

A Testület véleménye (a 70. cikk (1) bekezdésének s) pontja)



**32/2021. számú vélemény a személyes adatok Koreai
Köztársaságban biztosított megfelelő védelméről szóló,
2016/679/EU rendelet szerinti európai bizottsági
végrehajtási határozat tervezetéről**

1.0 változat

Elfogadás időpontja: 2021. szeptember 24.

TARTALOMJEGYZÉK

1.	ÖSSZEFOGLALÓ.....	4
1.1.	Felzárkózási területek	5
1.2.	Kihívások	5
1.2.1.	Általános kérdések.....	5
1.2.2.	Általános adatvédelmi kérdések	6
1.2.3.	A közhatalmi szervek Koreai Köztársaságba továbbított adatokhoz való hozzáférésére	7
1.3.	Következtetés	8
2.	BEVEZETÉS	8
2.1.	A koreai adatvédelmi keret	8
2.2.	Az Európai Adatvédelmi Testület értékelésének hatóköre	9
2.3.	Általános megjegyzések és aggályok.....	10
2.3.1.	A Koreai Köztársaság által vállalt nemzetközi kötelezettségek	10
2.3.2.	A megfelelőségi határozat hatálya.....	11
3.	ÁLTALÁNOS ADATVÉDELMI SZEMPONTOK.....	12
3.1.	Tartalmi elvek	12
3.1.1.	Fogalmak	12
3.1.2.	Az adatvédelmi törvény szerinti részleges mentességek	14
3.1.3.	A jogos célokból végzett jogszerű és tisztességes adatkezelés alapjai	16
3.1.4.	A célhoz kötöttség elve.....	17
3.1.5.	Az adatminőség és az arányosság elve	18
3.1.6.	Az adatmegőrzés elve.....	18
3.1.7.	A biztonság és a titoktartás elve	18
3.1.8.	Az átláthatóság elve.....	19
3.1.9.	A személyes adatok különleges kategóriái	20
3.1.10.	A hozzáféréshez, helyesbítéshez, törléshez és tiltakozáshoz való jog.....	20
3.1.11.	Az újbóli továbbítás korlátozása	23
3.1.12.	Közvetlen üzletszerzés.....	25
3.1.13.	Automatizált döntéshozatal és profilalkotás.....	26
3.1.14.	Elszámoltathatóság.....	27
3.2.	Eljárási és végrehajtási mechanizmusok.....	27
3.2.1.	Illetékes független felügyeleti hatóság	27
3.2.2.	A szabályok betartásának jó szintjét biztosító biztosító rendszer létezése	28

3.2.3. Az adatvédelmi rendszernek támogatást és segítséget kell nyújtania az érintetteknek a jogaik és a megfelelő jogorvoslati mechanizmusok gyakorlása során	30
4. A DÉL-KOREAI KÖZHATALMI SZERVEK ÁLTALI HOZZÁFÉRÉS ÉS FELHASZNÁLÁS AZ EURÓPAI UNIÓBÓL TOVÁBBÍTOTT SZEMÉLYES ADATOK ESETÉBEN	30
4.1. A kormányzati hozzáféréssel összefüggő általános adatvédelmi keret	30
4.2. A hírközlési metaadatokhoz való bűnüldözési célú kormányzati hozzáférés vonatkozásában biztosított védelem és garanciák.....	31
4.3. A koreai közhatalmi szervek nemzetbiztonsági célú hozzáférése a hírközlési adatokhoz	32
4.3.1. A külföldi állampolgárok közötti közlésekhez való hozzáférésről szóló értesítés kötelezettségének hiánya	32
4.3.2. A külföldi állampolgárok közötti közlésekre vonatkozó adatgyűjtés előzetes független engedélyezésének a hiánya	34
4.4. Önkéntes adatközlés	35
4.5. Az adatok további felhasználása	36
4.6. Újbóli továbbítás és a hírszerzési adatok megosztása	36
4.6.1. A bűnüldöző hatóságok általi újbóli továbbításra alkalmazandó jogi keret	37
4.6.2. A nemzetbiztonsági célokból végzett újbóli továbbításra alkalmazandó jogi keret	38
4.6.3. Nemzetközi megállapodások	39
4.7. Felügyelet	40
4.8. Bírósági jogorvoslat.....	41

Az Európai Adatvédelmi Testület

tekintettel 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 szóló, 2016. április 27-i 2016/679/EU európai parlamenti és tanácsi rendelet (GDPR) 70. cikke (1) bekezdésének s) pontjára,

tekintettel az az Európai Gazdasági Térségről (EGT) szóló megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és annak 37. jegyzőkönyvére¹,

tekintettel eljárási szabályzatának 12. és 22. cikkére,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

1. ÖSSZEFOGLALÓ

1. Az Európai Bizottság 2021. június 16-án indította meg a személyes adatok Koreai Köztársaságban biztosított, a személyes adatok védelméről szóló koreai törvényen alapuló megfelelő védelméről szóló végrehajtási határozattervezetének (**határozattervezet**) elfogadására irányuló, GDPR szerinti hivatalos eljárást².
2. Ugyanezen a napon az Európai Bizottság kikérte az Európai Adatvédelmi Testület (EDPB) véleményét³. Az Európai Adatvédelmi Testület a határozattervezet vizsgálata, valamint az Európai Bizottság által rendelkezésre bocsátott dokumentumok⁴ elemzése alapján értékelte a Koreai Köztársaságban biztosított védelmi szint megfelelőségét.
3. Az értékelés egyaránt kiterjedt a határozattervezet általános, GDPR-ral kapcsolatos vonatkozásaira és a közhatalmi szervek EGT-ből továbbított személyes adatokhoz való, bűnüldözési és nemzetbiztonsági célú hozzáféréseire, az EGT-állampolgárok rendelkezésére álló jogorvoslati lehetőségeket is beleértve. Az Európai Adatvédelmi Testület a koreai jogi keret által biztosított garanciák működését és hatékonyságát is vizsgálta.
4. E munka során elsősorban a GDPR-nak való megfelelés értékeléséhez készült, 2018 februárjában elfogadott referenciaanyagra⁵ (GDPR-megfelelési referencia) és az Európai Adatvédelmi Testület megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról szóló 02/2020. számú ajánlására⁶ támaszkodott.

¹ A jelen véleményben a „tagállamokra” történő bármely hivatkozást „EGT-tagállamokra” történő hivatkozásként kell érteni.

² Lásd a sajtóközleményt: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.

³ Uo.

⁴ Az Európai Adatvédelmi Testület elemzése a koreai kormány által készített hivatalos fordításokon alapul.

⁵ WP254, GDPR-megfelelési referencia, 2018. február 6. (az Európai Adatvédelmi Testület által elfogadott dokumentumot lásd: <https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines>).

⁶ Lásd az Európai Adatvédelmi Testület 2020. november 10-én elfogadott, a megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról szóló 02/2020. számú ajánlását: https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

1.1. Felzárkózási területek

5. Az Európai Adatvédelmi Testület alapvető célkitűzése, hogy véleményt adjon az Európai Bizottság számára arról, hogy megfelelő szintű védelmet biztosítanak-e azoknak a természetes személyeknek, akiknek a személyes adatait a Koreai Köztársaságba továbbítják. Fontos felismerni, hogy az Európai Adatvédelmi Testület nem azt várja el, hogy a koreai jogi keret az európai adatvédelmi jogszabályok pontos másolata legyen.
6. Az Európai Adatvédelmi Testület emlékeztet azonban arra, hogy a GDPR 45. cikke és az Európai Unió Bírósága (a továbbiakban: **EUB**) ítélkezési gyakorlata alapján ahhoz, hogy a biztosított védelmi szint megfelelőnek tekinthető legyen, a harmadik ország jogszabályait összhangba kell hozni a GDPR-ben foglalt alapelvek lényeges tartalmával. Ebben az összefüggésben a koreai adatvédelmi keret számos hasonlóságot mutat az európai adatvédelmi kerettel: mind az állami, mind a magánszektorra egy fő jogszabály vonatkozik, amelyet ágazatspecifikus jogszabályok egészítenek ki.
7. A tartalmat illetően az Európai Adatvédelmi Testület véleménye szerint vannak olyan fontos területek, ahol a koreai adatvédelmi keretet bizonyos alapvető rendelkezések tekintetében össze kell hangolni a GDPR által nyújtott kerettel – ilyenek például a fogalmak (pl. „személyes adat”, „adatkezelés”, „érintett”), a jogos célokból történő jogszerű és tisztességes adatkezelés alapjai; a célhoz kötöttség; az adatminőség és az arányosság; az adatmegőrzés, az adatbiztonság és a titoktartás; az átláthatóság; és a személyes adatok különleges kategóriái.
8. A fentiek mellett az Európai Adatvédelmi Testület üdvözli az Európai Bizottság és a koreai hatóságok annak biztosítására tett erőfeszítéseit, hogy a Koreai Köztársaság a GDPR által előírtaknak megfelelő szintű védelmet nyújtson, és ennek érdekében a koreai felügyeleti hatóság Értesítéseket fogadjon el a GDPR és a koreai adatvédelmi keret közötti különbségek csökkentése céljából (amelyeket nem csupán az EGT-ből Koreába továbbított személyes adatokra kell alkalmazni). Ebben az összefüggésben az Európai Adatvédelmi Testület szeretné kiemelni ezeknek az Értesítéseknek a fontosságát a Koreai Köztársaság megfelelőségének értékelése szempontjából, megjegyezve például, hogy lényeges pontosításokkal szolgálnak egyes fontos garanciákkal kapcsolatban, többek között az adatvédelmi törvény alóli mentességek alkalmazási körét illetően az álnevesített személyes adatok tudományos, kutatási és statisztikai célú kezelése, az újbóli továbbítás és a közhatalmi szervek adatokhoz való hozzáféréseire vonatkozó szabályok esetében.

1.2. Kihívások

9. Noha az Európai Adatvédelmi Testület sok olyan szempontot azonosított, amelyek tekintetében a koreai adatvédelmi keret lényegében megegyezik az európai adatvédelmi kerettel, azt is megállapította, hogy bizonyos szempontok alaposabb vizsgálatot és tisztázást igényelnek. Az Európai Adatvédelmi Testület úgy véli, hogy az alapvetően azonos szintű védelem megvalósulása érdekében a következőkben ismertetett elemeket tovább kell értékelnie és szoros figyelemmel kell kísérnie az Európai Bizottságnak.

1.2.1. Általános kérdések

10. Az Európai Adatvédelmi Testület tudomásul veszi, hogy a 2021-1. számú Értesítés *a személyesadat-kezelőre nézve jogilag kötelező erejű közigazgatási szabálynak minősül abban az értelemben, hogy az Értesítésben foglaltak bármilyen megsértése az adatvédelmi törvény vonatkozó rendelkezései megsértésének tekinthető*⁷. Figyelembe véve azonban azt, hogy az Értesítés nem további önálló szabályokat, hanem inkább az adatvédelmi törvény szövegének az értelmezését és alkalmazását segítő magyarázatokat tartalmaz, és tekintve, hogy összességében milyen fontos szerepet tölt be, különösen az adatvédelmi törvény álnevesítést szabályozó rendelkezései vonatkozásában, amelyek az Európai

⁷ Lásd a határozattervezet I. mellékletének I. szakaszát.

Adatvédelmi Testület tudomása szerint folyamatban lévő bírósági ügyek tárgyát is képezik, az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy nyújtson további felvilágosítást a 2021-1. számú Értesítés kötelező jellegét, érvényesíthetőségét és érvényességét illetően, és ajánlja a benne foglaltak gyakorlatban való tiszteletben tartásának a gondos figyelemmel kísérését, különös tekintettel nemcsak a koreai felügyeleti hatóság, hanem a bíróságok általi alkalmazásra is, elsősorban azokban az esetekben, amikor a koreai jogi keret által biztosított azonos szintű védelem az Értesítésben nyújtott magyarázatokon alapul.

1.2.2. Általános adatvédelmi kérdések

11. A megfeleléségi határozat hatályával kapcsolatban az Európai Adatvédelmi Testület megjegyzi, hogy a határozat az EGT-ből az adatvédelmi törvény hatálya alá tartozó személyesadat-kezelőkhöz történő adattovábbításra vonatkozik majd, egyaránt beleértve az állami és a magánszektorbeli „személyesadat-kezelők” felé történő továbbítást. Az Európai Adatvédelmi Testület úgy értelmezi, hogy ez a kifejezés a GDPR szerinti adatfeldolgozókat is magában foglalja, de a félreértések elkerülése végett felkéri az Európai Bizottságot, hogy tegye egyértelműbbé azt, hogy a megfeleléségi határozat hatálya a Koreában tevékenykedő „adatfeldolgozók” részére történő adattovábbításra is kiterjed.
12. Az Európai Adatvédelmi Testület szeretné felhívni a figyelmet a koreai adatvédelmi keret egy fontos elemére, amely az álnevesített adat fogalmához kapcsolódik. A koreai jog értelmében számos vonatkozó rendelkezés alóli mentesség, az érintettek egyéni jogaira és az adatmegőrzésre vonatkozó rendelkezések alóli mentességeket is beleértve, álnevesített személyes adatok kezelése esetén is alkalmazható. Az Európai Bizottság szerint ez csak akkor van így, ha az álnevesített személyes adatok kezelését statisztikai, tudományos kutatási vagy közérdekű archiválási célokból végzik. Ezt az állítást azonban főként a 2021-1. számú Értesítés támasztja alá, ami ebben az összefüggésben különösen szükségessé teszi az Értesítés kötelező jellegére, érvényesíthetőségére és érvényességére vonatkozó további információkat és ellenőrzéseket. Mindezeket túl az Európai Adatvédelmi Testület annak további értékelésére is felkéri az Európai Bizottságot, hogy a koreai jog értelmében milyen hatást gyakorol az álnevesítés és – ami a legfontosabb – hogyan befolyásolhatja az alapvető jogait és szabadságait azoknak az érintetteknek, akiknek a személyes adatait a megfeleléségi határozat alapján a Koreai Köztársaságba továbbítják. Az Európai Adatvédelmi Testület különösen arra szólítja fel az Európai Bizottságot, hogy végezzen további értékelést az adatvédelmi törvény 28. cikkének (7) bekezdésében és a hiteladat-védelmi törvény 40. cikkének (3) bekezdésében foglalt eltéréseket illetően, valamint kísérje gondos figyelemmel ezek alkalmazását és a vonatkozó ítélkezési gyakorlatot annak biztosítása érdekében, hogy az érintettek jogait ne korlátozzák indokolatlanul a megfeleléségi határozat alapján továbbított személyes adatok e célokból történő kezelése során.
13. Az Európai Adatvédelmi Testület megállapítja továbbá, hogy a koreai jog értelmében a hozzájárulás visszavonásának joga csak bizonyos körülmények között gyakorolható, és ezért felkéri az Európai Bizottságot, hogy a hozzájárulás visszavonásához való általános jog hiányának a hatását illetően folytasson további értékelést, és nyújtson további biztosítékokat arra, hogy az alapvető szintű adatvédelem mindig garantált, szükség esetén tisztázva ehhez azt is, hogy a hozzájárulás visszavonásához való általános jog hiányára figyelemmel milyen szerepet tölt be az adatvédelmi törvény szerinti felfüggesztési jog.
14. Az újbóli továbbítást illetően az Európai Adatvédelmi Testület elismeri, hogy a koreai személyesadat-kezelőtől a harmadik országbeli címzetthez történő adattovábbítás általában az érintett tájékozott hozzájárulásán alapul, és a 2021-1. számú Értesítés szerint az egyéneket tájékoztatni kell arról a harmadik országról, amelybe az adataikat továbbítják. Mindazonáltal az Európai Adatvédelmi Testület felkéri az Európai Bizottságot annak biztosítására, hogy az érintettnek nyújtandó tájékoztatás az adattovábbítás harmadik ország által biztosított megfelelő védelem és a megfelelő garanciák hiányából adódó lehetséges kockázataira vonatkozó információkat is tartalmazzon. Az Európai Adatvédelmi Testület örömmel fogadná továbbá azt, ha a megfeleléségi határozat további biztosítékokat

tartalmazna arra, hogy a koreai személyesadat-kezelők nem továbbítanak személyes adatokat harmadik országba olyan helyzetekben, amikor a GDPR szerinti érvényes hozzájárulást nem lehetett megadni, például egyenlőtlen erőviszonyok következtében.

15. Ami a koreai felügyeleti hatóság tagjainak a kinevezését illeti, bár a hivatalos eljárás összhangban áll a GDPR-ral, és ezáltal teljesíti az EGT-re vonatkozó jogi kerettel való azonosság feltételeit, az Európai Adatvédelmi Testület üdvözlőné, ha az Európai Bizottság figyelemmel kísérné azokat a fejleményeket, amelyek a dél-koreai felügyeleti hatóság tagjainak a függetlenségére hatással lehetnek.
16. A költségvetést illetően – ugyancsak az Európai Bizottságtól kapott tájékoztatás alapján – semmilyen utalás nem szerepel az Adatvédelmi Bizottság személyzetének jellemzőire vagy a rendelkezésére bocsátott pénzügyi forrásokra. Az Európai Adatvédelmi Testület ezért örömmel venné, ha a határozattervezet további információkat tartalmazna erre a két fontos témára vonatkozóan.

1.2.3. A közhatalmi szervek Koreai Köztársaságba továbbított adatokhoz való hozzáférésére

17. Az Európai Adatvédelmi Testület az EGT-ből Koreába továbbított személyes adatokhoz való, bűnüldözési és nemzetbiztonsági célú kormányzati hozzáférés tekintetében is elemezte a koreai jogi keretet. Miközben elismeri a koreai kormány által nyújtott információkat és biztosítékokat, amelyek vázlatos ismertetését a határozattervezet II. melléklete tartalmazza, az Európai Adatvédelmi Testület több olyan szempontot azonosított, amely tisztázásra szorul, vagy aggodalomra ad okot.
18. Az Európai Adatvédelmi Testület megállapítja, hogy az adatvédelmi törvény rendelkezései korlátozás nélkül alkalmazandók a bűnüldözés területén. Megállapítja továbbá, hogy a nemzetbiztonság területén folytatott adatkezelést az adatvédelmi törvény rendelkezéseinek szűkebb köre szabályozza.
19. A személyes adatok nemzetbiztonsági hatóságok számára történő, távközlési szolgáltatók általi önkéntes kiadása kapcsán az Európai Adatvédelmi Testületet aggasztja, hogy nem világos, hogy a határozattervezet I. mellékletének 3. szakasza, amely szerint az adatközlésre vonatkozó felhívás önkéntes teljesítése esetén az adatközlőnek elvileg értesítenie kell az érintettet, milyen kapcsolatban áll az adatvédelmi törvény 58. cikke (1) bekezdésének 2. pontjával, azaz a nemzetbiztonsági célú részleges mentesítéssel. Ez csökkentheti a tájékoztatásra vonatkozó követelmények hatékonyságát, jelentős mértékben megnehezítve az érintettek számára adatvédelmi jogaik érvényesítését, különösen a bírósági jogorvoslat vonatkozásában.
20. Bár a határozattervezet kifejezetten nem tesz róla említést, az Európai Bizottság által adott magyarázatok alapján az Európai Adatvédelmi Testület úgy véli, hogy a koreai jogi keret nem teszi lehetővé a távközlés tömeges lehallgatását. Ezért az Emberi Jogok Európai Bíróságának (EJEB) tömeges lehallgatásra vonatkozó szabályokra vonatkozó közelmúltbeli ítélkezési gyakorlata nem bír közvetlen jelentőséggel a Koreában biztosított adatvédelmi szint értékelése szempontjából.
21. A határozattervezet semmilyen információt nem tartalmaz a nemzetbiztonság területén végzett újbóli továbbításra vonatkozó jogi keretet illetően. Az Európai Adatvédelmi Testület úgy értelmezte, hogy az Európai Bizottság véleménye szerint a nemzetbiztonsági célokból végzett újbóli továbbítást kellően szabályozzák az alkotmányos keretből és az adatvédelmi törvényből következő általános garanciák és elvek, de aggódik amiatt, hogy ez mennyiben tekinthető a jogi pontosság és egyértelműség követelményei teljesülésének, és mennyire hatékony és érvényesíthető garanciákat biztosít. A garanciák, amelyekre az Európai Bizottság hivatkozik, nagyon általános jellegűek, és a jogalapjuk nem tér ki arra, hogy a nemzetbiztonsági célokból végzett újbóli továbbításra milyen konkrét körülmények között és feltételek mellett kerülhet sor. Ezzel kapcsolatban az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az Európai Bizottság nem vette figyelembe, hogy létezhetnek olyan, a Koreai Köztársaság és harmadik országok, illetve nemzetközi szervezetek között létrejött nemzetközi megállapodások, amelyek a személyes adatok bűnüldözési és/vagy hírszerzői szolgálatok általi, harmadik országok felé történő nemzetközi továbbítására vonatkozó külön rendelkezéseket tartalmazhatnak. Az Európai Adatvédelmi Testület úgy véli, hogy a bűnüldözési vagy hírszerzési együttműködés céljából

harmadik országokkal kötött két- vagy többoldalú megállapodások hatással lehetnek az adatvédelemre vonatkozó koreai jogi keret értékelésére.

22. Az Európai Adatvédelmi Testület megállapítja, hogy a bűnüldöző és nemzetbiztonsági hatóságok felügyeletét különböző belső és külső szervek együttese – különösen az elegendő végrehajtói hatáskörrel felruházott Adatvédelmi Bizottság – biztosítja.
23. A hatékony jogorvoslat biztosítása megköveteli, hogy az érintettek olyan illetékes szervhez fordulhassanak, amely megfelel az Európai Unió Alapjogi Chartája (**a Charta**) 47. cikkében foglalt előírásoknak, azaz hatáskörrel rendelkezik ahhoz, hogy megállapítsa az adatkezelés tényét, ellenőrizze az adatkezelés jogszerűségét, és jogellenes adatkezelés esetén jogorvoslatot biztosítson. Ennek tükrében az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy ismertesse a Adatvédelmi Bizottságnál történő panasztételre vagy a bíróság előtti keresetindításra vonatkozó tartalmi és/vagy eljárási követelményeket, így például a bizonyítási teherre vonatkozó szabályokat, és tisztázza, hogy az EGT-állampolgárok képesek lennének-e teljesíteni ezeket az előfeltételeket.

1.3. Következtetés

24. Az Európai Adatvédelmi Testület úgy véli, hogy ez a megfeleléségi határozat rendkívüli jelentőséggel bír, figyelembe véve azt is, hogy – a véleményben kiemelt kivételekkel – a hatálya egyaránt kiterjed majd az állami és a magánszektorbeli adattovábbításra.
25. Az Európai Adatvédelmi Testület üdvözli az Európai Bizottság és a koreai hatóságok azon erőfeszítéseit, hogy a koreai jogi keretet összehangolják az európaival. A 2021-1. számú Értesítés által a két keretrendszer közötti különbségek áthidalása érdekében bevezetni kívánt fejlesztések nagyon fontosak és a fogadtatásuk is jó. Mindazonáltal az Európai Adatvédelmi Testület szerint számos aggály továbbra is fennáll, többek között a 2021-1. számú Értesítéssel kapcsolatban, és vannak kérdések, amelyek további tisztázást igényelnek. Ezért azt ajánlja az Európai Bizottságnak, hogy vizsgálja meg az Európai Adatvédelmi Testület által megfogalmazott aggodalmakat és pontosításra irányuló kéréseket, és adjon további felvilágosítást és magyarázatokat a véleményben felvetett problémákat illetően.

2. BEVEZETÉS

2.1. A koreai adatvédelmi keret

26. A Koreai Köztársaság adatvédelmet szabályozó fő jogszabálya a személyes adatok védelméről szóló törvény (a legutóbb a 2020. február 4-i 16930. számú törvénnyel módosított, 2011. március 29-i 10465. számú törvény, az „**adatvédelmi törvény**”). A törvényt kiegészítő végrehajtási rendelet (a legutóbb a 2020. augusztus 4-i 30892. számú elnöki rendelettel módosított, 2011. szeptember 29-i 23169. számú elnöki rendelet, az „adatvédelmi törvény végrehajtási rendelete”), jogilag kötelező erejű és végrehajtható.
27. Az adatvédelmi törvény mellett a koreai adatvédelmi kerethez tartoznak továbbá a koreai felügyeleti hatóság által kiadott „Értesítések”, valamint a személyes adatok védelméért felelős bizottság (**Adatvédelmi Bizottság**), amely az adatvédelmi törvény értelmezésére és alkalmazására vonatkozó további szabályokat határozza meg. Az Adatvédelmi Bizottság nemrégiben fogadta el az adatvédelmi törvény egyes rendelkezéseinek értelmezéséről, alkalmazásáról és végrehajtásáról szóló, 2021. január 21-i 2021-1. számú Értesítést (amely a korábbi 2020. szeptember 1-i 2020-10. számú Értesítést módosította, a továbbiakban: **2021-1. számú Értesítés**). Ez az Értesítés a koreai hatóságok és az Európai Bizottság megfeleléség tárgyában tartott megbeszéléseinek az eredménye. Az adatvédelmi törvény egyes rendelkezéseinek, többek között a Koreába továbbított személyes adatok tervezett megfeleléségi határozaton alapuló kezeléséről szóló rendelkezéseknek az alkalmazására vonatkozó

magyarázatokat tartalmaz⁸, és a személyes adat-kezelőre nézve jogilag kötelező erejű közigazgatási szabálynak minősül abban az értelemben, hogy az Értesítésben foglaltak bármilyen megsértése az adatvédelmi törvény vonatkozó rendelkezései megsértésének tekinthető⁹. Ezzel kapcsolatban az Európai Adatvédelmi Testület meg kívánja jegyezni, hogy bár a határozattervezet „kiegészítő szabályokként” utal rá, az Értesítés nem további önálló szabályokat tartalmaz, hanem inkább magyarázatokat nyújt, melyek célja annak pontosítása, hogy az adatvédelmi törvény szövege hogyan értelmezendő és alkalmazandó, különösen az EGT-ből továbbított adatok vonatkozásában. Ennek fényében az Európai Adatvédelmi Testület ajánlja a 2021-1. számú Értesítés gyakorlatban való tiszteletben tartásának gondos figyelemmel kísérését, különös tekintettel nemcsak az Adatvédelmi Bizottság, hanem a bíróságok általi alkalmazásra is, elsősorban azokban az esetekben, amikor a koreai jogi keret által biztosított azonos szintű védelem a 2021-1. számú Értesítésben nyújtott magyarázatokon alapul.

28. A személyes adatok kezelésének egyes ágazatokra vonatkozó szabályait a koreai jogszabályi kerethez tartozó más vonatkozó adatvédelmi jogszabályok határozzák meg, például
- a hiteladatok felhasználásáról és védelméről szóló törvény (**hiteladat-védelmi törvény**), beleértve annak végrehajtási rendeletét (**a hiteladat-védelmi törvény végrehajtási rendelete**), amely a pénzügyi vagy kereskedelmi tranzakciókban részt vevő felek hitelképességének meghatározásához szükséges személyes hiteladatokat kezelő gazdasági szereplőkre és szakosodott szervezetekre (például hitelminősítő intézetekre, pénzügyi intézményekre) alkalmazandó szabályokat határozza meg;
 - az információs és kommunikációs hálózatok használatának előmozdításáról és a hálózaton továbbított adatok védelméről szóló törvény (**a hálózatokra vonatkozó törvény**); valamint
 - a hírközlési adatvédelmi törvény.
29. A kormányzati hozzáférés terén az adatvédelmi törvény és a hírközlési adatvédelmi törvény vonatkozó rendelkezései mellett más jogszabályokat is figyelembe vett az Európai Adatvédelmi Testület. Ezek a büntetőeljárás törvény, a távközlési vállalkozásokról szóló törvény, a bizonyos pénzügyi tranzakciók adatainak jelentéséről és felhasználásáról szóló törvény (a pénzmosás és terrorizmus-finanszírozás elleni törvény) és a nemzeti hírszerző szolgálatról szóló törvény voltak.

2.2. Az Európai Adatvédelmi Testület értékelésének hatóköre

30. Az Európai Bizottság határozattervezete a koreai adatvédelmi keret értékelésének és az azt követő, a koreai kormánnyal folytatott megbeszéléseknek az eredménye. A GDPR 70. cikke (1) bekezdésének s) pontja szerint az Európai Adatvédelmi Testületnek független véleményt kell adnia az Európai Bizottság megállapításairól, azonosítania kell a megfelelőségi keret hiányosságait (ha vannak), és törekednie kell arra, hogy javaslatokat tegyen ezek kezelésére.
31. Az ismétlések elkerülése érdekében és a koreai jogi keret értékelésének a segítése céljából az Európai Adatvédelmi Testület úgy döntött, hogy a határozattervezetben bemutatott néhány konkrét szempontra összpontosítva nyújt elemzést és véleményt, tartózkodva attól, hogy a ténymegállapítások és értékelések többségét megismételje, amennyiben nincs oka feltételezni, hogy a Koreai Köztársaság joga lényegében nem azonos az EGT-joggal. Emellett – az EUB ítélezési gyakorlatával összhangban – az elemzésnek egy nagyon fontos része a Koreai Köztársaságba továbbított személyes adatokhoz való nemzetbiztonsági hozzáférés jogi szabályozásával és a nemzetbiztonsági apparátus gyakorlatával foglalkozik.

⁸ Lásd a határozattervezet I. mellékletének I. szakaszát.

⁹ Uo.

32. Értékelése során az Európai Adatvédelmi Testület figyelembe vette az alkalmazandó európai adatvédelmi keretet, többek között a Charta magán- és családi élethez való jog tiszteletben tartásáról szóló 7. cikkét, a személyes adatok védelméhez való jogról szóló 8. cikkét, valamint a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogról szóló 47. cikkét, továbbá az Emberi Jogok Európai Egyezménye (EJEE) magán- és családi élethez való jog tiszteletben tartásáról szóló 8. cikkét. A fentiek mellett az Európai Adatvédelmi Testület a GDPR előírásait és a vonatkozó ítélkezési gyakorlatot is megvizsgálta.
33. E munka célja az volt, hogy az Európai Bizottságnak véleményt adjon a Koreai Köztársaságban biztosított védelmi szint megfelelőségének az értékeléséről. A „megfelelő szintű védelem” fogalmát, amely már akkor is létezett, amikor még a 95/46/EK irányelv volt hatályban, az EUB továbbfejlesztette. Fontos emlékeztetni az EUB által a Schrems I ügyben felállított normára, vagyis arra, hogy – bár a harmadik országban biztosított „védelmi szintnek” „lényegében azonosnak” kell lennie az EU-ban biztosítottal – *„azok az eszközök, amelyeket a harmadik ország az ilyen védelmi szint biztosításához e tekintetben igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket az Unióban alkalmaznak”*¹⁰. Ezért nem az a cél, hogy pontról pontra lemásolják az európai jogszabályokat, hanem az, hogy létrejöhessen a vizsgált jogszabályok alapvető és fő követelményei. A megfelelőség az érintetteknek biztosított jogok, a személyes adatok kezelői vagy az adatkezelést ellenőrzők számára előírt kötelezettségek és a független szervezetek által végzett felügyelet együttes alkalmazásával érhető el. Az adatvédelmi szabályok azonban csak akkor eredményesek, ha végrehajthatók és a gyakorlatban követhetők. Ezért nemcsak a harmadik országba vagy nemzetközi szervezetekhez továbbított személyes adatokra vonatkozó szabályok tartalmát, hanem az ezeknek a szabályoknak az eredményességét biztosító rendszer tartalmát is figyelembe kell venni. Az adatvédelmi szabályok eredményessége szempontjából rendkívül fontosak a hatékony végrehajtási mechanizmusok¹¹.

2.3. Általános megjegyzések és aggályok

2.3.1. A Koreai Köztársaság által vállalt nemzetközi kötelezettségek

34. A GDPR 42. cikke (2) bekezdésének (c) pontja és a GDPR-megfelelőségi referencia szerint¹² egy harmadik ország adatvédelmi szintje megfelelőségének értékelése során az Európai Bizottságnak figyelembe kell vennie többek között a harmadik ország által vállalt nemzetközi kötelezettségeket, illetve a harmadik ország többoldalú vagy regionális rendszerekben való részvételéből fakadó egyéb kötelezettségeket, különös tekintettel a személyes adatok védelméhez kapcsolódókra, és az ilyen kötelezettségek teljesítését is vizsgálnia kell.
35. Korea részes fél több olyan nemzetközi megállapodásban, amely a magánélethez való jogot garantálja – ilyen például a Polgári és Politikai Jogok Nemzetközi Egyezségokmánya (17. cikk), a Fogyatékosjogi Egyezmény (22. cikk) és a Gyermejjogi Egyezmény (16. cikk). Korea emellett tagja az OECD-nek, és betartja a magánélet védelmével kapcsolatos OECD-keretben és különösen a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelvekben foglaltakat.
36. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy Korea megfigyelő államként részt vesz az Európa Tanács 108(+) Egyezményének tanácsadó bizottsága által végzett munkában, bár az egyezményhez való csatlakozásról még nem döntött.

¹⁰ C-362/14, *Maximilian Schrems kontra adatvédelmi biztos*, 2015. október 6., ECLI:EU:C:2015:650, 73-74. bekezdés.

¹¹ WP254, 2. o.

¹² WP254, 2. o.

2.3.2. A megfeleléségi határozat hatálya

37. A határozattervezet (5) preambulumbekzdése szerint az Európai Bizottság arra a következtetésre jutott, hogy a Koreai Köztársaság megfelelő szintű védelmet biztosít az Unióban tevékenykedő adatkezelőtől vagy adatfeldolgozótól az adatvédelmi törvény hatálya alá eső személyesadat-kezelők (pl. természetes vagy jogi személyek, szervezetek, közintézmények) felé továbbított személyes adatok számára, kivéve azokat az eseteket, amikor a személyesadat-kezelés célja vallási szervezet által végzett hittérítő tevékenység vagy politikai párt általi jelöltállítás¹³, vagy a személyes hiteladatok hiteladatvédelmi törvény szerinti kezelését a Pénzügyi Szolgáltatások Bizottságának felügyelete alá tartozó adatkezelők végzik.
38. Az Európai Adatvédelmi Testület megjegyzi, hogy a határozat az EGT-ből az adatvédelmi törvény hatálya alá tartozó személyesadat-kezelőkhöz történő adattovábbításra vonatkozik majd, az állami és a magánszektorbeli „személyesadat-kezelők” felé történő továbbítást egyaránt beleértve. Az Európai Adatvédelmi Testület úgy értelmezi, hogy a „személyesadat-kezelő” kifejezés a GDPR szerinti értelemben vett adatfeldolgozókat is magában foglalja, mivel az adatvédelmi törvény rájuk is vonatkozik, és hogy egyedi kötelezettségek vonatkoznak arra az esetre, amikor a személyesadat-kezelő (az adatkezelést kihelyező megbízó) egy harmadik felet (a kihelyezett tevékenységet végző szolgáltatót) bíz meg a személyes adatok kezelésével, de a félreértések elkerülése végett felkéri az Európai Bizottságot, hogy tegye egyértelműbbé azt, hogy a megfeleléségi határozat hatálya a Koreában tevékenykedő „adatfeldolgozók” részére történő adattovábbításra is kiterjed majd, és hogy az EGT-ből továbbított személyes adatok számára biztosított védelem szintje ezekben az esetekben sem lehet alacsonyabb.
39. Emellett, figyelembe véve, hogy a megfeleléségi határozat hatálya a személyes adatok közfeladatot ellátó szervek közötti továbbítására is kiterjed, az Európai Adatvédelmi Testület úgy értelmezi, hogy ez az adatvédelmet felügyelő hatóságok közötti továbbítást is magában foglalja majd, és felkéri az Európai Bizottságot, hogy az egyértelműség érdekében ezt kifejezetten említse meg a határozatban.
40. A megfeleléségi határozat hatálya alól kizárt jogalanyokat illetően az Európai Adatvédelmi Testület hangsúlyozni szeretné, hogy a megfeleléségi határozat hasznára válna, ha pontosabban meghatározná az Adatvédelmi Bizottság felügyelete alá tartozó „gazdasági szervezeteket” (a hiteladat-védelmi törvény 45. cikkének (3) bekezdése) annak érdekében, hogy a hiteladat-védelmi törvény hatálya alá tartozó jogalanyok részére történő adattovábbítást megelőzően az EGT-beli adatkezelők és adatfeldolgozók könnyen megállapíthassák, hogy a megfeleléségi határozat hatálya kiterjed-e az importőrre, vagy legalább tudatában legyenek annak, hogy ezt ellenőrizniük kell.
41. A megfeleléségi határozat hatályával kapcsolatban az Európai Adatvédelmi Testület azt szűrte le az Európai Bizottság kiegészítő magyarázataiból, hogy a Pénzügyi Szolgáltatások Bizottsága keretében létrehozott Koreai Pénzügyi Hírszerző Egység (KOFIU), amely a bizonyos pénzügyi tranzakciók adatainak jelentéséről és felhasználásáról szóló törvény alapján a pénzmosás és a terrorizmus-finanszírozás megelőzését felügyeli¹⁴, szintén ki van zárva a határozat hatálya alól, mivel a hatásköre csak olyan pénzügyi intézményekre terjed ki, amelyek maguk sem tartoznak a határozattervezet hatálya alá. A határozattervezet 1. cikke (2) bekezdésének (c) pontja azonban csak a Pénzügyi Szolgáltatások Bizottságának a felügyelete alá tartozó és a hiteladat-védelmi törvény alapján személyes hiteladatok kezelését végző személyesadat-kezelőket zárja ki a határozat hatályából. Mindezek alapján az Európai Adatvédelmi Testület kéri az Európai Bizottságot, hogy tegye egyértelművé, vajon a KOFIU és az KOFIU által végzett adatkezelési tevékenységek a határozattervezet hatálya alá tartoznak-e.

¹³ Részletesebben lásd alább a jelen vélemény 3.1.2. szakaszában.

¹⁴ Lásd a II. melléklet., 2.2.3.1. szakaszát.

3. ÁLTALÁNOS ADATVÉDELMI SZEMPONTOK

3.1. Tartalmi elvek

42. A „tartalmi elvekkel” a GDPR-megfelelőségi referencia 3. fejezete foglalkozik. Egy harmadik ország rendszerének ezeket tartalmaznia kell ahhoz, hogy a biztosított védelmi szintet az uniós jogszabályok által biztosítottal lényegében azonosnak lehessen tekinteni.
43. Bár a koreai alkotmány önálló jogként kifejezetten nem rögzíti a személyes adatok védelméhez való jogot, alapvető jogként való elismerése olyan alkotmányos jogokból következik, mint az emberi méltósághoz és boldogságra törekvéshez való jog (10. cikk), a magánélet tiszteletben tartásához való jog (17. cikk) és a hírközlési adatvédelemhez való jog (18. cikk). Ezt a Legfelsőbb Bíróság és az Alkotmánybíróság is megerősítette, amint azt az Európai Bizottság határozattervezete is említi¹⁵. Az Európai Adatvédelmi Testület fontosnak tartja az adatvédelemhez való jog alapvető jogként való elismerését, mert ebből eredően az adatvédelemhez való jogot mint alapvető jogot a koreai alkotmány 37. cikke szerint *„csak törvénnyel lehet korlátozni és csak akkor ha az nemzetbiztonsági okból, a közrend fenntartása vagy a közjó érdekében szükséges”, és „a szabadság vagy jog lényegét még az ilyen korlátozás sem érintheti”*.
44. Az Európai Bizottság állítása szerint¹⁶ az Alkotmánybíróság kimondta, hogy az alapvető jogok a külföldi állampolgárokat is megilletik. A koreai kormány hivatalos nyilatkozatai szerint¹⁷ eddig nem született olyan ítélet, amely kifejezetten a nem koreai állampolgárok magánélethez való jogára vonatkozna, de tudós körökben általánosan elfogadott, hogy az alkotmány 12-22. cikkei az „emberi jogokat” tartalmazzák. A Koreai Köztársaság egy sor olyan jogszabályt fogadott el az adatvédelem területén, így például az adatvédelmi törvényt, amelyek állampolgárságtól függetlenül minden ember számára garanciákat nyújtanak. E tekintetben az Európai Adatvédelmi Testület megjegyzi, hogy az alkotmány 6. cikkének (2) bekezdése szerint a külföldi állampolgárokat megillető jogok a nemzetközi jog és egyezmények előírásainak, valamint a határozattervezetben említett ítélkezési gyakorlatnak megfelelően garantáltak, azaz a „külföldieket” is megilletik az „alapvető jogok”. Tekintettel a „külföldi állampolgárok” adatvédelemhez való joga elismerésének a fontosságára, az Európai Adatvédelmi Testület felhívja az Európai Bizottság figyelmét, hogy folyamatosan figyelemmel kell kísérni a nemcsak a koreai állampolgárok, hanem minden érintett alapvető jogaként elismert adatvédelemhez való joggal kapcsolatos ítélkezési gyakorlatot annak biztosítása érdekében, hogy a természetes személyek GDPR által garantált védelmi szintje ne csökkenjen a személyes adatok megfeleléségi határozat alapján történő, Koreába irányuló továbbítása során.

3.1.1. Fogalmak

45. A GDPR-megfelelőségi referencia alapján az alapvető adatvédelmi fogalmaknak és/vagy elveknek léteznük kell a harmadik ország jogi keretében. Nem kell megegyezniük a GDPR terminológiájával, de tükrözniük kell az európai adatvédelmi törvényben foglalt fogalmakat, és azokkal összhangban kell állniuk. A GDPR például az alábbi fontos fogalmakat tartalmazza: „személyes adat”, „a személyes adatok kezelése”, „adatkezelő”, „adatfeldolgozó”, „címezett” és „különleges adat”¹⁸.
46. Az adatvédelmi törvény számos fogalom meghatározása nagyon hasonlít az adott fogalom GDPR szerinti megfelelőjének a meghatározására – ilyen például a „személyes adat”, az „adatkezelés” és az „érintett” fogalmának a meghatározása.

¹⁵ Lásd a határozattervezet (8) preambulumbekendését és a 10. lábjegyzetben hivatkozott vonatkozó ítélkezési gyakorlatot, amelyről csak angol nyelvű összefoglalók állnak rendelkezésre.

¹⁶ Lásd a határozattervezet (9) preambulumbekendését.

¹⁷ A határozattervezet II. mellékletének 1.1. szakasza.

¹⁸ WP254, 4. o.

3.1.1.1. Az álnevesített adat fogalma

47. A fogalom meghatározások között az adatvédelmi törvény 2. cikkének (1) bekezdése a személyes adatot úgy határozza meg mint az élő természetes személyre vonatkozó következő adatok bármelyike: (a) egy adott természetes személyt teljes neve, lakossági nyilvántartási száma, képe stb. alapján azonosító adat, valamint (b) olyan adat, amely önmagában nem azonosít egy adott természetes személyt, de könnyen összekapcsolható más adatokkal oly módon, hogy egy adott természetes személy azonosítható legyen. Ez utóbbi esetben a könnyű összekapcsolhatóság megítélése az azonosításhoz szükséges idő, költség, technológia stb. ésszerű mérlegelésén alapul, így például annak valószínűségén, hogy az adat, amivel a szóban forgó adatot össze lehetne kapcsolni, előállítható-e.
48. Az adatvédelmi törvény 2. cikke (1) bekezdésének (c) pontja szerint az „álnevesített adat” is személyes adatnak minősül. Meghatározása szerint az álnevesített adat olyan, a fenti (a) vagy (b) pont alá tartozó adat, amely az 1-2. albekezdés szerinti álnevesítés következtében az eredeti állapotba történő visszaállításhoz szükséges információ felhasználása vagy az azzal való összekapcsolása nélkül nem teszi lehetővé egy adott természetes személy azonosítását. A teljes mértékben anonimizált adatok nem tartoznak az adatvédelmi törvény hatálya alá. Az adatvédelmi törvény 58. cikkének (2) bekezdése szerint a törvény nem vonatkozik azokra az adatokra, amelyek a szükséges idő, költség, technológia stb. ésszerű mérlegelése alapján már más információval összekapcsolva sem teszik lehetővé egy adott személy azonosítását.
49. Határozattervezete (17) preambulumbekkezdésében az Európai Bizottság kijelenti, hogy ez megfelel a GDPR tárgyi hatályának és a „személyes adat”, az „álnevesítés”, valamint az „anonimizált adat” GDPR szerinti fogalmainak.
50. Az adatvédelmi törvény 28. cikkének (7) bekezdése szerint viszont a 20., 21. és 27. cikkek, a 34. cikk (1) bekezdése, a 35-37. bekezdések, a 39. cikk (3) bekezdése, a 39. cikk (4) bekezdése és a 39. cikk (6)-(8) bekezdései az álnevesített személyes adatokra nem alkalmazandók.
51. Határozattervezetében az Európai Bizottság kijelenti, hogy az adatvédelmi törvény 28. cikkének (7) bekezdése csak akkor alkalmazandó az álnevesített személyes adatokra, ha azok kezelését statisztikai, tudományos kutatási vagy közérdekű archiválási célokból végzik¹⁹. Ez azonban nem közvetlenül a törvény szövegéből, hanem a 2021-1. számú Értesítésben nyújtott magyarázatokból következik²⁰. Az Európai Adatvédelmi Testület elismeri, hogy az adatvédelmi törvény felépítése és logikája alátámasztja azt az érvet, hogy a törvény 28. cikkének (2) bekezdését akként kell érteni és logikusan értelmezni, hogy az a 28. cikk (7) bekezdésére is vonatkozik, de tekintettel arra, hogy a 2021-1. számú Értesítés milyen fontos szerepet tölt be a személyes adatok Koreai Köztársaságban biztosított védelmi szintje megfelelőségének Európai Bizottság általi értékelésében, a kétségek elkerülése végett az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy adjon további felvilágosítást a 2021-1. számú Értesítés kötelező jellegét, érvényesíthetőségét és érvényességét illetően, és kísérje figyelemmel az értesítés ezen konkrét összefüggésben történő alkalmazását.
52. Ezzel kapcsolatban az Európai Adatvédelmi Testület szeretne emlékeztetni arra, hogy a GDPR szerint az álnevesítés ajánlott biztonsági intézkedésként értelmezendő. Másképp fogalmazva, a GDPR szerint az álnevesített adatok továbbra is személyes adatok, amelyekre a GDPR teljes mértékben alkalmazandó. A fentiek alapján az Európai Adatvédelmi Testület aggodalmát fejezi ki amiatt, hogy az álnevesített személyes adatok GDPR által előírt védelmi szintje a személyes adatok Koreába történő továbbítása során sérülhet. Az Európai Adatvédelmi Testület ezért felkéri az Európai Bizottságot annak további értékelésére, hogy az adatvédelmi törvény alapján milyen hatást gyakorol az álnevesítés és –

¹⁹ Lásd többek között a határozattervezet (82) preambulumbekkezdését.

²⁰ A határozattervezet I. mellékletének 4. szakasza.

ami a legfontosabb – hogyan befolyásolhatja az alapvető jogait és szabadságait azoknak az érintetteknek, akiknek a személyes adatait a megfelelőségi határozat alapján a Koreai Köztársaságba továbbítanák. Következésképp az Európai Adatvédelmi Testület felszólítja az Európai Bizottságot, hogy nyújtson biztosítékot arra, hogy az EGT-beli érintettek személyes adatai számára biztosított védelem szintje abban az esetben sem fog csökkenni a Koreai Köztársaságba történő továbbítást követően, ha álnevesített személyes adatokat továbbítanak.

3.1.1.2. A személyesadat-kezelő fogalma

53. A „személyesadat-kezelő” az adatvédelmi törvény 2. cikkének (5) bekezdésében szereplő meghatározás szerint olyan közintézmény, jogi személy, szervezet vagy természetes személy, stb., amely vagy aki „tevékenysége keretében”, személyesadat-állományok működtetése céljából közvetlenül vagy közvetve személyes adatokat kezel. A kiegészítő garanciákat tartalmazó 2021-1. számú Értesítés azonban úgy határozza meg a személyesadat-kezelő fogalmát mint az olyan közintézmény, jogi személy, szervezet, természetes személy, stb., amely vagy aki személyesadat-állományok „üzleti célú” működtetése céljából közvetlenül vagy közvetve személyes adatokat kezel. A határozattervezet 272. lábjegyzete viszont a következőt írja a személyesadat-kezelő fogalmáról: *Ahogy az adatvédelmi törvény 2. cikke meghatározza, vagyis olyan közintézmény, jogi személy, szervezet, természetes személy, stb., amely vagy aki személyesadat-állományok „hivatalos vagy üzleti célú” működtetése céljából közvetlenül vagy közvetve személyes adatokat kezel.*
54. Az Európai Adatvédelmi Testület elismeri, hogy ezek az eltérések adódhatnak az eredeti szövegek koreai hatóságok által végzett fordításából, és felkéri az Európai Bizottságot, hogy rendszeresen ellenőrizze a fordítások minőségét és megbízhatóságát. Mindazonáltal az Európai Adatvédelmi Testület hangsúlyozza azt a tényt, hogy ahhoz, hogy a koreai jogi keret által biztosított adatvédelmi szint lényegi azonosságát értékelni lehessen, az adatvédelmi törvény hatálya alá eső adatkezelési célok világos megértésére van szükség. Ezzel kapcsolatban az Európai Adatvédelmi Testület megállapítja továbbá, hogy az „adatkezelő” és az „adatfeldolgozó” fogalmát illetően az adatvédelmi törvény nem ugyanazt a terminológiát használja, mint a GDPR, és felkéri az Európai Bizottságot, hogy pontosítsa, hogyan kell helyesen meghatározni „a személyesadat-kezelő” fogalmát, és hogy mit takar ez a fogalom, különös tekintettel arra, hogy a GDPR meghatározása szerinti adatfeldolgozókat is magában foglalja-e, mivel ez közvetlenül befolyásolja a megfelelőségi határozat hatályát²¹.

3.1.2. Az adatvédelmi törvény szerinti részleges mentességek

55. Az adatvédelmi törvény 58. cikkének (1) bekezdése szerint az adatvédelmi törvény egyes részei (azaz a 15-57. cikkek) nem alkalmazandók a személyesadat-kezelés alábbiakban ismertetett négy kategóriájára. A mentességek az adatvédelmi törvény különleges okokból történő adatkezelést szabályozó rendelkezéseit, bizonyos adatvédelmi köztelezettségeket, az egyéni jogok gyakorlásának részletes szabályait, valamint a vitarendezésre vonatkozó szabályokat érintik. Az Európai Adatvédelmi Testület ugyanakkor megjegyzi, hogy az adatvédelmi törvény egyes általános rendelkezései, így például az adatvédelmi elvekkel és az egyéni jogokkal kapcsolatos rendelkezések (az adatvédelmi törvény 3. és 4. cikke) továbbra is alkalmazandók maradnak. Emellett az adatvédelmi törvény 58. cikkének (4) bekezdése egyedi kötelezettségeket ír elő az adatkezelés e négy kategóriájára vonatkozóan.
56. Először is, részleges mentességet élveznek a statisztikai törvény alapján a közintézmények általi feldolgozás céljából gyűjtött személyes adatok. Határozattervezete (27) preambulumbekkezdésében az Európai Bizottság kijelenti, hogy a koreai kormánytól kapott pontosítások szerint általában koreai állampolgárok személyes adatait kezelik az ebben az összefüggésben, és külföldiek adatai csak kivételes esetekben – nevezetesen a Koreai Köztársaság területére történő belépésre és az onnan történő kilépésre, illetve a külföldi befektetésekre vonatkozó statisztikák esetében – szerepelhetnek a

²¹ Lásd még fentebb a 38. bekezdést.

kezelt adatok között. A határozattervezet szerint az adatokat még ezekben az esetekben sem EGT-beli adatkezelők/adatfeldolgozók továbbítják, hanem általában közvetlenül a közhatalmi szervek gyűjtik Koreában.

57. Az Európai Adatvédelmi Testület elfogadja az Európai Bizottság érvelését, hogy a statisztikai törvény alkalmazása a megfelelőségi határozat alapján továbbított személyes adatok kezelésére kivételes jellegű; mindazonáltal örömmel fogadna további információkat és biztosítékokat azzal kapcsolatban, hogy milyen külön garanciákat alkalmaznának abban az esetben, ha a közhatalmi szervek a későbbiekben az EGT-ből továbbított személyes adatokat gyűjtenének a statisztikai törvény alapján a közintézmények általi feldolgozás céljából, különös tekintettel az érintettek egyéni jogainak GDPR 89. cikke (2) bekezdése szerinti gyakorlására, amennyiben nem valószínű, hogy ezek a jogok lehetetlenné teszik vagy súlyosan hátráltatják az adott célok elérését, és azok megvalósításához nincs szükség ilyen eltérésre.
58. E tekintetben biztosítéknak tűnik, hogy az adatvédelmi törvény 4. cikke az ilyen típusú adatkezelésre is vonatkozik, de az Európai Adatvédelmi Testület üdvözlé, ha a megfelelőségi határozat további információkkal és pontosításokkal szolgálna azokat az egyedi kötelezettségeket illetően, amelyeket az adatvédelmi törvény 58. cikkének (4) bekezdése ír elő az ilyen adatkezelési tevékenységek esetére, konkrétan az adattakarékosság, a korlátozott idejű adatmegőrzés, a biztonsági intézkedések és a panaszkezelés tekintetében.
59. Másodsor, részleges mentességet élveznek a nemzetbiztonsággal kapcsolatos információk elemzése céljából gyűjtött vagy kért személyes adatok. Az Európai Adatvédelmi Testület tudatában van annak, hogy a nemzetbiztonsági kérdések megítélése terén nagy mozgásteret biztosít az államoknak az EJB. Azt is megállapítja, hogy a koreai alkotmány 37. cikkének (82) bekezdése szerint a szabadságok és jogok korlátozása – például ha az a nemzetbiztonság védelme érdekében szükséges – nem sértheti az adott szabadság vagy jog lényeges elemét. Tudomásul veszi továbbá a 2021-1. számú Értesítés 6. szakaszában foglalt, a személyes adatok nemzetbiztonsági célokból, többek között a jogsértések kivizsgálása és a végrehajtás céljából végzett kezelésére vonatkozó garanciákat. Mindazonáltal ebben az összefüggésben felszólítja az Európai Bizottságot a mentességek alkalmazási körének további pontosítására, mivel tudni szeretné, hogy az adatvédelmi törvény 58. cikke (1) bekezdésének 2. pontjában (III-VII. fejezetek) biztosított valamennyi mentesség vonatkozik-e a hírszerző szolgálatok munkájára, és hogy a szükségesség és arányosság elveinek való megfelelés biztosított-e. Különösen annak további pontosítására kéri az Európai Bizottságot, hogy egy hírszerző szolgálat milyen körülmények között alkalmazhatja ezeket a mentességeket. Az Európai Adatvédelmi Testület úgy véli, hogy szorosan figyelemmel kell kísérni ezeknek a korlátozásoknak a hatását a gyakorlatban.
60. Harmadsor, részleges mentességet élveznek az *„ideiglenesen kezelt személyes adatok, amennyiben azok a közbiztonság, közegészség, stb. fenntartásához sürgősen szükségesek”*. Az Európai Bizottság határozattervezetének (29) preambulumbekzdése szerint az Adatvédelmi Bizottság ezt a kategóriát szigorúan értelmezi, és csak sürgős fellépést igénylő vész helyzetben, például fertőző kórokozók nyomon követése vagy természeti katasztrófa áldozatainak mentése és segítése céljából alkalmazható.
61. Az Európai Adatvédelmi Testület is hangsúlyozza, hogy a személyes adatok számára biztosított védelem szintjétől való bármilyen eltérés lehetőségét szigorúan kell értelmezni. Ugyanakkor megjegyzi, hogy a rendelkezés nem pontosan meghatározott, és nem tartalmazza azoknak a helyzeteknek a teljes körű felsorolását, amikor a személyes adatok kezelése *„sürgősen szükségesnek” tekinthető*. Aggodalmát fejezi ki például azzal kapcsolatban, hogy ez a mentesség vajon vonatkozik-e az egészségügyi adatok jelenleg zajló koronavírus-világjárvány során történő nemzetközi továbbítására. A fentiek fényében az Európai Adatvédelmi Testület felszólítja az Európai Bizottságot arra, hogy pontosítsa ennek a mentességnek az alkalmazási körét, és teljes körűen kísérje figyelemmel az alkalmazását és a hatókörét annak biztosítása érdekében, hogy az EGT-ből származó személyes adatok védelmi szintje a megfelelőségi határozat alapján történő továbbítást követően se csökkenjen.

62. Végül, részleges mentességet élveznek a sajtó általi tájékoztatás, a vallási szervezetek általi hittérítő tevékenység és a politikai pártok általi jelöltállítás céljából gyűjtött vagy használt személyes adatok²². A személyes adatok sajtó általi, újságírói tevékenység céljából történő kezelését illetően az Európai Bizottság határozattervezete (17) preambulumbekzdésében kijelenti, hogy a szólásszabadság és más jogok, többek között a magánélethez való jog közötti egyensúly megteremtését a sajtóközlemények által okozott kár esetén igénybe vehető jogorvoslatról és egyeztetésről, stb. szóló törvény (a továbbiakban: **sajtótörvény**) szabályozza, és bemutatja a sajtótörvényből következő garanciákat. Mindazonáltal az Európai Adatvédelmi Testület felszólítja az Európai Bizottságot ennek a mentességnek és a vonatkozó ítélkezési gyakorlatnak a teljes körű figyelemmel kísérésére annak biztosítása érdekében, hogy a koreai jogi keret által biztosított azonos szintű adatvédelem a gyakorlatban is megvalósuljon.

3.1.3. A jogos célokból végzett jogszerű és tisztességes adatkezelés alapjai

63. A GDPR-ral összhangban a GDPR-megfelelőségi referencia előírja, hogy 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 és az adatkezelő vagy harmadik fél jogos érdekeit, amelyek nem írják felül az érintett érdekeit.
64. A GDPR-hoz hasonló felépítésű adatvédelmi törvény először bevezeti a jogszerűség, tisztességesség és átláthatóság elvét a törvény elején (a 3. cikk (1) és (2) bekezdésében), az alkalmazására vonatkozó egyedi szabályokat pedig a későbbiekben határozza meg (a törvény 15- 19. cikkében). Az adatvédelmi törvény 15. cikke tartalmazza azoknak a jogalapoknak a felsorolását, amelyekre hivatkozva a személyesadat-kezelők személyes adatokat gyűjthetnek és használhatnak fel az adatgyűjtés céljának megfelelően. Ezek a jogalapok a következőket foglalják magukba: (1) az érintett tájékozott hozzájárulása; (2) jogszabályi felhatalmazás vagy jogi kötelezettség teljesítéséhez való szükségesség; (3) közintézmény feladatellátásához való szükségesség; (4) az érintettel való szerződéskötéshez vagy az érintettel kötött szerződés teljesítéséhez való szükségesség; (5) az érintett vagy harmadik fél életének, testi épségének vagy vagyoni érdekének közvetlen veszélytől való megóvásához való szükségesség (és az előzetes hozzájárulás nem szerezhető meg); (6) a személyesadat-kezelő érintetténél magasabb rendű jogos érdekének az érvényesítéséhez való szükségesség.
65. Ezt követően az adatvédelmi törvény 17. cikke a személyes adatok harmadik féllel történő megosztásának a jogalapjait sorolja fel, amelyekbe beletartozik (1) az érintett tájékozott hozzájárulása, (2) jogszabályi felhatalmazás vagy jogi kötelezettség teljesítéséhez való szükségesség; (3) közintézmény feladatellátásához való szükségesség; és (4) az érintett vagy harmadik fél életének, testi épségének vagy vagyoni érdekének közvetlen veszélytől való megóvásához való szükségesség (és az előzetes hozzájárulás nem szerezhető meg). A személyes adatok megosztása az érintett hozzájárulása nélkül is megengedett, amennyiben olyan célból történik, amely elfogadható módon kapcsolódik azokhoz a célokhoz, amelyekre a személyes adatokat eredetileg gyűjtötték (az adatvédelmi törvény 17. cikkének (4) bekezdése).
66. Az adatvédelmi törvény 18. cikke a személyes adatok gyűjtésük vagy szolgáltatásuk eredeti céljától eltérő felhasználásának és megosztásának egyedi szabályait határozza meg. Az engedély feltétele ezen szabályok esetében is többek között a hozzájárulás.

²² Ennek megfelelően a személyes adatok vallási szervezetek által hittérítő tevékenység céljából végzett kezelése és a személyes adatok politikai pártok által jelöltállítással összefüggésben végzett kezelése sem tartozik a megfelelőségi határozat hatálya alá. Lásd még fentebb a 37. bekezdést a 2.3.2 szakaszban.

67. Elismerve, hogy a jogszerűség elve és a személyes adatok hozzájárulás alapján történő kezelése esetén is érvényesíthető általános felfüggesztési jog (az adatvédelmi törvény 37. cikke) tekintetében alapvető hasonlóság áll fenn a koreai jog és a GDPR között, az Európai Adatvédelmi Testület szeretné megjegyezni, hogy a hozzájárulás visszavonásához való általános jog nem szerepel az adatvédelmi törvényben²³. Annak fényében, hogy a hozzájárulás a fent ismertetett esetek mindegyikében fontos jogalap, és figyelembe véve azt, hogy az egyéni jogok milyen szerepet töltenek be az adatvédelem jogi rendszerében az érintettek alapvető jogainak és szabadságainak a védelme szempontjából, az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy folytasson további értékelést a hozzájárulás visszavonásához való általános jog koreai jogrendszerből való hiányának a hatását illetően, és nyújtson további biztosítékokat arra, hogy a GDPR előírásainak megfelelő alapvető szintű adatvédelem mindig garantált, szükség esetén tisztázva, hogy a felfüggesztési jognak milyen szerepe van ebben az összefüggésben.

3.1.4. A célhoz kötöttség elve

68. A GDPR-ral összhangban a GDPR-megfelelőségi referencia előírja, hogy a személyes adatokat konkrét célból kell kezelni, és később csak olyan mértékben lehet használni, amely nem összeegyeztethetetlen az adatkezelés céljával.
69. Az adatvédelmi törvény 3. cikkének (1) és (2) bekezdése szerint a személyesadat-kezelőnek egyértelműen meg kell határoznia az adatkezelés céljait, és biztosítania kell az adatkezelés e célokkal való összeegyeztethetőségét. Miközben ezt az elvet az adatvédelmi törvény más rendelkezései (a 15. cikk (1) bekezdése, a 18. cikk (1) bekezdése és a 19. cikk (1) bekezdése) is megerősítik, bizonyos körülmények között megengedett az „elfogadható módon kapcsolódó” célból történő adatkezelés (lásd az adatvédelmi törvény 17. cikkének (4) bekezdését)²⁴, valamint a személyes adatok céltól eltérő felhasználása és szolgáltatása (lásd az adatvédelmi törvény 18. és 19. cikkét)²⁵.
70. Az Európai Adatvédelmi Testület értelmezése szerint a személyes adatok megfelelőségi határozaton alapuló, az EGT-ből a Koreai Köztársaságba irányuló továbbítása esetében az EGT-beli adatkezelők adatgyűjtésének a célját kell az adattovábbítás céljának és a koreai címzett általi személyesadat-kezelés céljának tekinteni. A koreai adatkezelő ettől a céltól csak az adatvédelmi törvény 18. cikke (2) bekezdésének 1-3. pontjaiban meghatározott esetekben térhet el, „feltéve, hogy azzal nem sérti tisztességtelen módon az érintett vagy harmadik fél érdekeit”²⁶. Ebben az összefüggésben az Európai Adatvédelmi Testület elfogadja az Európai Bizottság határozattervezet (55) preambulumbekkezdésben tett állítását, mely szerint a céltól való eltérést engedélyező jogszabálynak mindenkor tiszteletben kell tartania a magánélethez és az adatvédelemhez való alapvető jogot. Mindazonáltal megjegyzi, hogy ezt az állítást semmilyen konkrét információ nem támasztja alá, például nem történik hivatkozás a koreai alkotmány 37. cikkére. Ezért felszólítja az Európai Bizottságot, hogy a határozattervezetben adjon további biztosítékokat és garanciákat arra, hogy az adatkezelés céljának megváltoztatását engedélyező

²³ Jóllehet az érintettek bizonyos körülmények között megtagadhatják a hozzájárulást, lásd például az adatvédelmi törvény 18. cikkének (3) bekezdését. A hozzájárulás visszavonásának a joga viszont úgy tűnik, hogy csak egyedi esetekben gyakorolható: az adatvédelmi törvény 27. cikke (1) bekezdésének 2. pontja szerint az érintettnek jogában áll visszavonni a hozzájárulását abban az esetben, ha nem kívánja, hogy személyes adatait harmadik fél részére továbbítsák a személyesadat-kezelő vállalkozás üzleti tevékenységének részben vagy teljes egészében történő átruházása, összeolvadás, stb. esetén; az adatvédelmi törvény 39. cikkének (7) bekezdése szerint a felhasználók bármikor visszavonhatják a személyes adataik gyűjtéséhez, felhasználásához és szolgáltatásához való, infokommunikációs szolgáltatóknak stb. adott hozzájárulást; és a hiteladat-védelmi törvény 37. cikke alapján az érintett visszavonhatja a személyes hiteladatai átadására vagy felhasználására vonatkozó hozzájárulást.

²⁴ A céllal való összeegyeztethetőségről előzetesen meg kell győződni az adatvédelmi törvény végrehajtási rendeletének 14-2. cikkében meghatározott feltételek alapján.

²⁵ Lásd még fentebb a 66. bekezdést.

²⁶ Az adatvédelmi törvény 18. cikkének (2) bekezdése.

jogszabálynak mindenkor tiszteletben kell tartania az érintettek magánélet védelmével és adatvédelemmel kapcsolatos alapvető jogait és szabadságait.

3.1.5. Az adatminőség és az arányosság elve

71. A GDPR-megfeleléségi referencia szerint az adatoknak pontosnak, és szükség esetén naprakésznek kell lenniük. Az adatoknak a kezelésük céljaihoz képest megfelelőnek és relevánsnak kell lenniük, és azokkal arányban kell állniuk.
72. Az adatvédelmi törvény szerint a személyesadat-kezelőknek biztosítaniuk kell, hogy a személyes adatok a kezelésük céljai tekintetében szükséges mértékben pontosak, teljes körűek és naprakészek legyenek (az adatvédelmi törvény 3. cikkének (3) bekezdése). A személyesadat-kezelők csak az adott cél eléréséhez feltétlenül szükséges mennyiségű személyes adatot gyűjthetnek. E tekintetben rájuk hárul a bizonyítási teher (az adatvédelmi törvény 16. cikkének (1) bekezdése).
73. E háttér ismeretében az Európai Adatvédelmi Testület egyetért az Európai Bizottság értékelésével, hogy az adatvédelmi törvény által biztosított védelem szintje ebben a tekintetben alapvetően azonos azzal, amit a GDPR előír.

3.1.6. Az adatmegőrzés elve

74. A GDPR-megfeleléségi referencia szerint az adatokat általános szabályként csak az adatkezelés céljai érdekében feltétlenül szükséges ideig lehet megőrizni. Az adatvédelmi törvény 21. cikkének (1) bekezdése alapján ez az elv is létezik a koreai jogban. Az adatvédelmi törvény szerint a személyesadat-kezelőknek késedelem nélkül meg kell semmisíteniük a személyes adatokat, mielőtt azok a megőrzési időszak leteltét vagy az adatkezelés tervezett céljának elérését követően szükségtelenné váltak, kivéve, ha jogszabály más adatmegőrzési időszakot ír elő.
75. Az Európai Adatvédelmi Testületet azonban aggasztja, hogy az álnevesített személyes adatokra nem alkalmazandó az adatvédelmi törvény 21. cikkének (1) bekezdése. Tudomásul veszi azt a tényt, hogy a 2021-1. számú Értesítés 4. szakaszának (iii) pontja szerint „*álnevesített személyes adatok statisztikák összeállítása, tudományos kutatás, köznyilvánartartás fenntartása stb. céljából végzett kezelése esetén, ha az álnevesített személyes adatokat az adatkezelés konkrét céljának az elérését követően nem semmisíti meg a személyesadat-kezelő az Alkotmány 37. cikke és a 3. cikk (a személyes adatok védelmének elvei) szerint, akkor az adatokat anonimizálnia kell annak biztosítása érdekében, hogy azok – az adatvédelmi törvény 58. cikke (2) bekezdésének megfelelően – a szükséges idő, költség, technológia stb. ésszerű mérlegelése alapján sem önmagukban, sem más adatokkal összekapcsolva ne tegyék lehetővé egy adott személy azonosítását*”. Figyelembe véve a 2021-1. számú Értesítés fontosságát, a megfeleléségi határozat alapján a Koreai Köztársaságba továbbított személyes adatok számára biztosított azonos szintű védelmet illető jogi bizonyosság végett az Európai Adatvédelmi Testület megismétli azon kérését az Európai Bizottsághoz, hogy szolgáltatson további információkat különösen arról, hogyan biztosítják a 2021-1. számú Értesítés kötelező erejét, érvényesíthetőségét és érvényességét²⁷.

3.1.7. A biztonság és a titoktartás elve

76. A GDPR-megfeleléségi referenciában leírtak szerint a biztonság és a titoktartás elve alapján a személyesadat-kezelőknek 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

²⁷ Lásd még a jelen vélemény 51. bekezdését a 3.1.1.1. szakaszban, valamint az Európai Adatvédelmi Testület álnevesítés koreai jog szerinti hatásával kapcsolatos általános aggályait az 52. bekezdésben.

megfelelő technikai és szervezési intézkedések alkalmazásával. A biztonsági szint tervezésénél figyelembe kell venni a legmodernebb technikákat és a kapcsolódó költségeket.

77. Az Európai Bizottság megállapította, hogy az adatvédelmi törvény 3. cikkének (4) bekezdése az adatbiztonság hasonló elvét fogalmazza meg, melynek részletesebb meghatározását a törvény 29 cikke tartalmazza. Az adatbiztonsági rendelkezések azokra az esetekre is vonatkoznak, amikor a személyes adat-kezelő külső szolgáltatóhoz helyezi ki a személyes adatok kezelését. Az adatkezelés biztonságát műszaki és vezetési-szervezési garanciák révén kell biztosítani, amelyeket a kötelező erejű adatkezelési megállapodásba is bele kell foglalni (az az adatvédelmi törvény 26. cikke és az adatvédelmi törvény végrehajtási rendeletének 28. cikke). Emellett az adatvédelmi törvény szerint adatvédelmi incidens esetén egyedi kötelezettségeknek kell eleget tenni, többek között értesíteni kell az érintetteket és – amennyiben az érintettek száma meghaladja az alkalmazandó határértéket – a felügyeleti hatóságot (az adatvédelmi törvény 34. cikke, az adatvédelmi törvényt kiegészítő elnöki rendelet 39. cikkével együttesen értelmezve), kivéve, ha az érintett adatok statisztikai, tudományos kutatási vagy közérdekű archiválási célból kezelt álnevesített személyes adatok (az adatvédelmi törvény 28. cikkének (7) bekezdése). Az Európai Adatvédelmi Testület ismét²⁸ aggodalmát fejezi ki az álnevesített adatokra vonatkozó mentességek széles köre miatt, és megismétli azon kérését az Európai Bizottsághoz, hogy végezzen további értékelést ebben a témakörben annak biztosítása érdekében, hogy a koreai jog alapján biztosított védelem szintje alapvetően azonos legyen²⁹.
78. Mindazonáltal az Európai Adatvédelmi Testület összességében elfogadja az Európai Bizottságnak a koreai jog biztonság és titoktartás elve tekintetében fennálló lényegi azonosságára vonatkozó értékelését és következtetését.

3.1.8. Az átláthatóság elve

79. A GDPR 5. cikke (1) bekezdésének (a) pontja alapján az átláthatóság az uniós adatvédelmi rendszer egyik alapelve. Ezen elv alapvető fontosságáról szólva a GDPR (39) preambulumbekkezdése kijelenti, hogy *„[a] természetes személyek számára átláthatónak kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni. (...) A természetes személyt a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról tájékoztatni kell, valamint arról, hogy hogyan gyakorolhatja az adatkezelés kapcsán megillető jogokat.”*
80. A GDPR-megfelelőségi referencia kifejezetten említi az „átláthatóságot” azon tartalmi elvek között, amelyet egy harmadik országban biztosított védelmi szint lényegi azonosságának az értékelése során figyelembe kell venni. Konkrétan úgy fogalmaz, hogy *„[m]inden 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 lehetnek kivételek, például a büntetőeljárások, a nemzetbiztonság, a bírói függetlenség és a bírósági eljárások vagy egyéb fontos közérdekű célok védelme érdekében, ahogy az a GDPR 23. cikkében is szerepel.”*
81. A GDPR-hoz hasonlóan az adatvédelmi törvény is tartalmazza az átláthatóság általános elvét, amely alapján a személyes adat-kezelőknek nyilvánosságra kell hozniuk az adatvédelmi politikájukat és a személyes adatok kezelésével kapcsolatos egyéb anyagokat (az adatvédelmi törvény 3. cikkének (5) bekezdése). Egyedi kötelezettségek vonatkoznak azokra az esetekre, amikor a személyes adat-kezelő az érintett hozzájárulását kéri a személyes adatok gyűjtéséhez és kezeléséhez (az adatvédelmi törvény

²⁸ Mint korábban az 51-52. bekezdésekben és a jelen vélemény 3.1.1.1. részében.

²⁹ Lásd még a jelen vélemény 3.1.6 és 3.1.10 szakaszait.

15. cikkének (2) bekezdése), a személyes adatok harmadik féllel történő megosztásához (az adatvédelmi törvény 17. cikkének (2) bekezdése) és a céltól eltérő adatkezeléshez (az adatvédelmi törvény 18. cikkének (2) bekezdése). Megjegyzendő, hogy ezek a kötelezettségek értelemszerűen a kihelyezett adatkezelést végző szolgáltatóra is vonatkoznak (az adatvédelmi törvény 26. cikkének (7) bekezdése).

82. Az Európai Adatvédelmi Testület üdvözli azokat a kiegészítő garanciákat, amelyeket a 2021-1. számú Értesítés 3. szakaszának (i) és (ii) pontja biztosít³⁰ az érintettek adataik EGT-beli jogalany általi továbbítása esetén történő tájékoztatásával kapcsolatban, figyelembe véve azt a tényt, hogy az adatvédelmi törvény 20. cikkének (1) bekezdése szerint abban az esetben, ha az adatokat nem az érintettől szerezték be, az érintettet csak kérésre kell tájékoztatni, a tájékoztatáshoz való általános jogot pedig az adatvédelmi törvény 20. cikkének (2) bekezdése alapján csak azokban az esetekben kell elismerni, amikor bizonyos adatkezelési műveletek az az adatvédelmi törvény végrehajtási rendeletében (15. cikk (2) bekezdése) meghatározott küszöböt átlélik.
83. Összességében az Európai Adatvédelmi Testület elfogadja, hogy az átláthatóság elvét tekintve a koreai jog által biztosított védelmi szint alapvetően azonos a GDPR által biztosítottal.

3.1.9. A személyes adatok különleges kategóriái

84. Egy harmadik ország adatvédelmi rendszeréről akkor ismerhető el, hogy alapvetően ugyanolyan szintű védelmet biztosít a személyes adatok számára, mint a GDPR, ha személyes adatok GDPR 9. és 10. cikke értelmében vett különleges kategóriáit érintő esetekben külön garanciákat biztosít.
85. Az adatvédelmi törvény egyedi rendelkezéseket állapít meg az úgynevezett különleges adatok kezelésére vonatkozóan, amely a következőkre terjed ki: a világnézetre, meggyőződésre, szakszervezetbe vagy politikai pártba való felvételre vagy onnan való kilépésre, politikai véleményre, egészségi állapotra, szexuális életre utaló és egyéb személyes adatok, amelyek esetében valószínűsíthető az érintett magánélethez való jogának a jelentős veszélyeztetése, továbbá – az adatvédelmi törvény végrehajtási rendeletére hivatkozva – a genetikai vizsgálat során szerzett DNS-információk, a bűnügyi nyilvántartási adatok; egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó, sajátos technikai eljárásokkal nyert, az adott természetes személy egyedi azonosítását célzó személyes adatok; és a faji vagy etnikai származásra utaló adatok.
86. A GDPR-hoz hasonlóan a koreai adatvédelmi jog is tiltja a különleges adatok kezelését, kivéve, ha egyedi mentesség alkalmazható abban az esetben, ha (1) az érintettet tájékoztatták, és beszerzték a konkrét hozzájárulását, vagy (2) az adatkezelésre jogszabályi rendelkezés ad engedélyt (az adatvédelmi törvény 23. cikkének (2) bekezdése).
87. Mindezek alapján az Európai Adatvédelmi Testület elvben egyetért az Európai Bizottságnak a koreai jog személyes adatok különleges kategóriáinak a kezelése tekintetében fennálló lényegi azonosságára vonatkozó következtetésével. Mindazonáltal szeretné megjegyezni, hogy nem kapta meg sem az adatvédelmi törvény kézikönyvét, sem az Adatvédelmi Bizottság arra vonatkozó felvilágosítását, hogy a „szexuális élet” kifejezés az egyén szexuális irányultságát vagy preferenciáit is magában foglalja-e, mert ezekről nem esik szó a 2021-1. számú Értesítésben. Ezért felszólítja az Európai Bizottságot ezeknek az információknak a megadására annak érdekében, hogy függetlenül értékelhesse azokat. Felkéri továbbá az Európai Bizottságot, hogy pontosan jelölje meg azokat a dokumentumokat, amelyekben az ezzel a témával kapcsolatban hivatkozott információk szerepelnek.

3.1.10. A hozzáféréshez, helyesbítéshez, törléshez és tiltakozáshoz való jog

88. A koreai jogi keretben az érintettek jogainak elismerése az adatvédelmi törvény 3. cikkének (5) bekezdésén alapul, amely szerint a személyesadat-kezelőnek biztosítania kell az érintettnek az

³⁰ A határozattervezet I. melléklete.

adatvédelmi törvény 4. cikkében felsorolt jogokat, amelyek részletesebb meghatározását az adatvédelmi törvény 35-37. és 39. cikkei, 39. cikkének (2) bekezdése, valamint – a „személyes hiteladatok”, azaz „a pénzügyi vagy kereskedelmi tranzakciókban részt vevő felek hitelképességének meghatározásához szükséges hiteladatok” (lásd a határozattervezet (9) preambulumbekkezdését) vonatkozásában – a hiteladat-védelmi törvény 37. és 38. cikke, valamint 38. cikkének (3) bekezdése tartalmazza.

89. Az Európai Adatvédelmi Testület megállapítja, hogy a hozzáférési jog (és „*a személyes adataihoz az adatvédelmi törvény 35. cikke alapján hozzáférő érintett*” által gyakorolható helyesbítési és törlési jog) korlátozható vagy megtagadható, „*ha a hozzáférést törvény tiltja vagy korlátozza*”, „*ha a hozzáférés egy harmadik fél életét vagy testi épségét veszélyeztetheti, vagy bármely más személy vagyoni és egyéb érdekeinek indokolatlan sérelmét okozhatja*”, továbbá – a közintézmények esetében – ha a hozzáférés biztosítása „*súlyos nehézségeket okozna*” bizonyos feladatok ellátása terén, amelyet az adatvédelmi törvény 35. cikkének (4) bekezdése határoz meg részletesebben³¹. A személyes adatok kezelésének felfüggesztéséhez való jog vonatkozásában hasonló rendelkezéseket tartalmaz az adatvédelmi törvény 37. cikke.
90. A GDPR 23. cikke szerint uniós vagy tagállami jog korlátozhatja az egyéni jogokat, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint a következők védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban: az érintett védelme vagy mások jogainak és szabadságainak védelme; és „*az ugyanezen cikk a)–e) és a g) pontjában említett esetekben – akár alkalmanként – a közhatalmi feladatok ellátásához kapcsolódó ellenőrzési, vizsgálati vagy szabályozási tevékenység*”.
91. Tekintettel erre a háttérre az Európai Adatvédelmi Testület örömmel venné, ha a határozattervezet általános biztosítékokat tartalmazna arra nézve, hogy az érintettek jogait korlátozó bármely törvénynek vagy jogszabálynak teljesítenie kell a koreai alkotmány azon követelményeit, hogy egy alapvető jog csak akkor korlátozható, ha az nemzetbiztonsági okból, a közrend fenntartása vagy a közjó érdekében szükséges, és a korlátozás nem érintheti az adott szabadság vagy jog lényegét (a koreai alkotmány 37. cikkének (2) bekezdése).
92. Továbbá, a „*bármely más személy vagyoni vagy egyéb érdekeinek indokolatlan sérelmével*”, kapcsolatos kivételt illetően az Európai Adatvédelmi Testület elismeri, hogy ez „*arra utal, hogy meg kell teremteni az egyensúly egyrészt az egyén, másrészt a más személyek alkotmányban védett jogai és szabadságai között*”³², de ennek ellenére felszólítaná az Európai Bizottságot ennek a kivételnek és a vonatkozó ítélkezési gyakorlatnak a teljes körű figyelemmel kísérésére annak biztosítása érdekében, hogy az érintettek jogainak koreai jogi keret által biztosított azonos szintű védelme a gyakorlatban is megvalósuljon.
93. Hasonlóképpen, az Európai Adatvédelmi Testület üdvözléne a közfeladatot ellátó szervekre vonatkozó kivétel alkalmazásának gondos figyelemmel kísérését, különös tekintettel azokra az esetekre, amikor úgy tekinthető, hogy a hozzáférés biztosítása „*súlyos nehézségeket*” okoz a feladataik ellátása terén, mivel ez tágabb fogalomnak látszik, mint az, amely az adatvédelmi törvény más rendelkezéseiben, például a 18. cikk (2) bekezdésének 5. pontjában szerepel³³, és az érintetteket megillető jogok indokolatlan korlátozásának az elkerülése érdekében szűken kellene értelmezni.

³¹ A személyes hiteladatokhoz való hozzáférésre és az azok helyesbítésére vonatkozó, a hiteladat-védelmi törvény által szabályozott jogok esetében ugyanazok a feltételek és kivételek alkalmazandók, mint amelyeket az adatvédelmi törvény a hozzáférési és helyesbítési joggal kapcsolatban meghatároz (a határozattervezet 135. lábjegyzete).

³² A határozattervezet (76) preambulumbekkezdése.

³³ A személyes adatok céltól eltérő felhasználásának és szolgáltatásának a korlátozása alóli kivételekkel kapcsolatban az adatvédelmi törvény 18. cikke (2) bekezdésének 5. pontja olyan helyzetekre utal, amikor a közintézmények számára „*lehetetlen*” a feladatellátás.

94. Emellett az Európai Adatvédelmi Testület aggodalmát fejezi ki amiatt, hogy a kivételek, amelyek szerint a kérésre biztosított átláthatóságra és egyéni jogokra vonatkozó rendelkezések (az adatvédelmi törvény 20., illetve 35-37. cikkei) – valamint az infokommunikációs szolgáltatók számára előírt követelményeket tartalmazó hasonló rendelkezések (az adatvédelmi törvény 39. cikkének (2) bekezdése és 39. cikkének (6)-(8) bekezdései) és a hiteladat-védelmi törvény vonatkozó rendelkezései (lásd a hiteladat-védelmi törvény 40. cikkének (3) bekezdése szerinti kivételek) – nem vonatkoznak a statisztikai, tudományos kutatási vagy közérdekű archiválási célból kezelt álnevesített személyes adatokra (az adatvédelmi törvény 28. cikkének (7) bekezdése), összhangban állnak-e az európai jogi keretben biztosított garanciákkal.
95. Úgy tűnik, hogy ezek a rendelkezések általános eltérést engednek az ilyen típusú adatkezelés esetén, miközben a GDPR szerint a személyes adatok (az álnevesített személyes adatokat is beleértve) tudományos és történelmi kutatási célból vagy statisztikai célból folytatott kezelése vonatkozásában az uniós vagy a tagállami jog csak akkor állapíthat meg eltérést az érintett jogait illetően, *„ha e jogok valószínűsíthetően lehetetlenné teszik vagy súlyosan hátráltatják az adott célok elérését, és azok megvalósításához szükség van ilyen eltérésre”*, hiszen az álnevesítés pusztán az adattakarékosság elvének betartását biztosító technikai és szervezési intézkedések egyike (a GDPR 89 cikkének (1) bekezdése).
96. Az Európai Bizottság indokoltnak tartja az adatvédelmi törvény 28. cikkének (7) bekezdésében megállapított eltérést annak fényében, hogy az adatvédelmi törvény 28. cikkének (5) bekezdése kifejezetten tiltja, hogy a személyesadat-kezelő az álnevesített adatokat egy bizonyos természetes személy azonosítása céljából kezelje, és az azonosítást nem igénylő adatkezelés GDPR 11. cikkének (2) bekezdése szerinti (a GDPR preambulumbekkezdésével együttesen értelmezett) megközelítésre hivatkozik³⁴.
97. A GDPR 11. cikke szerint az adatkezelő valóban nem köteles *„kiegészítő információkat megőrizni, beszerezni vagy kezelni annak érdekében, hogy azonosítsa az érintettet”*, ha ezt pusztán abból a célból tenné, hogy a GDPR-nak megfeleljen, amennyiben azok a célok, amelyekből a személyes adatokat kezeli, nem vagy már nem teszik szükségessé az érintett azonosítását; ha ezekben az esetekben az adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet, az érintett jogai nem alkalmazandók. Amint az Európai Bizottság is megállapítja³⁵, a GDPR azt írja elő, hogy ezekben az esetekben „gyakorlatilag” lehetetlen legyen az adatkezelő számára az azonosítás, és az adattakarékosság elvével összhangban elismeri, hogy pusztán a GDPR „céljából” nem kell kiegészítő információkat kezelni.
98. Az Európai Adatvédelmi Testület megítélése szerint azonban ez a helyzet más, mint az, amikor az adatkezelőnek gyakorlatilag módjában áll azonosítani az érintettet, de egy jogszabályi rendelkezés, mint amelyet például az adatvédelmi törvény 28. cikkének (5) bekezdése tartalmaz, nem engedi, hogy ezt megtegye. E tekintetben az Európai Adatvédelmi Testület üdvözli az Adatvédelmi Bizottság 2021-1. számú Értesítésben nyújtott pontosításait³⁶, amelyek megerősítik, hogy az adatvédelmi törvény 3. szakasza (és azon belül a 28. cikk (7) bekezdése) és a hiteladat-védelmi törvény 40. cikkének (3) bekezdése szerinti kivétel csak abban az esetben alkalmazandó, ha az álnevesített adatok kezelését tudományos kutatási, statisztikai vagy közérdekű archiválási célból végzik. Ennek ellenére – a 2021-1.

³⁴ Meg kell jegyezni, hogy ugyanez az indoklás nem lenne elfogadható az álnevesített hiteladatok kezelésének hiteladat-védelmi törvény 40. cikkének (3) bekezdése szerinti kivétele esetén, mivel e cikk szerint *„egy hitelinformációs cég, stb. nem kezelhet álnevesített személyes adatokat olyan módon, ami lehetővé teszi egy természetes személy bármely haszonszerzési vagy tisztességtelen célból történő azonosítását”*, tehát a tisztességes célból történő újraazonosítást megengedi például abban az esetben, ha az egy érintett kérésének a teljesítését szolgálja.

³⁵ Lásd a határozattervezet (82) preambulumbekkezdését.

³⁶ A határozattervezet I. mellékletének 4. szakasza.

számú Értesítés kötelező jellegét, érvényesíthetőségét és érvényességét illetően korábban már megfogalmazott aggodalmak mellett³⁷ – továbbra is nyitott az a kérdés, hogy az adatvédelmi törvény 28. cikkének (7) bekezdése és a hiteladat-védelmi törvény 40. cikkének (3) bekezdése által engedélyezett eltérések vajon szükségesnek és arányosnak tekinthetők-e egy demokratikus társadalomban, tekintve, hogy az érintett jogait minden olyan esetben korlátozzák, amikor az álnevesített adatok kezelése az említett célokat szolgálja, azaz akkor is, amikor a személyesadat-kezelőnek gyakorlatilag módjában áll azonosítani az érintettet, és nem valószínű, hogy a jogok lehetetlenné teszik vagy súlyosan hátráltatják a meghatározott célok elérését.

99. Konkrétan az aggasztja az Európai Adatvédelmi Testületet, hogy ezek az eltérések nem lennének indokoltak, és további vizsgálatot igényelnének különösen „*a statisztikai, tudományos kutatási, közérdekű archiválási, stb. célú*” adatok álnevesítését az adatvédelmi törvény 28. cikkének (2) bekezdése szerint „*az érintettek hozzájárulása nélkül*” (és az adatvédelmi törvény 20. cikke szerinti tájékoztatás nélkül) végrehajtó személyesadat-kezelő általi alkalmazás esetén³⁸, amennyiben az ilyen adatkezelő megőrzi az újraazonosítást lehetővé tevő információkat. A GDPR szerint az egyéni jogok gyakorlását lehetővé kell tenni minden olyan adat tekintetében, amely egy adott természetes személy azonosítását vagy kiválasztását lehetővé teszi, még akkor is, ha az adat „álnevesítettnek” tekinthető, kivéve, ha a GDPR korábban említett 11. cikke alkalmazandó. E tekintetben az Európai Adatvédelmi Testület megjegyzi, hogy csak a harmadik félnek ugyanazon statisztikai, tudományos kutatási vagy közérdekű archiválási célból átadott ilyen adatok esetében áll fenn, hogy nem tartalmaznak az egy bizonyos természetes személy azonosítására használható adatokat, és ezért valószínűleg csak az a személyesadat-kezelő nincs „gyakorlatilag” abban a helyzetben, hogy az érintettet további információk felhasználása nélkül azonosítsa, akinek az álnevesített adatokat az adatvédelmi törvény 28-2. cikkének (2) bekezdése alapján adják át.
100. Röviden összefoglalva: tekintettel arra, hogy – amint azt az Európai Bizottság is elismeri – „*az adatvédelmi törvény nem lehetséges garanciaként tekint az álnevesítésre, hanem előfeltételeként írja elő bizonyos statisztikai, tudományos kutatási vagy közérdekű archiválási célból folytatott adatkezelési tevékenységek végzéséhez (például a hozzájárulás nélküli adatkezeléshez vagy a különböző adatbázisok összekapcsolásához)*”³⁹, ám ezekben az esetekben megengedi az érintettek jogainak komoly korlátozását, az Európai Adatvédelmi Testület felszólítja az Európai Bizottságot, hogy végezzen további értékelést az adatvédelmi törvény 28. cikkének (7) bekezdése és a hiteladat-védelmi törvény 40. cikkének (3) bekezdése által engedélyezett eltéréseket illetően, valamint kísérje gondos figyelemmel ezek alkalmazását és a vonatkozó ítélkezési gyakorlatot⁴⁰ annak biztosítása érdekében, hogy az érintettek jogait ne korlátozzák indokolatlanul a megfelelőségi határozat alapján továbbított személyes adatok e célokból történő kezelése során, figyelembe véve, hogy ezek a jogok az adatkezelőknek is segítségére vannak abban, hogy a kezelt adatok minőségét biztosítsa.

3.1.11. Az újbóli továbbítás korlátozása

101. A GDPR-megfelelőségi referencia egyértelművé teszi, hogy a megfelelőségi határozat alapján történő adattovábbítással érintett természetes személyek védelmének szintjét az újbóli adattovábbítás nem csökkentheti, és ezért az újbóli továbbítás „*kizárólag akkor lehet engedélyezett, ha a további*

³⁷ Lásd fentebb a 3.1.1.1. szakaszt.

³⁸ Lásd az adatvédelmi törvény 28 cikkének (7) bekezdését és annak 2021-1. számú Értesítésben adott magyarázatát, amely szerint az adatvédelmi törvényben foglalt bizonyos garanciák, azaz „*a 20., 21. és 27. cikkek, a 34. cikk (1) bekezdése, a 35-37. cikkek, a 39. cikk (3) bekezdése, a 39. cikk (4) bekezdése és a 39. cikk (6)-(8) bekezdése*”, nem alkalmazandó a statisztikák összeállítása, tudományos kutatás, köznyilvántartás fenntartása stb. célból kezelt álnevesített adatokra.

³⁹ A határozattervezet (42) preambulumbekkezdése.

⁴⁰ Lásd például az Open Net kezdeményezés alkotmányos kihívásait (a csak koreai nyelven rendelkezésre álló dokumentum elérhetősége: <https://opennet.or.kr/19909>).

címzettek (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”.

102. A kihelyezett adatkezelést végző harmadik országbeli szolgáltatók (azaz „adattfeldolgozók”) részére történő újbóli továbbítást illetően az Európai Adatvédelmi Testület megjegyzi, hogy a koreai jogi keret nem tartalmaz az ilyen esetekre vonatkozó különleges szabályokat, és hogy az Európai Bizottság véleménye szerint⁴¹ a koreai személyesadat-kezelőnek egy jogilag kötelező erejű eszközzel kell biztosítania az adatvédelmi törvény adatkezelési tevékenység kihelyezésére vonatkozó rendelkezéseinek (a 26. cikknek) való megfelelést, és ő tartozik felelősséggel azokért a személyes adatokért, amelyek kezelését kihelyezi (az adatvédelmi törvény 26. cikke).
103. Ami a harmadik fél (azaz más személyesadat-kezelő) részére történő újbóli továbbítást illeti, az adatvédelmi törvény 17. cikkének (3) bekezdése szerint a koreai személyesadat-kezelőnek tájékoztatnia kell az érintetteket adataik külföldre történő továbbításáról, be kell szereznie az érintettek ahhoz való hozzájárulását, és *„nem köthet az adatvédelmi törvényt sértő szerződést a személyes adatok határon átnyúló továbbításáról”*. Az Európai Adatvédelmi Testület megállapítja, hogy ez az utolsó rendelkezés – az Európai Bizottság véleménye szerint⁴² – biztosítja azt, hogy a határon átnyúló adattovábbításra vonatkozó szerződések nem tartalmazhatnak az adatvédelmi törvény személyesadat-kezelőkre vonatkozó követelményeinek ellentmondó kötelezettségeket, és ezért garanciának tekinthető, viszont nem írja elő, hogy garanciákat kell nyújtani arra vonatkozóan, hogy a címzett az adatvédelmi törvény által biztosítottal azonos szintű védelmet fog biztosítani. Ezért az Európai Adatvédelmi Testület elismeri, hogy a koreai személyesadat-kezelőtől a harmadik országbeli címzethez történő adattovábbítás általában az érintett tájékozott hozzájárulásán alapul.
104. E tekintetben az Európai Adatvédelmi Testület üdvözli az Adatvédelmi Bizottság 2021-1. számú Értesítésben nyújtott pontosítását, amely szerint az egyéneket tájékoztatni kell arról a harmadik országról, amelybe az adataikat továbbítják⁴³, mivel ez – miként az Európai Bizottság rámutat⁴⁴ – elősegíti azt, hogy az EGT-beli érintettek teljes körű tájékoztatáson alapuló döntést hozhassanak a külföldre történő adatszolgáltatáshoz való hozzájárulásról.
105. A személyes adatok Japánban való megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről szóló 28/2018. számú véleményben foglaltakhoz hasonlóan hangsúlyozni kell azonban, hogy a GDPR szerint a hozzájárulás előtt az érintetteket kifejezetten tájékoztatni kell az ilyen adattovábbítás harmadik ország által biztosított megfelelő védelem és a megfelelő garanciák hiányából adódó lehetséges kockázatairól. A tájékoztatásnak tartalmaznia kell például azt az információt, hogy a harmadik országban esetleg nem működik felügyeleti hatóság, és/vagy nem léteznek adatkezelési elvek, és/vagy nem biztosítják az érintettek jogait⁴⁵. Az Európai Adatvédelmi Testület szerint ez a tájékoztatás elengedhetetlen ahhoz, hogy az érintett az adattovábbítás e konkrét tényeinek teljes tudatában adhasson beleegyezést⁴⁶. Ezért az Európai Adatvédelmi Testület aggályosnak találja az Európai Bizottságnak az adattovábbítás ezen sajátos fajtájára vonatkozó megállapításait a megfelelőségi határozattervezetben. Az érintettek általában nem ismerik a harmadik ország adatvédelmi keretét. Tehát nem lehet azt a következtetést levonni, hogy az adattovábbítás kockázatát pusztán a célország ismerete alapján fel tudnák mérni. Hozzájárulásuk megadása előtt pontos

⁴¹ A határozattervezet (87) preambulumbekkezdése.

⁴² A határozattervezet (88) preambulumbekkezdése.

⁴³ Uo.

⁴⁴ Uo.

⁴⁵ Az Európai Adatvédelmi Testület 2/2018. számú iránymutatásai a 2016/679. számú rendelet 49. cikke szerinti eltérésekről, 2018. május 25., 8. o.

⁴⁶ Az Európai Adatvédelmi Testület 2/2018. számú iránymutatásai a 2016/679. számú rendelet 49. cikke szerinti eltérésekről, 2018. május 25., 7. o.

tájékoztatást kell kapniuk a személyes adatok Koreai Köztársaság területén kívül eső országba történő továbbításának a sajátos kockázatairól.

106. Ezért az Európai Adatvédelmi Testület felkéri az Európai Bizottságot annak biztosítására, hogy az érintettnek nyújtandó tájékoztatás „*az adattovábbítás körülményeiről*” a harmadik ország által biztosított megfelelő védelem és a megfelelő garanciák hiányából adódó lehetséges kockázatokra vonatkozó információkat is tartalmazzon. Az Európai Adatvédelmi Testület számára ez fontos annak megállapításához, hogy a hozzájárulásra vonatkozó követelmények alapvetően azonosak-e a GDPR szerintiekkel.
107. Tekintettel arra, hogy a hozzájárulásnak önkéntesnek, tájékoztatáson alapulónak, konkrétan és egyértelműnek kell lennie, az Európai Adatvédelmi Testület örömmel fogadná továbbá azt, ha a megfelelőségi határozat további biztosítékokat tartalmazna arra vonatkozóan, hogy a koreai személyesadat-kezelők nem továbbítanak személyes adatokat harmadik országban tevékenykedő harmadik fél részére olyan helyzetekben, amikor a GDPR szerinti érvényes hozzájárulást nem lehetett megadni, például egyenlőtlen erőviszonyok következtében.
108. Azokat az eseteket illetően, amikor a személyesadat-kezelő az érintett hozzájárulása nélkül adhat át személyes adatokat egy külföldön tevékenykedő harmadik fél számára, azaz (1) ha a személyes adat átadása az adatvédelmi törvény 17. cikkének (4) bekezdése szerint az adatgyűjtés eredeti céljához elfogadható módon kapcsolódó célból történik, és (2) azokban a kivételes esetekben, amikor az adatvédelmi törvény 18. cikkének (2) bekezdése szerint a személyes adat harmadik fél részére átadható, az Európai Adatvédelmi Testület tudomásul veszi az Adatvédelmi Bizottság által a 2021-1. számú Értesítés 2. szakaszában nyújtott magyarázatokat (és üdvözli azt a koreai adatkezelő és a külföldi címzett számára előírt kötelezettséget, hogy egy jogilag kötelező érvényű eszközzel (például szerződéssel) biztosítsák az adatvédelmi törvényben előírtnak megfelelő szintű védelmet – az érintett jogainak vonatkozásában is).

3.1.12. Közvetlen üzletszerzés

109. A GDPR 21. cikkének (2) és (3) bekezdése, valamint a GDPR-megfelelőségi referencia szerint az érintettnek bármikor képesnek kell lennie a profilalkotási és közvetlen üzletszerzési célokból sorra kerülő adatkezelés elleni tiltakozásra anélkül, hogy ennek kapcsán bármilyen költség merülne fel.
110. Az adatvédelmi törvény 37 cikkében meghatározott felfüggesztési jogot illetően az Európai Adatvédelmi Testület elfogadja, hogy az Európai Bizottság szerint ez a jog arra az esetre is vonatkozik, amikor az adatokat közvetlen üzletszerzési célokra használják⁴⁷. Mindazonáltal örömmel venné, ha a megfelelőségi határozat további információkkal és pontosításokkal szolgálna ezzel a megállapítással kapcsolatban, különös tekintettel a felfüggesztési jog közvetlen üzletszerzéssel összefüggésben történő alkalmazására (pl. hivatkozás a vonatkozó ítélkezési gyakorlatra, stb.). Ebben a vonatkozásban kiemelné azt is, hogy a hiteladat-védelmi törvény (37. cikkének (2) bekezdése) kifejezetten rögzíti az annak kéréséhez való jogot, hogy egy hiteladat-szolgáltató/felhasználó hagyjon fel az áruk vagy szolgáltatások bemutatása vagy megvásárlásra kínálása céljából történő megkeresésekkel.
111. Amint azt az Európai Bizottság elismeri⁴⁸, a koreai jogi keret az ilyen célokból végzett adatkezelést az érintett konkrét (további) hozzájárulásához köti (lásd az adatvédelmi törvény 15. cikke (1) bekezdésének 1. pontját és 17. cikke (2) bekezdésének 1. pontját).
112. Mivel nem zárható ki, hogy az EGT-ből továbbított személyes adatokat Koreában ilyen célokból fogják kezelni, az Európai Adatvédelmi Testület azt is üdvözölné, ha a megfelelőségi határozat pontosítaná,

⁴⁷ A határozattervezet (79) preambulumbekzdése.

⁴⁸ Uo.

hogy az érintettnek joga van ahhoz, hogy hozzájárulását visszavonja⁴⁹, és hogy személyes adatait töröljék, és a továbbiakban ne kezeljék, amennyiben az adatkezelés hozzájáruláson alapul (mint például a marketing célokból folytatott adatkezelés esetében), és azt az érintett visszavonta.

3.1.13. Automatizált döntéshozatal és profilalkotás

113. Határozattervezetében az Európai Bizottság elismeri⁵⁰, hogy sem az adatvédelmi törvény, sem annak végrehajtási határozata nem tartalmaz a személyes adatok kizárólag automatizált módon történő kezelésén alapuló és az érintettre kiható döntésekre vonatkozó általános rendelkezéseket. Ettől függetlenül a koreai jogrendszerben létezik ez a jog: az automatizált döntéshozatalra vonatkozó szabályokat a hiteladat-védelmi törvény tartalmazza (36. cikk (2) bekezdés), bár úgy tűnik, hogy ezek alkalmazását nem az Adatvédelmi Bizottság felügyeli (és ekként kívül esnek a határozattervezet hatályán – a határozattervezet hatályáról lásd fentebb a 2.3.2. szakaszt).
114. Amint azt a 29. cikk szerinti munkacsoport⁵¹ az adatvédelmi pajzsról szóló 1/2016. számú véleményében és az Európai Adatvédelmi Testület a Japánra vonatkozó megfelelőségi határozatáról szóló korábbi véleményében⁵² már megállapította, az automatizált döntéshozatal, a profilalkotás és a mesterséges intelligencia növekvő fontossága indokolná a magasabb szintű védelem biztosítását ezen a területen. Az Európai Bizottság érvelésével szemben⁵³ – mely szerint nem valószínű, hogy az Unióban gyűjtött személyes adatok védelmi szintjére hatással lenne az, hogy az adatvédelmi törvényből hiányoznak az automatizált döntéshozatalra vonatkozó egyedi szabályok (mivel az automatizált adatkezelésen alapuló döntéseket jellemzően az érintettel közvetlen kapcsolatban álló unióbeli adatkezelő hozza) – az Európai Adatvédelmi Testület úgy véli, hogy nem zárható ki, hogy a koreai személyesadat-kezelő automatizált döntéshozatalt alkalmaz a megfelelőségi határozat alapján továbbított adatok esetében (például a foglalkoztatással összefüggésben a munkahelyi teljesítmény, a megbízhatóság, a viselkedés, stb. értékelése céljából).
115. A fejlődő új technológiák megkönnyítik a vállalatok számára az automatizált döntéshozatali rendszerek megvalósítását, vagy lehetővé teszik számukra, hogy fontolóra vegyék az ilyen rendszerek kialakítását, ami gyengítheti az egyének helyzetét. Azokban az esetekben, amikor a kizárólag ilyen automatizált rendszerek által hozott döntések hatással vannak az egyének jogi helyzetére, vagy jelentős mértékben érintik őket (például feketelistára helyezés és ezáltal a jogaikból való megfosztás következtében), döntő fontosságú a hatékony garanciák biztosítása, 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 elleni tiltakozáshoz való jogot⁵⁴.
116. Ezzel összefüggésben az Európai Adatvédelmi Testület aggodalmát fejezi ki amiatt, hogy az adatvédelmi törvény nem tartalmaz az automatizált döntéshozatalra vonatkozó jogi rendelkezéseket,

⁴⁹ Lásd még fentebb a 67. bekezdést: Miközben a hiteladat-védelmi törvény 37. cikke (1) bekezdésében egyértelműen szerepel a hozzájárulás visszavonásához való jog, az adatvédelmi törvény csak két helyen – a 27. cikk (1) bekezdésének 2. pontjában és a 39. cikk (7) bekezdésében – tesz említést arról, hogy ez a jog meghatározott körülmények között létezik.

⁵⁰ Lásd a határozattervezet (81) preambulumbekendését.

⁵¹ A 95/46/EK irányelv 29. cikke alapján felállított munkacsoport, amely független európai tanácsadó testületként szolgál az adatvédelem és a magánélet védelme területén. Feladatainak leírása a 95/46/EK irányelv 30. cikkében és a 2002/58/EK irányelv 15. cikkében található. Ebből a munkacsoportból (WP29) lett az Európai Adatvédelmi Testület.

⁵² 2018. december 5-én elfogadott 28/2018. számú vélemény a személyes adatok Japánban való megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről.

⁵³ A határozattervezet (81) preambulumbekendése.

⁵⁴ WP 254, 7. o.

és ezért felkéri az Európai Bizottságot ennek a kérdésnek a vizsgálatára, valamint a koreai jogszabályi keret e tekintetben történő fejlesztése folyamatos figyelemmel kísérésére.

3.1.14. Elszámoltathatóság

117. A koreai jogi keret több olyan szabályt tartalmaz, amelyek célja annak biztosítása, hogy a személyes adat-kezelők megfelelő technikai és szervezési intézkedéseket hozzanak annak érdekében, hogy adatvédelmi kötelezettségeiknek ténylegesen megfeleljenek, és ezt a megfelelést bizonyítani tudják, többek között az illetékes felügyeleti hatóság számára. Az Európai Adatvédelmi Testület különösen üdvözli a következő szabályok meglétét: a belső irányítási terv elfogadásának előírása (az adatvédelmi törvény 29. cikke), az úgynevezett adatvédelmi hatásvizsgálat (AVHV) végzésének kötelezettsége az olyan adatkezelésre vonatkozóan, amikor nagyobb a kockázata annak, hogy az adatvédelem sérülhet (az adatvédelmi törvény 29. cikkének (1) bekezdése és az adatvédelmi törvény végrehajtási rendeletének 35. cikke), a személyzet képzésére és felügyeletére vonatkozó szabályok (az adatvédelmi törvény 28. cikke), valamint az adatvédelmi tisztviselő kinevezésének kötelezettsége (az adatvédelmi törvény 31. cikke, az adatvédelmi törvény végrehajtási rendeletének 32. cikkével együttesen értelmezve).
118. Az Európai Adatvédelmi Testület osztja az Európai Bizottság ezek által biztosított alapvetően azonos védelemmel kapcsolatos nézetét, még azokra az esetekre vonatkozóan is, amikor úgy tűnik, hogy a szabályok eltérnek azoktól, amelyeket a GDPR megfogalmaz – például nincs olyan rendelkezés, amely kimondja, hogy az adatvédelmi tisztviselőnek függetlennek kell lennie, de az egyértelműen meg van határozva, hogy a személyes adat-kezelő vezetésének tartozik felelősséggel (az adatvédelmi törvény 31. cikkének (4) bekezdése) –, és javasolná, hogy a megfelelőségi határozat felülvizsgálata során az Európai Bizottság ellenőrizze ezeknek a rendelkezéseknek a tényleges alkalmazását annak érdekében, hogy a végrehajtásuk hatékonyságát értékelhesse.

3.2. Eljárási és végrehajtási mechanizmusok

119. Az Európai Adatvédelmi Testület a koreai adatvédelmi keret megfelelőségi határozattervezet hatálya alá tartozó következő vonatkozásait elemezte a GDPR-megfelelőségi referenciában meghatározott szempontok alapján: független felügyeleti hatóság létezése és hatékony működése; a szabályok betartásának jó szintjét biztosító rendszer létezése, valamint a megfelelő jogorvoslati mechanizmusokhoz való hozzáférést biztosító rendszer létezése, amely lehetővé teszi az EGT-állampolgárok számára, hogy jogukat gyakorolják, és jogorvoslatot keressenek anélkül, hogy a közigazgatási és bírósági jogorvoslatot megnehezítő akadályokba ütköznenek.
120. A GDPR VI. fejezetével és a GDPR-megfelelőségi referencia 3. fejezetével összhangban a harmadik országban léteznie kell egy vagy több olyan független felügyeleti hatóságnak, amelynek feladata, hogy az EGT-beli szinttel azonos szintű védelem biztosítása érdekében figyelje, biztosítsa és érvényre juttassa az adatvédelemre és a magánélet védelmére vonatkozó rendelkezéseknek való megfelelést.
121. Ebben az összefüggésben a harmadik ország felügyeleti hatóságának teljesen függetlenül és pártatlanul eljárva kell feladatait ellátnia és hatásköreit gyakorolnia, melynek során nem kérhet vagy fogadhat el utasításokat. Emellett a felügyeleti hatóságnak rendelkeznie kell mindazokkal a hatás- és feladatkörökkel, amelyek az adatvédelmi jogok tudatosításához és tiszteletben tartásuk biztosításához szükségesek és elérhetők. A felügyeleti hatóság személyzetét és költségvetését is figyelembe kell venni. A felügyeleti hatóságnak képesnek kell lennie arra is, hogy saját kezdeményezésre eljárást indítson.

3.2.1. Illetékes független felügyeleti hatóság

122. A Koreai Köztársaságban az Adatvédelmi Bizottság az adatvédelmi törvény figyelemmel kíséréseért és betartatásáért felelő független hatóság. Az Adatvédelmi Bizottság egy elnökből, egy alelnökből és hét

biztosból áll. Az Adatvédelmi Bizottság elnökét és alelnökét a Koreai Köztársaság elnöke nevezi ki a miniszterelnök javaslata alapján. Két biztos kinevezésére a bizottság elnöke tesz javaslatot, két biztost annak a politikai pártnak a képviselői jelölnek, amelyhez a köztársaság elnöke is tartozik, a fennmaradó három biztos kinevezése pedig a többi politikai párt képviselőinek a javaslata alapján történik (az adatvédelmi törvény 7. cikke (1) bekezdésének 2. pontja). Az Adatvédelmi Bizottság munkáját titkárság segíti (az adatvédelmi törvény 7. cikkének (13) bekezdése), amely bizottságokat hozhat létre az enyhébb jogsértések és az ismétlődő ügyek kezelésére (az adatvédelmi törvény 7. cikkének (12) bekezdése).

123. E tekintetben az Európai Adatvédelmi Testület elismeri, hogy az Adatvédelmi Bizottság a jogállását és jogkörét jelentősen módosító, közelmúltban történt átszervezése ellenére komoly erőfeszítéseket tett az adatvédelmi törvény és annak legújabb módosításai végrehajtására alkalmas, szükséges infrastruktúra kiépítése érdekében. Ezen erőfeszítések közül megemlíthető az Adatvédelmi Bizottság szabályainak megállapítása, az adatvédelmi törvény értelmezését segítő útmutató kidolgozása, egy telefonos ügyfélszolgálat létrehozása, amely gazdasági szereplők és természetes személyek számára nyújt tanácsadást az adatvédelmi rendelkezésekkel kapcsolatban, valamint egy panaszkezelés célját szolgáló közvetítői szolgálat felállítása. Az Adatvédelmi Bizottság feladatai különösen a következőket foglalják magukban: az adatvédelemmel kapcsolatos törvényekkel és rendeletekkel kapcsolatos tanácsadás, adatvédelmi politikák és iránymutatások kidolgozása, az egyéni jogokat érintő jogsértések kivizsgálása, panaszkezelés és vitás felek közötti közvetítés, az adatvédelmi törvény betartatása, az adatvédelem területén végzett felvilágosítás és az adatvédelem előmozdítása, valamint a harmadik országok adatvédelmi hatóságaival folytatott eszmecsere és együttműködés⁵⁵.
124. Az Adatvédelmi Bizottság tagjainak kijelölését és összetételét az adatvédelmi törvény 7. cikkének (2) bekezdése határozza meg. Bár az Adatvédelmi Bizottság a miniszterelnök hatáskörébe tartozik (elnökét és alelnökét a miniszterelnök javaslatára nevezi ki a koreai elnök), a jogi keret felhatalmazást ad a biztosoknak arra, hogy feladataikat függetlenül, a jognak és lelkiismeretüknek megfelelően végezzék. Az Európai Adatvédelmi Testület elismeri az adatvédelmi törvényben és különösen annak 7. cikke (4)-(7) bekezdéseiben foglalt intézményi és eljárási garanciákat. Mindazonáltal üdvözlendő, ha az Európai Bizottság figyelemmel kísérrné azokat a fejleményeket, amelyek a dél-koreai felügyeleti hatóság tagjainak a függetlenségére hatással lehetnek.
125. A határozattervezet még nem tartalmazza az Adatvédelmi Bizottság költségvetésének a finanszírozási forrásokra és a költségvetés átláthatóságára is kiterjedő elemzését. Az Európai Adatvédelmi Testület úgy véli, hogy ez az elem – amely említésre kerül mind a GDPR 56. cikkének (1) bekezdésében, mind azon eljárási és végrehajtási adatvédelmi elvek és mechanizmusok között, amelyeket a GDPR-megfelelőségi referencia szerint egy ország vagy egy nemzetközi szervezet rendszerének az értékelése során figyelembe kell venni – alapos vizsgálatot igényel, mivel ez jelzi, hogy a felügyeleti hatóságnak milyen gazdasági és emberi erőforrások állnak rendelkezésére a törvényben előírt adatvédelmi kötelezettségei és feladatai független teljesítéséhez, és ezért azt tanácsolná az Európai Bizottságnak, hogy részletesebben térjen ki rá a határozattervezetben.

3.2.2. A szabályok betartásának jó szintjét biztosító biztosító rendszer létezése

126. A végrehajtás terén az Európai Adatvédelmi Testület tisztában van az Adatvédelmi Bizottság adatvédelmi törvényben és hiteladat-védelmi törvényben szabályozott végrehajtási jogkörével és az általa alkalmazható szankciók körével, és tudomásul veszi a 2021-1. számú Értesítésben foglalt pontosításokat, melyek szerint az adatvédelmi törvény 64. cikkének (1) bekezdésében és a hiteladat-

⁵⁵ Az Adatvédelmi Bizottság feladatait és hatásköreit elsősorban az adatvédelmi törvény 7. cikkének (8)-(9) bekezdései, valamint 61-66. cikkei szabályozzák.

védelmi törvény 45. cikkének (4) bekezdésében hivatkozott feltételek⁵⁶ alkalmazandók minden olyan esetben, amikor a személyes adatok védelme céljából törvénybe foglalt elvek, jogok és köteleességek sérülnek. Mindazonáltal javasolná az Európai Bizottságnak az Adatvédelmi Bizottság arra vonatkozó hatásköre gyakorlati alkalmazásának a szoros figyelemmel kísérését, hogy a jogsértőt kötelezze a 64. cikk (1) bekezdésében és a hiteladat-védelmi törvény 45. cikkének (4) bekezdésében meghatározottak közül megfelelőnek talált intézkedés meghozatalára.

127. Ami az adatvédelmi törvény 64. cikkének (1) bekezdésében meghatározott korrekciós intézkedéseket illeti, az Adatvédelmi Bizottság 50 millió koreai won összegig terjedő bírságot szabhat ki egy korrekciós intézkedés végrehajtásának az elmulasztásáért (az adatvédelmi törvény 75. cikke (1) bekezdésének 13. pontja). Ez az összeg 36 564 eurónak felel meg. Az Európai Adatvédelmi Testület véleménye szerint az alkalmazható pénzbüntetésnek ez a korlátozása aggodalomra ad okot, mivel előfordulhat, hogy nem gyakorol olyan erőteljes elrettentő hatást a jogsértőkre, mint amelyet a törvény az adatvédelmi szabályok betartatása érdekében el kíván érni, mert ez az összeg nem tűnik elegendőnek ahhoz, hogy megfelelő visszatartó erőt biztosítson, különösen a jelentős pénzügyi forrásokkal rendelkező nagy szervezetek vagy vállalkozások esetében.
128. Tekintettel arra a lehetőségre, hogy az Adatvédelmi Bizottság követelheti, hogy egy központi igazgatási szerv vezetője végezzen vizsgálatot a személyesadat-kezelőnél vagy vegyen részt az adatvédelmi törvény megsértésének közös kivizsgálásában, melynek során korrekciós intézkedést is előírhat a hatásköre alá tartozó személyesadat-kezelők számára (az adatvédelmi törvény 63. cikkének (4)-(5) bekezdései), az Európai Adatvédelmi Testület megállapítja, hogy bár a határozattervezet (122) preambulumbekendése ad némi felvilágosítást, ezeknek a szervezeteknek a jellege és az Adatvédelmi Bizottsággal való jogi kapcsolata összességében meglehetősen homályos marad. Emellett az adatvédelmi törvény 68. cikkének (1) bekezdése sok olyan jogalanyt említ, amelyre az Adatvédelmi Bizottság hatásköre átruházható. Habár úgy tűnik, hogy ezt a rendelkezést csak a Koreai Internet és Biztonsági Ügynökség vonatkozásában alkalmazták⁵⁷, az Európai Adatvédelmi Testület örömmel venné az ezen jogalanyok közötti lehetséges kapcsolatok jellegének a tisztázását és a szóban forgó rendelkezés jövőbeli gyakorlati alkalmazásának a gondos figyelemmel kísérését az adatvédelmi szabályok alkalmazásával megbízott jogalanyok függetlenségének a biztosítása érdekében.
129. A szankciókat illetően úgy tűnik, hogy a koreai rendszer ötvözi a különböző típusú szankciókat a korrekciós intézkedésektől és közigazgatási bírságoktól a valószínűleg komoly elrettentő erővel bíró büntetőjogi szankciókig terjedően, és a koreai hatóságok számos példát mutattak be az Adatvédelmi Bizottság által a közelmúltban kivetett bírságokra, megemlítve többek között, hogy 2020. decemberében 6,7 milliárd won összegű bírsággal sújtott egy céget az adatvédelmi törvény különböző rendelkezéseinek a megsértése miatt, 2021. április 28-án pedig 103,3 millió won fizetésére kötelezett egy MI-technológiai céget az adatkezelés jogszerűségére, konkrétan a hozzájárulásra és az álnevesített adatok kezelésére vonatkozó szabályok megszegéséért.
130. Noha a fenti összegek visszatartó erejük lehetnek, az Európai Adatvédelmi Testület üdvözlölné a további felvilágosítást arra vonatkozóan, hogy az Adatvédelmi Bizottság milyen módszerrel határozza meg a közigazgatási bírság összegét, például az adatvédelmi törvény 64. cikkének (1) bekezdése alapján előírt korrekciós intézkedés végrehajtásának az elmulasztása miatt kiszabott bírság esetében (lásd az adatvédelmi törvény 75. cikke (2) bekezdésének 13. pontja). Ez különösen a büntetőjogi szankciók és a (koreai) büntető törvénykönyv alkalmazása szempontjából fontos.

⁵⁶ Azaz „valószínűsíthető, hogy a jogsértés következtében a személyes adatokhoz fűződő egyéni jogok és szabadságok sérülnek, és az intézkedés hiánya valószínűleg olyan kárt okozna, amely nehezen orvosolható.”

⁵⁷ Lásd a határozattervezet (117) preambulumbekendését és a végrehajtási rendelet 62. cikkét.

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

131. A jogorvoslatot illetően úgy tűnik, hogy a koreai rendszer különféle lehetőségeket kínál a megfelelő védelem biztosítására és különösen az egyéni jogok hatékony közigazgatási és bírósági jogorvoslat révén történő érvényesítésére, amely a kártérítést is magában foglalja.
132. A közigazgatási és bírósági jogorvoslati lehetőségek mellett alternatív mechanizmusokat is kínál a jogorvoslatot kereső érintettek számára a koreai rendszer, ahogy azt a határozattervezet (132) és (133) preambulumbekendései az adatvédelmi telefonos ügyfélszolgálat és a vitarendezési közvetítő bizottság kapcsán leírják. Mivel ezek kiegészítő jogorvoslati lehetőségek, az Európai Adatvédelmi Testület örömmel fogadná annak részletesebb magyarázatát, hogy ezek hogyan egészítik ki az Adatvédelmi Bizottság és a bíróságok előtti jogorvoslati lehetőségeket azoknak az érintetteknek az esetében, akiknek a személyes adatait a megfelelőségi határozat alapján Koreába továbbítják.

4. A DÉL-KOREAI KÖZHATALMI SZERVEK ÁLTALI HOZZÁFÉRÉS ÉS FELHASZNÁLÁS AZ EURÓPAI UNIÓBÓL TOVÁBBÍTOTT SZEMÉLYES ADATOK ESETÉBEN

133. A bűnüldözés és a nemzetbiztonság területein biztosított adatvédelmi szint értékelésével kapcsolatban teljes körű tájékoztatást nyújtott az Európai Bizottság a határozattervezetben és a rendelkezésre bocsátott mellékletekben. Ezért az Európai Adatvédelmi Testület tartózkodik attól, hogy a ténymegállapítások és értékelések többségét ebben a véleményben megismételje.
134. Az Európai Bizottság arra a következtetésre jutott, hogy a fent említett területeken biztosított adatvédelem szintje megegyezik az EUB ítélkezési gyakorlata során felállított követelményekkel, és ezért alapvetően azonosnak tekinthető az Európai Unió adatvédelmi szintjével.
135. Az Európai Adatvédelmi Testület általános megjegyzésként hangsúlyozni szeretné, hogy a koreai adatvédelmi szint megfelelőségének értékelését azokra az esetekre is helyénvaló kiterjeszteni, amikor úgy tűnik, vagy amelyekről az Európai Bizottság azt állítja, hogy a vonatkozó koreai jog valószínűleg nem érinti az EU-ból Dél-Koreába továbbított adatokat. Az ilyen esetek fontosságát az a tény is bizonyítja, hogy az Európai Bizottság maga is foglalkozott velük a határozattervezetben.

4.1. A kormányzati hozzáféréssel összefüggő általános adatvédelmi keret

136. A közhatalmi szervek személyes adatokhoz való hozzáféréseinek a vizsgálata során különféle koreai jogszabályok értékelése alapján állapítható meg, hogy milyen szinten biztosított a magánélethez való jog védelme és az adatvédelem. Az Európai Adatvédelmi Testület mindenekelőtt megjegyzi, hogy az adatvédelmi törvény – mint az adatvédelmet szabályozó legfontosabb jogszabály – széles hatállyal rendelkezik. Azonban, miközben a bűnüldözés területén teljes körűen alkalmazandó, a nemzetbiztonsági célokból folytatott adatkezelésre való alkalmazhatósága korlátozott. Az adatvédelmi törvény 58. cikke (1) bekezdésének 2. pontja értelmében a III-VII. fejezetek a személyes adatok nemzetbiztonsági célokból végzett kezelésére nem vonatkoznak. Az I., II., IX. és X. fejezetek azonban a nemzetbiztonsági területen is érvényben maradnak. Az adatvédelmi törvényben foglalt alapelvek, az érintett jogaira vonatkozó alapvető garanciák, valamint a felügyeletre, végrehajtásra és jogorvoslatra vonatkozó rendelkezések tehát a nemzetbiztonsági hatóságok személyes adatokhoz való hozzáféréseire és a személyes adatok nemzetbiztonsági hatóságok általi felhasználására is alkalmazandók.

137. Az alapvető adatvédelmi elveket, nevezetesen a jogszerűség, a szükségesség és az arányosság elvét a dél-koreai alkotmány is rögzíti. Ezek az elvek a dél-koreai közhatalmi szervek személyes adatokhoz való bűnüldözési és nemzetbiztonsági célú hozzáféréseire is alkalmazandók⁵⁸.
138. A bűnüldözés területén a rendőrség, az ügyészség, a bíróságok és más közfeladatot ellátó szervek gyűjthetnek személyes adatokat külön jogszabály alapján, mint amilyen például a büntetőeljárás törvény, a hírközlési adatvédelmi törvény, a távközlési vállalkozásokról szóló törvény és a bizonyos pénzügyi tranzakciók adatainak jelentéséről és felhasználásáról szóló törvény, amely a pénzmosás és a terrorizmus-finanszírozás megelőzését és üldözését szabályozza. Ezek a törvények további korlátozásokat, garanciákat és mentességeket határoznak meg.
139. A nemzetbiztonság területén a nemzeti hírszerző szolgálatról szóló törvény és más „nemzetbiztonsági jogszabályok”⁵⁹ alapján a Nemzeti Hírszerző Szolgálat (**NHSZ**) gyűjthet személyes adatokat és végezhet lehallgatásokat. Az Európai Adatvédelmi Testület értelmezése szerint az NHSZ jogkörei gyakorlása során köteles betartani a fent említett jogszabályi rendelkezéseket és az adatvédelmi törvényt.
140. Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot annak pontosítására, hogy az NHSZ mellett vannak-e a nemzetbiztonságot felelő más hatóságok is Koreában, mert az I. melléklet 6. szakaszában azt a benyomást kelti, hogy az NHSZ csak egy példája a nemzetbiztonsági szervezeteknek.

4.2. A hírközlési metaadatokhoz való bűnüldözési célú kormányzati hozzáférés vonatkozásában biztosított védelem és garanciák

141. A vonatkozó jogszabály, azaz a hírközlési adatvédelmi törvény alapján a bűnüldöző hatóságok kétféle intézkedést hozhatnak a hírközlési adatokhoz való hozzáférés érdekében. A hírközlési adatvédelmi törvény megkülönbözteti a hírközlést korlátozó intézkedéseket, melyek a hagyományos levelek tartalmának a megszerzését és a távközlés lehallgatását jelentik⁶⁰, valamint az úgynevezett hírközlési metaadatok gyűjtését. Ez utóbbi a hívások időpontjára, kezdetének és befejezésének idejére, a kimenő és beérkező hívások számára, a másik fél előfizetői számára, a használat gyakoriságára, a távközlési szolgáltatások használatát rögzítő naplóállományokra és a helyadatokra terjed ki⁶¹.
142. Az Európai Adatvédelmi Testület megjegyzi, hogy úgy tűnik, mintha a hírközlési metaadatok vonatkozásában nem biztosítanak ugyanazokat a garanciákat, mint a korlátozó intézkedések, azaz a hírközlés tartalma esetében. Észrevehető, hogy a bűnüldözési célokból végzett adatgyűjtés területén több garancia vonatkozik a hírközlés tartalmára, mint az ahhoz tartozó metaadatokra. Először is, a tartalomtól eltérően, a metaadatok gyűjtése nem korlátozódik bizonyos súlyos bűncselekmények nyomozására, hanem végezhető bármikor, amikor valamely „nyomozás folytatásához vagy büntetés végrehajtásához” szükségesnek tartják (a hírközlési adatvédelmi törvény 13. cikkének (1) bekezdése). Másodsorban, a metaadatok gyűjtése elvileg nem egy legvégső esetben való alkalmazásra kialakított intézkedés, és nem csak akkor vehető igénybe, ha egy egyébként nehéz lenne megakadályozni egy bűncselekmény elkövetését, elfogni egy bűnelkövetőt, vagy bizonyítékot szerezni⁶². Hírközlési metaadatok gyűjthetők bármikor, amikor azt egy ügyész, bírósági tisztviselő vagy rendőr egy bűncselekmény nyomozásához vagy egy büntetés végrehajtásához „szükségesnek tartja”. Egy kivétel azonban létezik: a hírközlési adatvédelmi törvény 13. cikkének (2) bekezdése tiltja egy adott

⁵⁸ Lásd a határozattervezet (145) preambulumbekkezdését.

⁵⁹ A nemzetbiztonsági jogszabályok közé tartozik például a hírközlési adatvédelmi törvény, az állampolgárok terrorizmus elleni védelméről és a közbiztonságról szóló törvény, valamint a távközlési vállalkozásokról szóló törvény.

⁶⁰ A hírközlési adatvédelmi törvény 2. cikkének (2), (6) és (7) bekezdései.

⁶¹ A hírközlési adatvédelmi törvény 2. cikkének (11) bekezdése.

⁶² A tartalomra vonatkozó adatok esetében ezt a hírközlési adatvédelmi törvény 3. cikkének (2) bekezdése és 5. cikkének (1) bekezdése írja elő.

bázisállomás adatainak és metaadatainak a valós idejű nyomon követését. Harmadszor, a hírközlés tartalmára vonatkozó adatokat gyűjtő bűnüldöző szerveknek azonnal abba kell hagyniuk az adatgyűjtést, amint annak folytatását már nem tartják szükségesnek⁶³. A metaadatok vonatkozásában ezt nem, vagy kifejezetten legalábbis nem írja elő sem a hírközlési adatvédelmi törvény, sem annak végrehajtási rendelete.

143. Az Európai Adatvédelmi Testület elismeri, hogy hírközlési metaadatok gyűjtésére csak bírósági felhatalmazás alapján kerülhet sor. A hírközlési adatvédelmi törvény emellett előírja, hogy mind a bírósági felhatalmazásban, mind az arra irányuló kérelemben részletes tájékoztatást kell nyújtani⁶⁴. Az előzetes bírósági felhatalmazás arra szolgál, hogy korlátozza a bűnüldöző hatóságok jogalkalmazási szabadságát, és hogy minden esetben igazolható legyen az, hogy a hírközlési metaadatok gyűjtése kellően indokolt volt. Az Európai Adatvédelmi Testület elismeri továbbá, hogy úgy tűnik, a Koreai Köztársaság joga nem rendelkezik a hírközlési metaadatok általános és különbségtétel nélküli megőrzéséről. Ezért az ilyen adatokhoz való kormányzati hozzáférés mindig csak magának a távközlési szolgáltatásnak a nyújtása és számlázása céljából még fenntartott adatok esetében lehetséges.
144. Az Európai Adatvédelmi Testület hangsúlyozza azonban, hogy az EUB megkérdőjelezte azt, hogy a forgalmi adatok más adatoknál és különösen a tartalomra vonatkozó adatoknál kevésbé különlegesek⁶⁵. Figyelembe véve, hogy a hírközlési metaadatok több szempontból is alacsonyabb szintű védelemben részesülnek, mint a tartalomra vonatkozó adatok, az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy kísérje szoros figyelemmel, vajon a koreai jog alapján a személyes adatok e kategóriája vonatkozásában nyújtott garanciák biztosítják-e az EU-ban garantált alapvetően azonos szintű védelmet, különös tekintettel az arányosságra és a jogi kiszámíthatóságra.

4.3. A koreai közhatalmi szervek nemzetbiztonsági célú hozzáférése a hírközlési adatokhoz

145. A nemzetbiztonsági hatóságok EGT-ből Koreába továbbított hírközlési adatokhoz való hozzáféréseire vonatkozó jogi keretet illetően az Európai Adatvédelmi Testület két aggályt fogalmazott meg, amelyek mindegyike a nem koreai állampolgárok közötti közlésekhez való hozzáférés különleges eseteire vonatkozó szabályokhoz kapcsolódik (lásd a 29. bekezdést). Ezekben az esetekben bizonyos egyébként biztosított garanciák nem alkalmazandók sem a hírközlési metaadatok, sem a tartalomra vonatkozó adatok tekintetében. Másképp fogalmazva: ezekben az egyedi esetekben ezeknek az adatoknak a vonatkozásában nem biztosítják ugyanazokat a garanciákat, mint azokban az esetekben, amikor legalább egy koreai állampolgár is részt vesz a kommunikációban.

4.3.1. A külföldi állampolgárok közötti közlésekhez való hozzáférésről szóló értesítés kötelezettségének hiánya

146. A fent említett esetben, azaz amikor a kommunikációban részt vevő felek egyike sem koreai állampolgár, a nemzetbiztonsági hatóságok nem kötelesek értesíteni az érintetteket személyes adataik gyűjtéséről és kezeléséről. Az Európai Adatvédelmi Testület elismeri, hogy ez a probléma csak bizonyos

⁶³ A hírközlési adatvédelmi törvény végrehajtási rendeletének 2. cikke.

⁶⁴ Lásd a határozattervezet (156) preambulumbekkezdését.

⁶⁵ Lásd az EUB 2020. október 6-i *Privacy International* ítélete, C-623/17, ECLI:EU:C:2020:790, 71. bekezdés: „A forgalmi és helymeghatározó adatoknak a biztonsági és hírszerző szolgálatok részére történő továbbítása által a Charta 7. cikkében biztosított jogba megvalósított beavatkozás különösen súlyosnak tekintendő, figyelembe véve elsősorban azt, hogy ezek az adatok különleges információkat hordozhatnak, és ezekből kiindulva felállítható az érintett személyek profilja, amely ugyanolyan különleges információnak minősül, mint a közléseknek maga a tartalma. Ezenkívül az érintett személyekben azt az érzést keltheti, hogy magánéletük állandó felügyelet alatt áll (lásd analógia útján: 2014. április 8-i *Digital Rights Ireland és társai* ítélet, C-293/12 és C-594/12, EU:C:2014:238, 27. és 37. pont; 2016. december 21-i *Tele2* ítélet, C-203/15 és C-698/15, EU:C:2016:970, 99. és 100. pont).”

eseteket érint. Először is, a korábban említettek szerint, ha legalább egy koreai állampolgár is részt vesz a kommunikációban, akkor a hírközlési adatvédelmi törvény szerinti értesítési követelmények a kommunikációban részt vevő valamennyi fél vonatkozásában felállnak, függetlenül attól, hogy az érintettek milyen állampolgárok⁶⁶. Másodszor, a kizárólag külföldi állampolgárok közötti közlésekből származó személyes adatok gyűjtése csak különleges esetekben megengedett. Ezek olyan esetek, amikor a hozzáférési jog a következők általi közléseket érinti: a) a Koreai Köztársasággal szemben ellenséges országok, b) a Korea-ellenes tevékenység folytatásával gyanúsított külföldi szervezetek, csoportok vagy állampolgárok⁶⁷ és c) a Koreai-félszigeten, de ténylegesen a Koreai Köztársaság felségterületén kívül tevékenykedő, külföldi országbeli ernyőcsoportokhoz tartozó csoportok tagjai. Az uniós állampolgárok közötti, EGT-ből Koreába továbbított közléseket érintő, nemzetbiztonsági célú adatgyűjtésre tehát csak a fenti három kategória valamelyikébe sorolható közlések esetén kerülhet sor⁶⁸. Az Európai Bizottság kiegészítő magyarázatai alapján további korlátozó tényezőként értelmezi az Európai Adatvédelmi Testület azt, hogy az alkalmazandó jogi keret nem teszi lehetővé az adatok Koreán kívüli, továbbítás közben történő megszerzését.

147. Ezért az értesítésre vonatkozó követelmény hiányának a jelentősége – a gyakorlati hatások szempontjából nézve – korlátozottnak tekinthető. Mindazonáltal az Európai Adatvédelmi Testület hangsúlyozza a kormányzati hozzáférésről való (utólagos) értesítés fontosságát, különösen a hatékony jogorvoslat biztosítására való tekintettel. Az EUB szerint az értesítés „szükséges ahhoz, hogy lehetővé tegye e személyek számára a Charta 7. és 8. cikkéből eredő, arra irányuló jogaik gyakorlását, hogy hozzáférést kérjenek az ezen intézkedések tárgyát képező személyes adataikhoz és adott esetben azok helyesbítését vagy törlését kérjék, valamint hogy a Charta 47. cikke első bekezdésének megfelelően bíróság előtti hatékony jogorvoslatot kezdeményezzenek”⁶⁹. A nemzetbiztonsági célú kormányzati hozzáférés gyakran titkos megfigyelési intézkedéseket is magában foglal, ami azt jelenti, hogy a megfigyelés tárgya, vagyis az érintett, nincs tudatában adatai kezelésének. Ezért „elvben az érintettnek kevés lehetősége van arra, hogy bírósághoz forduljon, kivéve, ha tájékoztatják a tudomása nélkül hozott intézkedésekről, és ebből következően visszamenőlegesen vitatni tudja azok jogszerűségét, illetve egy másik esetben, ha az a személy, aki gyanítja, hogy közléseit lehallgatják vagy lehallgatták, bírósághoz fordulhat úgy, hogy a bíróság hatásköre nem a lehallgatott arról való értesítésétől függ, hogy közléseit lehallgatták”⁷⁰. Ebben az összefüggésben és ezzel összhangban az Európai Adatvédelmi Testület már sokszor kifejezte aggodalmát a megfigyelési ügyekben biztosított jogorvoslat hatékonyságát illetően. Hangsúlyozza, hogy a kormányzati intézkedések titkossága nem eredményezheti azt, hogy az ilyen intézkedések gyakorlatilag megtámadhatatlanok. Mindezek alapján az általános értékelés keretében azt is vizsgálni kell, hogy az értesítésre vonatkozó követelmény hiánya a külföldi állampolgárok közötti közlések esetében hatással van-e az adatvédelem határozattervezetben megállapított szintjére, különös tekintettel a koreai jog alapján biztosított felügyeleti és jogorvoslati mechanizmusokra (lásd a 4.7. és 4.8. szakaszokat).

⁶⁶ Lásd a határozattervezet (192) preambulumbekendését.

⁶⁷ Lásd a II. melléklet 244. lábjegyzetét, amely szerint a Korea-ellenes tevékenység fogalma a nemzet létét és biztonságát, a demokratikus rendet vagy a nép fennmaradását és szabadságát fenyegető tevékenységekre utal.

⁶⁸ Lásd a határozattervezet (187) preambulumbekendését.

⁶⁹ Az EUB 2020. október 6-i *La Quadrature du Net és társai* ítélete, C-511/18, C-512/18 és C-520/18 egyesített ügyek, ECLI:EU:C:2020:791, 190. bekezdés.

⁷⁰ Az EJEB 2021. május 25-i *Big Brother Watch és társai kontra Egyesült Királyság* ítélete, ECLI:CE:ECHR:2021:0525JUD005817013, 337. bekezdés és az EJEB 2015. december 4-i *Roman Zakharov kontra Oroszország* ítélete, ECLI:CE:ECHR:2015:1204JUD004714306, 234. bekezdés.

148. Az Európai Adatvédelmi Testület ebben az összefüggésben megjegyzi még azt is, hogy a törvény elég tág fogalmakra, például Korea-ellenes vagy nemzetellenes tevékenységekre⁷¹ utal, és nehéz előre meghatározni, hogy ezeket a fogalmakat hogyan értelmezik a koreai jog alapján. Ezért felkéri az Európai Bizottságot annak figyelemmel kísérésére, hogy ezeket a fogalmakat hogyan töltik meg tartalommal a koreai jogban, és hogy a gyakorlati alkalmazásuk megfelel-e az arányosság uniós jogból következő követelményeinek.

4.3.2. A külföldi állampolgárok közötti közlésekre vonatkozó adatgyűjtés előzetes független engedélyezésének a hiánya

149. Az EGT-állampolgárok nem koreai állampolgárok közötti (és a fent említett esetek valamelyikébe tartozó) közlésekből származó személyes adatainak a gyűjtéséhez nem szükséges egy független szerv előzetes engedélye azokban az esetekben, amikor az így gyűjtött adatokat nemzetbiztonsági célokból kezelik Koreában (ellentétben azokkal az esetekkel, amikor az érintett természetes személyek közül legalább egy koreai állampolgár)⁷².
150. Különös tekintettel az Emberi Jogok Európai Bíróságának (EJEB) nemrégiben hozott „Big Brother Watch és társai kontra Egyesült Királyság” és „Centrum för Rättvisa kontra Svédország” ítéleteire, az Európai Adatvédelmi Testület szükségesnek tartja annak vizsgálatát, hogy ezt vajon a koreai adatvédelmi keret súlyos hiányosságának kell-e tekinteni. Ezzel kapcsolatban emlékeztet arra, hogy amint azt a megfigyelési intézkedésekre vonatkozó alapvető európai garanciáról szóló frissített ajánlásában hangsúlyozta⁷³, az Európai Unióról szóló szerződés 6. cikkének (3) bekezdése szerint az EJEE által biztosított alapvető jogok az uniós jogrend részét képezik mint annak általános elvei. Az EUB azonban ítélezési gyakorlatában emlékeztet arra, hogy ez az egyezmény nem minősül az uniós jogrendbe szervesen beépülő jogforrásnak addig, amíg az Unió nem csatlakozott hozzá⁷⁴. Tehát az alapvető jogok védelmének GDPR 45. cikkében előírt szintjét a GDPR rendelkezései alapján kell meghatározni, a Chartában rögzített alapvető jogok fényében értelmezve e rendelkezéseket. Ezt követően, a Charta 52. cikkének (3) bekezdése szerint amennyiben a Charta olyan

jogokat tartalmaz, amelyek megfelelnek az EJEE-ben biztosított jogoknak, akkor e jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az említett egyezményben szerepelnek. Ebből következően az EJEB Charta által is előírt jogokra vonatkozó ítélezési gyakorlatát a Chartában szereplő megfelelő jogok értelmezése során minimális védelmi szintként kell figyelembe venni, amennyiben a Charta az EUB értelmezése szerint nem nyújt magasabb szintű védelmet⁷⁵.

151. Az Európai Adatvédelmi Testület megjegyzi, hogy bár a megfigyelési intézkedések előzetes (független) engedélyezése fontos garanciát jelent az önkénnyel szemben, az EUB ítélezési gyakorlatából nem vezethető le az, hogy az ilyen engedély feltétlen követelmény a megfigyelési intézkedések arányosságának a biztosításához. Az EJEB azonban már kifejezetten is megfogalmazta az előzetes független engedélyezés követelményét a tömeges lehallgatással kapcsolatban⁷⁶. Bár a

⁷¹ Az Európai Bizottság elmagyarázta, hogy a koreai kormánytól kapott magyarázatok szerint ez „a nemzet létét és biztonságát, a demokratikus rendet vagy a nép fennmaradását és szabadságát fenyegető tevékenységekre” utal, lásd még a megfelelőségi határozattervezet 319. lábjegyzetét.

⁷² Lásd a határozattervezet (190) preambulumbekendését.

⁷³ Lásd az Európai Adatvédelmi Testület 2020. november 10-én elfogadott, a megfigyelési intézkedésekre vonatkozó alapvető európai garanciáról szóló 02/2020. számú ajánlásának 10-11. bekezdéseit.

⁷⁴ Lásd az EUB 2020. július 16-i *Adatvédelmi biztos kontra Facebook Ireland Ltd. és Maximilian Schrems* ítélete, C-311/18, ECLI:EU:C:2020:559 (a továbbiakban: *Schrems II* ítélet), 98. bekezdés.

⁷⁵ Lásd az EUB 2020. október 6-i *La Quadrature du Net és társai* ítélete, C-511/18, C-512/18 és C-520/18 egyesített ügyek, 124. bekezdés.

⁷⁶ Lásd az EJEB 2021. május 25-i *Big Brother Watch és társai kontra Egyesült Királyság* ítélete, ECLI:CE:ECHR:2021:0525JUD005817013, 351. bekezdés: „A tömeges lehallgatást a megkezdése előtti független

határozattervezetben ez így kifejezetten nem szerepel, az Európai Adatvédelmi Testület úgy értelmezi, hogy a Koreai Köztársaság jogi kerete csak a távközlés célzott lehallgatását teszi lehetővé, nem pedig a tömeges lehallgatást⁷⁷. Ezt az értelmezést az Európai Bizottság megerősítette.

152. Mindezek alapján az EJB fent említett, az EUB ítélkezési gyakorlatával összhangban álló ítéletei⁷⁸ és az EJB korábbi ítélkezési gyakorlata⁷⁹ is a független felügyeleti hatóságok általi átfogó felügyelet fontosságát jelzik. Az Európai Adatvédelmi Testület hangsúlyozza, hogy a független felügyelet a bűnüldözési és nemzetbiztonsági célú kormányzati hozzáférés folyamatának minden szintjén fontos garancia az önkényes megfigyelési intézkedésekkel szemben, és ennél fogva ahhoz, hogy az adatvédelmi szint megfelelősége megállapítható legyen. A felügyeleti hatóságok Charta 8. cikkének (3) bekezdésében előírt függetlenségére vonatkozó garancia célja, hogy biztosítsa a természetes személyeknek a személyes adatok kezelése tekintetében való védelmére vonatkozó szabályok betartásának a hatékony és megbízható ellenőrzését. Ez különösen azokra az esetekre vonatkozik, amikor a megfigyelés titkos jellegéből adódóan az egyénnek nincs lehetősége arra, hogy a megfigyelési intézkedés végrehajtása előtt vagy közben jogorvoslatot keressen, vagy bármilyen jogorvoslati eljárásban közvetlenül részt vegyen.
153. Az előzetes független engedélyezés hiánya önmagában nem tekinthető a koreai jog lényeges hiányosságának az alapvetően azonos szintű adatvédelem megállapítása szempontjából. A megfelelőség értékeléséhez ebben az esetben is minden körülményt figyelembe kell venni, különös tekintettel az utólagos felügyelet és a koreai jogi keretben biztosított jogorvoslati lehetőségek hatékonyságára (lásd még a 4.7. és 4.8. szakaszokat).

4.4. Önkéntes adatközlés

154. A távközlési vállalkozásokról szóló törvény 83. cikkének (3) bekezdése szerint a távközlési szolgáltatók kérésre önkéntesen átadhatják az úgynevezett „előfizetői adatokat”⁸⁰ a nemzetbiztonsági és bűnüldöző hatóságoknak. Az Európai Adatvédelmi Testület elismeri, hogy az EGT-ből Koreába továbbított személyes adatok esetében ez ritkán fordul elő, de az adatvédelmi szint értékelése során a korábban már említetteknek megfelelően figyelembe kell venni.
155. Az Európai Adatvédelmi Testület értelmezése szerint az adatvédelmi törvény által biztosított garanciák ezekre az esetekre is vonatkoznak, vagyis a közhatalmi szerveknek és a távközlési szolgáltatóknak is be kell tartaniuk a vonatkozó előírásokat⁸¹, és az érintettek jogainak és szabadságainak megsértése esetén felelősségre vonhatók⁸². Továbbá, ezen értelmezés szerint, a távközlési szolgáltatók nem kötelesek az adatközlésre vonatkozó felhívást teljesíteni.

engedélyezéshez kell kötni”, „a tömeges lehallgatást egy független szervnek, vagyis a végrehajtó hatalomtól független szervnek kell engedélyeznie”.

⁷⁷ Csak a II. melléklet 3.2. szakasza tartalmaz kifejezetten a nemzetbiztonsági célokra vonatkozó megállapítást, amely szerint a korlátozásoknak és a garanciáknak *„biztosítaniuk kell, hogy az adatok gyűjtése és kezelése a jogos cél eléréséhez feltétlenül szükséges mértékre korlátozódik. Ez kizárja a személyes adatok nemzetbiztonsági célokból történő tömeges és különbségtétel nélküli gyűjtését.”*

⁷⁸ Lásd például az EUB *Tele2 Sverige AB és társai* ítélete, C-203/15 és C-698/15 egyesített ügyek, ECLI:EU:C:2016:970.

⁷⁹ Lásd például az EJB 2015. december 4-i *Roman Zakharov kontra Oroszország* ítélete, ECLI:CE:ECHR:2015:1204JUD004714306.

⁸⁰ Az érintett adathalmazok a következők: a felhasználók neve, lakossági nyilvántartási száma, címe és telefonszáma, az előfizetés vagy az előfizetés lemondásának időpontja, valamint a felhasználói azonosító kódok (amelyek a számítógépes rendszerek vagy kommunikációs hálózatok használatára való jogosultsággal rendelkezők azonosítására szolgálnak).

⁸¹ Lásd a határozattervezet (164) és (169) preambulumbekzdését.

⁸² Lásd a határozattervezet (166) preambulumbekzdését.

156. Mindazonáltal a nemzeti hatóságok előfizetői adatokhoz való bűnüldözési és különösen nemzetbiztonsági célú hozzáférése a távközlési szolgáltatók általi „önkéntes adatközlés” révén aggályos, mert növeli az érintettek jogait és szabadságait érintő kockázatokat, elsősorban a tájékoztatáshoz való joguk tekintetében.
157. Az adatvédelmi törvény 58. cikke (1) bekezdésének 2. pontja szerint a III-VII. fejezetek rendelkezései nem alkalmazandók abban az esetben, ha a személyes adatok közlését a nemzetbiztonsággal kapcsolatos célokból kérik. Így például az adatvédelmi törvény 18. cikke (a személyes adatok céltól eltérő felhasználása és szolgáltatása) és 20. cikke (a harmadik féltől származó személyes adatok forrásaira, stb. vonatkozó tájékoztatás) sem vonatkozik az ilyen adatkérésekre. A nemzetbiztonsági hatóság adatközlésre vonatkozó felhívása kapcsán egyrészt felmerül az a kérdés, hogy ilyenkor az adatvédelmi törvény 58. cikke (1) bekezdésének 2. pontja a távközlési szolgáltatókat is kizárja-e az adatvédelmi törvény alkalmazása alól. Másrészt az a kérdés merül fel, hogy ezekben az esetekben az adatvédelmi törvény 20. cikkének az alkalmazása alóli kizárás vajon az I. melléklet 3. szakaszában szereplő idevágó rendelkezésre is vonatkozik-e (Tájékoztatás arról, hogy a személyes adatokat nem az érintettől szerezték be (a törvény 20. cikke)). Ha ez így lenne, és az 58. cikk (1) bekezdésének 2. pontja a távközlési szolgáltatókra is vonatkozna, akkor ugyanis a rendelkezésre álló információk alapján fennállna a kockázata annak, hogy nincs olyan jogi kötelezettség, amely az érintettek önkéntes adatközléséről való tájékoztatását előírná.
158. Az Európai Adatvédelmi Testület ezért aggodalmát fejezi ki amiatt, hogy a tájékoztatási követelmények veszíthetnek hatékonyságukból, ami jelentős mértékben megnehezítheti az érintettek számára adatvédelmi jogaik érvényesítését, különösen a bírósági jogorvoslati lehetőségek vonatkozásában. E tekintetben felkéri az Európai Bizottságot, hogy pontosítsa a vonatkozó rendelkezések hatályát.

4.5. Az adatok további felhasználása

159. A célhoz kötöttség elve az adatvédelem egyik alapvető jogi követelményét fogalmazza meg. Megköveteli, hogy a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Emellett az uniós jog megengedi a közhatalmi szervek számára a személyes adatok bűncselekmények megelőzése, nyomozása vagy vádeljárás lefolytatása céljából végzett kezelését akkor is, ha az adatokat eredetileg más célra szerezték be, ha ezek a hatóságok a vonatkozó jog alapján jogalappal rendelkeznek az ilyen adatok kezelésére, és a további adatkezelés nem aránytalan.⁸³
160. Ennek megfelelően az Európai Adatvédelmi Testület megállapítja, hogy a bűnüldözési és nemzetbiztonsági célokból gyűjtött adatok további felhasználására vonatkozóan a koreai adatvédelmi keret hasonló garanciákat és korlátozásokat határoz meg, mint az uniós jog. A célhoz kötöttség elvét például az adatvédelmi törvény 3. cikkének (1)-(2) bekezdései tartalmazzák.

4.6. Újbóli továbbítás és a hírszerzési adatok megosztása

161. A GDPR 44. cikke szerint a személyes adatok továbbítására vagy újbóli továbbítására csak akkor kerülhet sor, ha a GDPR-ben garantált védelem szintje nem sérül. Tehát az EGT-ből Koreába továbbított személyes adatok számára biztosított védelem szintje a harmadik országbeli címzettek részére történő újbóli továbbítás során nem sérülhet, vagyis az újbóli továbbítás csak akkor megengedett, ha az uniós jog alapján biztosított védelemmel alapvetően azonos szintű védelem folyamatosan biztosított. Következésképpen annak értékelése során, hogy a harmadik ország megfelelő szintű védelmet biztosít-

⁸³ Lásd a LED 4. cikkének (2) bekezdését.

e, figyelembe kell venni a harmadik ország újbóli továbbításra vonatkozó jogi keretét. Ez nem vitatott, és mind az Európai Bizottság⁸⁴, mind az Európai Adatvédelmi Testület véleményével összhangban áll.

162. Ebben az összefüggésben az Európai Adatvédelmi Testület megállapítja, hogy az EJEB a nemrégiben hozott „Big Brother Watch és társai kontra Egyesült Királyság” és „Centrum för Rättvisa kontra Svédország” ítéleteiben⁸⁵ útmutatást adott arra vonatkozóan, hogy tömeges adatgyűjtés esetén milyen adatvédelmi óvintézkedéseket kell betartani a szerződő államokban a személyes adatok más felekkel történő, bűnüldözési és nemzetbiztonsági célú közlése során: *„Mindenekelőtt a hazai jogban egyértelműen meg kell határozni, hogy milyen körülmények között kerülhet sor ilyen adattovábbításra. Másodsor, a továbbító államnak biztosítania kell azt, hogy az átvevő állam a visszaélés és az aránytalan beavatkozás megakadályozására alkalmas garanciákat alkalmaz az adatkezelés során. Az átvevő államnak garantálnia kell különösen az anyag biztonságos tárolását, és korlátoznia kell annak újbóli közzétételét. [...] Harmadsor, fokozott óvintézkedések szükségesek akkor, ha egyértelmű, hogy a továbbított anyag különösen bizalmas kezelést igényel, például azért, mert bizalmas újságírói anyag”*⁸⁶.
163. E normákat alkalmazva az EJEB a „Centrum för Rättvisa kontra Svédország” ügyben megállapította, hogy az EJE 8. cikke megsértésének minősül az, ha a lehallgatásra vonatkozó szabályok nem tartalmazzák kifejezetten azt a jogi követelményt, hogy a hírszerzési adatok megosztásának szükségességét és arányosságát a magánélet védelméhez való jogra gyakorolt lehetséges hatások szempontjából értékelni kell. Az EJEB bírálta, hogy a törvény általános jellege következtében a lehallgatási anyagot külföldre lehetett küldeni bármikor, amikor úgy vélték, hogy az nemzeti érdeket szolgál, függetlenül attól, hogy a külföldi átvevő biztosítja-e a garanciák minimálisan elfogadható szintjét⁸⁷.
164. Elismerve, hogy Dél-Korea jogi kerete nem teszi lehetővé a tömeges lehallgatást, az Európai Adatvédelmi Testület az EJEB fentiekben ismertetett ítéletéből levonható következtetések fényében mindazonáltal úgy véli, hogy az uniós jog EUB általi értelmezéséből következő követelmények mellett az EJEB érvelését is figyelembe kell venni annak értékelése során, hogy egy harmadik ország újbóli továbbításra vonatkozó jogi kerete vajon megfelelő adatvédelmi normákat ír-e elő.

4.6.1. A bűnüldöző hatóságok általi újbóli továbbításra alkalmazandó jogi keret

165. Az Európai Bizottság magyarázatai alapján az Európai Adatvédelmi Testület úgy értelmezi, hogy a határozattervezet I. mellékletének 2. szakasza – az újbóli továbbítás korlátozása – az illetékes hatóságok által bűnüldözési célokból végzett újbóli továbbításra is alkalmazandó, beleértve azokat az eseteket is, amikor a továbbítás az adatvédelmi törvénytől eltérő jogszabály alapján történik. E szabály szerint *„a külföldön tevékenykedő harmadik félnek való átadás esetén a személyes adatok védelmének koreai adatvédelmi törvény által biztosított szintje sérülhet amiatt, hogy a különböző országok adatvédelmi rendszerei eltérnek. Ennek megfelelően ezt vagy a törvény 17. cikkének (4) bekezdésében említett esetnek kell tekinteni, »ami az érintettnek hátrányt okozhat«, vagy a törvény 18. cikkének (2)*

⁸⁴ Lásd a határozattervezet (84) és azt követő preambulumbekendéseit.

⁸⁵ Az itt következő megállapítások a tömeges lehallgatásra vonatkozó szabályokat érintő *Big Brother Watch és Centrum för Rättvisa* ügyekben születtek. Az anyagok más felekkel való közlése esetén alkalmazandó óvintézkedésekre vonatkozó követelmény már az EJEB célzott lehallgatással összefüggésben kidolgozott követelményei között is szerepelt, és nem került további részletezésre (lásd *Big Brother Watch és társai kontra Egyesült Királyság* ítélet, 335. és 362. bekezdés).

⁸⁶ Az EJEB 2021. május 25-i *Big Brother Watch és társai kontra Egyesült Királyság* ítélete, ECLI:CE:ECHR:2021:0525JUD005817013, 362. bekezdés

⁸⁷ Lásd az EJEB 2021. május 25-i *Centrum för Rättvisa kontra Svédország* ítélete, ECLI:CE:ECHR:2021:0525JUD003525208, 326. bekezdés.

bekezdésében és az ugyanezen törvény végrehajtási rendelete 14. cikkének (2) bekezdésében említett esetnek, »ami az érintett vagy harmadik fél érdekét tisztességtelen módon sérti«. Ezért annak érdekében, hogy az ezekben a rendelkezésekben foglalt követelményeket teljesítsék, a személyes adatkezelőnek és a harmadik félnek jogilag kötelező erejű dokumentumban, például szerződésben kifejezetten rögzítenie kell, hogy a személyes adatok külföldre történő továbbítását követően is biztosítják a törvényben előírtak megfelelő szintű védelmet, az érintett jogainak gyakorlására vonatkozó garanciákat is beleértve»⁸⁸.

166. Az Európai Adatvédelmi Testület üdvözli ezt a rendelkezést, amely – feltételezve e célból a koreai adatvédelmi szint megfelelőségét – biztosítja az uniós jog által az újbóli továbbítás vonatkozásában nyújtottal alapvetően azonos szintű védelem folyamatosságát. A Bizottság megerősítette, hogy az Európai Adatvédelmi Testület értelmezése helyes, vagyis hogy az I. mellékletnek ez a szakasza az illetékes hatóságok által bűnüldözési célokból végzett újbóli továbbítás valamennyi esetére alkalmazandó. Az Európai Adatvédelmi Testület azonban rámutat arra, hogy világossá kell tenni, hogy ez a szabály a védelmi szint gyakorlatban történő folyamatos biztosítását írja elő, mivel bizonytalanság lehet azzal kapcsolatban, hogy milyen szerződéses garanciák és kötelezettségek vagy hasonló mechanizmusok alkalmazhatók az ilyen szintű védelem elérésére a bűnüldözési célokból végzett adatkezelés esetében. E tekintetben meg kellene említeni például azt is, hogy a személyes adatokat csak a harmadik ország megfelelő illetékes hatóságaival lehet megosztani.
167. Visszaulva arra a fentebb megfogalmazott kérdésre, hogy a KOFIU a határozattervezet hatálya alá esik-e, az Európai Adatvédelmi Testület megjegyzi, hogy a kormányzati hozzáférésre vonatkozó hivatalos nyilatkozatban⁸⁹ szereplő magyarázat szerint a pénzmosás és terrorizmus-finanszírozás elleni törvény 8. cikkének (1) bekezdése alapján a KOFIU biztosa az e törvényben meghatározott pénzügyi tranzakciókra vonatkozó adatokat külföldi pénzügyi hírszerző szolgálatoknak átadhatja, amennyiben azt a törvény céljának az eléréséhez szükségesnek tartja⁹⁰. A pénzmosás és terrorizmus-finanszírozás elleni törvény 8. cikke önmagában nem teszi kötelezővé a külföldi ország által nyújtott adatvédelmi garanciák megfelelőségének az ellenőrzését és biztosítását. A II. melléklet e tekintetben nem tartalmaz hivatkozást az I. melléklet új szakaszára. Ezért az Európai Adatvédelmi Testület felszólítja az Európai Bizottságot, hogy pontosítsa az I. melléklet újbóli továbbítás korlátozására vonatkozó szakasza és az újbóli továbbítás pénzmosás és terrorizmus-finanszírozás elleni törvény szerinti jogalapja közötti összefüggést.

4.6.2. A nemzetbiztonsági célokból végzett újbóli továbbításra alkalmazandó jogi keret

168. A határozattervezet semmilyen információt nem tartalmaz a nemzetbiztonság területén végzett újbóli továbbításra vonatkozó jogi keretét illetően. Ezért az Európai Adatvédelmi Testület értelmezése szerint az I. melléklet 2. szakasza – a bűnüldözési célokból végzett újbóli továbbítástól eltérően – a nemzetbiztonsági célokból végzett újbóli továbbításra nem alkalmazandó. Az adatvédelmi törvény 17. és 18. cikkei, amelyek az I. melléklet szóban forgó szakaszának a tárgyát képezik, az adatvédelmi törvény III. fejezetében szerepelnek, amely viszont nem alkalmazandó a személyes adatok nemzetbiztonsági célokból végzett kezelésére (az adatvédelmi törvény 58. cikkének (1) bekezdése).
169. Az Európai Adatvédelmi Testület feltételezése szerint azonban előfordulhat, hogy Koreának nemzetbiztonsági célokból személyes adatokat kell továbbítania külföldi hírszerző szolgálatok számára,

⁸⁸ A határozattervezet I. melléklete, 7. o.

⁸⁹ Lásd a határozattervezet II. mellékletét.

⁹⁰ Lásd a határozattervezet II. mellékletének 2.2.3.2. szakaszát. Bár ilyen átadásra csak azzal a feltétellel kerülhet sor, hogy a külföldi szolgálat az adatközlés céljától eltérő célra, különösen bűnüldözési nyomozás vagy büntetőtárgyalás céljára nem használhatja fel az adatokat (a pénzmosás és terrorizmus-finanszírozás elleni törvény 8. cikkének (2) bekezdése), a külföldi ország kérésére a KOFIU biztosa az igazságügyminiszter előzetes engedélyével hozzájárulhat az adatok bűncselekmények nyomozása vagy tárgyalása céljára való felhasználásához (a törvény 8. cikkének (3) bekezdése).

és ezt meg is teszi, mégpedig a határokon átnyúló nemzetbiztonsági fenyegetések elleni küzdelem terén folytatott együttműködés, külföldi kormányok ilyen fenyegetésekre való figyelmeztetése, vagy az azok azonosításához való segítségkérés céljából.

170. Az Európai Adatvédelmi Testület úgy értelmezte, hogy az Európai Bizottság véleménye szerint a koreai jogban a nemzetbiztonsági célokból végzett újbóli továbbítást kellően szabályozzák az átfogó alkotmányos keretből következő általános garanciák, különösen a szükségesség és arányosság elvei, valamint az adatvédelmi törvényben szabályozott adatvédelmi elvek, például a jogszerű és tisztességes adatkezelés, a célhoz kötöttség, az adattakarékosság, az adatbiztonság és a személyes adatokkal való visszaélést és a helytelen felhasználást akadályozó általános kötelezettségek.
171. Az Európai Adatvédelmi Testület felismeri és elismeri, hogy ezek a kulcsfontosságú (adatvédelmi) elvek általánosan alkalmazandók, de aggodalmának ad hangot amiatt, hogy ezek a garanciák nagyon általános jellegűek, és a jogalapjuk nem utal vagy tér ki arra, hogy a nemzetbiztonsági célokból végzett újbóli továbbításra milyen konkrét körülmények között és feltételek mellett kerülhet sor. Miközben ezek az általános és átfogó elvek széles körben alkalmazandók, felmerül a kérdés, hogy úgy tekinthetők-e, mint amelyek megfelelnek az egyértelmű és pontos szabályok követelményének, és kellően hatékony és érvényesíthető garanciákat biztosítanak. Különösen azokban az esetekben, amikor a személyes adatokhoz való kormányzati hozzáférés és a személyes adatkezelés titkosan történik, és az adatokból levonható következtetések nagy súllyal esnek latba, elengedhetetlenül fontosak a világos és részletes szabályok. Ahhoz, hogy az egyénnek megfelelő védelmet nyújtson, a törvénynek megfelelő egyértelműséggel kell megjelölnie, hogy az illetékes hatóságok milyen mértékű mérlegelési jogkört gyakorolhatnak, és milyen módon. A *Schrems II* ítéletben az EUB emlékeztet arra, hogy a szükségesség és az arányosság elveiből fakadó követelményeknek való megfelelés érdekében az alapvető jogokba való beavatkozást lehetővé tevő jogalaprak magának kell meghatároznia az érintett jog gyakorlásával kapcsolatos korlátozás terjedelmét, és egyértelmű és pontos szabályokat kell tartalmaznia a szóban forgó intézkedés hatálya és alkalmazása tekintetében, valamint minimumkövetelményeket kell előírnia⁹¹. Az Európai Adatvédelmi Testület aggodalmát fejezi ki amiatt, hogy nem elegendő az, ha ezeket a garanciákat általánosan tartalmazza egy magasabb rendű jogszabály, amennyiben a jogalapjuk maga nem határozza meg pontosan például az arányosság fogalmának az alkalmazását.
172. Ezeket az aggodalmakat az EJEB fent említett ítélete is alátámasztja, amelyben a bíróság megállapította, hogy nem összeegyeztethető az EJEE 8. cikkében foglalt, magánélethez való joggal az, ha csak egy általános szabály létezik anélkül, hogy kifejezetten előírnák a szükségesség és arányosság értékelését vagy a magánélet védelmével összefüggő aggályok figyelembe vételét. E tekintetben az Európai Adatvédelmi Testület megjegyzi, hogy a szóban forgó ügyben az adott ország jogában (miként a koreai jogban is) léteztek a szükségesség és arányosság átfogó (alkotmányosan garantált) elvei, például a Charta alapján és az EJEE-hez való csatlakozás révén.
173. Ezért felkéri az Európai Bizottságot, hogy pontosítsa a jogalapot és azt, hogy a hírszerző szolgálatok hogyan, milyen mértékben és milyen konkrét feltételek esetén kötelesek figyelembe venni a magánélet védelmével összefüggő aggályokat és az adatvédelmi garanciákat azt megelőzően, hogy személyes adatokat nemzetbiztonsági célokból külföldi partnereknek átadnának. Amennyiben a kötelezettség közvetlenül az alkotmányos elvekből származik, az Európai Bizottságnak azt is értékelnie kell, hogy a vonatkozó jogszabály megfelel-e a pontosság és egyértelműség követelményeinek, és meg kell erősítenie az általános alkotmányos és adatvédelmi elvek megfelelő alkalmazását és végrehajtását.

4.6.3. Nemzetközi megállapodások

174. Az Európai Adatvédelmi Testület megállapítja, hogy a megfelelés értékelése során az Európai Bizottság nem vette figyelembe, hogy létezhetnek olyan, Korea és harmadik országok, illetve

⁹¹ Lásd *Schrems II* ítélet, 175. és 180. bekezdés.

nemzetközi szervezetek között létrejött nemzetközi megállapodások, amelyek a személyes adatok bűnüldöző és/vagy hírszerző szolgálatok általi, harmadik országok felé történő nemzetközi továbbítására vonatkozó külön rendelkezéseket tartalmazhatnak. Úgy véli, hogy a bűnüldözési vagy hírszerzési együttműködés céljából harmadik országokkal kötött két- vagy többoldalú megállapodások hatással lehetnek Korea adatvédelemre vonatkozó jogi keretének az értékelésére.

175. Az Európai Adatvédelmi Testület ezért felkéri az Európai Bizottságot, hogy tisztázza, vajon léteznek-e, illetve milyen feltételekkel köthetők ilyen megállapodások, valamint értékelje, hogy a nemzetközi megállapodások rendelkezései befolyásolhatják-e az EGT-ből Koreába továbbított személyes adatok védelmének a koreai jogszabályi keret által biztosított szintjét és a bűnüldözési és nemzetbiztonsági célokat szolgáló, külföldre történő adattovábbítás gyakorlatát.

4.7. Felügyelet

176. Az Európai Adatvédelmi Testület megállapítja, hogy a bűnüldöző és nemzetbiztonsági hatóságok felügyeletét különböző belső és külső szervek együttese biztosítja.
177. Ezzel kapcsolatban meg kell jegyezni, hogy az EUB többször hangsúlyozta a független felügyeletnek – mint a természetes személyek személyes adataik kezelésével összefüggő védelme elengedhetetlen összetevőjének – a szükségességét. A függetlenség fogalma az intézményi autonómia, az utasításmentesség és az anyagi függetlenség területeit foglalja magában. Az adatvédelmi jogszabályok következetes figyelemmel kísérése és betartatása érdekében a felügyeleti hatóságokat tényleges hatáskörökkel kell felruházni, a korrekciós és jogorvoslati hatásköröket is beleértve.
178. Az Európai Adatvédelmi Testület egyetért az Európai Bizottság következtetésével, hogy Korea felügyeleti rendszere összességében értékelve függetlennek és hatékonynak tekinthető, jóllehet a felügyeleti rendszer több tagja önmagában véve nem felel meg a fenti követelményeknek. Többségük nem rendelkezik például végrehajtói hatáskörrel, és csak ajánlásokat adhat ki – ilyen például a Nemzeti Emberi Jogi Bizottság vagy az Ellenőrzési és Vizsgálati Testület. A rendszerhez tartozó közintézmények többsége nem kizárólag adatvédelmi intézmény, hanem általában más feladatokat is ellát az alapvető jogok védelme területén.
179. Az Európai Bizottság magyarázatai alapján azonban az Európai Adatvédelmi Testület arra a megállapításra jutott, hogy a bűnüldöző hatóságok felügyeletét kivétel nélkül az Adatvédelmi Bizottság biztosítja. Ezért az Adatvédelmi Bizottság az adatvédelmi törvény és a bűnüldöző és nemzetbiztonsági hatóságok személyes adatokhoz való hozzáféréseinek teljes területét lefedő más adatvédelmi jogszabályok (pl. a hírközlési adatvédelmi törvény) alapján vizsgálati, jogorvoslati és végrehajtási hatáskörrel is rendelkezik.
180. Ebben az összefüggésben az Európai Adatvédelmi Testület szeretné ismét hangsúlyozni, hogy a felügyeleti hatóságok számára elegendő emberi, műszaki és pénzügyi erőforrást kell biztosítani feladataik ellátásához és hatásköreik gyakorlásához. E tekintetben sajnos semmilyen információ nem áll rendelkezésre a kijelölt felügyeleti hatóságokról, különösen az Adatvédelmi Bizottságról. Ezért az Európai Adatvédelmi Testület megismétli azt a kérését, hogy az Európai Bizottság nyújtson további felvilágosítást ebben a kérdésben.
181. Az Európai Adatvédelmi Testület szeretné általánosságban megjegyezni, hogy a határozattervezet szinte egyáltalán nem tartalmaz arra vonatkozó kijelentést, példát vagy számadatot, hogy a bűnüldözés és a nemzetbiztonság területén milyen felügyeleti tevékenységeket folytatnak, és milyen jogi eszközökkel biztosítják az adatvédelmi jogszabályok betartását a felügyeleti szervek. Ezek hasznosak lennének a felügyeleti szervek hatékonyságának az értékeléséhez.

4.8. Bírósági jogorvoslat

182. Az Európai Adatvédelmi Testület emlékeztet arra, hogy a megfelelő szintű adatvédelemhez elengedhetetlen az, hogy az érintettek széles körű jogorvoslati lehetőségeket vehessenek igénybe az adataikhoz való jogosulatlan hozzáférés vagy az adataik jogosulatlan kezelése esetén. Ezeknek a jogorvoslati lehetőségeknek biztosítaniuk kell az érintettnek azt, hogy a róla tárolt adatokba betekinthessen, és azok helyesbítését vagy törlését kérhesse.
183. Az EUB *Schrems I* és *Schrems II* ítéletei fényében egyértelmű, hogy az illetékes hatóságokhoz való fordulás joga mellett a Charta 47. cikkének (1) bekezdése szerinti hatékony bírói jogvédelem is alapvető fontosságú ahhoz, hogy egy harmadik ország jogának a megfelelése feltételezhető legyen.
184. Az Európai Adatvédelmi Testület elismeri, hogy Korea különféle lehetőségeket teremtett a természetes személyek adatvédelmi törvény szerinti hozzáférési, adatmegőrzési, helyesbítési és felfüggesztési jogainak az érvényesítésére. Ezek a jogok érvényesíthetők magával az adatkezelővel szemben, vagy az Adatvédelmi Bizottsághoz vagy más felügyeleti szervhez, például a Nemzeti Emberi Jogi Bizottsághoz benyújtott panasz útján. Az Európai Adatvédelmi Testület elismeri továbbá, hogy az adatkezelők vagy a közhatalmi szervek kérésükre válaszul hozott döntése a közigazgatási peres eljárásról szóló törvény alapján megtámadható.
185. Emellett az Európai Bizottság által adott magyarázatok alapján az Európai Adatvédelmi Testület úgy értelmezi, hogy a bűnüldöző és nemzetbiztonsági hatóságok intézkedéseit az érintettek a közigazgatási peres eljárásról szóló törvény és az alkotmánybíróságról szóló törvény alapján az illetékes bíróság előtt kifogásolhatják, és az állami kártalanításról szóló törvény alapján kártérítést igényelhetnek⁹².
186. Ennek kapcsán azonban az Európai Adatvédelmi Testület aggodalmát fejezi ki amiatt, hogy az uniós állampolgárok mennyire hatékony jogorvoslatot juthatnak olyan nemzetbiztonsági ügyekben, amelyekben koreai állampolgár nem érintett. Ahogy a 33. és az azt követő bekezdésekben szerepel, a nemzetbiztonsági hatóságoknak nem kell értesíteniük az érintetteket személyes adataik gyűjtéséről és kezeléséről. Mivel ezekben az esetekben jóval nehezebb a hatékony jogvédelmet biztosítani, az Európai Adatvédelmi Testület szeretne rámutatni, hogy az EGT-ből továbbított adatokat érintő ilyen esetekben bizonyos jogi garanciákat kell nyújtani. Ezeknek a garanciáknak lehetővé kell tenniük az érintettek számára, hogy a jogellenes adatkezelés ellen hatékonyan és jogilag biztonságos módon fellépjenek anélkül, hogy túlságosan korlátozó eljárási követelményekbe ütköznenek, például az érintettre hárulna a tudta nélkül folytatott adatkezelés bizonyításának a terhe. Biztosítani kell továbbá, hogy az érintettek olyan illetékes szervhez fordulhassanak, amely megfelel az Alapjogi Charta 47. cikkében foglalt előírásoknak, azaz hatáskörrel rendelkezik ahhoz, hogy megállapítsa az adatkezelés tényét, ellenőrizze az adatkezelés jogszerűségét, és jogellenes adatkezelés esetén jogorvoslatot biztosítson. Mindezek alapján nem lenne elegendő például pusztán a Nemzeti Emberi Jogi Bizottságnál történő panasztételhez való jogot biztosítani. Az Európai Adatvédelmi Testület ezért felszólítja az Európai Bizottságot arra, hogy adjon részletesebb magyarázatot ezeknek a követelményeknek az eljárási és tartalmi szempontból történő teljesítését illetően, például arra vonatkozóan, hogy az érintettek fordulhatnak-e az Adatvédelmi Bizottsághoz vagy bírósághoz anélkül, hogy bizonyítaniuk kellene az adatkezelés tényét.
187. Emellett az Európai Adatvédelmi Testület megállapítja, hogy a határozattervezet lehetővé teszi a panaszok illetékes hatósághoz történő továbbítását, vagyis azt, hogy az uniós állampolgárok a saját országuk nemzeti adatvédelmi hatóságán vagy az Európai Adatvédelmi Testületen keresztül is nyújtsanak be panaszt az Adatvédelmi Bizottsághoz. A vizsgálat lezárását követően az Adatvédelmi Bizottság ugyanazon a csatornán keresztül értesíti a panasztevőt, mint amelyen keresztül a panaszt benyújtották⁹³. Az Európai Adatvédelmi Testület üdvözlö a koreai nemzetbiztonsági hatóságokkal

⁹² Lásd a II. melléklet 3.2.4. pontját annak 2.4.3. pontjával együttesen értelmezve.

⁹³ Lásd a határozattervezet (205) preambulumbekzdését és I. mellékletének 19. oldalát.

szembeni jogorvoslathoz való hozzáférés megkönnyítését célzó törekvést. Ugyanakkor azt javasolja, hogy az illetékes hatósághoz továbbítandó panaszokat inkább az állampolgárokhoz közelebb álló, panaszkezelésben illetékes európai nemzeti adatvédelmi hatóságokhoz nyújtsák be, és ne az Európai Adatvédelmi Testülethez.

188. Az önkéntes adatközlés kapcsán az Európai Adatvédelmi Testület felhívja a figyelmet egy lehetséges ellentmondásra. A határozattervezet egyrészt azt állítja, hogy adataik önkéntes adatközlésre vonatkozó felhívást követő jogellenes közlése esetén az érintettek jogorvoslattal élhetnek, többek között az adatközlésre vonatkozó felhívást kiadó bűnüldöző hatósággal szemben⁹⁴. Másrészt a közhatalmi szervek intézkedései elleni kifogás joga kapcsán a határozattervezet utal a közvetlen hatás követelményére, és a magánélethez való jogra közvetlen hatást gyakorló közigazgatási intézkedés (egyedüli) példaként az adatközlésre vonatkozó kötelező erejű felhívásokat említi⁹⁵. Az Európai Bizottságtól kapott magyarázatok alapján az Európai Adatvédelmi Testület úgy értelmezi, hogy az önkéntes adatközléssel szembeni jogorvoslati lehetőségek gyakorlása valójában nem korlátozott, és ezért arra kéri az Európai Bizottságot, hogy ezt mind a bűnüldözés, mind a nemzetbiztonság területére vonatkozóan pontosítsa a határozatban (a bűnüldözés területét érintő résszel szemben a nemzetbiztonsági célokból történő önkéntes adatközlésről szóló rész nem foglalkozik kifejezetten az ebben a vonatkozásban nyújtott jogorvoslati lehetőségekkel).

⁹⁴ Lásd a határozattervezet (166) preambulumbekendését.

⁹⁵ Lásd a határozattervezet (181) preambulumbekendését (a bűnüldözés területét illetően) és a (208) és (181) preambulumbekendését (a nemzetbiztonság területét illetően).