eredménytől függően fokozatosan módosítani a felülvizsgálati ciklust.

19. Mivel az Európai Adatvédelmi Testület feladata, hogy az Európai Bizottság rendelkezésére bocsássa a véleményét arról, ha a harmadik ország, annak valamely területe vagy meghatározott ágazata vagy valamely nemzetközi szervezet már nem biztosítja a megfelelő adatvédelmi szintet, az Európai Adatvédelmi Testületnek megfelelő időben érdemi információkat kell kapnia az adott harmadik országban vagy nemzetközi szervezetnél bekövetkezett releváns fejlemények Európai Bizottság általi nyomon követéséről. Az Európai Adatvédelmi Testületet ezért a harmadik országban vagy a nemzetközi szervezetnél folytatott valamennyi felülvizsgálati folyamatról és felülvizsgálati misszióról tájékoztatni kell. Az Európai Adatvédelmi Testület javasolja, hogy hívják meg az említett felülvizsgálati folyamatokban és küldetésekben való részvételre, amint azt az adatvédelmi pajzsról szóló határozat is előirányozta, és amelyről a Japánnal kapcsolatos megfelelőségi határozat rendelkezik.

20. Megjegyzendő az is, hogy az irányelv 36. cikkének (5) bekezdése szerint az Európai Bizottságnak hatásköre, hogy – ha a harmadik ország vagy a nemzetközi szervezet már nem biztosít megfelelő védettségi szintet – a meglévő megfelelőségi határozatokat hatályon kívül helyezze, módosítsa vagy felfüggessze. A hatályon kívül helyezésre, módosításra vagy felfüggesztésre irányuló

eljárásban az Európai Adatvédelmi Testület véleményét is ki kell kérni az irányelv 51. cikke (1) bekezdésének g) pontjával összhangban.

21. Ezen kívül – az ügyészségek hatásköreinek tiszteletben tartásával – a felügyeleti hatóságokat is fel kell jogosítani arra, hogy az irányelv megsértése esetén az igazságügyi hatóságokhoz forduljanak vagy bírósági eljárást kezdeményezzenek[13]. Különösen a Bíróság Schrems I. ítéletéből következik, hogy az adatvédelmi hatóságoknak lehetőséget kell biztosítani arra, hogy a nemzeti bíróságok előtt bírósági eljárást indítsanak, ha egy személynek a megfelelőségi határozattal szembeni panaszát megalapozottnak találják[14]. Ezt az értékelést a Schrems II. ítélet[15] is megerősítette.

4. A BÜNTETŐÜGYEKBEN FOLYTATOTT RENDŐRSÉGI ÉS IGAZSÁGÜGYI EGYÜTTMŰKÖDÉS MEGFELELŐSÉGÉRE VONATKOZÓ UNIÓS NORMÁK

22. Ami a tartalmat illeti, a megfelelőségi határozatnak – az irányelv 36. cikkében meghatározott értékelési kritériumok fényében – az érintett harmadik országban meglévő joganyag egészének elméleti és gyakorlati értékelésére kell összpontosítania. A harmadik ország vagy nemzetközi szervezet rendszerének a következő alapvető általános, eljárási és végrehajtási adatvédelmi elveket és mechanizmusokat kell tartalmaznia.

23. Az irányelv 36. cikkének (2) bekezdése meghatározza azokat az elemeket, amelyeket az Európai Bizottságnak figyelembe kell vennie egy harmadik ország vagy nemzetközi szervezet védelmi szintje megfelelőségének értékelésekor.

24. A Bizottság különösen figyelembe veszi a jogállamiságot, az emberi jogok és alapvető szabadságok[16] tiszteletben tartását, a vonatkozó jogszabályokat, valamint e jogszabályok végrehajtását, azon érintettek tényleges és érvényesíthető jogait és hatékony közigazgatási és bírósági jogorvoslati lehetőségeit, akiknek személyes adatait továbbítják, egy vagy több független

[13] Lásd az irányelv 47. cikkének (5) bekezdését és (82) preambulumbekezdését.
[14] Lásd: Schrems I. ügy, 65. pont: „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”.
[15] Lásd: Schrems II. ügy, 120. pont: „Még a Bizottság megfelelőségi határozata esetében is a valamely személy által a rá vonatkozó személyes adatok kezelése vonatkozásában a jogainak vagy szabadságainak védelmével kapcsolatban benyújtott panaszt elbíráló nemzeti felügyeleti hatóságnak jogosultnak kell lennie arra, hogy teljes függetlenséggel megvizsgálja, hogy ezen adattovábbítás tiszteletben tartja-e a GDPR-ban támasztott követelményeket, és adott esetben a nemzeti bíróságok előtt keresetet indítson annak érdekében, hogy amennyiben az utóbbiak osztják e hatóságnak a megfelelőségi határozat érvényessége tekintetében fennálló kétségeit, előzetes döntéshozatali eljárást kezdeményezhessenek ezen érvényesség vizsgálata céljából”.
[16] A harmadik ország jogi keretének értékelésekor figyelembe kell venni annak lehetőségét, hogy az EU-ból továbbított adatok alapján ki lehet-e szabni halálbüntetést vagy egyéb kegyetlen és embertelen bánásmódot. Amennyiben a harmadik ország joga ilyen büntetést vagy bánásmódot ír elő, további biztosítékokat kell találni a harmadik ország jogi keretében annak érdekében, hogy az EU-ból továbbított adatokat ne használják fel halálbüntetés vagy egyéb kegyetlen és embertelen bánásmód kérelmezéséhez, kiszabásához vagy végrehajtásához (pl. a továbbítás feltételeit meghatározó nemzetközi megállapodás, a harmadik ország arra vonatkozó kötelezettségvállalása, hogy az EU-ból továbbított adatok alapján nem szab ki halálbüntetést vagy egyéb kegyetlen és embertelen bánásmódot vagy halálbüntetési moratórium).

felügyeleti hatóság meglétét és hatékony működését, valamint a harmadik ország vagy nemzetközi szervezet nemzetközi kötelezettségeit.

25. Ezért egyértelmű, hogy a megfelelő védelem érdemi elemzésének két alapvető elemet kell megvizsgálnia: az alkalmazandó szabályok tartalmát és az azok eredményes gyakorlati végrehajtását biztosító eszközöket. Az Európai Bizottság feladata rendszeresen ellenőrizni, hogy a bevezetett szabályok a gyakorlatban is eredményesek-e.

26. A – megfelelő védelem minimumkövetelményének tekinthető – általános adatvédelmi elvek, továbbá eljárási és végrehajtási követelmények alapját az Európai Unió Alapjogi Chartája (Charta) és az irányelv képezi. A harmadik ország adatvédelemmel és magánélettel kapcsolatos általános rendelkezései nem elegendők. Éppen ellenkezőleg, a harmadik ország vagy a nemzetközi szervezet jogi keretének konkrét rendelkezéseket kell tartalmaznia a bűnüldözés területén az adatvédelemhez való jogra vonatkozóan. A harmadik országnak olyan garanciákat kell vállalnia, amelyek megfelelő – az Unión belül biztosítottal lényegében egyenértékű – védelmi szintet biztosítanak. Ezeknek a rendelkezéseknek kikényszeríthetőnek kell lenniük.

27. Továbbá, ami az arányosság elvét[17] illeti, a Bíróság a tagállami jogszabályokkal kapcsolatban úgy ítélte meg, hogy a magánélethez és az adatvédelemhez való jog korlátozásának igazolhatóságát, egyrészt az ilyen korlátozással járó **beavatkozás súlyosságának** felmérésével[18], másrészt pedig annak ellenőrzésével kell értékelni, hogy ezzel a súlyossággal arányos-e az említett korlátozással elérni kívánt **közérdekű cél jelentősége**[19].

28. A Bíróság ítélkezési gyakorlata szerint az alapvető jogokba való beavatkozást megengedő jogalapnak – az arányosság elvének való megfelelés érdekében – magának kell meghatároznia az érintett jog korlátozásának terjedelmét[20]. A személyes adatok védelmétől való eltérések és a védelem korlátozásai csak a feltétlenül szükséges mértéket érhetik el[21]. E követelmény teljesüléséhez az érintett szabályozásnak – amellett, hogy egyértelmű és pontos szabályokat állapít meg a szóban forgó intézkedés hatályára és alkalmazására vonatkozóan – minimális biztosítékokat kell előírnia annak érdekében, hogy azok a személyek, akiknek az adatait továbbították, elegendő garanciát kapjanak személyes adataiknak a visszaéléssel szembeni hatékony védelmére. „Meg kell jelölnie különösen, hogy milyen körülmények között és milyen feltételek mellett lehet az ilyen adatok kezelését előíró intézkedést megtenni, biztosítva ezáltal, hogy a beavatkozás a szigorúan szükséges mértékre korlátozódjék. Az ilyen biztosítékokkal való rendelkezés szükségessége még fontosabb abban az esetben, ha a személyes adatokat automatikusan kezelik”[22].

29. Az Európai Adatvédelmi Testület elfogadott egy ajánlást, amely azonosítja a Bíróság és az Emberi Jogok Európai Bírósága (EJEB) megfigyeléssel kapcsolatos ítélkezési gyakorlatát tükröző, harmadik országok jogában található alapvető garanciákat, amikor értékelni kell az ilyen harmadik országbeli felügyeleti intézkedéseknek az érintettek jogaiba való beavatkozását abban az esetben,

[17] A Charta 52. cikkének (1) bekezdése.
[18] A bíróság például megjegyezte, hogy „a végberendezés helyének megállapítását lehetővé tevő, valós idejű adatgyűjtés által megvalósított beavatkozás különösen súlyosnak tekinthető, mivel ezek az adatok eszközt nyújtanak az illetékes nemzeti hatóságok számára a mobiltelefon-használók helyváltoztatásainak pontos és folyamatos nyomonkövetésére.” (A Bíróság 2020. október 6-i ítélete, La Quadrature du Net és társai egyesített ügyek C-511/18., C-512/18 és C-520/18, ECLI:EU:C:2020:791, 187. pont, beleértve a hivatkozott ítélkezési gyakorlatot is).
[19] La Quadrature du Net és társai, 131. pont.
[20] Schrems II. ügy, 180. pont.
[21] Schrems II. ügy, 176. pont, beleértve a hivatkozott ítélkezési gyakorlatot is.
[22] Schrems II. ügy, 176. pont, beleértve a hivatkozott ítélkezési gyakorlatot is.

ha az adatokat a GDPR alapján továbbítják az adott harmadik országba[23]. Annak értékeléséhez, hogy teljesülnek-e az irányelv 36. cikke (2) bekezdésének a) pontja szerinti feltételek, az Európai Adatvédelmi Testület úgy véli, hogy az ezen ajánlásban meghatározott garanciákat kell figyelembe venni annak értékelésekor, hogy egy harmadik ország a megfigyelés terén megfelel-e az irányelvnek, figyelembe véve ezzel összefüggésben a megfigyelés terén fennálló további konkrét feltételeket is.

30. A 36. cikk (2) bekezdésének b) pontjával kapcsolatban a harmadik országnak nemcsak a hatékony, független adatvédelmi felügyeletről kell gondoskodnia, hanem a tagállami adatvédelmi hatóságokkal való együttműködés mechanizmusairól is[24].

31. A 36. cikk (2) bekezdésének c) pontjával kapcsolatban a harmadik ország vagy nemzetközi szervezet nemzetközi kötelezettségein kívül figyelembe kell venni a harmadik ország vagy nemzetközi szervezet multilaterális vagy regionális rendszerekben való részvételéből eredő kötelezettségeket is (különös tekintettel a személyes adatok védelmére), valamint e kötelezettségek végrehajtását, különösen a harmadik ország csatlakozását más nemzetközi adatvédelmi megállapodásokhoz, mint például az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló 1981. január 28-i egyezményéhez és kiegészítő jegyzőkönyvéhez (108. sz. egyezmény[25], és modernizált változata a 108+ egyezmény). Szintén figyelembe lehet venni, ha a harmadik ország megfelel az olyan nemzetközi dokumentumokban foglalt elveknek, mint például az Európa Tanácsnak a személyes adatok rendőrségi ágazatban való felhasználásáról szóló gyakorlati útmutatója (Practical guide on the use of personal data in the police sector).

32. A megfelelőségi határozatnak biztosítania kell, hogy a magánélethez és az adatvédelemhez való jogok tartalmán, valamint azok hatékony végrehajtásán, felügyeletén és érvényesítésén keresztül a külföldi rendszer egésze biztosítsa a szükséges szintű védelmet, többek között az ebbe a harmadik országba továbbított adatoknál is. Amint azt a Bíróság a Schrems II. ítéletben is hangsúlyozta, a magas szintű védelmet az adatok harmadik országba történő továbbítása során is biztosítani kell[26].

33. Végezetül a harmadik országnak csupán valamely területére vagy meghatározott ágazatára vonatkozó megfelelőségi határozat elfogadásakor az Európai Bizottságnak olyan egyértelmű és objektív kritériumokat szükséges figyelembe vennie, mint például a konkrét adatkezelési tevékenységekre való hivatkozások vagy a harmadik országban alkalmazandó jogi normák és jogszabályok hatálya[27].

A. Általános elvek és biztosítékok

a) Fogalmak

34. Létezni kell alapvető adatvédelmi fogalmaknak. Ezeknek nem kell szó szerint követniük az irányelv terminológiáját, azonban tükrözniük kell az európai adatvédelmi jogszabályok fogalmait. Az irányelv például az alábbi fontos fogalmakat tartalmazza: „személyes adat”, „személyes adatok kezelése”, „illetékes hatóságok”, „adatkezelő”, „adatfeldolgozó”, „címzett”, „érzékeny adatok”,

[23] Az Európai Adatvédelmi Testület 2020. november 10-én elfogadott, 02/2020 ajánlása a megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról.
[24] Az irányelv (67) preambulumbekezdése.
[25] Az irányelv (68) preambulumbekezdése.
[26] Lásd: 93. pont.
[27] Az irányelv (67) preambulumbekezdése.

„pontosság”, „profilalkotás”, „beépített és alapértelmezett adatvédelem”, „felügyeleti hatóság” és „álnevesítés”.

b) A személyes adatok kezelésének jogszerűsége és tisztességessége (4. cikk és (26) preambulumbekezdés)

35. A Charta 8. cikkének (2) bekezdése szerint a személyes adatokat többek között csak „meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni”[28]. A bűnüldözéssel összefüggésben azonban megjegyzendő, hogy mivel a bűncselekmények megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása feladatának ellátását a jog intézményesen ruházza az illetékes hatóságokra, azok elrendelhetik vagy megkövetelhetik a természetes személyektől kérésük teljesítését. Ilyen esetben az érintettnek hozzájárulása nem szolgálhat jogalapul a személyes adatok illetékes hatóságok általi kezeléséhez[29].

36. Ennek a jogalapnak egyértelmű és pontos szabályokat kell megállapítania a vonatkozó adatkezelési tevékenységek hatályára és alkalmazására vonatkozóan, és minimális biztosítékokat kell előírnia[30]. Emellett a Bíróság emlékeztetett arra, hogy „e szabályozásnak a belső jogban jogilag kötelező erejűnek kell lennie”[31].

37. Ahhoz, hogy a jogalap jogszerű legyen, az illetékes hatóság[32] által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása – többek között a közbiztonságot fenyegető veszélyekkel szembeni biztosítékok és e veszélyek megelőzése – céljából végzett feladat végrehajtásához adatkezelést[33] kellene végezni. Ezeket a célokat a nemzeti jogban kell meghatározni.

38. A személyes adatokat tisztességesen kell kezelni. A tisztességes adatkezelés elve – mint adatvédelmi elv – a tisztességes eljáráshoz való jognak a Charta 47. cikkében és az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény (EJEE) 6. cikkében meghatározott fogalmától elkülönülő fogalom[34].

c) A célhoz kötöttség elve (4. cikk)

[28] Lásd: Schrems II. ügy, 173. pont.

[29] Az irányelv (35) preambulumbekezdése azt is kimondja, hogy „[h]a az érintett jogi kötelezettséget teljesít, nincs valós és szabad választási lehetősége, ezért az érintett reakciója nem tekinthető akarata szabad kinyilvánításának. Ez nem akadályozhatja meg a tagállamokat abban, hogy jogszabályban előírják azt, hogy az érintett hozzájárulhat a személyes adatainak ezen irányelv alkalmazásában történő kezeléséhez, például bűnügyi nyomozások keretében végzett DNS-vizsgálat lefolytatásához vagy büntetőjogi szankciók végrehajtásakor az érintett feltalálásának elektronikus azonosító igénybevételével történő figyelemmel kíséréséhez.”

[30] Lásd a Schrems II. ügy 175. és 180. pontját, valamint az 1/15. sz. vélemény 139. pontját és az idézett ítélkezési gyakorlatot.

[31] Lásd: a Bíróság 2020. október 6-i ítélete, Privacy International kontra Secretary of State for Foreign and Commonwealth Affairs és társai, C-623/17, ECLI:EU:C:2020:790, 68. pont. Megjegyzendő, hogy az ítélet francia és magyar nyelvű változatában a Bíróság a *réglementation*, illetve a *szabályozás* szót használja, ami tágabb értelmű, mint a parlamenti jogszabályok.

[32] Az illetékes hatóságok az ilyen célokra hatáskörrel rendelkező hatóságok, vagy bármely más olyan szerv vagy szervezet, amelyet a törvény e célból közhatósági és közhatalmi jogosítványok gyakorlására bíz meg.

[33] A személyes adatok részben vagy egészben automatizált módon történő kezelése, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelése, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

[34] Az irányelv (26) preambulumbekezdése.

39. A személyes adatok kezelése konkrét céljainak már a személyes adatok gyűjtésének időpontjában kifejezettnek és jogszerűnek, továbbá meghatározottnak kell lenniük[35].

40. Az adatokat meghatározott, egyértelmű és jogszerű célból lehet kezelni bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából[36], beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését a harmadik országban, és ezt követően lehet őket felhasználni ezekre a célokra, amennyiben ez nem összeegyeztethetetlen az adatkezelés eredeti céljával (pl. párhuzamos kikényszerítési eljárási vagy közérdekű archiválási, tudományos, statisztikai vagy történelmi célok), az érintettek jogaira és szabadságaira vonatkozó megfelelő garanciák mellett. Ha a személyes adatok kezelését azonos vagy más adatkezelő (illetékes hatóság)[37] a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzi, amely eltér attól a céltól, amelyre az adatgyűjtés eredetileg irányult, az ilyen adatkezelést azzal a feltétellel kell lehetővé tenni, hogy az ilyen adatkezelésre a vonatkozó jogi rendelkezések megfelelő felhatalmazást adnak, továbbá az adatkezelés az említett eltérő cél szempontjából szükséges és arányos[38]. Figyelembe kell venni azt is, hogy létezik-e olyan mechanizmus, amellyel az érintett tagállamok illetékes hatóságai tájékoztatást kapnak az ilyen további adatkezelésről[39]. Ezenkívül az irányelv által a természetes személyeknek védelmének az Unióban biztosított szintjét semmi esetre sem szabad aláásni, ideértve azokat az eseteket is, amikor a személyes adatokat a harmadik országból ugyanazon harmadik országbeli adatkezelőknek vagy adatfeldolgozóknak továbbítják[40].

d) Az egyéb célokból történő további adatkezelésre vonatkozó különös feltételek (9. cikk)

41. Az EU-ból továbbított adatoknak a nem bűnüldözési – például nemzetbiztonsági – célokból történő további kezelését vagy közlését szintén jogszabálynak kell előírnia, és szükségesnek és arányosnak kell lennie. Figyelembe kell venni azt is, hogy létezik-e olyan mechanizmus, amellyel az érintett tagállamok illetékes hatóságai tájékoztatást kapnak az ilyen további adatkezelésről[41]. További kezelésük és feldolgozásuk után az adatoknak itt is ugyanolyan szintű védelemben kell részesülniük, mint amikor az adatokat átvevő illetékes hatóság eredetileg kezelte azokat.

e) Az adattakarékosság elve

[35] Az irányelv (26) preambulumbekezdése.
[36] Ez magában foglalja „az annak előzetes ismerete nélkül végzett rendőri tevékenységeket is, hogy egy adott eset bűncselekménynek minősül-e. Az ilyen tevékenységek magukban foglalhatják a hatósági jogkör kényszerintézkedések alkalmazásával történő gyakorlását is, így például a tüntetések, jelentős sportesemények és zavargások során végzett rendőrségi tevékenységet is. Idetartozik továbbá a rendőrségre és egyéb bűnüldöző szervekre ruházott feladatként a közrend és közbiztonság fenntartása annak érdekében, hogy adott esetben védelmet biztosítsanak a közbiztonságot és a jog által védett alapvető társadalmi érdekeket fenyegető – esetleg bűncselekmény elkövetéséhez is vezető – veszélyekkel szemben, és megelőzzék e veszélyeket (az irányelv (12) preambulumbekezdése). Ezt meg kell különböztetni a nemzetbiztonsági céltól vagy az Európai Unióról szóló szerződés (EUSZ) V. címe 2. fejezetének hatálya alá tartozó tevékenységektől (az irányelv (14) preambulumbekezdése).
[37] Lásd: 33. lábjegyzet.
[38] Az irányelv (29) preambulumbekezdése.
[39] Ilyen mechanizmus lehet például a kölcsönösen elfogadott adatkezelési kódok használata, a nemzetközi jogi eszköz szerinti értesítési kötelezettség (ideértve az esetleges automatikus értesítéseket is) vagy más hasonló átláthatósági intézkedések.
[40] Az irányelv (64) preambulumbekezdése.
[41] Lásd: 39. lábjegyzet.

42. Az adatoknak a kezelési célokhoz képest megfelelőnek és relevánsnak kell lenniük, és azokkal arányban kell állniuk. Különösen figyelembe kell venni a beépített és alapértelmezett adatvédelmi követelmények – például a korlátozott beviteli mezők (strukturált kommunikáció) vagy az automatizált és nem automatizált minőség-ellenőrzések – alkalmazását.

f) Az adatok pontosságának elve

43. Az adatoknak pontosnak és ahol szükséges, naprakésznek kell lenniük. Mindazonáltal az adott adatkezelés jellegére és céljára tekintettel kell az adatok pontosságának elvét alkalmazni. Különösen a bírósági eljárásokban a személyes adatokat tartalmazó nyilatkozatok a természetes személy szubjektív megítélésén alapulnak, amelyek nem mindig visszaellenőrizhetők. A pontosság követelménye következésképpen nem a nyilatkozat pontosságára, hanem pusztán arra a tényre vonatkozik, hogy egy adott nyilatkozat megtételére sor került[42].

44. Biztosítani kell, hogy a pontatlan, hiányos vagy már nem naprakész személyes adatokat ne lehessen továbbítani vagy hozzáférhetővé tenni[43], valamint hogy a pontatlan adatok kijavítására vagy törlésére eljárások legyenek előirányozva. A forrás megbízhatósága és a tények ellenőrzésének szintje szempontjából különösen figyelembe kell venni a kezelt információk osztályozási rendszereit[44].

g) Az adatmegőrzés elve

45. Az adatok legfeljebb a kezelésük céljaihoz szükséges ideig őrizhetők meg. Megfelelő mechanizmusokat kell létrehozni a személyes adatok törlésére: ez lehet egy meghatározott időszak vagy a személyesadat-tárolás szükségességének időszakos felülvizsgálata (vagy a kettő kombinációja: meghatározott leghosszabb időtartam és időszakos felülvizsgálat bizonyos időközönként)[45]. A közérdekű archiválás, tudományos, statisztikai vagy történelmi felhasználás céljából hosszabb ideig tárolt személyes adatokra megfelelő biztosítékoknak kell vonatkozniuk (pl. a hozzáférés tekintetében)[46].

h) A biztonság és a bizalmas jelleg elve (29. cikk, (28) és (71) preambulumbekezdés)

46. A személyes adatokat kezelő minden jogalanynak biztosítania kell, hogy az adatok kezelése úgy történjék, amely biztosítja a személyes adatok biztonságát, többek között a személyes adatokhoz és az adatkezeléshez használt eszközökhöz való jogosulatlan hozzáférés vagy azok jogosulatlan felhasználásának megakadályozásával. Ez magában foglalja a jogellenes adatkezeléssel, valamint a véletlen adatvesztéssel, megsemmisüléssel vagy károsodással szembeni védelmet és az ezek kezelésére szolgáló megfelelő intézkedéseket, megfelelő technikai és szervezési intézkedések alkalmazásával. A biztonsági szint meghatározásakor figyelembe kell venni a tudomány és a technológia állását és a megvalósítás költségeit, továbbá az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a személyek jogaira és szabadságaira jelentett változó valószínűségű és súlyosságú kockázatot.

47. A személyes adatokat továbbító tagállami hatóságok és a harmadik államok átvevő hatóságai között biztonságos kommunikációs csatornákról kell gondoskodni.

[42] Az irányelv (30) preambulumbekezdése.
[43] Az irányelv (32) preambulumbekezdése.
[44] Például 4×4 táblázatok a megbízhatósági értékelésekhez és az adatkezelési kódokhoz.
[45] Az irányelv 5. cikke.
[46] Az irányelv (26) preambulumbekezdése.

i) Az átláthatóság elve (13. cikk, (26), (39), (42), (43), (44) és (46) preambulumbekezdés)

48. A természetes személyt tájékoztatni kell a személyes adatai kezelésével járó kockázatokról, szabályokról, garanciákról és jogokról, valamint arról, hogy hogyan élhet az adatkezeléssel kapcsolatban őt megillető jogokkal[47].

49. Az egyéneket tájékoztatni kell személyes adataik kezelésének valamennyi fő eleméről. Ennek az információnak könnyen hozzáférhetőnek és könnyen érthetőnek kell lennie, világos és közérthető nyelvezetet használva. A tájékoztatásnak ki kell térnie az adatkezelés céljára, az adatkezelő személyére, az érintett számára elérhető jogokra[48], valamint egyéb információkra, amennyiben azok a tisztességes eljárás biztosítása érdekében szükségesek.

50. A tájékoztatáshoz való jog alól létezhet néhány kivétel. Az ilyen korlátozást azonban jogszabályi intézkedéssel kell lehetővé tenni, és annak szükségesnek és arányosnak kell lennie a hivatalos vagy jogi vizsgálatok, nyomozások vagy eljárások akadályozásának elkerülése, valamint annak elkerülése érdekében, hogy a bűncselekmények megelőzése, felderítése, nyomozása, a vádeljárás lefolytatása vagy a büntetőjogi szankciók végrehajtása sérelmet szenvedjen, továbbá a közbiztonság vagy nemzetbiztonság védelme, illetve mások jogainak és szabadságainak védelme érdekében, amennyiben és ameddig ez a részleges vagy teljes korlátozás – kellő tekintettel az érintett természetes személy alapvető jogaira és jogos érdekeire – egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül. Az ilyen korlátozásokat – a felügyeleti hatóságnál történő panasztétel vagy jogorvoslat lehetőségének figyelembevételével – meg kell vizsgálni és értékelni kell. Mindenesetre minden lehetséges korlátozásnak átmenetinek és nem általános jellegűnek kell lennie, és azt a Chartában és az emberi jogok és alapvető szabadságok védelméről szóló egyezményben előírtakhoz hasonló feltételekkel, biztosítékokkal és korlátozásokkal kell szabályozni, ahogyan azt a Bíróságnak és az Emberi Jogok Európai Bíróságának ítélkezési gyakorlata értelmezi, és e jogok és szabadságok lényegét különösen tiszteletben kell tartania.

j) A hozzáféréshez, a helyesbítéshez és a törléshez való jog (14. és 16. cikk)

51. Az érintettnek jogot kell biztosítani arra, hogy megerősítést kapjon arról, hogy folyamatban van-e rá vonatkozó adatkezelés, és ha igen, akkor hozzáférhessen az adataihoz. Ennek a jognak magában kell foglalnia legalább az adatkezeléssel kapcsolatos bizonyos információkat, például az adatkezelés céljait és jogalapját, a felügyeleti hatóságnál történő panasztétel jogát vagy az érintett személyes adatok kategóriáit[49]. Ez különösen fontos abban akkor, ha az átláthatóságot általános értesítéssel érik el (pl. a hatóság honlapján található információk).

52. Az érintettnek biztosítani kell a jogot arra, hogy adatait meghatározott okokból helyesbítsék, ha például azok pontatlannak vagy hiányosnak bizonyulnak. Az érintettnek biztosítani kell azt a jogot is, hogy adatait töröljék, ha például az adatkezelés már nem szükséges vagy jogellenes.

53. E jogok gyakorlása nem lehet aránytalanul megterhelő az érintett számára.

k) Az érintett jogainak korlátozásai

[47] Az irányelv (26) preambulumbekezdése.
[48] Az anyagi (hozzáféréshez való jog, helyesbítéshez való jog stb.), és a jogorvoslathoz való jogokra egyaránt.
[49] Az irányelv 14. cikke.

54. E jogok korlátozása lehetséges a hivatalos vagy jogi vizsgálatok, nyomozások vagy eljárások akadályozásának elkerülése, valamint annak elkerülése érdekében, hogy a bűncselekmények megelőzése, felderítése, nyomozása, a vádeljárás lefolytatása vagy a büntetőjogi szankciók végrehajtása sérelmet szenvedjen, továbbá a közbiztonság vagy nemzetbiztonság védelme, illetve mások jogainak és szabadságainak védelme érdekében, amennyiben és ameddig ez a részleges vagy teljes korlátozás – kellő tekintettel az érintett természetes személy alapvető jogaira és jogos érdekeire – egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül. Az ilyen korlátozásokat – a felügyeleti hatóságnál történő panasztétel vagy bírósági jogorvoslat lehetőségének figyelembevételével – meg kell vizsgálni és értékelni kell.

l) Az újbóli továbbítás korlátozása (35. cikk, (64)–(65) preambulumbekezdés)

55. A személyes adatoknak az eredeti címzett által egy másik harmadik országba vagy nemzetközi szervezet részére történő újbóli továbbítása nem veszélyeztetheti azon természetes személyek – az Unióban biztosított – védelmének szintjét, akiknek az adatait továbbítják. Ezért az ilyen újbóli továbbítás csak akkor engedélyezhető, ha az uniós jog által szavatolt védelmi szint folytonossága biztosított[50]. Különösen a további címzettnek (azaz az újbóli továbbítás címzettjének) kell bűnüldözési célokból illetékes hatóságnak lennie[51], és az adatok ilyen újbóli továbbítására csak korlátozott és meghatározott célokból kerülhet sor, és csak ha az adatkezelésnek jogi oka van.

56. Figyelembe kell venni azt is, hogy létezik-e olyan mechanizmus, amely lehetővé teszi az érintett tagállam illetékes hatóságainak tájékoztatását és az ilyen újbóli adattovábbítás engedélyezését. Az EU-ból továbbított adatok eredeti címzettjének felelősséggel kell tartoznia, és képesnek kell lennie annak bizonyítására, hogy a tagállam érintett illetékes hatósága engedélyezte az újbóli adattovábbítást[52], valamint hogy megfelelő biztosítékok állnak rendelkezésre az adatok újbóli továbbítására, ha hiányzik az azon harmadik országra vonatkozó megfelelőségi határozat, amelybe az adatokat újból továbbítanák[53].

m) Az elszámoltathatóság elve (4. cikk (4) bekezdés)

57. Az adatkezelőnek felelősséget kell vállalnia az irányelv 4. cikkében foglalt adatvédelmi elvek betartásáért, és képesnek kell lennie bemutatni, hogy azokat betartja.

[50] Lásd: 1/15. vélemény.
[51] Lásd: 33. lábjegyzet.
[52] Ebben az összefüggésben figyelembe kell venni az adatokat továbbító tagállami hatóságok által meghatározott vonatkozó adatkezelési kódok végrehajtására vonatkozó kötelezettséget vagy kötelezettségvállalást is.
[53] A fenti követelmények nem érintik a megfelelő országba történő újbóli továbbításra vonatkozóan az irányelvben meghatározott különös feltételeket (35. cikk (1) bekezdés c) és e) pont).

B. Példák az egyes adatkezelési típusokra alkalmazandó további elvekre

a) Különleges adatkategóriák (10. cikk és (37) preambulumbekezdés)

58. Külön biztosítékoknak kell létezniük az „adatok különleges kategóriáit”[54] érintő konkrét kockázatok kezelésére[55]. Ezeknek a kategóriáknak meg kell felelniük az irányelv 10. cikkében foglaltaknak. A különleges adatkategóriák kezelésére ezért különleges biztosítékoknak kell vonatkozniuk, és csak akkor szabad engedélyezni, ha az bizonyos feltételek mellett feltétlenül szükséges, például az egyén létfontosságú érdekeinek védelme érdekében.

b) Automatizált döntéshozatal és profilalkotás (11. cikk és (38) preambulumbekezdés)

59. Kizárólag automatizált adatkezelésen (egyedi ügyekben történő automatizált döntéshozatal), többek között profilalkotáson, alapuló döntésekre, amelyek az érintettre nézve hátrányos jogi vagy egyéb jelentős következménnyel járnak, kizárólag a harmadik ország jogi keretében meghatározott, bizonyos körülmények között kerülhet sor[56].

60. Az európai uniós keretben ilyen feltétel lehet például az érintett külön tájékoztatásának biztosítása és az ahhoz való joga, hogy az adatkezelőtől emberi beavatkozást kapjon, különösen hogy kifejtse álláspontját, magyarázatot kapjon az effajta értékelés alapján hozott döntésről, és hogy megtámadja a döntést.

61. A harmadik ország jogának minden esetben rendelkeznie kell az érintett jogaira és szabadságaira vonatkozó szükséges biztosítékokról. Ebben a tekintetben figyelembe kell venni azt is, hogy létezik-e olyan mechanizmus, amely tájékoztatja az érintett tagállam illetékes hatóságait minden további adatkezelésről, például a továbbított adatok nagyléptékű profilalkotás céljából történő felhasználásáról.

c) Beépített és alapértelmezett adatvédelem (20. cikk)

62. A megfelelőség értékelésénél figyelmet kell szentelni annak, hogy az adatkezelőnek kötelessége-e olyan belső szabályokat alkalmaznia, valamint olyan intézkedéseket végrehajtania, amelyek tiszteletben tartják a beépített adatvédelem és az alapértelmezett adatvédelem elveit, figyelembe véve a tudomány és technológia állását és a megvalósítás költségeit, továbbá az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatot mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során, kötelessége-e olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – végrehajtania, amelyek célja egyrészt adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, és kötelessége-e a szükséges garanciák beépítése az adatkezelés folyamatába.

[54] Ezeket a különleges kategóriákat az irányelv (37) preambulumbekezdése „érzékeny adatokként” említi.
[55] Ilyen további biztosítékok lehetnek például konkrét biztonsági intézkedések, a személyzet korlátozott hozzáférési jogai, illetve a további adatkezelés, az automatizált döntéshozatal, az újbóli megosztás vagy az újbóli továbbítás korlátozásai.
[56] Az 1/15. sz. vélemény 173. pontja.

C. Eljárási és végrehajtási mechanizmusok

63. Bár azok az eszközök, amelyeket az adott harmadik ország a megfelelő adatvédelmi szint biztosítása érdekében alkalmaz, eltérhetnek az Európai Unión belül alkalmazott eszközöktől[57], az európai rendszerrel összhangban lévő rendszereket az alábbi elemek meglétének kell jellemeznie:

a) Illetékes független felügyeleti hatóság (36. cikk (2) bekezdés b) pont és (3) bekezdés, valamint (67) preambulumbekezdés)

64. A harmadik országban lennie kell egy vagy több független felügyeleti hatóságnak, amely az adatvédelmi és magánélet védelmét célzó rendelkezéseknek való megfelelés 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. Ebben az összefüggésben a felügyeleti hatóságnak minden megfelelő végrehajtási hatáskörrel rendelkeznie kell ahhoz, hogy hatékonyan biztosítani tudja az adatvédelmi jogok tiszteletben tartását és előmozdítsa a tudatosságot. Nem szabad megfeledkezni a felügyeleti hatóság személyzetéről és költségvetéséről sem. A felügyeleti hatóságnak képesnek kell lennie arra, hogy saját kezdeményezésére vizsgálatokat folytasson. Feladatának kell lennie továbbá, hogy az érintetteket jogaik gyakorlásában segítse és tanáccsal lássa el (lásd még az alábbi c) pontot). A megfelelőségi határozatokban adott esetben meg kell határozni a felügyeleti hatóságot vagy hatóságokat, valamint az adatvédelmi szabályok érvényesítése érdekében a tagállamok felügyeleti hatóságaival folytatott együttműködési mechanizmusokat.

b) Az adatvédelmi szabályok hatékony végrehajtása

65. A harmadik országbeli rendszereknek biztosítaniuk kell, hogy az adatkezelők és a személyes adatokat az ő nevükben kezelők magas szinten ismerjék kötelezettségeiket, feladataikat és felelősségi köreiket, az érintettek pedig jogaikat és azok gyakorlásának módját. A hatékony és visszatartó erejű szankciók fontos szerepet játszhatnak a szabályok betartásának biztosításában, éppen úgy, mint a hatóságok, ellenőrök vagy független adatvédelmi tisztviselők közvetlen ellenőrzései.

66. A harmadik országbeli adatvédelmi keretnek köteleznie kell az adatkezelőket vagy a nevükben személyes adatokat kezelőket arra, hogy feleljenek meg a keretnek, és különösen az illetékes felügyeleti hatóság előtt képesek legyenek bizonyítani a szabályoknak való megfelelést. Ezeknek az intézkedéseknek magukban kell foglalniuk az adatkezelési tevékenységek nyilvántartásának vagy naplófájljainak megfelelő ideig történő megőrzését is. Ide tartozhatnak például adatvédelmi hatásvizsgálatok, adatvédelmi tisztviselő kijelölése vagy a beépített és alapértelmezett adatvédelem.

c) Az adatvédelmi rendszer könnyítse meg az érintett jogainak gyakorlását (az irányelv 12., 17. és 46. cikke)

67. A harmadik országbeli adatvédelmi keretnek köteleznie kell az adatkezelőt arra, hogy segítse elő az érintett fenti A. j) szakaszban említett jogainak gyakorlását, és elő kell írnia, hogy a felügyeleti hatóság kérésre tájékoztassa az érintettet jogai gyakorlásáról[58].

[57] Schrems I. ügy, 74. pont.
[58] Az érintettek jogainak gyakorlása történhet közvetlen vagy közvetett módon.

d) Az adatvédelmi rendszer biztosítson megfelelő jogorvoslati mechanizmusokat

68. Bár jelenleg nincs ítélkezési gyakorlat a harmadik országok jogrendszerének irányelv szerinti megfelelőségéről, a Bíróság már értelmezte a Charta 47. cikkében foglalt hatékony bírói jogvédelemhez való alapvető jogot. A Charta 47. cikkének első bekezdése ugyanis előírja, hogy mindenkinek, akinek az Unió joga által biztosított jogait és szabadságait megsértették, a hivatkozott cikkben megállapított feltételek mellett joga van a bíróság[59] előtti hatékony jogorvoslathoz.

69. A Bíróság állandó ítélkezési gyakorlata szerint az uniós jogi rendelkezések tiszteletben tartásának biztosítására irányuló hatékony bírói felülvizsgálat fennállása a jogállamiság létének velejárója. Így az olyan szabályozás, amely nem biztosít a jogalany számára semmilyen jogorvoslati lehetőséget abból a célból, hogy a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltesse, nem tartja tiszteletben a hatékony bírói jogvédelemhez való jog lényegét, amelyet a Charta 47. cikke mond ki[60].

70. 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.

71. 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.

72. A szabályok be nem tartása esetén az érintettnek (akinek adatait a harmadik országba továbbították) hatékony közigazgatási és bírósági jogorvoslatot kell biztosítani a harmadik országban, beleértve a személyes adatainak jogellenes kezelése miatt felmerülő károk megtérítését is. Ez kulcsfontosságú elem, amelynek adott esetben tartalmaznia kell a kártérítések megfizettetését és szankciók elrendelését lehetővé tevő, független, bíróság előtti vitarendezési vagy választottbíráskodási rendszert is.

[59] A Bíróság úgy véli, hogy a hatékony bírói jogvédelmet nemcsak bíróság, hanem olyan szerv is biztosíthatja, amely a Charta 47. cikkében előírtakkal lényegében egyenértékű garanciákat nyújt (lásd Schrems II. ügy, 197. pont). Ez különösen nemzetközi szervezetek esetében lehet releváns.
[60] Schrems II. ügy, 187. és 194. pont, beleértve a hivatkozott ítélkezési gyakorlatot is.