14/2021. sz. vélemény a személyes adatoknak az Egyesült Királyságban történő megfelelő védelméről szóló, az (EU) 2016/679 rendelet szerinti európai bizottsági végrehajtási határozat tervezetéről

Elfogadás időpontja: 2021. április 13.

TARTALOM

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 (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének e) pontjára,

tekintettel az Európai Gazdasági Térségről (a továbbiakban „EGT") szóló Megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére[1],

tekintettel eljárási szabályzatának 12. és 22. cikkére,

A KÖVETKEZŐ VÉLEMÉNYT FOGADTA EL:

1. VEZETŐI ÖSSZEFOGLALÓ

1. Az Európai Bizottság 2021. február 19-én az általános adatvédelmi rendelet szerint jóváhagyta a személyes adatok Egyesült Királyság által biztosított megfelelő szintű védelméről szóló végrehajtási határozata tervezetét (a továbbiakban: határozattervezet)[2]. Ezt követően az Európai Bizottság megindította annak hivatalos elfogadási eljárását.

2. Ugyanezen a napon az Európai Bizottság kikérte az Európai Adatvédelmi Testület véleményét[3]. Az Európai Adatvédelmi Testület az Egyesült Királyságban biztosított védelem szintjének megfelelőségét magának a határozattervezetnek a vizsgálata, valamint az Európai Bizottság által rendelkezésre bocsátott dokumentumok elemzése alapján mérte fel.

3. Az Európai Adatvédelmi Testület a határozattervezet általános adatvédelmi rendelet szerinti általános szempontjainak értékelésére, valamint a hatóságoknak az EGT-ből bűnüldözési és nemzetbiztonsági célokból továbbított személyes adatokhoz való hozzáférésére összpontosított, beleértve az EGT-ben az egyének rendelkezésére álló jogorvoslati lehetőségeket is. Az Európai Adatvédelmi Testület azt is értékelte, hogy az Egyesült Királyság jogi kerete biztosít-e garanciákat és azok hatékonyak-e.

4. Az Európai Adatvédelmi Testület e munkához fő hivatkozási alapként az általános adatvédelmi rendeletnek való megfelelésről szóló, 2018 februárjában elfogadott megfelelőségi referenciát[4],

[1] Az e véleményben a „tagállamokra" való hivatkozásokat az „EGT-tagállamokra" való hivatkozásként kell értelmezni.
[2] Lásd az Európai Bizottság sajtóközleményét, Adatvédelem: az Európai Bizottság elindítja a személyes adatok Egyesült Királyságba történő áramlását biztosító folyamatot, 2021. február 19., https://ec.europa.eu/commission/presscorner/detail/hu/ip_21_661
[3] Ugyanott.
[4] Lásd: 29. cikk szerinti munkacsoport – Megfelelőségi referencia, elfogadás időpontja: 2017. november 28., a legutóbbi felülvizsgálat és elfogadás időpontja: 2018. február 6., WP 254 rev.01 (az Európai Adatvédelmi Testület által jóváhagyva, lásd: https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (a továbbiakban: *az általános adatvédelmi rendelettel kapcsolatos megfelelőségi referencia*).

valamint az EPDB-nek a megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról szóló 02/2020. sz. ajánlását[5] használta fel.

[5] Az Európai Adatvédelmi Testület 2020. november 10-én elfogadott 02/2020 ajánlása a megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_hu

1.1. A konvergencia területei

5. Az Európai Adatvédelmi Testület fő célja, hogy véleményt adjon az Európai Bizottságnak az Egyesült Királyságban az egyéneknek nyújtott védelem szintjének megfelelőségéről. Fontos annak felismerése, hogy az Európai Adatvédelmi Testület nem várja el, hogy az egyesült királyságbeli jogi keret reprodukálja az európai adatvédelmi jogot.

6. Az Európai Adatvédelmi Testület azonban emlékeztet arra, hogy ahhoz, hogy a harmadik ország jogszabályai az általános adatvédelmi rendelet 45. cikke és az Európai Unió Bíróságának (a továbbiakban: EUB) ítélkezési gyakorlata szerinti megfelelő adatvédelmi szintet nyújtónak minősüljenek, azoknak igazodniuk kell az általános adatvédelmi rendeletben foglalt alapelvek lényegéhez. Az Egyesült Királyság adatvédelmi kerete nagyrészt az uniós adatvédelmi kereten alapul (különösen az általános adatvédelmi rendeleten és az (EU) 2016/680 európai parlamenti és tanácsi irányelven, a továbbiakban: a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv), amely abból ered, hogy az Egyesült Királyság 2020. január 31-ig az EU tagállama volt. Ezen túlmenően a 2018. május 23-án hatályba lépett és az Egyesült Királyság 1998. évi adatvédelmi törvényét hatályon kívül helyező 2018. évi adatvédelmi törvény tovább pontosítja az általános adatvédelmi rendeletnek az Egyesült Királyság jogában történő alkalmazását, valamint átülteti az uniós bűnüldözési irányelvet, továbbá meghatározza a nemzeti adatvédelmi felügyeleti hatóság, az Egyesült Királyság Információs Biztosa Hivatalának jogköreit és kötelezettségeit (a továbbiakban az „Információs Biztos Hivatala”). Az Európai Adatvédelmi Testület ezért elismeri, hogy az Egyesült Királyság adatvédelmi keretrendszerében nagyrészt tükrözi az általános adatvédelmi rendeletet.

7. **Egy olyan harmadik ország jogának és gyakorlatának elemzésekor, amely a közelmúltig az EU tagállama volt, nyilvánvaló, hogy az Európai Adatvédelmi Testület számos szempontot lényegében megegyezőnek minősített.**

8. Az Európai Adatvédelmi Testület megjegyzi, hogy az adatvédelem területén az általános adatvédelmi rendeletre vonatkozó keret és az Egyesült Királyság jogi kerete szorosan igazodik egymáshoz bizonyos alapvető rendelkezések terén, ilyenek például a fogalmak (pl. „személyes adatok”; „a személyes adatok kezelése”; „adatkezelő”); a jogos célokból végzett jogszerű és tisztességes adatkezelés indokai; a célhoz kötöttség; az adatminőség és az arányosság elve; az adatmegőrzés, -biztonság és titoktartás; az átláthatóság; a különleges adatkategóriák; a közvetlen üzletszerzés; az automatizált döntéshozatal és a profilalkotás.

1.2. Kihívások

9. Az Egyesült Királyság egészen a közelmúltig az EU tagállama volt; ezért az Európai Adatvédelmi Testület a törvényeinek és gyakorlatának elemzésekor számos szempontot lényegében megegyezőnek minősített. Ugyanakkor a megfelelőségi megállapítás elfogadásának folyamatában betöltött szerepére, valamint az időbeli korlátokra tekintettel az Európai Adatvédelmi Testület úgy határozott, hogy figyelmét azokra a szempontokra összpontosítja, amelyek esetében úgy véli, hogy alaposabb és részletesebb vizsgálatra van szükség.

10. Továbbra is fennállnak ugyanis kihívások, és az Európai Adatvédelmi Testület úgy véli, hogy az alábbi pontokat alaposabban kell értékelni annak biztosítása érdekében, hogy a védelem lényegében megegyező szintje teljesüljön, és az Európai Bizottságnak szorosan figyelemmel kell kísérnie ezeket az Egyesült Királyságban.

1.2.1. Általános jellemzés

11. Az első, általános jellegű kihívás az Egyesült Királyság adatvédelmi jogrendszere egészének nyomon követéséhez kapcsolódik. Az Egyesült Királyság kormánya kinyilvánította azon szándékát, hogy különálló és független adatvédelmi politikákat dolgozzon ki, az uniós adatvédelmi jogtól való eltérés lehetőségével. Az ilyen vonatkozású politikai nyilatkozatokat még nem juttatták kifejezésre az Egyesült Királyság jogi keretében. Ez az **esetleges jövőbeli eltérés azonban kockázatot jelenthet az EU-ból továbbított személyes adatok védelmi szintjének fenntartására nézve**. **Ezért felkérjük az Európai Bizottságot, hogy kísérje szoros figyelemmel ezeket a fejleményeket a megfelelőségi határozatának hatálybalépésétől kezdődően, és tegye meg a szükséges intézkedéseket, beleértve a határozat szükség szerinti módosítását és/vagy felfüggesztését.**

1.2.2. Általános adatvédelmi szempontok

12. Először is a **2018. évi adatvédelmi törvény 2. melléklete 1. részének (4) bekezdésében** foglalt úgynevezett **„bevándorlási mentesség”** megfogalmazása **„széles körű”**. Nevezetesen akkor is alkalmazandó, ha a személyes adatokat nem a bevándorlás ellenőrzése céljából gyűjti az adatkezelő, hanem egy másik adatkezelő rendelkezésére bocsátja, aki az ilyen személyes adatokat a bevándorlás ellenőrzése céljából kezeli.

13. Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy vizsgálja meg az Open Rights Group & Anor, R (On the Application Of) kontra Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) ügy jelenlegi állását, és mivel ez az ítélet nem jogerős (*res judicata*), ellenőrizze, hogy azt a fellebbviteli ítélet megerősíti vagy felülvizsgálja-e, figyelembe véve az e tekintetben bekövetkezett változásokat, és pontosítva azokat a határozatban. **Az Európai Adatvédelmi Testület arra is felkéri az Európai Bizottságot, hogy megfelelőségi határozatában nyújtson további információkat a bevándorlási mentességről[6], különösen az Egyesült Királyság jogában szereplő, ilyen széles körű mentesség szükségességével és arányosságával kapcsolatban, különös tekintettel a *személyi hatály* széles alkalmazási körére.** Ezzel egyidejűleg az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy vizsgálja meg alaposabban, hogy léteznek vagy elképzelhetők-e további garanciák az Egyesült Királyság jogi keretében, például olyan jogilag kötelező erejű eszközök révén, amelyek kiegészítenék a bevándorlásra vonatkozó mentességet azáltal, hogy növelik annak kiszámíthatóságát és az érintettek számára biztosított garanciákat, lehetővé téve a szükségességi és az arányossági követelmények jobb és gyors értékelését és nyomon követését is.

14. Másodszor, bár az Európai Adatvédelmi Testület elismeri, hogy az Egyesült Királyság adatvédelmi keretrendszerében nagyrészt tükrözi az általános adatvédelmi rendelet V. fejezetét, az Európai Adatvédelmi Testület **a további adattovábbítás tekintetében** azonosította az Egyesült Királyság jogi keretének bizonyos aspektusait, amelyek alááshatják az EGT-ből továbbított személyes adatok védelmének szintjét.

[6] A bevándorlási mentesség alkalmazása folyamatban lévő felülvizsgálatának eredményeként is, amely az Egyesült Királyság kormányának a megfelelőséggel kapcsolatos vitákra vonatkozó magyarázó kerete 2. melléklete E3. szakaszának 5. oldalán szerepel: Korlátozások, 2020. március 13. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

15. Az általános adatvédelmi rendelet 44. cikke[7] ugyanis úgy rendelkezik, hogy személyes adatok továbbítására és újbóli továbbítására csak akkor kerülhet sor, ha az nem veszélyezteti a természetes személyeknek az általános adatvédelmi rendelet által garantált védelmi szintjét. **Ez nemcsak azt jelenti, hogy a jövőbeli megfelelőségi határozat értelmében az Egyesült Királyság jogszabályainak az uniós jogszabályokkal „lényegében megegyezőnek" kell lenniük az Egyesült Királyság részére továbbított személyes adatok kezelése tekintetében, hanem azt is, hogy az Egyesült Királyságban az említett adatok harmadik országokba történő újbóli továbbítására alkalmazandó szabályoknak biztosítaniuk kell, hogy továbbra is lényegében megegyező szintű védelem valósuljon meg.**

16. Bár az Európai Adatvédelmi Testület tudomásul veszi az Egyesült Királyság arra vonatkozó képességét, hogy jogi kerete szerint az Egyesült Királyság adatvédelmi keretére figyelemmel területeket megfelelő szintű adatvédelmet biztosító területként ismerjen el, az Európai Adatvédelmi Testület hangsúlyozni kívánja, hogy e területekre a mai napig nem feltétlenül vonatkozik az Európai Bizottság által kiadott, az EGT-ben biztosított védelemmel „lényegében megegyező" védelmi szintet biztosító megfelelőségi határozat. Ez az EGT-ből továbbított személyes adatok védelme tekintetében esetlegesen kockázatokat eredményezhet, különösen akkor, ha a jövőben az Egyesült Királyság adatvédelmi kerete eltérne az uniós vívmányoktól. Ezen túlmenően az Egyesült Királyság már megfelelőként ismerte el azokat a harmadik országokat, amelyek esetében az Európai Bizottság a 95/46/EK irányelv[8] értelmében megfelelőségi megállapítást tett, míg az Európai Bizottság hamarosan felülvizsgálja ezeket a megállapításokat, és e felülvizsgálat következtetései még nem ismertek.

17. **Ezért az Európai Bizottságnak a fenti helyzetek vonatkozásában be kell töltenie nyomonkövetési szerepét, és amennyiben az EGT-ből továbbított személyes adatok lényegében megegyező szintű védelmét nem tartják fenn, az Európai Bizottságnak fontolóra kell vennie a megfelelőségi határozat EGT-ből továbbított adatokra vonatkozó konkrét garanciák bevezetése és/vagy a megfelelőségi határozat felfüggesztése céljából történő módosítását.**

18. **Az Egyesült Királyság és harmadik országok között létrejött nemzetközi megállapodásokat illetően** felkérjük az Európai Bizottságot, hogy vizsgálja meg az egyrészről Egyesült Királyság adatvédelmi kerete, másrészről pedig az Egyesült Királyság és az Amerikai Egyesült Államok (a továbbiakban: Egyesült Államok) között létrejött, a súlyos bűncselekmények elleni küzdelem céljából az elektronikus adatokhoz való hozzáférésről szóló megállapodáson[9] (a továbbiakban: az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodás) túli nemzetközi kötelezettségvállalásai közötti kölcsönhatást, különösen annak biztosítása érdekében, hogy a személyes adatoknak az Egyesült Királyság megfelelőségi határozata alapján az EU-ból az Egyesült Királyságba történő továbbítása, majd más harmadik országokba történő újbóli továbbítása esetén biztosított legyen a védelem

---

[7] *„Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, e rendelet egyéb rendelkezéseinek betartása mellett, ha az adatkezelő és az adatfeldolgozó teljesíti az e fejezetben rögzített feltételeket. E fejezet valamennyi rendelkezését alkalmazni kell annak biztosítása érdekében, hogy a természetes személyek számára e rendeletben garantált védelem szintje ne sérüljön.*"

[8] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, HL L 281., 1995.11.23., 31. o.

[9] Lásd a Nagy-Britannia és Észak-Írország Egyesült Királyságának kormánya és az Amerikai Egyesült Államok kormánya között az elektronikus adatokhoz a súlyos bűncselekmények elleni küzdelem céljából történő hozzáférésről szóló megállapodást, Washington DC, USA, 2019. október 3., https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019

szintjének folytonossága; továbbá végezzen folyamatos nyomon követést és szükség esetén lépjen fel, amennyiben az Egyesült Királyság és harmadik országok közötti nemzetközi megállapodások megkötése veszélyeztetheti a személyes adatok Unióban garantált védelmi szintjét.

19. Felkérjük továbbá az Európai Bizottságot, hogy kövesse nyomon, hogy az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodás megfelelő kiegészítő garanciákat nyújt-e, figyelembe véve az érintett adatkategóriák érzékenységi szintjét, valamint az elektronikus bizonyítékoknak a szolgáltatók és nem a hatóságok közötti közvetlen továbbítására vonatkozó egyetlen követelményt, továbbá azt is, hogy milyen körülmények között biztosíthatók garanciák az EU-USA adatvédelmi keretmegállapodás[10] módosításainak megfelelő végrehajtása révén.

20. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az **Egyesült Királyság alkalmazandó adatvédelmi jogszabályai szerinti adattovábbítási eszközök alapján** az Egyesült Királyságból egy másik harmadik országba irányuló újbóli adattovábbításra is sor kerülhet[11]. A Schrems II-ügy[12] alapján az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy a megfelelőségi határozatban nyújtson garanciát arra vonatkozóan, hogy a szükséges garanciák ténylegesen bevezetésre kerülnek, figyelembe véve a fogadó harmadik ország jogszabályait is.

21. Ami az **általános adatvédelmi rendelet 48. cikke szerinti védelemnek** az Egyesült Királyság jogszabályaiban fennálló hiányát illeti, az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy nyújtson további garanciákat és az Egyesült Királyság jogszabályaira való konkrét hivatkozásokat, amelyek biztosítják, hogy az Egyesült Királyság jogi keretében biztosított védelem szintje lényegében megegyező az EGT-ben garantált védelmi szinttel.

22. Az **eljárási és végrehajtási mechanizmusok** tekintetében az Európai Adatvédelmi Testület megjegyzi, hogy a független felügyeleti hatóság létezése és hatékony működése, a megfelelés megfelelő szintjét biztosító rendszer megléte, valamint a megfelelő jogorvoslati mechanizmusokhoz való hozzáférés olyan rendszere, amely az EGT-ben az egyéneket felruházza a jogaik gyakorlásához és a jogorvoslathoz szükséges eszközökkel anélkül, hogy a közigazgatási és bírósági jogorvoslatot nehezítő akadályokba ütköznének, kulcsfontosságú elemek, amelyeknek az európai adatvédelmi rendszerekkel összhangban álló rendszereknek rendelkezniük kell.

23. Az Európai Adatvédelmi Testület elismeri, hogy az Egyesült Királyság a legtöbb esetben tükrözi az általános adatvédelmi rendelet vonatkozó rendelkezéseit az Egyesült Királyság általános adatvédelmi rendeletében és a 2018. évi adatvédelmi törvényben; mindenesetre felkérjük az Európai Bizottságot, hogy folyamatosan kísérje figyelemmel az Egyesült Királyság jogi keretének és gyakorlatának minden olyan fejleményét, amely káros hatásokkal járhat ezeken a területeken.

1.2.3. A hatóságoknak az Egyesült Királyságba továbbított adatokhoz való hozzáféréséről

24. Az Európai Adatvédelmi Testület tudomásul veszi a biztonsági és hírszerző ügynökségekre alkalmazandó egyesült királyságbeli jogi keret jelentős változásait, különösen a kommunikációs adatok lehallgatása és megszerzése tekintetében. Az Európai Adatvédelmi Testület megérti, hogy ezek a változások többek között az EUB és az Emberi Jogok Európai Bírósága (a továbbiakban: EJEB)

[10] Lásd az Amerikai Egyesült Államok és az Európai Unió közötti, a bűncselekmények megelőzésével, nyomozásával, felderítésével és a vádeljárás lefolytatásával kapcsolatos személyes adatok védelméről szóló, 2016. decemberi megállapodást (a továbbiakban: az EU-USA keretmegállapodás), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3A3104_8

[11] Lásd az Egyesült Királyság általános adatvédelmi rendeletének 46. és 47. cikkét.

[12] Lásd a Schrems II-ügyet.

előtt indított eljárásokra, valamint az ezzel összefüggésben a közelmúltban hozott ítéletekre adott válasznak minősülnek.

25. Az Európai Adatvédelmi Testület különösen üdvözli, hogy az Egyesült Királyság létrehozta az Investigatory Powers Tribunalt (nyomozati hatáskörrel rendelkező bíróságot) (a továbbiakban: IPT). Az IPT hatásköre nemcsak arra terjed ki, hogy a bűnüldöző hatóságok nyomozati hatáskörének gyakorlásával kapcsolatos ügyekben hozzon ítéletet, hanem a hírszerző szolgálatok hatáskörével kapcsolatban is. Ezért az Európai Adatvédelmi Testület úgy értelmezi, hogy az IPT az Európai Unió Alapjogi Chartájának (a továbbiakban: az Európai Unió Alapjogi Chartája) 47. cikke értelmében megfelelő bíróságként működik.

26. Az Európai Adatvédelmi Testület továbbá pozitívan értékeli, hogy jelentős előrelépésként bevezették az „igazságügyi biztosokat" a nyomozati hatáskörökről szóló 2016. évi törvénybe (a továbbiakban: IPA 2016). Úgy értelmezi, hogy az igazságügyi biztosok fontos feladata, hogy egyedi esetekben előzetesen jóváhagyjanak különböző felügyeleti intézkedéseket, ideértve a kommunikációs adatok célzott lehallgatását és tömeges beszerzését (úgynevezett „kettős zárolási" eljárás).

27. E további felügyeleti szint hatékonyságának értékelése érdekében azonban az Európai Adatvédelmi Testület úgy véli, hogy tovább kell pontosítani azokat a forgatókönyveket, amelyek esetében lehetséges a nyomozati hatáskörrel foglalkozó biztos (a továbbiakban: IPC) vagy az igazságügyi biztosok jóváhagyása nélküli jogszerű lehallgatás, és felkéri az Európai Bizottságot, hogy értékelje alaposabban és bizonyítsa, hogy még ha a kettős zárolási eljárás nem alkalmazandó is, az Egyesült Királyság jogi kerete megfelelő garanciákat ír elő, többek között hatékony utólagos felügyelet és jogorvoslati lehetőségek révén, amelyek az egyének számára az uniós szintű védelemmel lényegében megegyező védelmet biztosítják.

28. Az Európai Adatvédelmi Testület felkéri továbbá az Európai Bizottságot, hogy értékelje alaposabban azokat a feltételeket, amelyek mellett a sürgősségre lehet hivatkozni, és adjon felvilágosítást arról, hogy az érintettek milyen lehetséges módokon gyakorolhatják jogaikat, és milyen jogorvoslati lehetőségek állnak a rendelkezésükre a berendezésekkel végzett beavatkozási műveletekkel összefüggésben, különösen a kettős zárolási eljárástól való eltérés esetén.

29. Emellett az Európai Adatvédelmi Testület úgy véli, hogy a tömeges lehallgatások további tisztázására és értékelésére van szükség, különösen a válogatók kiválasztása és alkalmazása tekintetében annak tisztázása érdekében, hogy a személyes adatokhoz való hozzáférés milyen mértékben éri el az EUB által meghatározott küszöbértéket, és milyen garanciák vannak érvényben az olyan egyének alapvető jogainak védelme érdekében, akiknek az adatait ebben az összefüggésben lefoglalták, többek közt az adatmegőrzési idővel kapcsolatban is. Különösen hasznos lenne az Egyesült Királyság illetékes felügyeleti hatóságainak független értékelése. Az Európai Adatvédelmi Testület azt is hangsúlyozza, hogy annál is inkább kritikusnak tűnik, hogy a tömeges lehallgatási gyakorlatok körébe tartozó „tengerentúli kommunikáció" azt sugallja, hogy az Egyesült Királyság az EU-n belül közvetlenül feltartóztathatja és tömegesen összegyűjtheti az adatokat, ideértve az EU és az Egyesült Királyság közötti, átvitel alatt lévő adatokat is, amelyek a határozattervezet hatálya alá tartoznának. E szempont fontosságára tekintettel az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy szorosan kövesse nyomon az ezzel kapcsolatos fejleményeket.

30. Az Európai Adatvédelmi Testület a tömeges lehallgatással kapcsolatban továbbra is hangsúlyozza az EJEB és az EUB következetes értékelését, és emlékeztet a másodlagos adatokkal kapcsolatban kifejezett aggályokra, amelyekre érzékeny jellegük miatt egyedi garanciákat kell nyújtani. Az Európai Adatvédelmi Testület ezért arra kéri az Európai Bizottságot, hogy gondosan mérje fel, hogy az

Egyesült Királyság joga által a személyes adatok ilyen kategóriájára előírt garanciák az EGT-ben biztosítottal lényegében megegyező védelmi szintet biztosítanak-e.

31. Ezzel összefüggésben az Európai Adatvédelmi Testület tisztában van azzal, hogy a Hírszerzési és Biztonsági Bizottságnak a tömeges jogkörökről szóló, 2016. évi nyilvános jelentése[13] a korábbi jogi keret szerinti gyakorlatokra vonatkozik, amely keretet később felváltotta az IPA 2016. Mindazonáltal úgy véli, hogy további független értékelésre és felügyeletre van szükség az automatizált adatkezelési eszközöknek az Egyesült Királyság illetékes felügyeleti hatóságai általi használata tekintetében, és felszólítja az Európai Bizottságot, hogy vizsgálja tovább ezt a kérdést és azokat a garanciákat, amelyeket az EGT-beli érintettek számára ebben az összefüggésben biztosítani lehetne és/vagy biztosítani kellene.

32. Az Európai Adatvédelmi Testület egyetért az IPC-vel abban, hogy további felülvizsgálatra és nyomon követésre van szükség annak biztosítása érdekében, hogy a nemzetbiztonság és hírszerzés területén a vonatkozó jogszabályok alkalmazásával kapcsolatban felmerülő hiányosságok orvoslása érdekében az illetékes hatóságok által a gyakorlatban alkalmazott garanciák álljanak fenn, és azokat folyamatosan fejlesszék. Az Európai Adatvédelmi Testület továbbá üdvözli a tényt, hogy ennek következményeként az IPC 2019-ben felülvizsgálta a tömeges lehallgatás vizsgálatával kapcsolatos megközelítését, *„ami magában foglalta a tömeges lehallgatások tényleges végrehajtására vonatkozó, technikailag összetett módszerek gondos felülvizsgálatát*", valamint kötelezettséget vállalt arra, hogy 2020-tól kezdve beépítse *„az EJEB által hivatkozott válogatók és keresési feltételek részletes vizsgálatát*" a tömeges lehallgatások vizsgálatába. E szempont fontosságára tekintettel az Európai Adatvédelmi Testület aggodalmát fejezi ki amiatt, hogy az IPC még nem végezte el a válogatók és a keresési kritériumok részletes vizsgálatát, és felszólítja az Európai Bizottságot, hogy szorosan kövesse nyomon az ezzel kapcsolatos fejleményeket, különösen mivel e felügyelet konkrét formáját még tisztázni kell.

33. Az Európai Adatvédelmi Testület hangsúlyozza, hogy a tengerentúli közzétételek esetében az Egyesült Királyság joga által biztosított nemzetbiztonsági mentesség alkalmazása olyan garanciák hiányához vezethet, amelyek biztosítják, hogy a célhoz kötöttség, a szükségesség és az arányosság elvét is tiszteletben tartják, vagy előrevetítik, hogy az egyének megfelelő jogait, a felügyeletet és a jogorvoslatot a rendeltetési hely szerinti harmadik országban is biztosítják vagy tiszteletben tartják. Az Európai Adatvédelmi Testület ezért azt ajánlja az Európai Bizottságnak, hogy folytassa az Egyesült Királyság jogszabályai által a tengerentúli közzététel tekintetében biztosított általános garanciák vizsgálatát, különös tekintettel a nemzetbiztonsági mentességek alkalmazására.

34. Végezetül az Európai Adatvédelmi Testület aggodalmát fejezi ki a más eszközökön alapuló információmegosztás és -közlés egyéb formái miatt, különösen az Egyesült Királyság által más harmadik országokkal kötött különböző nemzetközi megállapodások miatt, különösen akkor, ha ezek az eszközök továbbra sem hozzáférhetők a nyilvánosság számára, mint például az Egyesült Királyság és az Egyesült Államok közötti távközlési felderítési megállapodás. Az ilyen megállapodás hatása a személyes adatokhoz való, nemzetbiztonsági célú hozzáféréssel és az adatok felhasználásával kapcsolatban megállapított garanciák megkerüléséhez vezethet. Az Európai Adatvédelmi Testület úgy véli továbbá, hogy a hírszerzési együttműködés céljából harmadik országokkal kötendő, olyan

[13] Lásd: Report of the bulk powers review of Terrorism Legislation (A terrorizmussal kapcsolatos jogszabályokban foglalt, tömeges jogkörök felülvizsgálatáról szóló jelentés), 2016. augusztus, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf

két- vagy többoldalú megállapodások, amelyek jogalapot biztosítanak közvetlen lehallgatáshoz és a személyes adatok megszerzéséhez vagy a személyes adatok ezen országok részére történő továbbításához, szintén jelentősen érinthetik az összegyűjtött információk további használatának feltételeit, mivel ezek a megállapodások nagy valószínűséggel befolyásolhatják az Egyesült Királyság értékelt adatvédelmi jogi keretét.

1.3. Következtetés

35. Az Európai Adatvédelmi Testület úgy véli, hogy az Egyesült Királyság uniós tagállamként betöltött korábbi státusza miatt az Egyesült Királyság megfelelőségi értékelése egyedülálló. Emellett ez lenne az első megfelelőségi határozat is, amely hatályvesztésre vonatkozó rendelkezést tartalmaz.

36. Ennek megfelelően az Európai Adatvédelmi Testület elismeri, hogy az Egyesült Királyság adatvédelmi kerete és az uniós adatvédelmi keret között számos területen konvergencia áll fenn. Ugyanakkor, valamint az Európai Bizottság határozattervezetének és az Egyesült Királyság adatvédelmi jogszabályainak alapos elemzését követően az Európai Adatvédelmi Testület számos kihívást azonosított, amelyeket ebben a véleményben részletesen megvizsgálunk. Ezzel összefüggésben az Európai Adatvédelmi Testület hangsúlyozni kívánja, hogy az Európai Bizottság kiemelkedő szerepet játszik az Egyesült Királyságban bekövetkező valamennyi releváns fejlemény nyomon követésében.

37. A fentiek fényében az Európai Adatvédelmi Testület azt ajánlja az Európai Bizottságnak, hogy foglalkozzon az e véleményben felvetett kihívásokkal. Az Európai Adatvédelmi Testület felkéri továbbá az Európai Bizottságot, hogy szorosan kövessen nyomon az Egyesült Királyságban bekövetkező minden olyan releváns fejleményt, amely hatással lehet a személyes adatok védelmi szintjének lényegi azonosságára, és szükség esetén mielőbb tegye meg a megfelelő intézkedéseket.

2. BEVEZETÉS

2.1. Az Egyesült Királyság adatvédelmi keretrendszere

38. Az Egyesült Királyság adatvédelmi kerete nagyrészt az uniós adatvédelmi kereten alapul (különösen az általános adatvédelmi rendeleten és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelven), amely abból ered, hogy az Egyesült Királyság 2020. január 31-ig az EU tagállama volt. Ezen túlmenően a 2018. május 23-án hatályba lépett és az Egyesült Királyság 1998. évi adatvédelmi törvényét hatályon kívül helyező 2018. évi adatvédelmi törvény tovább pontosítja az általános adatvédelmi rendeletnek az Egyesült Királyság jogában történő alkalmazását, valamint átülteti az uniós bűnüldözési irányelvet, továbbá meghatározza a nemzeti adatvédelmi felügyeleti hatóság, az Egyesült Királyság Információs Biztosának Hivatala jogköreit és kötelezettségeit.

39. Az Európai Bizottság határozattervezetének (12) preambulumbekezdésében említettek szerint az Egyesült Királyság kormánya hatályba léptette a European Union (Withdrawal) Act 2018 elnevezésű (2018. évi kilépési) törvényt, amely beépíti a közvetlenül alkalmazandó uniós jogszabályokat az Egyesült Királyság jogába. E törvény értelmében az Egyesült Királyság miniszterei hatáskörrel rendelkeznek arra, hogy jogi eszközök révén másodlagos jogszabályokat vezessenek be annak érdekében, hogy az Egyesült Királyság EU-ból való kilépését követően végrehajtsák a megtartandó uniós jog szükséges módosításait, hogy azok illeszkedjenek a hazai környezethez.

40. Következésképpen az átmeneti időszak[14] lejárta után az Egyesült Királyságban alkalmazandó vonatkozó jogi keret a következőkből áll:

- az Egyesült Királyság Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 elnevezésű jogszabály (a kilépéssel kapcsolatos 2019. évi adatvédelmi szabályozás) által módosított általános adatvédelmi rendelete (a továbbiakban: az Egyesült Királyság általános adatvédelmi rendelete), amelyet a 2018. évi kilépési törvény ültetett át az Egyesült Királyság jogába;
- a kilépéssel kapcsolatos 2019. évi adatvédelmi szabályozással módosított 2018. évi adatvédelmi törvény (a továbbiakban 2018. évi adatvédelmi törvény), valamint a Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 elnevezésű, az adatvédelemről, a magánélet védelméről és az elektronikus hírközlésről (módosítások stb.) (Kilépés az EU-ból) szóló 2020. évi rendelet; valamint
- a nyomozati hatáskörökről szóló, 2016. évi törvény.

(a továbbiakban együtt: az Egyesült Királyság adatvédelmi kerete).

2.2. Az Európai Adatvédelmi Testület általi értékelés terjedelme

41. Az Európai Bizottság határozattervezete az Egyesült Királyság adatvédelmi keretének értékelése alapján készült, amelyet az Egyesült Királyság kormányával folytatott megbeszélések követtek. Az általános adatvédelmi rendelet 70. cikke (1) bekezdésének s) pontjával összhangban az Európai Adatvédelmi Testületnek független véleményt kell adnia az Európai Bizottság megállapításairól, azonosítania kell a megfelelőségi keretrendszer esetleges hiányosságait, és javaslatokat kell tennie ezek kezelésére.

42. Az általános adatvédelmi rendelettel kapcsolatos megfelelőségi referenciában említettek szerint: „*az Európai Bizottság által rendelkezésre bocsátott tájékoztatásnak teljes körűnek kell lennie, és lehetővé kell tennie az Európai Adatvédelmi Testület számára, hogy elvégezze a harmadik ország adatvédelmi szintjével kapcsolatos saját értékelését*”[15].

43. E tekintetben meg kell jegyezni, hogy az Európai Adatvédelmi Testület időben az Egyesült Királyság jogi keretének vizsgálata szempontjából releváns dokumentumokat csak részben kapta meg. Az Európai Adatvédelmi Testület a határozattervezetben említett egyesült királyságbeli jogszabályok többségét az abban hivatkozott linkeken keresztül kapta meg. Az Európai Bizottság nem volt abban a helyzetben, hogy az Európai Adatvédelmi Testületnek írásbeli magyarázatokat és az Egyesült Királyság részéről kötelezettségvállalásokat adjon át az Egyesült Királyság hatóságai és az Európai Bizottság közötti, az értékeléssel kapcsolatos információcserékkel kapcsolatban[16].

[14] Az átmeneti időszak 2020. december 31-ig tart, amely időpontot követően az uniós jog már nem alkalmazandó az Egyesült Királyságban. Az „áthidaló időszak” legkésőbb 2021. június 30-ig tart, és arra a további időszakra utal, amely alatt a személyes adatoknak az EGT-ből az Egyesült Királyságba történő továbbítása nem minősül adattovábbításnak.

[15] Lásd: WP 254 rev.01, 3. o.

[16] A következők esetében: Az általános adatvédelmi rendelet 48. cikke (a határozattervezet 78. lábjegyzete); az adatkezelők által nemzetbiztonsági összefüggésben végzett adatkezelés során alkalmazott fokozott garanciák és biztonsági intézkedések (a határozattervezet 64. lábjegyzete); az adatkezelő azon kötelezettsége, hogy mérlegelje, hogy szükség van-e eseti alapon a mentességre akkor is, ha nemzeti biztonsági tanúsítványt állítottak ki (a határozattervezet (126) preambulumbekezdése és 172. lábjegyzete); a tény, hogy az EU és az

44. A fentiek figyelembevételével és az Európai Adatvédelmi Testület számára e vélemény elfogadására biztosított rövid (2 hónapos) határidő miatt az Európai Adatvédelmi Testület úgy döntött, hogy a határozattervezetben szereplő néhány konkrét pontra összpontosít, és ezekről készít elemzést és véleményt.

45. Egy olyan harmadik ország jogának és gyakorlatának elemzésekor, amely egészen a közelmúltig az EU tagállama volt, nyilvánvaló, hogy az Európai Adatvédelmi Testület számos szempontot lényegében megegyezőnek minősített. Tekintettel a megfelelőség megállapítása elfogadásának folyamatában betöltött szerepére, valamint az elemzendő jogszabályok és gyakorlatok mennyiségére, az Európai Adatvédelmi Testület úgy döntött, hogy figyelmét azokra a szempontokra összpontosítja, amelyek esetében a legnagyobb szükség van a részletesebb vizsgálatra. Emellett az EUB ítélkezési gyakorlatával összhangban az elemzés igen fontos része az Egyesült Királyságba továbbított személyes adatokhoz való nemzetbiztonsági hozzáférés jogi rendszerére, valamint az Egyesült Királyságban működő nemzetbiztonsági szerv gyakorlatára terjed ki. Szem előtt kell tartani azonban, hogy a nemzetbiztonság nyilvánvalóan olyan jogi és gyakorlati terület, ahol a tagállamok jogszabályai nem harmonizáltak uniós szinten, és ezért eltérőek lehetnek.

46. Az Európai Adatvédelmi Testület figyelembe vette az alkalmazandó európai adatvédelmi keretet, beleértve az Európai Unió Alapjogi Chartájának 7., 8. és 47. cikkét, amelyek rendre a magán- és a családi élethez való jogot, a személyes adatok védelméhez való jogot, valamint a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogot védik; valamint az emberi jogok európai egyezményének (a továbbiakban: EJEE) a magán- és a családi élethez való jogot védő 8. cikkét. A fentieken túlmenően az Európai Adatvédelmi Testület figyelembe vette az általános adatvédelmi rendelet követelményeit, valamint a vonatkozó ítélkezési gyakorlatot.

47. Az értékelés célja, hogy véleményt adjon az Európai Bizottságnak az Egyesült Királyságban érvényes védelmi szint megfelelőségéről. Az EUB továbbfejlesztette a már a 95/46/EK irányelv alapján is létező, „megfelelő adatvédelmi szintre" vonatkozó elvet. Fontos emlékeztetni arra a mércére, amelyet az EUB a Schrems I-ítéletben határozott meg, azaz, hogy míg a harmadik országban a „védelem szintjének" „lényegében megegyezőnek" kell lennie az EU-ban biztosított védelmi szinttel, *„azok az eszközök, amelyeket a harmadik ország az ilyen védelmi szint biztosításához e tekintetben igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket az Unióban alkalmaznak"*[17]. Ennek értelmében a cél nem az uniós jogszabályok pontról pontra történő lemásolása, hanem a vizsgált jogszabályok lényegi – alapvető követelményeinek megállapítása. A megfelelőség az érintettek

USA közötti keretmegállapodás szerinti védelem minden olyan személyes adatra alkalmazandó lesz, amelyet az Egyesült Királyság és az Egyesült Államok közötti CLOUDAct megállapodás szerint hoznak létre vagy őriznek meg, függetlenül a kérelmet benyújtó szervezet jellegétől vagy típusától, az Egyesült Királyság és az Egyesült Államok között még megbeszélések tárgyát képező adatvédelmi garanciák konkrét végrehajtására tekintettel az Egyesült Királyság hatóságai csak akkor fogják hatályba léptetni ezt a megállapodást, ha meggyőződtek arról, hogy a végrehajtása megfelel az abban foglalt jogi kötelezettségeknek, beleértve az e megállapodás alapján kért valamennyi adatra vonatkozó adatvédelmi szabványoknak való megfeleléssel kapcsolatos egyértelműséget (a határozattervezet (153) preambulumbekezdése); azok a helyzetek, amikor e határozattervezet keretében adatokat továbbítanak az EU-ból az Egyesült Királyságba, és az a tény, hogy mindig fennáll „a brit szigetek közötti kapcsolat", és az ilyen adatokra kiterjedő, berendezésekkel végzett beavatkozás minden esetben az IPA 2016 13. szakaszának (1) bekezdésében foglalt kötelező engedélyre irányuló követelmény hatálya alá tartozna (a határozattervezet (206) preambulumbekezdése); valamint a rendelkezésre bocsátott operatív célokra vonatkozó példák (a határozattervezet (216) preambulumbekezdése és 369. lábjegyzete).

[17] Lásd az EUB C-362/14. sz., Maximilian Schrems kontra adatvédelmi biztos ügyben 2015. október 6-án hozott ítéletének (ECLI:EU:C:2015:650) (a továbbiakban: Schrems I) 73–74. pontját.

számára biztosított jogok és az adatok kezelését végzők vagy az adatkezelést felügyelők és az ellenőrzést gyakorló független szervezetek számára előírt kötelezettségek kombinációjával érhető el. Az adatvédelmi szabályok azonban csak akkor hatékonyak, ha azok a gyakorlatban is kikényszeríthetők és betarthatók. Ezért a szabályok hatékonyságának biztosítása érdekében nem csupán a harmadik országokba vagy nemzetközi szervezetek részére továbbított személyes adatokra vonatkozó szabályok tartalmát kell figyelembe venni, hanem a bevezetett rendszert is. A hatékony végrehajtási mechanizmusok rendkívül fontosak az adatvédelmi szabályok hatékonysága tekintetében[18].

2.3. Általános észrevételek és aggályok

2.3.1. Az Egyesült Királyság nemzetközi kötelezettségvállalásai

48. Az általános adatvédelmi rendelet 45. cikke (2) bekezdésének c) pontja és az általános adatvédelmi rendelettel kapcsolatos megfelelőségi referencia[19] szerint harmadik ország védelmi szintje megfelelőségének értékelésekor az Európai Bizottság figyelembe veszi többek között a harmadik ország által vállalt nemzetközi kötelezettségeket, vagy a harmadik országnak a többoldalú vagy regionális rendszerekben való részvételéből eredő egyéb kötelezettségeket, különösen a személyes adatok védelmével kapcsolatban, valamint e kötelezettségek végrehajtását. Emellett figyelembe kell venni különösen azt, ha a harmadik ország csatlakozott a személyes adatok gépi feldolgozása során az egyének védelméről szóló, 1981. január 28-i Európa tanácsi egyezményhez (a továbbiakban: a 108. egyezmény)[20], valamint annak kiegészítő jegyzőkönyvéhez[21].

49. **E tekintetben az Európai Adatvédelmi Testület üdvözli, hogy az Egyesült Királyság csatlakozott az EJEE-hez, és az EJEB joghatósága alatt áll. Emellett az Egyesült Királyság csatlakozott az 108. egyezményhez és annak kiegészítő jegyzőkönyvéhez, 2018-ban aláírta az 108+ sz. egyezményt[22], és jelenleg folyik a munka annak megerősítésén.**

2.3.2. Az Egyesült Királyság adatvédelmi keretének esetleges jövőbeli eltérése

50. Amint az a határozattervezet (281) preambulumbekezdésében szerepel, az Európai Bizottságnak figyelembe kell vennie, hogy a kilépésről rendelkező megállapodás[23] által biztosított átmeneti időszak lejártával az Egyesült Királyság saját adatvédelmi rendszerét igazgatja, alkalmazza és juttatja érvényre, és amint az EU-Egyesült Királyság kereskedelmi és együttműködési megállapodás[24] FINPROV.10A. cikke szerinti áthidaló rendelkezés alkalmazása megszűnik, ez magában foglalhatja különösen a határozattervezetben értékelt adatvédelmi keret módosítását vagy megváltoztatását, valamint egyéb releváns fejleményeket.

[18] Lásd: WP 254 rev.01, 2. o.
[19] Lásd: WP 254 rev.01, 2. o.
[20] Lásd a személyes adatok feldolgozása során az egyének védelméről szóló, 1981. január 28-i 108. egyezményt.
[21] Lásd a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménynek a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról szóló, 2001. november 8-án aláírásra megnyitott kiegészítő jegyzőkönyvét.
[22] Lásd a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményt módosító, 2018. május 18-i jegyzőkönyvet (a továbbiakban: 108+ egyezmény).
[23] Lásd a Nagy-Britannia és Észak-Írország Egyesült Királyságának az Európai Unióból és az Európai Atomenergia-közösségből történő kilépéséről szóló megállapodást (HL L 29., 2020.1.31., 7. o.).
[24] Lásd az egyrészről az Európai Unió és az Európai Atomenergia-közösség, és másrészről Nagy-Britannia és Észak-Írország Egyesült Királysága közötti kereskedelmi és együttműködési megállapodást (HL L 444., 2020.12.31., 14. o.).

51. Az Európai Bizottság ezért úgy határozott, hogy felvesz egy hatályvesztésre vonatkozó rendelkezést – négy évvel a hatálybalépést követően – a határozattervezetébe[25].

52. Fontos megjegyezni, hogy az Egyesült Királyság miniszterei és az Egyesült Királyság külügyminiszterének azon lehetősége, hogy az áthidaló időszak végét követően másodlagos jogszabályokat vezessenek be, a jövőben az Egyesült Királyság adatvédelmi keretének az Unióétól való jelentős eltérését eredményezheti.

53. Az Egyesült Királyság kormánya kinyilvánította azon szándékát, hogy különálló és független adatvédelmi politikákat dolgozzon ki, amelyek akár el is térhetnek az uniós adatvédelmi jogtól[26]. Ez a szándék magában foglalja a személyes adatokkal kapcsolatos szempontoknak a kereskedelmi megállapodásokba való beépítését[27], ami azzal a kockázattal jár, hogy csökken a személyes adatok Egyesült Királyság által biztosított védelme[28].

54. Végül, nem csak az átmeneti időszak lejárta óta, az Egyesült Királyságot már nem köti az EUB ítélkezési gyakorlata, hanem az EUB már elfogadott ítéletei – amelyeket az Egyesült Királyság jogi keretében megtartott uniós ítélkezési gyakorlatnak tekintenek – már nem feltétlenül kötik az Egyesült Királyságot, mivel az Egyesült Királyságnak van lehetősége arra különösen, hogy módosítsa a megtartott uniós jogot az áthidaló időszak végét követően, és a Legfelsőbb Bíróságot nem köti a megtartott uniós ítélkezési gyakorlat[29].

---

[25] Lásd a határozattervezet 4. cikkét. Lásd még a határozattervezet (282) preambulumbekezdését.

[26] Az Egyesült Királyság nemzeti adatstratégiája (legutóbb 2020. december 9-én frissítve, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) egyik küldetéseként a következőket foglalja magában: „*A nemzetközi adatáramlás élharcosa. A határokon átnyúló információáramlás ösztönzi a globális üzleti műveleteket, az ellátási láncokat és a kereskedelmet, és világszerte fellendíti a növekedést. Ezenkívül szélesebb körű társadalmi szerepet is betölt. A személyes adatok továbbítása biztosítja az emberek fizetését, és segíti őket abban, hogy kapcsolatba lépjenek a távolról érkező szeretteikkel. Amint azt a koronavírus-világjárvány is mutatja, az egészségügyi adatok megosztása segítheti a betegségekre irányuló létfontosságú tudományos kutatásokat, miközben egyesíti az országokat a globális egészségügyi vészhelyzetekre adott válaszaikban.* ***Az Európai Unióból való kilépést követően az Egyesült Királyság kiáll az adatok nyújtotta előnyök mellett.*** *Elő fogjuk mozdítani a hazai bevált gyakorlatokat, és a nemzetközi partnerekkel annak biztosításán fogunk dolgozni,* ***hogy az adatokat ne korlátozzák helytelenül a nemzeti határok és a széttöredezett szabályozói rendszerek****, hogy a bennük rejlő teljes potenciált ki lehessen aknázni*." (utólagos kiemelés).

[27] Ugyanott: „*Az adatok határokon átívelő áramlásának megkönnyítése:* ***Globálisan azon fogunk munkálkodni, hogy felszámoljuk a nemzetközi adatáramlás előtt álló szükségtelen akadályokat. Kereskedelmi tárgyalásaink során ambiciózus adatrendelkezéseket fogadunk el,*** *és a Kereskedelmi Világszervezetben betöltött, újonnan független helyünket arra használjuk fel, hogy jobb irányba befolyásoljuk az adatokra vonatkozó kereskedelmi szabályokat.* ***Felszámoljuk a növekedést és az innovációt támogató nemzetközi adattovábbítás előtt álló akadályokat****, többek között az Egyesült Királyság olyan új kapacitásának kifejlesztésével, amely új és innovatív mechanizmusokat biztosít a nemzetközi adattovábbításhoz. A G20-ak partnereivel is együtt fogunk működni, hogy interoperabilitás jöjjön létre a nemzeti adatrendszerek között annak érdekében, hogy minimalizáljuk a súrlódást a különböző országok közötti adattovábbítás során*". (utólagos kiemelés).

[28] Lásd az Európai Parlament 2017. december 12-i, „*A digitális kereskedelmi stratégia felé*" c. állásfoglalásának (2017/2065=INI)) V. szakaszát, amelyben hangsúlyozza, hogy „*a személyes adatok védelme a[z uniós] kereskedelmi megállapodások tárgyalásakor nem képezheti alku tárgyát*", amely elérhető itt: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_HU.pdf Lásd még az Európai Parlament 2021. március 25-i állásfoglalását az általános adatvédelmi rendelet végrehajtásáról szóló bizottsági értékelő jelentésről – a rendelet alkalmazásának két éve, 28. pont, amely a következőket mondja ki: *„támogatja a Bizottság azon gyakorlatát, hogy a kereskedelmi megállapodásoktól elkülönítve kezeli az adatvédelmet és a személyes adatok áramlását"*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_HU.html

[29] Lásd a 2018. évi kilépési törvény 6. szakaszának (3)–(6) bekezdését.

55. **Figyelembe véve az Egyesült Királyság adatvédelmi keretének az áthidaló időszak végét követően az uniós vívmányoktól való esetleges eltérésével kapcsolatos kockázatokat, az Európai Adatvédelmi Testület üdvözli az Európai Bizottság azon döntését, hogy a határozattervezetre vonatkozóan négyéves megszüntetési záradékot vezet be. Az Európai Adatvédelmi Testület azonban szeretné kiemelni az Európai Bizottság nyomonkövetési szerepének fontosságát[30]. Az Európai Bizottságnak valójában a határozat hatálybalépésétől kezdve folyamatosan és állandóan nyomon kell követnie minden olyan releváns fejleményt az Egyesült Királyságban, amely hatással lehet az Egyesült Királyság megfelelőségi határozata alapján továbbított személyes adatok védelmi szintjének lényegi azonosságára. Emellett az Európai Bizottságnak a szóban forgó körülmények alapján megfelelő lépéseket kell tennie a megfelelőségi határozat felfüggesztése, módosítása vagy hatályon kívül helyezése révén, amennyiben a megfelelőségi határozat elfogadását követően az Európai Bizottság arra utaló jeleket észlel, hogy az Egyesült Királyságban már nem biztosított a megfelelő szintű védelem.**

56. Az Európai Adatvédelmi Testület a maga részéről minden tőle telhetőt megtesz annak érdekében, hogy tájékoztassa az Európai Bizottságot a tagállamok adatvédelmi felügyeleti hatóságai által a kereskedelmi vagy az állami szektorban hozott releváns intézkedésekről, különös tekintettel az EGT-beli érintettek által az EGT-ből az Egyesült Királyságba történő személyesadat-továbbítással kapcsolatban benyújtott panaszokra.

3. ÁLTALÁNOS ADATVÉDELMI SZEMPONTOK

3.1. Tartalmi elvek

57. Az általános adatvédelmi rendelettel kapcsolatos megfelelőségi referencia 3. fejezete a „tartalmi elvekről” szól. A harmadik ország rendszerének tartalmaznia kell ezeket annak érdekében, hogy adatvédelmi szintje lényegében megegyező legyen az EU-n belül garantálttal. Az Európai Adatvédelmi Testület tudomásul veszi, hogy az Egyesült Királyság nem rendelkezik kodifikált alkotmánnyal, mivel nincs egyetlen dokumentum, amely meghatározza az alapvető szabályokat. A magán- és családi élet tiszteletben tartásához való jogot (és e jog részeként az adatvédelemhez való jogot) és a tisztességes eljáráshoz való jogot[31] azonban az emberi jogokról szóló 1998. évi törvény tartalmazza, és ezen alapokmány alkotmányos értékét az Egyesült Királyság bíróságai is elismerték. Az emberi jogokról szóló, 1998. évi törvény valóban magában foglalja az EJEE-ben foglalt jogokat[32]. Ezenkívül az emberi jogokról szóló, 1998. évi törvény nagyon fontosnak tartja, hogy a hatóságok minden intézkedése összeegyeztethető legyen az EJEE-vel[33].

58. Az Európai Adatvédelmi Testület – az Egyesült Királyság és az EU jogszabályai közötti strukturális és formális különbségeken túl – megállapítja, hogy az Egyesült Királyság adatvédelmi megközelítése hasonló az EU-ban alkalmazott megközelítéshez, ami abból ered, hogy az Egyesült Királyság 2020. január 31-ig az EU tagállama volt. Ennek eredményeként számos tartalmi elv összhangban áll az általános adatvédelmi rendelettel; ezért az EU által biztosított védelemmel lényegében megegyező védelmi szintet biztosít. Az Európai Adatvédelmi Testület úgy határozott, hogy nem fejti ki részletesebben az uniós jogszabályokkal összhangban álló tartalmi elvek elemzését, és elégedett az Európai Bizottság által a határozattervezetben közölt elemzéssel. Ilyen tartalmi elvek például a

[30] Lásd az általános adatvédelmi rendelet 45. cikkének (4) bekezdését.
[31] Lásd: az EJEE 6. és 8. cikke (lásd még az emberi jogokról szóló 1998. évi törvény 1. mellékletét).
[32] További információkért lásd a határozattervezet (8)–(10) preambulumbekezdését.
[33] Lásd az emberi jogokról szóló, 1998. évi törvény 6. szakaszát.

következők: fogalmak (pl. „személyes adatok”; „a személyes adatok kezelése”; „adatkezelő”); a jogos célokból végzett jogszerű és tisztességes adatkezelés jogalapjai; a célhoz kötöttség; az adatminőség és az arányosság elve; az adatmegőrzés, -biztonság és titoktartás; az átláthatóság; a különleges adatkategóriák; a közvetlen üzletszerzés; az automatizált döntéshozatal és a profilalkotás. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi megállapodás olyan tartalmi elveket tartalmaz, amelyek túlmutatnak az általános adatvédelmi rendelet rendelettel kapcsolatos megfelelőségi referenciában előírtakon, és tükrözik az általános adatvédelmi rendeletben foglalt elveket; ezért emelik az Egyesült Királyságban biztosított védelem szintjét. Ilyen tartalmi elvek például az adatvédelmi incidensek bejelentéséhez, az adatvédelmi tisztviselőhöz, az adatvédelmi hatásvizsgálatokhoz, valamint a beépített és alapértelmezett adatvédelemhez kapcsolódnak.

59. Azonban, ahogyan azt a bevezetésben is említettük, az Európai Adatvédelmi Testület ebben a véleményben külön foglalkozni kíván bizonyos kérdésekkel, amelyekkel kapcsolatban kétségei vannak, és pontosítást kér az Európai Bizottságtól.

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

60. A **2018. évi adatvédelmi törvény 2. melléklete 1. részének 4. pontjában** meghatározott úgynevezett „bevándorlási mentesség” lehetővé teszi a határt átlépő személyforgalom ellenőrzésében részt vevő adatkezelők számára, hogy ne alkalmazzák az érintetteknek a 2018. évi adatvédelmi törvény által biztosított bizonyos jogait, amennyiben ez valószínűleg „*veszélyeztetné a határt átlépő személyforgalom hatékony ellenőrzésének fenntartását*” vagy „*olyan tevékenységek kivizsgálását vagy felderítését, amelyek aláássák a határt átlépő személyforgalom hatékony ellenőrzésének fenntartását*”.

61. Ahogyan azt az Európai Bizottság a határozattervezetében[34] elismerte, és ahogyan arra az Európai Parlament LIBE Bizottságának az EU nevében az EU és az Egyesült Királyság közötti kereskedelmi és együttműködési megállapodás megkötéséről alkotott véleménye[35] utalt, ez a mentesség **„széleskörűen” van megfogalmazva**. Ez a következő jogokra vonatkozik: tájékoztatáshoz való jog; hozzáféréshez való jog; törléshez való jog; az adatkezelés korlátozásához való jog; valamint a tiltakozáshoz való jog.

62. Ezenkívül fontos megjegyezni, hogy a mentesség akkor is alkalmazandó, ha a személyes adatokat nem a bevándorlás ellenőrzése céljából gyűjti az adatkezelő („1. adatkezelő)”, hanem egy másik

[34] Lásd a határozattervezet (62)–(65) preambulumbekezdését.

[35] E tekintetben a bevándorlási mentesség **széles körű megfogalmazásával** kapcsolatban lásd a LIBE bizottság véleményét az egyrészről az Európai Unió és az Európai Atomenergia-közösség, másrészről Nagy-Britannia és Észak-Írország Egyesült Királysága közötti kereskedelmi és együttműködési megállapodásnak, valamint az Európai Unió és Nagy-Britannia és Észak-Írország Egyesült Királysága közötti, a minősített adatok cseréjére és védelmére vonatkozó biztonsági eljárásokról szóló megállapodásnak az Unió nevében történő megkötéséről, (2020./0382(NLE)), 2021. február 5., https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_HU.pdf, 10. pont: *„e tekintetben emlékeztet az Európai Parlament 2020. februári és júniusi állásfoglalásaira, amelyek felhívták a figyelmet az Egyesült Királyság adatvédelmi törvényében a személyes adatok bevándorlási célú feldolgozása tekintetében biztosított **általános és széles körű mentességre***”, valamint a 11. pont: *„úgy véli, hogy az Egyesült Királyság adatvédelmi törvényében a személyes adatok bevándorlási célú feldolgozása tekintetében biztosított **általános és széles körű** mentességet [...] módosítani kell ahhoz, hogy érvényes megfelelőségi határozatot lehessen hozni”* (utólagos kiemelés).

adatkezelő („2. adatkezelő”) rendelkezésére bocsátja, aki az ilyen személyes adatokat a bevándorlás ellenőrzése céljából kezeli (pl. az Egyesült Királyság Belügyminisztériuma)[36].

63. Az Open Rights Group & Anor, R (On the Application Of) kontra Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (2019. október 3.) ügyben a felperesek vitatták a bevándorlási mentesség jogszerűségét azzal az indokkal, hogy az ellentétes az általános adatvédelmi rendelet 23. cikkével, és összeegyeztethetetlen az Európai Unió Alapjogi Chartájának a magánélet védelmére és a személyes adatok védelmére vonatkozó 7. és 8. cikkében biztosított jogokkal. A High Court of England and Wales (a továbbiakban: High Court) megvizsgálta, hogy a 2018. évi adatvédelmi törvény 2. melléklete 1. részének 4. pontjában szereplő, bevándorlásra vonatkozó mentesség jogszerű-e, és annak jogszerűsége mellett foglalt állást.

64. A High Court különösen a következőket állapította meg:

- *„[...] a bevándorlási mentesség egyértelműen a »fontos közérdek« körébe tartozik, és jogszerű célt szolgál. [...]”*, 30. pont;
- *„a bevándorlási mentesség megfelel az ahhoz szükséges követelményeknek, hogy az intézkedés a joggal összhangban legyen. […]”*, 38. pont;
- *„A bevándorlási mentességre csak akkor és annyiban lehet hivatkozni, ha és amennyiben »az általános adatvédelmi rendelet felsorolt rendelkezéseinek« való megfelelés **veszélyeztetheti** a határt átlépő személyforgalom hatékony ellenőrzésének fenntartását vagy olyan tevékenységek kivizsgálását vagy felderítését, amelyek aláássák a határt átlépő személyforgalom hatékony ellenőrzésének fenntartását. A »veszélyeztethetné« kifejezést az 1998. évi adatvédelmi törvénnyel összefüggésben (amely megelőzte a 2018. évi adatvédelmi törvényt) úgy értelmezték, hogy az nagyon jelentős és nagy eséllyel sértheti az adott közérdeket. A kockázat mértékének olyannak kell lennie, hogy „nagyon is” sérthesse ezeket az érdekeket, még akkor is, ha a kockázat valószínűsége sokkal kevésbé valószínű, mint nem valószínű […].*”, 39. pont (utólagos kiemelés).

[36] Lásd az Információs Biztos Hivatala „Guide to the General Data Protection Regulation (GDPR)” „Útmutató az általános adatvédelmi rendelethez (GDPR)” című dokumentumában szereplő példát, 2021. január 1., 307. o. (utólagos kiemelés): *„Egy magánszervezet (1. adatkezelő) értesíti a Belügyminisztériumot (2. adatkezelő) egy alkalmazottról, aki feltételezhetően hamis dokumentumokat nyújtott be személyazonosságának és képesítésének igazolására, hogy állást szerezzen. A munkáltató a Belügyminisztérium rendelkezésére bocsátja a vonatkozó információkat. Az egyén azon joga, hogy tájékoztatást kapjon arról, hogy személyes adatait továbbították a Belügyminisztériumnak, korlátozott, amennyiben annak érvényre juttatása valószínűleg sértené a nyomozást.*
*A **munkáltató tehát nem köteles tájékoztatni az egyént arról, hogy az információkat továbbították a Belügyminisztériumnak**, a **Belügyminisztérium** pedig nem köteles adatvédelmi nyilatkozatot tenni az egyén számára, amelyben tájékoztatná arról, hogy személyes adatait kezeli. A mentesség mindkét adatkezelőre azonos mértékben vonatkozik.*
*A munkavállaló azonban személyes adatairól másolatot kér a Belügyminisztériumtól, amely jelenleg vizsgálja azokat. A **Belügyminisztérium** az adatok egy részének visszatartásához **alkalmazhatja a mentességet**, ha a nyilvánosságra hozatal valószínűleg sértené a nyomozást. Amennyiben a munkavállaló hasonló kérelmet nyújt be a **munkáltatójához**, az ugyanolyan mértékben **alkalmazhatná a mentességet**.”*
Más szóval, a 300. oldalon kifejtettek szerint: *„Az esetek többségében a Belügyminisztérium vagy annak egyik ügynöksége és alvállalkozója lesz az e mentességet alkalmazó adatkezelő. Fontos azonban megjegyezni, hogy e mentesség alkalmazása nem korlátozódik a Belügyminisztériumra. Ez más adatkezelők, például a munkáltatók, az egyetemek és a rendőrség számára is releváns lehet, akik bevándorlási ügyekben kapcsolatot tartanak a Belügyminisztériummal.”*

65. Meg kell jegyezni, hogy ez az ítélet az Európai Adatvédelmi Testület tudomása szerint nem jogerős, és megfellebbezték.

66. Ahogyan az Európai Adatvédelmi Testületnek az általános adatvédelmi rendelet 23. cikke szerinti korlátozásokról szóló iránymutatásában („az általános adatvédelmi testület 23. cikkéről szóló iránymutatás")[37] szerepel, *„[...] az általános adatvédelmi rendelettel összefüggésben **jogalkotói intézkedésben** kell korlátozásokat biztosítani, amelynek az **érintettek jogainak és/vagy az adatkezelők kötelezettségeinek korlátozott számát kell érintenie**, amelyek az általános adatvédelmi rendelet 23. cikkében vannak felsorolva, **be kell tartania az alapvető jogok és szabadságok lényegét**, egy demokratikus társadalomban **arányos és szükséges intézkedésnek** kell lennie, valamint meg kell óvnia az általános adatvédelmi rendelet 23. cikke (1) bekezdésében foglalt valamely jogalapot [...]"*.[38]

67. Az Európai Adatvédelmi Testület emlékeztet továbbá arra, hogy az általános adatvédelmi rendelet (41) preambulumbekezdése kimondja, hogy *„[a]mikor ez a rendelet **jogalapra vagy jogalkotási intézkedésre** hivatkozik, az nem szükségszerűen jelenti – az érintett tagállam alkotmányos rendjéből fakadó követelmények sérelme nélkül – valamely parlament által elfogadott jogszabályt. Mindazonáltal az ilyen jogalapnak vagy jogalkotási intézkedésnek **világosnak és pontosnak kell lennie, alkalmazásának pedig előreláthatónak kell lennie a hatálya alá tartozó személyek számára**, összhangban az Európai Unió Bíróságának [...] és az Emberi Jogok Európai Bíróságának az ítélkezési gyakorlatával*" (utólagos kiemelés).

68. Bár az EJEB kifejtette, hogy *„[a]z egyezmény 8–11. cikkében szereplő »joggal összhangban« és »jog által előírt« kifejezések tekintetében az [EJEE] megjegyzi, hogy a »jog« kifejezést mindig »anyagi« és nem »formális« értelemben értelmezte; az magában foglalta mind az »írott jogot«, amely magában foglalja a szakmai szabályozó testületek által a Parlament által rájuk ruházott független szabályalkotási hatáskör alapján hozott alacsonyabb szintű jogszabályok és szabályozási intézkedések törvénybe iktatását, mind pedig az íratlan jogot. A »jogot« úgy kell értelmezni, hogy az magában foglalja mind a törvényekben előírt jogot, mind pedig **az ítélkezési gyakorlatot**"*[39], az általános adatvédelmi rendelet 23. cikkéről szóló iránymutatás emlékeztet arra, hogy az *„EUB ítélkezési gyakorlata szerint az általános adatvédelmi rendelet 23. cikkének (1) bekezdése alapján elfogadott valamennyi **jogalkotói intézkedésnek meg kell felelnie különösen az általános adatvédelmi rendelet 23. cikkének (2) bekezdésében foglalt konkrét követelményeknek**. Az általános adatvédelmi rendelet 23. cikkének (2) bekezdése kimondja, hogy az érintettek jogait és az adatkezelők kötelezettségeit korlátozó jogalkotási intézkedéseknek adott esetben az **alábbiakban felsorolt több kritériumra vonatkozó konkrét rendelkezéseket kell tartalmazniuk**. Fő szabályként az alábbiakban részletezett valamennyi követelményt **magában kell foglalnia a jogalkotási intézkedésnek**, amely korlátozásokat ír elő az általános adatvédelmi rendelet 23. cikke szerint*."[40]

---

[37] Lásd az Európai Adatvédelmi Testületnek az általános adatvédelmi rendelet 23. cikke szerinti korlátozásokról szóló, 2020. december 15-én elfogadott 10/2020. sz. iránymutatásának 1.0 verzióját, amely jelenleg véglegesítés alatt áll a nyilvános konzultációt követően, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en

[38] Lásd az általános adatvédelmi rendelet 23. cikkéről szóló iránymutatást, 9. pont, 5. o.

[39] Lásd: EJEB, Sanoma Uitgevers B.V. kontra Hollandia, 2010. szeptember 14., EC:ECHR:2010:0914JUD003822403, 83. pont (utólagos kiemelés).

[40] Lásd az általános adatvédelmi rendelet 23. cikkéről szóló iránymutatás 45. és 46. pontját, 11. o. Az EU Alapjogi Chartája 52. cikkének (3) bekezdése értelmében *„[a]mennyiben e Charta olyan jogokat tartalmaz, amelyek megfelelnek az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményben*

69. E tekintetben megállapítható, hogy a **bevándorlási mentesség** önmagában **nem határozza meg az általános adatvédelmi rendelet 23. cikkének (2) bekezdésében említett következő elemeket**:

- „a visszaélésre, illetve a jogosulatlan hozzáférésre vagy továbbítás megakadályozását célzó garanciák” (d) pont);
- „az adatkezelő vagy az adatkezelők kategóriái” (e) pont)[41];
- „az érintettek alapvető jogaira és szabadságaira jelentett kockázatok” (g) pont);
- „az érintettek arra vonatkozó joga, hogy tájékoztatást kapjanak a korlátozásról, kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját” (h) pont).

70. Az Információs Biztos Hivatala „Guide to the General Data Protection Regulation (GDPR)” (Útmutató az általános adatvédelmi rendelethez)[42] c. dokumentuma, beleértve a „bevándorlási mentességről” szóló fejezetet, pontosítja a bevándorlási mentességre vonatkozó rendelkezéseket, azonban *önmagában* **nem írhat elő** azt kiegészítő, kötelező erejű szabályokat. Ezenkívül a „jogminőség” kérdése különösen releváns, tekintettel a korlátozott jogok jelentőségére és a mentesség meghosszabbítására[43].

---

biztosított jogoknak, akkor e jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az említett egyezményben szerepelnek. Ez a rendelkezés nem akadályozza meg azt, hogy az Unió joga kiterjedtebb védelmet nyújtson.” Az EU Alapjogi Chartája 52. cikkének (1) bekezdésében foglalt „**jogban előírt**” kifejezéssel kapcsolatban az EJEB által kidolgozott kritériumokat az EUB főtanácsnoki indítványaiban javasoltak szerint kell alkalmazni, lásd például a C-203/15. és C-698/15. sz., Tele2 Sverige AB egyesített ügyekben született véleményeket, ECLI:EU:C:2016:572, 137–154. pont, valamint a C-70/10. sz., Scarlet Extended ügyben született véleményt, ECLI:EU:C:2011:255, 88–114. pont. Ezért hivatkozni lehet többek között az EJEB Weber és Saravia kontra Németország ügyben hozott ítéletének 84. pontjára: *„A Bíróság megismétli, hogy az [EJEE] 8. cikkének (2) bekezdése értelmében vett „**joggal összhangban**” kifejezés megköveteli először is, hogy a kifogásolt intézkedésnek legyen valamilyen alapja a **nemzeti jogban**; hivatkozik továbbá a szóban forgó **jog minőségére** is, előírva, hogy annak az érintett személy számára hozzáférhetőnek kell lennie, akinek továbbá képesnek kell lennie arra, hogy előre láthassa annak az őt érintő következményeit, valamint a jogállamisággal összeegyeztethetőnek kell lennie.*” (utólagos kiemelés).
Lásd még az általános adatvédelmi rendelet (41) preambulumbekezdését: *Mindazonáltal az ilyen jogalapnak vagy jogalkotási intézkedésnek **világosnak** és **pontosnak** kell lennie, alkalmazásának pedig **előreláthatónak kell lennie a hatálya alá tartozó személyek számára**, összhangban az Európai Unió Bíróságának [...] és az Emberi Jogok Európai Bíróságának az ítélkezési gyakorlatával*” (utólagos kiemelés).

[41] Lásd a fent említett High Court által hozott ítélet 54. pontját: *„Véleményem szerint nem jogellenes, hogy a bevándorlási mentesség a meghatározott célokból adatokat kezelő **valamennyi adatkezelő** rendelkezésére álljon. Ahogyan az alperesek rámutattak, a 4. bekezdés (3)–(4) pontja nélkül a bevándorlási mentesség érvénytelenné válna azokban az esetekben, ahol az adatokat harmadik felektől szerezték be (például a helyi hatóságtól vagy a vám- és Adóhivataltól) annak érdekében, hogy fenntartsák a határt átlépő személyforgalom hatékony ellenőrzését.”* (utólagos kiemelés), tehát ez megerősíti a korlátozások **általános** alkalmazását.

[42] Az Információs Biztos Hivatala „Guide to the General Data Protection Regulation (GDPR)” (Útmutató az általános adatvédelmi rendelethez) című dokumentuma, 2021. január 1., 299–307. o.

[43] Lásd a High Court fent említett ítéletének 57. pontját: *„Knight úr arról tájékoztatott, hogy a biztos véglegesíti a mentességre vonatkozó iránymutatást, de csak abban az értelemben lesz „kötelező”, hogy azt a biztosnak az általános adatvédelmi rendelet 57. cikkének (1) bekezdése szerinti hatáskörei alapján adják ki. A 2018. évi adatvédelmi törvény értelmében nem fog jogi státusszal rendelkezni.”*
Az Információs Biztos Hivatala által támogatott, jogilag kötelező erejű iránymutatás bevezetésének indokait különösen az ítélet 56–60. pontja említi:
„56. Végül rátérek a biztos azon bejelentésére, amely szerint a mentesség nem minősül az általános adatvédelmi rendelet 23. cikke (1) bekezdése arányos végrehajtásának, ha nem tartalmaz olyan jogszabályi

71. A „**sérelemteszt**” ráadásul nem határozza meg a visszaélések, illetve a jogellenes hozzáférés vagy továbbítás megelőzését szolgáló garanciákat, amelyeket például a Belügyminisztériumnak kell végrehajtania.

72. A fentiek fényében az Európai Adatvédelmi Testület megjegyzi, hogy további pontosításokra van szükség a bevándorlási mentesség alkalmazásával kapcsolatban.

73. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy nincs olyan jogilag kötelező erejű eszköz, amely egyértelművé tenné a bevándorlási mentességet azzal kapcsolatban, hogy az lényegében megegyező-e az általános adatvédelmi rendelet 23. cikkével, valamint az Európai Unió Alapjogi Chartájának 7. és 8. cikkével. Ugyanakkor az Európai Adatvédelmi Testület úgy véli, hogy a

---

iránymutatást, amely garanciákat nyújtana a bevándorlási mentesség jelentésére és alkalmazására vonatkozóan. Knight úr azt állítja, hogy az ilyen iránymutatással kiegészített rendelkezés arányos.
57. Knight úr arról tájékoztatott, hogy a biztos véglegesíti a mentességre vonatkozó iránymutatást, de csak abban az értelemben lesz „kötelező”, hogy azt a biztosnak az általános adatvédelmi rendelet 57. cikkének (1) bekezdése szerinti hatáskörei alapján adják ki. A 2018. évi adatvédelmi törvény értelmében nem fog jogi státusszal rendelkezni. Tudomásul veszem továbbá, hogy a Belügyminisztérium elkészítette a bevándorlási mentességgel kapcsolatos belső személyzeti iránymutatás tervezetét (lásd fent a [22.] pontot). A gyakorlatban a biztos által kiadott iránymutatás a jogalaptól függetlenül befolyással bír. A biztos azonban nem rendelkezik hatáskörrel arra, hogy olyan »kötelező erejű« iránymutatást adjon, amelyet a Legfelsőbb Bíróság a Christian Institute ügyben (a [101.] és [107.] pontban) figyelembe vett. Úgy tűnik, hogy elsődleges jogra lenne szükség, ha szükségesnek tartanák, hogy a bevándorlási mentességről szóló iránymutatás ugyanolyan jogállású legyen, mint a 2018. évi adatvédelmi törvény 121–124. cikkében jelenleg előírt gyakorlati kódexek.
58. A kötelező iránymutatásra vonatkozó érvelésében Knight úr azt állítja, hogy a bevándorlási mentesség alkalmazásának hátterében szükségszerűen felmerülnek a létének és használatának szükségességével és arányosságával kapcsolatos aggályok. A petíció benyújtója két témára hívja fel a figyelmet, különösen a jogi kontextusban. Először is, a bevándorlási mentesség hatálya alá tartozó személyes adatok természetüknél fogva valószínűleg az általános adatvédelmi rendelet 9. cikkének (1) bekezdése szerinti különleges kategóriájú adatokat (azaz „faji vagy etnikai származásra vonatkozó” adatokat) foglalnak magukban. Az ilyen adatokat az általános adatvédelmi rendelet azért azonosítja, mert magasabb szintű védelmi intézkedést igényelnek (1/15. vélemény [2019] 3 C.M.L.R. 25 a [141.] pontban). Másodszor, az adatvédelmi jog egyik alapvető rendelkezése, hogy a hozzáférési jog különösen nagy jelentőséggel bír az érintettek számára biztosított egyéb jogok gyakorlásának lehetővé tétele szempontjából (lásd: YS kontra Minister voor Immigratie, Integratie en Asiel ügyben hozott ítélet, C-141/12, EU:C:2014:2081; [2015] 1 C.M.L.R. 18 a [44.] pontban).
59. Knight úr négy, gyakorlati jellegű pontot jelöl meg. Először is, ha az adatkezelők nem magyarázzák meg az érintettek számára, hogy jogszabályban előírt mentességre hivatkoztak, és nem adnak átfogó összefoglalást az okokról sem, az érintettek nem fogják tudni, hogy a mentességet alkalmazták, és ennek következtében nem tudják azt hatékonyan megtámadni. Másodszor, az érintettek különösen nagy mértékben függnek az adatkezelőktől a tekintetben, hogy azok körültekintően és csak a szükséges mértékben alkalmazzák a mentességet. Bár bármely érintett panaszt tehet a biztosnál a mentesség alkalmazásával kapcsolatban, vagy bírósági eljárást indíthat, valószínű, hogy az érintett nem ismeri jogait és nem rendelkezik a jogi lépések megtételéhez szükséges forrásokkal olyan körülmények között, amikor az adatvédelmi jogok azonnali és pontos tiszteletben tartására van szükség. Harmadszor, az érintett bevándorlóként kiszolgáltatott helyzetben lehet. Negyedszer, ez nem elvont probléma az alpereseknek a bevándorlási mentesség alkalmazására vonatkozó bizonyítékai tükrében (lásd a fenti [4.] pontot).
60. Knight úr úgy véli, hogy szoros párhuzam áll fenn a bevándorlási mentesség jelenlegi vitatása és a Bíróság által a Christian Institute ([2016] UKSC 51) ügyben hozott ítélet indokolása között. A Christian Institute ügyhöz hasonlóan azt állítja, hogy a bevándorlási mentesség széles körű, meghatározatlan fogalmakat használ, alacsony küszöbértéket alkalmaz, a rendelkezésből nem nyilvánvaló ellenőrzés tárgyát képezi, továbbá a körülmények és jogok igen széles körére vonatkozik. A Christian Institute ügyben foglaltaktól eltérően a bevándorlási mentességre vonatkozóan nem áll rendelkezésre nyilvánosan hozzáférhető iránymutatás, sem kötelező státusz, amelyet figyelembe kellene venni.”

bevándorlási mentesség személyi hatályának szükségességét és arányosságát az Európai Bizottságnak további bizonyítékokkal kell alátámasztania.

74. **Ennek következtében az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy vizsgálja meg az Open Rights Group & Anor, R (On the Application Of) kontra Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) ügy jelenlegi állását, és mivel ez az ítélet nem jogerős (*res judicata*), ellenőrizze, hogy azt a fellebbviteli ítélet megerősíti vagy felülvizsgálja-e, figyelembe véve az e tekintetben bekövetkezett változásokat, és pontosítva azt a megfelelőségi határozatban. Az Európai Adatvédelmi Testület felkéri továbbá az Európai Bizottságot, hogy nyújtson további tájékoztatást a bevándorlási mentesség szükségességéről és arányosságáról, különös tekintettel a személyi hatály széles körére.**

75. **Ezzel egyidejűleg az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy vizsgálja meg alaposabban, hogy léteznek vagy elképzelhetők-e további garanciák az Egyesült Királyság jogi keretében, például olyan jogilag kötelező erejű eszközök révén, amelyek kiegészítenék a bevándorlásra vonatkozó mentességet azáltal, hogy növelik annak kiszámíthatóságát és az érintettek számára biztosított garanciákat, lehetővé téve a szükségességi és az arányossági követelmények jobb és gyors értékelését és nyomon követését is.**

3.1.2. Az újbóli adattovábbítás korlátozása

76. Az általános adatvédelmi rendelet 44. cikke úgy rendelkezik, hogy személyes adatok továbbítására és újbóli továbbítására csak akkor kerülhet sor, ha az nem veszélyezteti a természetes személyeknek az általános adatvédelmi rendelet által garantált védelmi szintjét. Ezért a megfelelőségi határozat alapján az EGT-ből az Egyesült Királyságba továbbított személyes adatokat az uniós adatvédelmi keret által biztosítottal lényegében megegyező szintű védelemben kell részesíteni. **Ez nemcsak azt jelenti, hogy a határozattervezet értelmében az Egyesült Királyság jogszabályainak az uniós jogszabályokkal „lényegében" megegyezőnek kell lenniük az Egyesült Királyság részére továbbított személyes adatok kezelése tekintetében, hanem azt is, hogy az Egyesült Királyságban az említett adatok harmadik országokba történő újbóli továbbítására alkalmazandó szabályoknak biztosítaniuk kell, hogy továbbra is lényegében megegyező szintű védelem valósuljon meg.**

77. Ezért fontos, hogy az EGT-ből származó személyes adatoknak az Egyesült Királyságból egy másik harmadik országba történő továbbítása megfelelő védelmet élvezzen a garanciákkal, vagy arra az eltérésekre vonatkozó szabályokkal[44] összhangban kerüljön sor az uniós jogszabályok által biztosított védelem folytonosságának biztosítása érdekében. **Amennyiben ilyen védelem nem biztosítható, nem kerülhet sor az EGT-beli személyes adatok további továbbítására.**

78. Az Európai Adatvédelmi Testület elismeri, hogy az Egyesült Királyság nagyrészt az általános adatvédelmi rendelet V. fejezetét tükrözi az Egyesült Királyság általános adatvédelmi rendeletében (44–49. cikk) és a 2018. évi adatvédelmi törvényben[45]. **Mindazonáltal az Európai Adatvédelmi Testület azonosította az Egyesült Királyság jogszabályi keretének bizonyos aspektusait a további adattovábbítás tekintetében, amelyek alááshatják az EGT-ből továbbított személyes adatok védelmének szintjét.**

79. Az Európai Adatvédelmi Testület által azonosított **első kihívás** arra vonatkozik, hogy az Egyesült Királyság a 2018. évi adatvédelmi törvényben kidolgozott eljárást követően harmadik országokat,

[44] Lásd az általános adatvédelmi rendelet 49. cikkét.
[45] Lásd a 2018. évi adatvédelmi törvény 17A., 17B., 17C. és 18. szakaszát.

nemzetközi szervezeteket vagy területeket[46] ismer el megfelelő címzettként. Az EGT-n belüli személyes adatoknak az Egyesült Királyságból más harmadik országokba történő továbbítására valóban sor kerülhet egy esetleges jövőbeli egyesült királyságbeli megfelelőségi rendelet alapján[47].

80. Pontosabban, amint azt a határozattervezet (77) preambulumbekezdése kifejti, az Egyesült Királyság külügyminisztere az Információs Biztos Hivatalával folytatott konzultációt követően jogosult elismerni, hogy egy harmadik ország (vagy egy harmadik országon belüli terület vagy ágazat), egy nemzetközi szervezet vagy az ilyen ország, terület, ágazat vagy szervezet leírása biztosítja a személyes adatok megfelelő szintű védelmét[48]. A védelmi szint megfelelőségének értékelésekor az Egyesült Királyság külügyminiszterének ugyanazokat az elemeket kell figyelembe vennie, amelyeket az Európai Bizottságnak értékelnie kell az általános adatvédelmi rendelet (104) preambulumbekezdésével és a megtartott uniós ítélkezési gyakorlattal együtt értelmezett 45. cikke (2) bekezdésének a)–c) pontja alapján. Ez azt jelenti, hogy egy harmadik ország megfelelő védelmi szintjének értékelésekor a vonatkozó mérce az, hogy a szóban forgó harmadik ország az Egyesült Királyságban biztosítottal „lényegében megegyező" szintű védelmet biztosít-e. Bár az Európai Adatvédelmi Testület tudomásul veszi az Egyesült Királyság arra vonatkozó képességét, hogy az Egyesült Királyság általános adatvédelmi rendelete szerint az Egyesült Királyság adatvédelmi keretére figyelemmel bizonyos területeket megfelelő szintű adatvédelmet biztosító területként ismerjen el, az Európai Adatvédelmi Testület hangsúlyozni kívánja, hogy ez utóbbi területekre a mai napig nem feltétlenül vonatkozik az Európai Bizottság által kiadott, az EU-ban biztosított védelemmel „lényegében megegyező" védelmi szintet elismerő megfelelőségi határozat. Ez az EGT-ből továbbított személyes adatok védelme tekintetében esetlegesen kockázatokat eredményezhet, különösen akkor, ha a jövőben az Egyesült Királyság adatvédelmi kerete eltérne az uniós vívmányoktól. Meg kell jegyezni, hogy 2020 júliusában az EUB Schrems II-ügyben hozott, mérföldkőnek számító ítélete[49] az Egyesült Államok adatvédelmi pajzsáról szóló határozat érvénytelenítését eredményezte, mivel a Bíróság szerint az USA jogi kerete nem tekinthető az EU-val lényegében megegyező szintű védelmet biztosítónak. Előfordulhat azonban, hogy az EUB már elfogadott, az Egyesült Királyság jogi keretében fenntartott ítélkezési gyakorlatnak minősülő ítéletei már nem kötik az Egyesült Királyságot, mivel az Egyesült Királyságnak lehetősége van különösen arra, hogy az áthidaló időszak végét követően módosítsa a megtartott uniós jogot, és Legfelsőbb Bíróságát nem köti a megtartott uniós ítélkezési gyakorlat[50].

81. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy szorosan kövesse nyomon az Egyesült Királyság hatóságai által más harmadik országok tekintetében végzett megfelelőségértékelés folyamatát és kritériumait, különösen azon harmadik országok vonatkozásában, amelyek megfelelőségét az EU az általános adatvédelmi rendelet alapján nem ismerte el. Amennyiben az Európai Bizottság megállapítja, hogy az Egyesült Királyság által megfelelőnek ítélt harmadik ország nem biztosít az EU-n belül biztosítottal lényegében megegyező szintű védelmet, az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy tegyen meg minden szükséges lépést, például módosítsa az Egyesült Királyság megfelelőségi határozatát az**

[46] Lásd a 2018. évi adatvédelmi törvény 17A. szakaszát.
[47] Az általános adatvédelmi rendelet szerinti megfelelőségi határozat egyesült királyságbeli megfelelője.
[48] Lásd a 2018. évi adatvédelmi törvény 182. szakaszának (2) bekezdését. Lásd még az egyetértési megállapodást az Információs Biztos Hivatalának az Egyesült Királyság új megfelelőségi értékeléseivel kapcsolatos szerepéről, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/
[49] Lásd a Schrems II-ügyet.
[50] Lásd a 2018. évi kilépési törvény 6. szakaszának (3)–(6) bekezdését.

EGT-ből származó személyes adatokra vonatkozó egyedi garanciák bevezetése érdekében, és/vagy fontolja meg az Egyesült Királyság megfelelőségi határozatának felfüggesztését, amennyiben az EGT-ből az Egyesült Királyságba továbbított személyes adatok újbóli továbbítása az Egyesült Királyság megfelelőségi szabályozása alapján történik.

82. A **második kihívás** az Európai Bizottság által a 95/46/EK irányelv alapján hozott, már meglévő megfelelőségi határozatok közelgő felülvizsgálatához kapcsolódik. E felülvizsgálatot követően előfordulhat, hogy az Európai Bizottság úgy dönt, hogy egyes országok, amelyek eddig a megfelelőségi határozat előnyeit élvezték, már nem biztosítanak lényegében megegyező szintű védelmet, figyelembe véve a hatályos uniós jogszabályokat és a legújabb ítélkezési gyakorlatot. Az Egyesült Királyság azonban a 2018. évi adatvédelmi törvény 21. mellékletének 4. pontjában előírtak szerint már elismerte, hogy ezek az országok megfelelő szintű védelmet biztosítanak. Bár az Egyesült Királyság külügyminiszterének négy éven belül felül kell vizsgálnia ezeket a megfelelőségi megállapításokat, az Európai Bizottság határozattervezetében megjegyzi, hogy ezek a megfelelőségi megállapítások nem szűnnek meg automatikusan, akkor sem, ha az Egyesült Királyság külügyminisztere nem végzi el a szükséges felülvizsgálatot az előírt négyéves határidőn belül[51].

83. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot annak nyomon követésére, hogy a már meglévő megfelelőségi határozatok uniós felülvizsgálatának lezárását követően az Egyesült Királyság továbbra is megfelelőnek tekinti-e azt az országot, amelyről az Európai Bizottság úgy véli, hogy már nem biztosít megfelelő szintű védelmet. Amennyiben igen, az Európai Adatvédelmi Testület a határozattervezet (277)–(280) preambulumbekezdése alapján felkéri az Európai Bizottságot, hogy hozzon megfelelő intézkedéseket a helyzet orvoslására, például módosítsa a megfelelőségi határozatot annak érdekében, hogy az EGT-ből származó személyes adatokra vonatkozó különleges követelményeket vezessen be, és/vagy függessze fel a megfelelőségi határozatot arra az esetre, ha az EGT-ből az Egyesült Királyságba továbbított személyes adatokat a szóban forgó harmadik országba továbbítják. Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy az Egyesült Királyságra vonatkozó megfelelőségi határozat időtartama alatt folytassa ezt a nyomon követést.**

84. A **harmadik kihívás** a személyes adatoknak az EGT-ből a megfelelőséget nem biztosító országokba történő, az Egyesült Királyság általános adatvédelmi rendeletének 46. és 47. cikkében előírt adattovábbítási eszközökön alapuló továbbításával kapcsolatos. Bár az Egyesült Királyság általános adatvédelmi rendelete ugyanazokat az adattovábbítási eszközöket írja elő, mint az általános adatvédelmi rendelet, az Európai Adatvédelmi Testület hangsúlyozza, hogy biztosítani kell, hogy az azokban foglalt garanciák hatékony védelmet nyújtsanak a harmadik országban, különösen a Schrems II-ítélet fényében.

85. A Schrems II-ügyben hozott ítéletet követően, amelyben az EUB emlékeztet arra, hogy az EU-ban a személyes adatoknak biztosított védelemnek érvényesnek kell lennie az adatokra, bárhová is továbbítják azokat, az Európai Adatvédelmi Testület már elfogadta a kiegészítő intézkedésekre vonatkozó első ajánlásokat[52], amelyek szükség esetén segítik az adatátadókat annak biztosításában, hogy az érintettek az EU-n belül biztosítottal lényegében megegyező védelmi szintben részesüljenek.

[51] Lásd a határozattervezet (82) preambulumbekezdését.

[52] Lásd az Európai Adatvédelmi Testületnek az adattovábbítási eszközöket a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében kiegészítő intézkedésekről szóló, 2020. november 10-i 01/2020. számú ajánlását, amelynek véglegesítése jelenleg folyamatban van a nyilvános konzultációt

86. Az EUB szerint az adatátadók feladata eseti alapon és adott esetben a harmadik országbeli adatátvevővel együttműködve ellenőrizni, hogy a harmadik ország joga vagy gyakorlata csorbítja-e az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközökben foglalt megfelelő garanciák hatékonyságát[53]. Amennyiben igen, az adatátadóknak olyan kiegészítő intézkedéseket kell végrehajtaniuk, amelyek megszüntetik a védelem hiányosságait, és az uniós jog által előírt szintre emelik azt.

87. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy a védelem folyamatosságának biztosítása érdekében vezesse be a határozattervezetbe, hogy amennyiben az Egyesült Királyság általános adatvédelmi rendeletének 46. és 47. cikkében előírt adattovábbítási eszközöket az egyesült királyságbeli adatátadók az EGT-n keresztül továbbított adatok más harmadik országokba történő továbbításához használják, akkor ezek az adatátadók eseti alapon értékeljék a harmadik ország adatvédelmi keretét; és szükség esetén tegyék meg a megfelelő intézkedéseket a választott adattovábbítási eszközben foglalt garanciák hatékony betartásának biztosítása érdekében, hogy az EU-n belül biztosított védelemmel lényegében megegyező szintű védelmet biztosítsanak. Az Európai Adatvédelmi Testület hangsúlyozza, hogy e garanciák nélkül fennáll a kockázata annak, hogy az Egyesült Királyságból történő további adattovábbítások gyengítik az EU-n belül biztosított védelemmel lényegében megegyező védelmi szintet.**

88. A további adattovábbításra vonatkozó **negyedik kihívás** az Egyesült Királyság által kötött vagy a jövőben megkötendő nemzetközi megállapodásokra, valamint az e megállapodásokat megkötő harmadik ország(ok) hatóságainak az EGT-ből származó személyes adatokhoz való lehetséges közvetlen hozzáférésére vonatkozik. Az Európai Adatvédelmi Testületnek komoly aggályai vannak a már megkötött, az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodással kapcsolatban, és az Európai Bizottság elismeri ezt a kihívást, hangsúlyozva, hogy *„a megállapodás esetleges hatálybalépése hatással lehet az e határozatban értékelt védelmi szintre”*[54]. E megállapodás alapján ugyanis a hatálybalépését követően e megállapodásnak az Egyesült Államok hatóságainak közvetlen hozzáférésére vonatkozó feltételeket meghatározó rendelkezései vonatkoznának a határozattervezet értelmében az EGT-ből az Egyesült Királyságba továbbított személyes adatokra, ami kihatna az Egyesült Királyság adatvédelmi keretére, beleértve a további adattovábbításra vonatkozó rendelkezéseket is. Ennek eredményeként az Egyesült Államokkal kötött megállapodás rendelkezései jelentősen érinthetik az EGT-ből továbbított adatok esetében biztosított védelem szintjét, és hatással lehetnek az ilyen adatok védelmének szintjére. Az Európai Adatvédelmi Testület ezzel összefüggésben megjegyzi, hogy az Európai Bizottság határozattervezetének (153) preambulumbekezdésében hivatkozik az Egyesült Királyság hatóságai által adott magyarázatokra anélkül, hogy konkrét írásbeli garanciát vagy kötelezettségvállalást idézne, és nem is utal az Egyesült Királyság jogának olyan konkrét jogi rendelkezéseire, amelyek érvényre juttatnák ezeket a magyarázatokat.

89. Az Európai Adatvédelmi Testület az Európai Parlamentnek címzett 2020. június 15-i levelében már felvetette ezeket az aggályokat[55]. Az Európai Adatvédelmi Testület kiemelte, hogy *„az adatvédelem*

---

követően, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_hu.pdf

[53] Lásd: Schrems II-ügy, 134. pont.

[54] Lásd a határozattervezet (153) preambulumbekezdését.

[55] Lásd az Európai Adatvédelmi Testület 2020. június 15-én elfogadott válaszát Sophie in’t Veld és Moritz Körner európai parlamenti képviselőknek az Egyesült Államok és az Egyesült Királyság közötti CLOUD Act

területére vonatkozó uniós vívmányok, és különösen az általános adatvédelmi rendelet és a bűnüldözésről szóló irányelv" alapján az Európai Adatvédelmi Testületnek fenntartásai vannak azzal kapcsolatban, hogy az Egyesült Királyságban a személyes adatokhoz való hozzáférésre vonatkozó megállapodásban foglalt garanciák alkalmazandók-e bizonyos körülmények között, amelyek az USA-val szemben közzétételi kötelezettséget írnak elő, valamint hogy ezek a garanciák az uniós normák fényében elegendőek-e ahhoz, hogy ne ássák alá az EU-ban biztosított védelem szintjét.

90. Ezen túlmenően az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodás rendelkezései jelentősen érinthetik azokat az anyagi és eljárási feltételeket, amelyek mellett az egyesült királyságbeli adatkezelők vagy adatfeldolgozók birtokában lévő személyes adatokhoz az Egyesült Államok hatóságai közvetlenül hozzáférhetnek, ami kihat az Egyesült Királyság joga által biztosított védelem szintjére. Az uniós jog által biztosítottal lényegében megegyező védelmi szint biztosítása érdekében például „*alapvető fontosságú, hogy az ilyen megállapodás szerinti garanciák magukban foglalják a kötelező előzetes bírói engedélyt, amely alapvető garanciát jelent a metaadatokhoz és a tartalmi adatokhoz való hozzáféréshez. Előzetes értékelése alapján az Európai Adatvédelmi Testület – bár megállapította, hogy a megállapodás a nemzeti jog alkalmazására utal – nem tudott ilyen egyértelmű rendelkezést azonosítani az Egyesült Királyság és az Egyesült Államok között létrejött megállapodásban*"[56].

91. Míg az Európai Bizottság kiemeli, hogy az e megállapodás alapján megszerzett adatok az úgynevezett „EU-USA közötti keretmegállapodásban" foglalt konkrét garanciákkal egyenértékű védelemben részesülnének, az Európai Adatvédelmi Testületnek aggályai vannak azzal kapcsolatban, hogy e garanciáknak az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodásba való belefoglalása – az értelemszerű alkalmazásra való puszta utalással – megfelelne-e az egyértelmű, pontos és hozzáférhető szabályok kritériumainak a személyes adatokhoz való hozzáférés tekintetében, vagy kellően rögzítené-e ezeket a garanciákat ahhoz, hogy az Egyesült Királyság joga szerint érvényesek és végrehajthatóak legyenek.

92. **Az Európai Adatvédelmi Testület ezért azt ajánlja, hogy az Európai Bizottság tisztázza, hogy az Egyesült Királyság joga szerint hogyan és mely jogi eszközön keresztül érnék el az EU-USA közötti keretmegállapodás által biztosított konkrét garanciákkal egyenértékű védelmet, és annak hogyan lenne kötelező jellege.**

93. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodás rendelkezései – az adatok jogszerű tengerentúli felhasználásáról szóló amerikai törvény (CLOUD Act) 3. szakaszával[57] összefüggésben értelmezve – kérdéseket vetnek fel a megállapodásban az Egyesült Államok bűnüldöző hatóságainak az Egyesült Királyságban az USA joghatósága alá tartozó elektronikus hírközlési szolgáltatók vagy távoli számítástechnikai szolgáltatók (a továbbiakban: CSP-k) által kezelt személyes adatokhoz való hozzáférésére vonatkozóan kínált garanciák tényleges alkalmazásával kapcsolatban. Amennyiben ugyanis az Egyesült Királyságban található CSP az Egyesült Államok jogának hatálya alá tartozik (pl. mivel egy egyesült államokbeli vállalat leányvállalata), meg kell bizonyosodni arról, hogy az Egyesült Államok hatóságai kötelesek lennének-e az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodásra támaszkodni ezen adatok megszerzése érdekében. Mivel az Európai Bizottság

megállapodásról, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf

[56] Lásd az Európai Adatvédelmi Testület fent említett levelét.

[57] Lásd az Egyesült Államok törvényét az adatok jogszerű tengerentúli felhasználásáról (CLOUD Act), https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

rámutat arra, hogy *„[k]ülönös figyelmet fordítanak a keretmegállapodás garanciáinak az Egyesült Királyság és az Egyesült Államok közötti megállapodás hatálya alá tartozó adattovábbítások konkrét típusaira alkalmazására és azokhoz való hozzáigazítására”*, az Európai Adatvédelmi Testület hangsúlyozza, hogy előzetes értékelése alapján nem egyértelmű, hogy az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodásban foglalt garanciák, és ezért az USA és az Egyesült Királyság közötti keretmegállapodás által biztosított garanciák alkalmazandók-e az Egyesült Államok CLOUD törvénye alapján az Egyesült Államok hatóságai által benyújtott, az adatokhoz való hozzáférés iránti kérelmekre.

94. Előfordulhat, hogy az Egyesült Királyság a jövőben további nemzetközi megállapodásokat vagy kötelezettségvállalásokat köt harmadik országokkal, amelyek a határozattervezet értelmében az EGT-ből az Egyesült Királyságba továbbított személyes adatokra vonatkoznának[58]. E megállapodások rendelkezéseitől és a garanciákra vonatkozó konkrét feltételek alkalmazásától függően ezek a nemzetközi megállapodások – az Egyesült Királyság adatvédelmi keretét érintően – jelentős hatást gyakorolhatnak a harmadik országok hatóságainak az egyesült királyságbeli személyes adatokhoz való hozzáférésére vonatkozó anyagi és eljárási feltételekre is. Ez különösen igaz az Európa Tanács számítástechnikai bűnözésről szóló egyezménye (a továbbiakban: budapesti egyezmény) második kiegészítő jegyzőkönyvének tervezetére, amelyről jelenleg tárgyalnak ezen egyezmény részes felei, köztük több nem uniós ország. A jegyzőkönyvtervezet tartalmaz olyan kikötéseket, amelyeket a felek diszkrecionálisan aktiválhatnak, például a tartalmi adatokhoz való hozzáférés engedélyezésére vonatkozó felhatalmazást illetően. Bár valamennyi uniós tagállam az uniós adatvédelmi szabályoknak megfelelően aktiválná a kikötéseket, nincs garancia az Egyesült Királyságra vonatkozóan, amely jelentősen eltérhet az EU-n belül biztosított védelem szintjétől. A fent ismertetett kérdések egy másik példája az Egyesült Királyság és Japán közötti átfogó gazdasági partnerségi megállapodás (CEPA)[59], az Egyesült Királyság első, brexit utáni kereskedelmi megállapodása, amely 2021. január 1-jén lépett hatályba[60], és amely személyes adatokra vonatkozó rendelkezéseket tartalmaz[61]. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az Egyesült Királyság 2021. február 1-jén hivatalosan bejelentette a Csendes-óceáni Partnerségi Megállapodást („TPP”) is magában foglaló átfogó és progresszív Csendes-óceáni Partnerséghez („CPTPP”) való csatlakozásra irányuló kérelmét[62].

95. Az Európai Adatvédelmi Testület megjegyzi, hogy az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodáson kívül a határozattervezet nem foglalkozik a fent említett nemzetközi megállapodásokkal.

---

[58] Lásd a fenti 2.3.3. szakaszt.

[59] Lásd: Egyesült Királyság/Japán: Átfogó gazdasági partnerségi megállapodás [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020

[60] Lásd az Egyesült Királyság kormányának az Egyesült Királyság harmadik országokkal kötött kereskedelmi megállapodásairól szóló iránymutatását, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries

[61] A CEPA 8.80. cikkének (5) bekezdése értelmében a felek vállalják, hogy ösztönzik olyan mechanizmusok kidolgozását, amelyek elősegítik a (személyes) adatok védelmére vonatkozó különböző jogi megközelítéseik összeegyeztethetőségét. A 8.84. cikk értelmében a felek kötelezettséget vállalnak arra, hogy nem tiltják vagy korlátozzák az információk elektronikus úton történő, határokon átnyúló továbbítását, ideértve a személyes adatokat is, amennyiben ez a tevékenység a CEPA értelmében vett érintett személy üzleti tevékenységének folytatására irányul.

[62] A TPP 14.11. cikkének (2) bekezdése értelmében minden fél engedélyezi az információk – köztük a személyes adatok – határokon átnyúló továbbítását elektronikus úton, amennyiben ez a tevékenység az érintett személy üzleti tevékenységének folytatására irányul.

96. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot a következőkre:**

- **Az Egyesült Királyság adatvédelmi kerete és nemzetközi kötelezettségvállalásai közötti kölcsönhatás vizsgálata az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodáson túl, különösen annak biztosítása érdekében, hogy az EGT-ből az Egyesült Királyságba továbbított személyes adatoknak az Egyesült Királyság megfelelőségi határozata alapján más harmadik országokba történő továbbítása esetén biztosított legyen a védelem szintjének folyamatossága; valamint az Egyesült Királyság és harmadik országok közötti olyan nemzetközi megállapodások megkötésének folyamatos figyelemmel kísérése, amelyek veszélyeztethetik a személyes adatok Unióban garantált védelmi szintjét, és szükség esetén intézkedések meghozatala.**

- **Az Egyesült Királyság hatóságai írásbeli kötelezettségvállalásainak rendelkezésre bocsátása az Európai Adatvédelmi Testület számára, és az Egyesült Királyság joga szerinti konkrét rendelkezések azonosítása az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodás lehetséges alkalmazásával és végrehajtásával kapcsolatos magyarázattal kapcsolatban, a határozattervezet (153) preambulumbekezdésében említettek szerint.**

- **Ezzel összefüggésben annak nyomon követése, hogy az Egyesült Királyság és az Egyesült Államok közötti keretmegállapodás kiigazításának megfelelő végrehajtása révén biztosítható garanciák mellett az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodás megfelelő további garanciákat nyújt-e az érintett adatkategóriák érzékenységi szintjének és az elektronikus bizonyítékoknak a hatóságok közötti közvetlen továbbítására vonatkozó egyedi követelményeknek a figyelembevételéhez.**

- **Az Egyesült Királyság által nemrégiben aláírt nemzetközi megállapodásokban, például a CEPA-ban foglalt, a személyes adatokra vonatkozó rendelkezések hatásának és lehetséges kockázatainak értékelése.**

97. Az **ötödik kihívás** a személyes adatok harmadik országba történő továbbítására vonatkozó eltérések alkalmazásához kapcsolódik. Bár az Egyesült Királyság általános adatvédelmi rendelete alapján rendelkezésre álló eltérések megegyeznek az általános adatvédelmi rendelet szerinti eltérésekkel, fontos, hogy az Információs Biztos Hivatala jelenleg és a későbbiekben is alkalmazza ezen eltéréseknek az Európai Adatvédelmi Testületével összehangolt értelmezését. Ha ez nem így történik, vagy ha az Egyesült Királyság a jövőben eltér ettől az értelmezéstől, fennállna a kockázata annak, hogy az EGT-ből az Egyesült Királyságon keresztül harmadik országokba továbbított adatok védelmi szintje veszélybe kerülne.

98. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy nyomonkövetési feladata keretében kifejezetten ellenőrizze, hogy az eltérések alkalmazására vonatkozó egyesült királyságbeli értelmezés továbbra is összhangban van-e az uniós értelmezéssel. Ha azonban az Egyesült Királyság az eltérések alkalmazásának eltérő értelmezését követné, ami aláásná a védelem szintjét, akkor alapvető fontosságú, hogy az Európai Bizottság megtegye a szükséges lépéseket a megfelelőségi határozat módosítása révén annak biztosítása érdekében, hogy az EGT-ből az Egyesült Királyságba továbbított személyes adatokhoz nyújtott védelem szintje ne kerüljön veszélybe, ha ezeket az adatokat az Egyesült Királyságból harmadik országokba továbbítják az eltérések eltérő értelmezése alapján.**

99. Az e szakaszban foglalt utolsó, **hatodik kihívás** arra vonatkozik, hogy az Egyesült Királyság adatvédelmi kerete nem tartalmazza az általános adatvédelmi rendelet 48. cikke szerinti védelmet.

100. Az Európai Bizottság határozattervezetében pontosítja, hogy a megfelelőségi rendeletek vagy megfelelő garanciák hiányában a továbbításra csak az Egyesült Királyság általános adatvédelmi rendeletének 49. cikkében foglalt eltérések alapján kerülhet sor, „*az (EU) 2016/679 rendelet 48. cikkének kivételével, amelynek esetében az Egyesült Királyság úgy döntött, hogy nem veszi fel az Egyesült Királyság általános adatvédelmi rendeletébe*”.[63] Az, hogy az Egyesült Királyság adatvédelmi keretében nem szerepel az általános adatvédelmi rendelet 48. cikkével lényegében megegyező rendelkezés a más harmadik ország bírósági vagy törvényszéki ítéletét vagy közigazgatási hatósági határozatát követő adattovábbítással vagy -közléssel kapcsolatban, jogbizonytalanságot eredményezhet a tekintetben, hogy a határozattervezet alapján az EGT-ből az Egyesült Királyságba továbbított személyes adatok védelmének szintje lényegesen módosul-e.

101. Az Európai Adatvédelmi Testület az általános adatvédelmi rendelettel kapcsolatos megfelelőségi referenciában rámutat arra, hogy a további adattovábbítás tekintetében a „*személyes adatoknak az eredeti adattovábbítás elsődleges címzettje általi újbóli továbbítása kizárólag akkor lehet engedélyezett, ha a további címzettekre olyan szabályok vonatkoznak, amelyek megfelelő adatvédelmi szintet biztosítanak, és követik az adatkezelő nevében végzett adatkezelésre vonatkozó utasításokat*”[64]. Az Európai Adatvédelmi Testület hangsúlyozza továbbá, hogy „*az EU-ból továbbított adatok első címzettje felelős azért, hogy megfelelőségi határozat hiányában meggyőződjön az újbóli adattovábbításra vonatkozó megfelelő garanciák előírásáról. Ezekre az újbóli adattovábbításokra kizárólag korlátozott és meghatározott célokból kerülhet sor, és kizárólag abban az esetben, ha az adatkezelésnek van jogalapja*”[65]. Az általános adatvédelmi rendelet V. fejezetének részeként a 48. cikket teljes mértékben figyelembe kell venni annak értékelése során, hogy az Egyesült Királyság jogi kerete e tekintetben lényegében megegyező szintű védelmet biztosít-e[66].

102. Az Európai Adatvédelmi Testület ezzel összefüggésben hangsúlyozza az Európai Unió Bíróságának az adatokkal való visszaélés, illetve az adatokhoz való jogellenes hozzáférés és azok jogellenes felhasználásának kockázatával kapcsolatos ítélkezési gyakorlatát, megállapítva különösen, hogy „*az alapvető jogok és szabadságok védelmének az Európai Unión belül garantált szintje tekintetében az olyan uniós szabályozásnak, amely beavatkozást jelent az Európai Unió Alapjogi Chartája 7. és 8. cikkében biztosított alapvető jogokba, a Bíróság elfogadott ítélkezési gyakorlatával összhangban egyértelmű és pontos szabályokat kell tartalmaznia a szóban forgó intézkedés hatálya és alkalmazása vonatkozásában, és minimális követelményeket kell előírnia annak érdekében, hogy azon személyek, akiknek a személyes adatai érintettek, elegendő olyan biztosítékkal rendelkezzenek, amely lehetővé teszi az adataiknak a visszaélések veszélyeivel, valamint az ezen adatokat érintő minden jogellenes hozzáféréssel és felhasználással szembeni hatékony védelmét. Az ilyen biztosítékokkal való rendelkezés szükségessége még fontosabb abban az esetben, ha a személyes adatokat automatikusan kezelik és jelentős veszélye áll fenn az említett adatokhoz való jogellenes hozzáférésnek*”[67].

103. Az Európai Adatvédelmi Testület e tekintetben megjegyzi, hogy a határozattervezetben rendelkezésre álló információk alapján az Egyesült Királyság adatvédelmi kerete nem rendelkezik egyértelműen arról, hogy valamely harmadik ország bíróságának vagy törvényszékének bármely

[63] Lásd a határozattervezet 78. lábjegyzetét.
[64] Lásd: WP 254 rev.01, 6. o.
[65] Lásd: WP 254 rev.01, 6. o.
[66] Lásd az általános adatvédelmi rendelet 44. cikkének utolsó mondatát, különösen: „*E fejezet valamennyi rendelkezését alkalmazni kell annak biztosítása érdekében, hogy a természetes személyek számára e rendeletben garantált védelem szintje ne sérüljön.*”
[67] Lásd: Schrems I-ügy, 91. pont.

olyan ítélete, valamint harmadik ország közigazgatási hatóságának bármely olyan határozata, amely az adatkezelőt vagy -feldolgozót személyes adatok továbbítására vagy közlésére kötelezi, csak akkor ismerhető el vagy érvényesíthető bármilyen módon, ha az a kérelmező harmadik ország és az Egyesült Királyság között hatályban lévő nemzetközi megállapodáson alapul. Az általános adatvédelmi rendelet 48. cikke az általános adatvédelmi rendelet V. fejezetének alapvető rendelkezése, mivel előírja, hogy a személyes adatok harmadik országbeli bíróság/törvényszék vagy közigazgatási hatóság ítéletét vagy határozatát követő továbbítása vagy közlése csak akkor ismerhető el vagy hajtható végre, ha az a kérelmező harmadik ország és az Unió vagy valamely tagállam között hatályban lévő nemzetközi megállapodáson alapul, az általános adatvédelmi rendelet V. fejezete szerinti adattovábbítás egyéb indokainak sérelme nélkül. Az Európai Adatvédelmi Testület emlékeztet arra, hogy *„egy külföldi hatóság megkeresése önmagában nem jelent jogalapot a továbbításra. A végzés csak akkor ismerhető el, ha az a kérelmező harmadik ország és az Unió vagy valamely tagállam között hatályban lévő nemzetközi megállapodáson alapul”*[68]. Ezért kulcsfontosságú, hogy a lényegében megegyező rendelkezések azonosíthatók legyenek az Egyesült Királyság jogában.

104. A határozattervezetben az Európai Bizottság beszámol az Egyesült Királyság hatóságaitól kapott magyarázatokról, amelyek szerint a szokásjog vagy az alapokmányok értelmében az adatokat kérő külföldi határozatok nemzetközi megállapodás nélkül nem érvényesíthetők az Egyesült Királyságban, és a külföldi bíróság vagy közigazgatási hatóság kérésére történő adattovábbításhoz olyan adattovábbítási eszközre van szükség, mint például a megfelelőségi rendelet vagy a megfelelő garanciák, kivéve, ha az Egyesült Királyság általános adatvédelmi rendeletének 49. cikke szerinti eltérés alkalmazandó. Az Európai Adatvédelmi Testület azonban nem kapott tájékoztatást az Európai Bizottság és az Egyesült Királyság hatóságai között e tekintetben folytatott információcseréről[69], és ezért nem képes elemezni és függetlenül értékelni, hogy az Egyesült Királyság hatóságai által nyújtott garanciák elegendőek-e az általános adatvédelmi rendelet 48. cikkében foglalt garanciákkal lényegében megegyező védelmi szint biztosításához.

105. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy nyújtson további garanciákat és konkrét hivatkozásokat az Egyesült Királyság azon jogszabályaira, amelyek biztosítják, hogy az Egyesült Királyság jogi kerete szerinti védelem szintje lényegében megegyező legyen az EGT-n belül garantálttal. Az Európai Adatvédelmi Testület ezért felkéri az Európai Bizottságot, hogy nyújtson írásbeli magyarázatot és az Egyesült Királyság hatóságai részéről vállalt kötelezettségvállalásokat az általános adatvédelmi rendelet 48. cikkében előírtakkal lényegében megegyező védelem végrehajtásával kapcsolatban.**

106. **Az Európai Adatvédelmi Testület úgy véli, hogy az Egyesült Királyság joga szerinti olyan rendelkezések azonosítása, amelyek lényegében megegyező szintű védelmet biztosítanak az általános adatvédelmi rendelet 48. cikkében foglalt garanciákkal kapcsolatban, még fontosabb az Egyesült Államok vagy más harmadik országok hatóságai által az Egyesült Királyságban benyújtott, adatokhoz való hozzáférés iránti kérelmekkel kapcsolatban korábban felvetett aggályok fényében, és figyelembe véve, hogy a megfelelőségi határozat értelmében a személyes adatok továbbíthatók az EGT-ből az Egyesült Királyságba anélkül, hogy a címzett további garanciát vagy kötelező erejű**

[68] Lásd az Európai Adatvédelmi Testület és az európai adatvédelmi biztos által a LIBE bizottságnak küldött, az adatok jogszerű tengerentúli felhasználásáról szóló amerikai törvénynek (CLOUD tAct) a személyes adatok védelmére vonatkozó európai jogi keretre gyakorolt hatásáról szóló, 2019. július 10-én elfogadott közös válaszának mellékletét, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en

[69] Lásd a határozattervezet 78. lábjegyzetét.

kötelezettséget vállalna más harmadik országbeli hatóságok adatokhoz való hozzáférés iránti kérelmeivel kapcsolatban.

3.2. Eljárási és végrehajtási mechanizmusok

107. Az Európai Adatvédelmi Testület az általános adatvédelmi rendelettel kapcsolatos megfelelőségi referenciában meghatározott kritériumok alapján elemezte az Egyesült Királyság adatvédelmi keretének a határozattervezet hatálya alá tartozó alábbi szempontjait: a független felügyeleti hatóság létezése és hatékony működése, a megfelelés megfelelő szintjét biztosító rendszer megléte, valamint a megfelelő jogorvoslati mechanizmusokhoz való hozzáférés rendszere, amely felruházza az egyéneket az EU-ban a jogaik gyakorlásához és a jogorvoslat igénybevételéhez szükséges eszközökkel anélkül, hogy nehézkes akadályokba ütköznének a közigazgatási és bírósági jogorvoslat során.

3.2.1. Illetékes független felügyeleti hatóság

108. Az Európai Adatvédelmi Testület üdvözli az Európai Bizottság arra irányuló erőfeszítéseit, hogy a határozattervezet 2.6. fejezetében átfogóan megvizsgálja az Egyesült Királyság felügyeleti hatóságának létrehozását, működését és hatásköreit. Az Egyesült Királyságban az információs biztos feladata az Egyesült Királyság általános adatvédelmi rendeletének és a 2018. évi adatvédelmi törvénynek való megfelelés felügyelete és érvényesítése. A 2018. évi adatvédelmi törvény 12. melléklete szerint az információs biztos „jogi személyiségű örökíthető hivatal" („Corporation Sole"), azaz különálló jogi személy, amelyet egyetlen személy alkot, és amelyet egy hivatal, az Információs Biztos Hivatala támogat.

109. Az információs biztos függetlenségét illetően az Európai Adatvédelmi Testület hangsúlyozza, hogy az Egyesült Királyság általános adatvédelmi rendeletének 51. cikke nem tartalmazza azt a kifejezett pontosítást, hogy az információs biztos független közigazgatási szervnek minősül, amint azt az általános adatvédelmi rendelet 51. cikke a felügyeleti hatóságok tekintetében kimondja. Az Európai Adatvédelmi Testület mindazonáltal elismeri, hogy az Egyesült Királyság általános adatvédelmi rendelete 52. cikkében hasonló módon tükrözi az általános adatvédelmi rendelet 52. cikkének (1)–(3) bekezdésében meghatározott, a függetlenségre vonatkozó megfelelő szabályokat.

110. Az Európai Adatvédelmi Testület továbbá rámutat arra, hogy az Egyesült Királyság általános adatvédelmi rendeletének 52. cikke nem írja elő az általános adatvédelmi rendelet 52. cikke (4)–(6) bekezdésének megfelelő kötelezettségeket, amelyek kifejezetten biztosítják, hogy az érintett felügyeleti hatóság rendelkezzen a feladatai hatékony ellátásához és hatáskörei gyakorlásához szükséges erőforrásokkal. Az Európai Adatvédelmi Testület ugyanakkor elismeri, hogy a 2018. évi adatvédelmi törvény olyan rendelkezéseket tartalmaz, amelyek célja az Információs Biztos Hivatala megfelelő finanszírozásának biztosítása[70], valamint azt a körülményt, hogy az Információs Biztos Hivatala jelenleg az egyik legnagyobb felügyeleti hatóság az EU/EGT-n belüli felügyeleti hatóságok között. Mivel a megfelelő erőforrások folyamatos elosztása – különösen a személyzet és a költségvetés tekintetében[71] – elengedhetetlen a felügyeleti hatóság megfelelő működésének biztosításához annak érdekében, hogy el tudja látni az összes rábízott feladatot, és ezt az Európai Parlament is kiemelt fontosságúnak minősítette a közelmúltban[72], az Európai Adatvédelmi Testület

[70] Lásd a 2018. évi adatvédelmi törvény 137., 138. és 182. szakaszát, valamint 12. mellékletének 9. pontját.
[71] Lásd: WP 254 rev.01, 7. o.
[72] Az Európai Parlament 2021. március 25-i állásfoglalása az általános adatvédelmi rendelet végrehajtásáról szóló bizottsági értékelő jelentésről – a rendelet alkalmazásának két éve, 15. bekezdés, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_HU.html

alapvető fontosságúnak tartja, hogy különös figyelmet fordítsanak az e területen bekövetkező jövőbeli fejleményekre.

111. **Az Európai Adatvédelmi Testület ezért felkéri az Európai Bizottságot, hogy vizsgáljon meg minden olyan fejleményt az Információs Biztos Hivatalának történő forráselosztással kapcsolatban, amely hátrányosan érintené az Információs Biztos Hivatala feladatainak megfelelő teljesítését.**

3.2.2. A megfelelés megfelelő szintjét biztosító adatvédelmi rendszer megléte

112. A határozattervezet átfogóan megvizsgálja azokat a hatásköröket, amelyekkel az Információs Biztos Hivatala rendelkezik az Egyesült Királyság általános adatvédelmi rendeletének 58. cikke és a 2018. évi adatvédelmi törvény alapján a jogszabályok nyomon követésének és végrehajtásának biztosítása érdekében. Az Európai Adatvédelmi Testület elismeri, hogy az Egyesült Királyság általános adatvédelmi rendeletének 58. cikke szorosan tükrözi a felügyeleti hatóságok hatáskörei tekintetében az általános adatvédelmi rendelet 58. cikkében meghatározott megfelelő szabályokat. Ami az egyes esetek körülményeitől függő közigazgatási bírságok kiszabására vonatkozó hatáskört illeti, az Egyesült Királyság általános adatvédelmi rendeletének 83. cikke az általános adatvédelmi rendelet 83. cikkében meghatározottakhoz hasonló rendelkezéseket tartalmaz, és maximális összegeket határoz meg. Ezért az Európai Adatvédelmi Testület úgy véli, hogy az Egyesült Királyság e területre vonatkozó jogi kerete jelenleg összhangban van a vonatkozó uniós jogszabályokban meghatározott normákkal. Mindazonáltal e tekintetben az Európai Adatvédelmi Testület kiemeli, hogy a *hatékony* szankciók megléte fontos szerepet játszik a szabályok betartásának biztosításában.[73]

113. **A fentiek fényében az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy kövesse nyomon az Egyesült Királyság adatvédelmi keretében foglalt szankciók és megfelelő jogorvoslatok hatékonyságát.**

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

114. A hatékony felügyeleti mechanizmus, amely az érintettek jogai megsértésének gyakorlati azonosítása és szankcionálása érdekében lehetővé teszi a panaszok független kivizsgálását, valamint a hatékony közigazgatási és bírósági jogorvoslatot (beleértve az érintett személyes adatainak jogellenes kezelése miatt elszenvedett károk megtérítését), kulcsfontosságú annak értékelése során, hogy az adatvédelmi rendszer megfelelő szintű védelmet nyújt-e.

115. Az Európai Adatvédelmi Testület üdvözli, hogy az Információs Biztos Hivatala átfogó tájékoztatást és iránymutatást nyújt honlapján, amelynek célja, hogy felhívja az adatkezelők és -feldolgozók figyelmét a kötelezettségeikre és feladataikra, valamint támogassa az érintetteket abban, hogy tájékoztatást kapjanak személyes adataikkal kapcsolatos jogaikról, és hogy érvényesíthessék az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi törvény szerinti egyéni jogaikat.

116. **A jelenlegi helyzet ellenére az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy folyamatosan kövesse nyomon az Információs Biztos Hivatala által kifejezetten azon egyéneknek nyújtott támogatás szintjét, akiknek a személyes adatait a megfelelőségi határozat értelmében továbbították az Egyesült Királyság részére, annak érdekében, hogy segítséget kapjanak az Egyesült Királyság adatvédelmi rendszere szerinti jogaik gyakorlásában.**

[73] Lásd: WP 254 rev.01, 7. o.

4. AZ EU-BÓL TOVÁBBÍTOTT SZEMÉLYES ADATOKHOZ VALÓ HOZZÁFÉRÉS ÉS AZ ILYEN ADATOK FELHASZNÁLÁSA AZ EGYESÜLT KIRÁLYSÁG HATÓSÁGAI ÁLTAL

4.1. Az egyesült királyságbeli közigazgatási szervek hozzáférése az adatokhoz és az adatok használata bűnüldözés céljából

4.1.1. Jogalapok és az alkalmazandó korlátozások/garanciák

117. Ami az Európai Bizottság által elvégzett és **a bűnüldözési célú hozzáférésről szóló** határozattervezet (132) és azt követő preambulumbekezdéseiben dokumentált értékelést illeti, az Európai Bizottság árnyalt és részletes információkkal szolgál, és általában érthető következtetéseket von le. Az Európai Adatvédelmi Testület ezért tartózkodik attól, hogy a véleményben szereplő ténymegállapítások és értékelések többségét megismételje. Vannak azonban olyan helyzetek, ahol a tények bemutatása vagy a következtetések magyarázata nem elegendő ahhoz, hogy az Európai Adatvédelmi Testület egyetértsen velük.

4.1.1.1. A hozzájárulás használata

118. Az Európai Adatvédelmi Testület tudomásul veszi az Európai Bizottság határozattervezet 184. lábjegyzetében tett kijelentését[74], miszerint **a hozzájárulás használata** nem releváns a megfelelőségi esetkörben, mivel egy adattovábbítási helyzetben az Egyesült Királyság bűnüldöző hatóságai nem hozzájárulás alapján gyűjtik az adatokat közvetlenül egy uniós érintettől. Következésképpen a hozzájárulásnak a rendfenntartásban jogalapként való felhasználását az Európai Bizottság nem értékeli.

119. E tekintetben az Európai Adatvédelmi Testület emlékeztet arra, hogy az általános adatvédelmi rendelet 45. cikke (2) bekezdésének a) pontja olyan elemek széles körének értékelését írja elő, amelyek nem korlátozódnak az adattovábbítás esetkörére, ideértve „*a jogállamiságot, az emberi jogok és alapvető szabadságok tiszteletben tartását, a vonatkozó általános és ágazati jogszabályokat, beleértve [...] a büntetőjogra vonatkozó jogszabályokat is*”.

120. Az Európai Adatvédelmi Testület – többek között az Európai Bizottság által a személyes adatok Egyesült Királyság általi megfelelő védelméről szóló (EU) 2016/680 európai parlamenti és tanácsi irányelv (a továbbiakban: a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv megfelelőségi határozattervezete) szerinti végrehajtási határozat tervezetének (38) preambulumbekezdésében nyújtott információk alapján – megjegyzi, hogy a hozzájárulásnak az Egyesült Királyság jogrendszerében a bűnüldözéssel összefüggésben történő használatához mindig jogalapra lenne szükség. Ez azt jelenti, hogy még abban az esetben is, ha a rendőrségnek törvényes hatásköre van arra, hogy nyomozás céljára feldolgozza az adatokat, bizonyos különleges körülmények között (például DNS-minta gyűjtése céljából), a rendőrség megfelelőnek ítélheti, hogy kikérje az érintett hozzájárulását.

121. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy a megfelelőségi határozatban vezesse be a hozzájárulás bűnüldözési célú lehetséges használatára vonatkozó elemzését, amelyről a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv megfelelőségi határozattervezete rendelkezik**.

[74] Lásd a határozattervezet 37. oldalát.

4.1.1.2. Körözési parancsok és közlésre kötelezések

122. Bár az Európai Adatvédelmi Testületnek nincs észrevétele arra vonatkozóan, hogy a bizonyítékokat a körözési parancsok és általában a közlésre kötelezések révén visszakeresi, a határozattervezet (136) preambulumbekezdéséből az következik, hogy az Európai Bizottság a rendőrségre összpontosított a bűnüldözési hozzáférési megfontolások tekintetében, és hogy a személyes adatok más bűnüldöző szervek általi kezelését kevésbé vizsgálta meg.

123. Például az Egyesült Királyság megfelelőségi megbeszélésekre vonatkozó magyarázatának Bűnüldözés című, F. szakaszának[75] 11. oldala arra enged következtetni, hogy a **Nemzeti Bűnügyi Hivatal** (a továbbiakban: NCA) különösen fontos bűnüldözési ügynökség lehet, amelynek többek között szélesebb körű bűnügyi hírszerzési feladatköre van. Az NCA küldetését akként írja le, hogy a különböző forrásokból származó hírszerzési információkat egyesíti az elemzés, az értékelés és a taktikai lehetőségek maximalizálása érdekében, ideértve a kommunikáció technikai lehallgatásából, az egyesült királyságbeli és a tengerentúli bűnüldözési partnerektől, valamint a biztonsági és hírszerző ügynökségektől származó információkat[76]. Az NCA emellett a nemzetközi bűnüldözési partnerek egyik fő kapcsolattartója és kulcsszerepet tölt be a bűnüldözési operatív információk cseréjében[77].

124. Az Európai Adatvédelmi Testület tudomásul veszi továbbá azt a tényt, hogy a Kormányzati Kommunikációs Központ – amelynek tevékenységei jellemzően a 2018. évi adatvédelmi törvény 4. részének, azaz a nemzetbiztonságnak a hatálya alá tartoznak – aktív szerepet tölt be az Egyesült Királyságnak a súlyos és szervezett bűnözés által okozott társadalmi és pénzügyi károk csökkentésében, szorosan együttműködve a Belügyminisztériummal, az NCA-val, Őfelsége Adó és Vámhatóságával és más kormányzati szervekkel[78]. Tevékenységei a gyermekek szexuális zaklatása elleni küzdelemhez; a csaláshoz; a gazdasági bűnözés egyéb típusaihoz, ideértve a pénzmosást is; a technológia bűncselekményként való alkalmazásához; a kiberbűnözéshez; a bevándorlással

[75] Lásd az Egyesült Királyság magyarázatát a megfelelőségi megbeszélésekre, H. szakasz: Bűnüldözés, 2020. március 13., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

[76] Lásd a Nemzeti Bűnügyi Hivatal weboldalát, Hírszerzés: az Egyesült Királyságot érintő súlyos szervezett bűnözésről alkotott kép javítása, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk

[77] Bár az NCA által feldolgozott bűnüldözési hírszerzési információk nem mindegyike személyes adat, jelentős részük lehet személyes információ, és az itt ismertetett tevékenységek eltérhetnek a klasszikus rendészeti tevékenységektől, így az Egyesült Királyságban a bűnüldöző szervek személyes adatokhoz való hozzáférésének értékelése nem lenne teljes az NCA tevékenységeinek alapos értékelése nélkül. Észszerűnek tűnik annak biztosítása, hogy az adatvédelmi elveknek valamennyi érintett bűnüldöző szerv esetében azonos jelentést tulajdonítsanak, ezzel pontosítva a kifejezetten adatvezérelt szervek, például az NCA szerepét. Ezen túlmenően, a „jövőbe tekintés" kapcsán a magyarázat így folytatódik: *„[f]olyamatosan új lehetőségeket keresünk a hagyományos képességek gyűjtésére, fejlesztésére és továbbfejlesztésére, hogy növeljük az Egyesült Királyságban és külföldön egyaránt hasznosításra elérhető hírszerzési információk mennyiségét és minőségét."* *„Ennek részeként fejlesztjük az új nemzeti adathasznosítási képességet, felhasználva a bűncselekményekről és bíróságokról szóló törvény által a hivatalra ruházott hatásköröket, hogy a kormányzati kézben tárolt adatokat összekapcsoljuk, azokhoz hozzáférjünk és azokat felhasználjuk."* [...] *„Mindez növelni fogja gyorsaságunkat és rugalmasságunkat az új fenyegetésekre való reagálásban és a proaktív módon való működésben, a felmerülő fenyegetésekre vonatkozó információk és hírszerzési információk összegyűjtésében és elemzésében, hogy a fenyegetések valóra válása előtt cselekedhessünk*."

[78] Lásd a Kormányzati Kommunikációs Központ weboldalát, Küldetés, súlyos és szervezett bűnözés, https://www.gchq.gov.uk/section/mission/serious-crime

kapcsolatos szervezett bűnözéshez, beleértve az emberkereskedelmet is; valamint a kábítószerekhez, lőfegyverekhez és egyéb tiltott csempészéshez kapcsolódnak.

125. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy elemzését egészítse ki azon bűnüldözési területén tevékenykedő szervek elemzésével, amelyek napi működésének központi eleme az adatok – köztük a személyes adatok – gyűjtése és elemzése, ilyen különösen az NCA. Emellett az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy alaposabban vizsgálja meg azon szerveket, így a Kormányzati Kommunikációs Központot, amelyek tevékenysége egyszerre tartozik a bűnüldözés és a nemzetbiztonság körébe, valamint az azokra a személyesadat-kezelés tekintetében vonatkozó jogi keretet.**

4.1.1.3. Bűnüldözési célú nyomozati hatáskörök

126. Az általános adatvédelmi rendelettel kapcsolatos megfelelőségi referencia 4. fejezete („A **bűnüldözői** és nemzetbiztonsági szervek hozzáférésére vonatkozó lényeges garanciák a **harmadik országokban** az alapvető jogokba való beavatkozás korlátozása érdekében") szerint az Európai Adatvédelmi Testület emlékeztet arra, hogy *„[e] tekintetben a Bíróság kritikus módon megjegyezte, hogy a minimum mentesítési szabályra vonatkozó korábbi határozat »nem tartalmaz semmilyen megállapítást azzal kapcsolatban, hogy az Egyesült Államokban léteznek azon személyek alapvető jogaiba való esetleges beavatkozások korlátozására irányuló állami szabályok, akiknek az adatait az Unióból az Egyesült Államokba továbbítják, **e beavatkozásokat az állami szervek megengedik, amennyiben azok jogszerű célokat követnek**, mint például a nemzetbiztonság«"*[79]. E referenciában az Európai Adatvédelmi Testület kijelenti, hogy a megfelelőség érdekében **az adatokhoz való hozzáférés tekintetében négy európai alapvető garanciát**[80] **kell betartania minden harmadik országnak, legyen szó akár nemzetbiztonsági vagy bűnüldözési célokról**, és **különösen a jogszerű célokkal kapcsolatos szükségességet és arányosságot kell bizonyítani.**

127. A határozattervezet e szakaszában az Európai Bizottság megállapítja ((139) preambulumbekezdés), hogy *„mivel a nyomozati hatáskörökről szóló 2016. évi törvény által biztosított célzott nyomozati hatáskörök megegyeznek a nemzetbiztonsági ügynökségek rendelkezésére álló jogokkal, az említett hatáskörökre alkalmazandó feltételekkel, korlátozásokkal és garanciákkal a személyes adatokhoz az Egyesült Királyság hatóságai által nemzetbiztonsági célokból való hozzáférésről és azok felhasználásáról szóló szakasz részletesen foglalkozik*". Az EUB ítélkezési gyakorlatából azonban az következik, hogy amikor a szükségesség és az arányosság vizsgálatát a tagállamok azon jogszabályaira alkalmazzák, amelyek lehetővé teszik a személyes adatok hatóságok általi megőrzését és az azokhoz való hozzáférést, az olyan jogszerű célok, mint a nemzetbiztonság vagy a súlyos bűncselekmények elleni küzdelem eltérőek, és ezért egyes tagállamok megindokolhatnak bizonyos típusú beavatkozásokat, míg mások nem[81].

128. **Az Európai Adatvédelmi Testület ezért üdvözölné a (174) és az azt követő preambulumbekezdésekben ismertetett feltételek, korlátozások és garanciák szükségességének és arányosságának – azaz a nemzetbiztonsági célokat szolgáló intézkedéseknek szentelt szakasz – külön értékelését a szóban forgó feltételek, korlátozások és garanciák bűnüldözési célú intézkedéssel összefüggésben történő alkalmazása tekintetében. Ezért felkéri az Európai Bizottságot, hogy pontosítsa, hogy a személyes adatok megőrzése és bűnüldözési célú hozzáférése**

[79] Lásd: WP 254 rev.01, 9. o.
[80] Lásd az Európai Adatvédelmi Testület megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról szóló 02/2020. számú ajánlását.
[81] Lásd az EUB C-511/18., C-512/18. és C-520/18. számú, La Quadrature du Net és társai egyesített ügyekben 2020. október 6-án hozott ítéletét, ECLI:EU:C:2020:791.

kellően korlátozott-e ahhoz, hogy az EU-n belüli védelemmel lényegében megegyező szintű védelem biztosított legyen.

4.1.2. A bűnüldözési célokra gyűjtött információk további felhasználása ((140)–(154) preambulumbekezdés)

129. Az Európai Adatvédelmi Testület megjegyzi, hogy az Egyesült Királyság adatvédelmi kerete a bűnüldözési célból gyűjtött információk további felhasználására vonatkozóan az uniós jog által előírtakhoz hasonló garanciákat és korlátozásokat ír elő.

4.1.2.1. További felhasználás egyéb bűnüldözési célokra

130. A 2018. évi adatvédelmi törvény lehetővé teszi az illetékes hatóságok által bűnüldözési célból gyűjtött személyes adatok további feldolgozását (akár az eredeti adatkezelő vagy egy másik adatkezelő által) bármely más bűnüldözési célra, feltéve, hogy az adatkezelőt törvény felhatalmazza az adatok más célú kezelésére, és az adatkezelés szükséges és arányos az említett célra. Az Európai Bizottság megjegyzi, hogy a 2018. évi adatvédelmi törvény 3. részében előírt valamennyi garancia alkalmazandó az átvevő hatóság által végzett adatkezelésre. Az Európai Adatvédelmi Testület ugyanakkor kiemeli, hogy a 2018. évi adatvédelmi törvény 3. részében a 44. szakasz (4) bekezdése, a 45. szakasz (4) bekezdése, a 48. szakasz (3) bekezdése és a 68. szakasz (7) bekezdése lehetőséget biztosít az érintettek jogainak korlátozására, a 79. szakasz pedig lehetővé teszi olyan tanúsítványok kiállítását, amelyek igazolják, hogy a korlátozás a nemzetbiztonság védelméhez szükséges és arányos intézkedés. **Az Európai Adatvédelmi Testület ezért azt ajánlja, hogy az Európai Bizottság értékelje alaposabban az ilyen korlátozásoknak a személyes adatok védelmi szintjére gyakorolt lehetséges hatását az összegyűjtött információk további felhasználása tekintetében. Hasonlóképpen további pontosításra van szükség az ilyen további megosztást lehetővé tevő egyesült királyságbeli jogi kerettel, különösen a digitális gazdaságról szóló, 2017. évi törvénnyel, valamint a bűncselekményekről és a bíróságokról szóló, 2013. évi törvénnyel kapcsolatban is, amely lehetővé teszi az információknak az NCA-val való megosztását.**

4.1.2.2. Nem bűnüldözési célokra történő további felhasználás az Egyesült Királyságban

131. A 2018. évi adatvédelmi törvény továbbá előírja, hogy a bűnüldözési célokból gyűjtött személyes adatokat a bűnüldözés céljától eltérő célból is lehet kezelni, amennyiben az adatkezelést törvény engedélyezi. Ebben az esetben a megosztást engedélyező jogalap a terrorizmus elleni küzdelemről szóló, 2008. évi törvény 19. szakasza. E tekintetben az Európai Adatvédelmi Testület megjegyzi, hogy az Európai Bizottság értékelése nem foglalkozik teljes körűen a terrorizmus elleni küzdelemről szóló, 2008. évi törvény 19. szakasza hatályával és rendelkezéseivel, és ez jelentheti az adatok tágabb jellegű további felhasználását, különösen a 19. szakasz (2) bekezdését illetően, amely előírja, hogy „*minden hírszerző szolgálat felhasználhatja a bármely funkciójának gyakorlásával kapcsolatban megszerzett információkat e szolgálat bármely más funkciójának gyakorlásával kapcsolatban*”.

132. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az Európai Bizottság arra a tényre való hivatkozása, hogy az illetékes hatóságok olyan hatóságok, amelyeknek az EJEE-vel összhangban kell eljárniuk, ideértve annak 8. cikkét is, biztosítva ezáltal, hogy a bűnüldöző szervek és a hírszerző szolgálatok közötti valamennyi adatmegosztás megfeleljen az adatvédelmi jogszabályoknak és az EJEE-nek, jobban alátámasztható lenne, ha azonosítani lehetne az Egyesült Királyság jogrendje szerinti vonatkozó jogi aktusokat és jogszabályokat, amelyek egyértelműen és pontosan meghatározzák ezeket a korlátokat.

4.1.2.3. További felhasználás az Egyesült Királyságon kívülre történő további adattovábbítással összefüggésben

133. Míg az Európai Bizottság utalt arra, hogy az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodásnak hatása lehet az egyesült királyságbeli CSP-k által az Egyesült Államokba irányuló adattovábbításokra, az Európai Adatvédelmi Testület kiemeli továbbá, hogy e megállapodás hatálybalépése hatással lehet az Egyesült Királyság bűnüldöző hatóságaitól történő adattovábbítások során gyűjtött adatok további felhasználására is, különösen a végzéseknek az Egyesült Királyság és az Egyesült Államok közötti CLOUD Act megállapodás 5. cikke szerinti kiállítása és továbbítása tekintetében.

134. Az Európai Adatvédelmi Testület úgy véli továbbá, hogy a bűnüldözési együttműködés céljából harmadik országokkal kötendő jövőbeli olyan kétoldalú megállapodások, amelyek jogalapot biztosítanak a személyes adatok ezen országok részére történő továbbításához, szintén jelentősen érinthetik az összegyűjtött információk további felhasználásának feltételeit, mivel ezek a megállapodások befolyásolhatják az Egyesült Királyság értékelt adatvédelmi keretét. Az Európai Adatvédelmi Testület ezért azt ajánlja, hogy az Európai Bizottság vizsgálja meg alaposabban ezt a kérdést, és állapítsa meg, hogy léteznek-e ilyen nemzetközi megállapodások, valamit pontosítsa, hogy e megállapodások rendelkezései befolyásolhatják-e az Egyesült Királyság adatvédelmi jogának alkalmazását, és rendelkeznek-e további korlátozásról vagy kivételekről a bűnüldözési célból gyűjtött információk további felhasználása és közzététele tekintetében. Az Európai Adatvédelmi Testület megítélése szerint ezek az információk és értékelések elengedhetetlenek ahhoz, hogy elvégezhető legyen az Egyesült Királyság jogszabályi kerete és gyakorlata által a tengerentúli közlésekkel és további felhasználással kapcsolatban nyújtott védelem szintjének átfogó értékelése.

4.1.3. Felügyelet

135. Az Európai Adatvédelmi Testület megjegyzi, hogy a bűnüldöző hatóságok felügyeletéről az Információs Biztos Hivatala mellett különböző biztosok együttesen gondoskodnak. A megfelelőségi megállapítások tervezete megemlíti az IPC-t, a biometrikus anyagok megőrzéséért és felhasználásáért felelős biztost, valamint a térfigyelő kamerák biztosát. Ezzel összefüggésben meg kell jegyezni, hogy az EUB ismételten kihangsúlyozta a független felügyelet szükségességét. Különösen fontos az IPC az Egyesült Királyságba továbbított személyes adatokhoz való hozzáféréssel kapcsolatos kérdésekben. Az Európai Adatvédelmi Testület úgy értelmezi, hogy az IPC – más igazságügyi biztosokhoz – hasonlóan úgynevezett „igazságügyi biztos”, akit a nemzetbiztonságról szóló fejezettel összefüggésben kell megemlíteni, és hogy ezen igazságügyi biztosok biztosi feladataik ellátásakor bírói függetlenséget élveznek. Az Európai Bizottság az IPC hivatalát illetően a határozattervezet (245) preambulumbekezdésében kifejti, hogy függetlenül, úgynevezett független testületként működik, noha a Belügyminisztérium finanszírozza.

136. Az Európai Adatvédelmi Testület a határozattervezetben nem talált további utalást a biometrikus anyagok megőrzéséért és felhasználásáért felelős biztos, valamint a térfigyelő kamerák biztosa függetlenségének értékelésére.

137. **Felkérjük az Európai Bizottságot, hogy értékelje részletesebben az igazságügyi biztosok függetlenségét, ideértve azokat az eseteket is, amikor a biztos (már) nem bírói hivatalt tölt be, valamint értékelje a biometrikus anyagok megőrzéséért és felhasználásáért felelős biztos és a térfigyelő kamerák biztosa függetlenségét.**

4.2. Az adatvédelem általános jogi kerete a nemzetbiztonság területén

4.2.1. Nemzetbiztonsági tanúsítványok

138. A 2018. évi adatvédelmi törvény 111. szakasza szerint az adatkezelők kérelmezhetnek a miniszter, a kabinet tagja, a főügyész vagy a skóciai főügyész által kiállított nemzetbiztonsági tanúsítványokat, amelyek igazolják, hogy a 2018. évi adatvédelmi törvény 4–6. részében foglalt kötelezettségek és jogok alóli mentesség a nemzetbiztonság védelméhez szükséges és arányos intézkedésnek minősül. E tanúsítványok célja, hogy az adatkezelők számára nagyobb jogbiztonságot nyújtsanak, és döntő bizonyítékot szolgáltatnak arra vonatkozóan, hogy a személyes adatok kezelése során a nemzetbiztonság irányadó. Meg kell azonban említeni, hogy ezekre a tanúsítványokra nem azért van szükség, hogy a nemzetbiztonsági mentességekre lehessen hagyatkozni, hanem átláthatósági mércét jelentenek[82].

139. Az Európai Adatvédelmi Testület a 2018. évi adatvédelmi törvény 20. mellékletének 17. és 18. pontját úgy értelmezi, hogy az 1998. évi adatvédelmi törvény alapján kiállított nemzetbiztonsági tanúsítvány (a továbbiakban: korábbi tanúsítvány) 2019. május 25-ig kiterjedt a személyes adatoknak a 2018. évi adatvédelmi törvény szerinti kezelésére. Addig az időpontig lecserélés vagy visszavonás kivételével a korábbi tanúsítványokat úgy kezelték, mintha azokat a 2018. évi adatvédelmi törvény szerint állították volna ki.

140. Amennyiben azonban az 1998. évi adatvédelmi törvény alapján kiállított nemzetbiztonsági tanúsítványnak nincs kifejezett lejárati ideje, az Európai Adatvédelmi Testület értelmezése szerint az ilyen tanúsítvány az 1998. évi adatvédelmi törvény szerinti adatkezelés tekintetében továbbra is hatályban marad, kivéve, ha a tanúsítványt visszavonják vagy megsemmisítik[83]. Bár az e korábbi tanúsítványok által biztosított védelem az 1998. évi adatvédelmi törvény szerinti személyesadat-kezelésre korlátozódik, az Európai Adatvédelmi Testület tudomásul veszi, hogy az 1998. évi adatvédelmi törvény alapján új nemzetbiztonsági tanúsítványok állíthatók ki az 1998. évi adatvédelmi törvény alapján kezelt személyes adatok tekintetében[84].

141. **A teljesség érdekében az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy határozattervezetében tegye egyértelművé, hogy nemzeti biztonsági tanúsítványok továbbra is kiállíthatók az 1998. évi adatvédelmi törvény alapján. Az Európai Adatvédelmi Testület felkéri továbbá az Európai Bizottságot, hogy határozattervezetében ismertesse az 1998. évi adatvédelmi törvény alapján kiadott tanúsítványokra vonatkozó jogorvoslati és felügyeleti mechanizmusokat. Végezetül az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy határozattervezetébe foglalja bele az 1998. évi adatvédelmi törvény alapján kiadott meglévő tanúsítványok számát, és gondosan kövesse nyomon ezt a szempontot.**

---

[82] Lásd: Egyesült Királyság Belügyminisztériuma, a 2018. évi adatvédelmi törvény, Nemzetbiztonsági tanúsítványokról szóló útmutató, 2020. augusztus, 4. pont, 3. o., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

[83] Lásd: Egyesült Királyság Belügyminisztériuma, a 2018. évi adatvédelmi törvény, Nemzetbiztonsági tanúsítványokról szóló útmutató, 2020. augusztus, 5. o.

[84] Lásd: Egyesült Királyság Belügyminisztériuma, a 2018. évi adatvédelmi törvény, Nemzetbiztonsági tanúsítványokról szóló útmutató, 2020. augusztus, 8. pont, 5. o.

4.2.2. A helyesbítéshez és törléshez való jog

142. Ami a helyesbítéshez és törléshez való jogot illeti, az Európai Adatvédelmi Testület tudomásul veszi, hogy a 2018. évi adatvédelmi törvény 100. és 149. szakasza értelmében az érintetteknek lehetőségük van arra, hogy a Legfelsőbb Bírósághoz (High Court) (Skóciában a Court of Session) forduljanak annak érdekében, hogy az adatkezelőt kötelezzék adataik indokolatlan késedelem nélküli helyesbítésére vagy törlésére.

143. **Az Európai Adatvédelmi Testület hangsúlyozza, hogy hatékonyan biztosítani kell az érintettek jogainak gyakorlását; ezért felkéri az Európai Bizottságot, hogy határozattervezetében ismertesse, hogy a 2018. évi adatvédelmi törvény 100. szakasza miként működik a gyakorlatban, és szorosan kövesse nyomon e szakasz alkalmazását.**

4.2.3. Nemzetbiztonsági kivételek

144. Az Európai Adatvédelmi Testület fel kívánja hívni a figyelmet a 2018. évi adatvédelmi törvény 110. szakaszára és különösen 11. mellékletére, amely meghatározza azokat a konkrét célokat, amelyek érdekében a hírszerző szolgálatok eltérhetnek bizonyos adatvédelmi elvektől, többek között az érintettek jogaival kapcsolatban, és nem kötelesek tájékoztatni az Információs Biztos Hivatalát az adatvédelmi incidensekről.[85]

145. Az **Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy pontosítsa részletesebben a kivételek alkalmazási körét, mivel nem biztos benne, hogy a 2018. évi adatvédelmi törvény 11. mellékletében foglalt valamennyi kivétel releváns-e a hírszerző szolgálatok munkája szempontjából, és hogy azok biztosítják-e a szükségesség és arányosság elvével való egyenértékűséget**. Az **Európai Adatvédelmi Testület különösen arra kéri az Európai Bizottságot, hogy adjon pontosabb tájékoztatást arról, hogy egy hírszerző szolgálat milyen körülmények között támaszkodhat a 2018. évi adatvédelmi törvény 11. mellékletének 10. szakaszára, amely kimondja, hogy *„[a] felsorolt rendelkezések nem alkalmazandók az adatkezelőnek az érintettel folytatott tárgyalásokkal kapcsolatos szándékairól készült feljegyzésekből álló személyes adatokra, amennyiben a felsorolt rendelkezések alkalmazása valószínűleg sértené a tárgyalásokat*”.**

4.3. Az egyesült királyságbeli közigazgatási szervek hozzáférése az adatokhoz és az adatok használata nemzetbiztonsági célokból

146. Általános megjegyzésként az Európai Adatvédelmi Testület elismeri, hogy az államok széles mérlegelési jogkörrel rendelkeznek nemzetbiztonsági kérdésekben, amit az EJEB is elismer. Az Európai Adatvédelmi Testület emlékeztet továbbá arra, hogy – amint azt a felügyeleti intézkedésekre vonatkozó alapvető európai garanciákról szóló aktualizált ajánlásai is kiemelik[86] –, az Európai Unióról szóló szerződés 6. cikkének (3) bekezdése kimondja, hogy az EJEE-ben rögzített alapvető jogok az uniós jog általános elveit képezik. Amint azonban az EUB ítélkezési gyakorlatában emlékeztet rá, ez utóbbi – mindaddig, amíg az EU nem csatlakozott hozzá – nem minősül olyan jogi eszköznek, amely

[85] E célok a következők lehetnek: a „bűncselekmények” megelőzése és feltárása, „a jog szerint vagy jogi eljárásokkal kapcsolatban közzéteendő információk”, a „parlamenti kiváltság”, a „bírósági eljárások”, „a korona becsülete és méltósága”, a „fegyveres erők”, a „gazdasági jólét”, az „ügyvédi titoktartási kötelezettség”, a „tárgyalások”, az „adatkezelő által megadott bizalmas referenciák”, a „vizsgafeladatok és jegyek”, a „kutatás és statisztika”, valamint a „közérdekű archiválás”.

[86] Lásd az Európai Adatvédelmi Testület megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról szóló 02/2020. számú ajánlását.

hivatalosan be van építve az uniós jogba[87]. Így az alapvető jogoknak az általános adatvédelmi rendelet 45. cikkében előírt védelmi szintjét az e rendeletnek az Alapjogi Chartában rögzített alapvető jogokra tekintettel értelmezett rendelkezései alapján kell meghatározni. Mindemellett az EU Alapjogi Chartája 52. cikkének (3) bekezdése szerint az abban foglalt jogoknak, amelyek megfelelnek az EJEE által biztosított jogoknak, ugyanazzal a jelentéssel és hatállyal kell rendelkezniük, mint az EJEE-ben rögzített jogoknak. Következésképpen, amint arra az EUB emlékeztetett, az EJEB-nek az uniós Chartában is szereplő jogokra vonatkozó ítélkezési gyakorlatát az uniós Chartában foglalt megfelelő jogok értelmezéséhez szükséges minimális védelmi szintként kell figyelembe venni[88]. Az EU Alapjogi Chartája 52. cikke (3) bekezdésének utolsó mondata szerint azonban „*[e]z a rendelkezés nem akadályozza meg azt, hogy az Unió joga kiterjedtebb védelmet nyújtson*”.

147. Ezért a következő értékelés során az Európai Adatvédelmi Testület figyelembe vette az EJEB ítélkezési gyakorlatát, amennyiben az EU Alapjogi Chartája az EUB értelmezése szerint nem rendelkezik olyan magasabb szintű védelemről, amely az EJEB ítélkezési gyakorlatán kívül más követelményeket írna elő.

4.3.1. Jogalapok, korlátozások és garanciák – A nemzetbiztonsággal összefüggésben gyakorolt nyomozati hatáskörök

4.3.1.1. Általános megjegyzések

148. Az Európai Adatvédelmi Testület emlékeztet arra, hogy a nyomozati hatáskörökről szóló, 2016. évi törvény közelmúltbeli törvény, amely módosította a hírszerző szolgálatokról szóló 1994. évi törvény több rendelkezését. Meghatározza, hogy bizonyos vizsgálati jogkörök milyen mértékben használhatók fel a magánéletbe való beavatkozásra[89]. Az IPC két jelentése ellenére, amelyek hasznos információkkal szolgálnak ezen új jogi keret alkalmazásával kapcsolatban, még mindig nem került sor bizonyos szempontok felülvizsgálatára, különösen az alkalmazott választók és keresési kritériumok tekintetében.

149. Emellett az Európai Adatvédelmi Testület a nyomozati hatáskörökről szóló, 2016. évi törvényre és annak alkalmazási körére vonatkozó általános megjegyzésként a következő négy pontot emeli ki:

150. Ami az **első pontot** illeti, a jog jellegzetességeit illetően az Európai Adatvédelmi Testület két szempontot kíván hangsúlyozni:

151. Először is, az Európai Adatvédelmi Testület megjegyzi, hogy a jogszabály a nyomozati hatáskörökről szóló, 2016. évi törvényben előírt eljárások alkalmazásának tág céljaira hivatkozik, nem pedig azon személyek kategóriáira, akiket a nyomozati hatáskörökről szóló, 2016. évi törvény 2–7. része alapján érinthet az adatgyűjtés. E tekintetben az Európai Adatvédelmi Testület emlékeztet arra, hogy kapcsolatnak kell fennállnia azon személyek kategóriái között, akikre felügyeleti intézkedések vonatkozhatnak, valamint a jogszabály által követett, a törvény személyi hatályának meghatározására irányuló célok között.

152. Az Európai Adatvédelmi Testület továbbá hangsúlyozza, hogy a „távközlési szolgáltatók”, a „távközlési szolgáltatás” és a „távközlési rendszer” fogalommeghatározása, amely meghatározza a törvény hatályát, szintén igen tág és bizonyos mértékben nem egyértelmű. Az Európai Adatvédelmi Testület kiemeli, hogy ezeket a fogalmakat a nyomozati hatáskörökről szóló 2016. évi törvény

[87] Lásd: Schrems II-ügy, 98. pont.
[88] Lásd az EUB C-511/18., a C-512/18. és a C-520/18. sz., La Quadrature du Net és társai egyesített ügyekben 2020. október 6-án hozott ítélet (ECLI:EU:C:2020:791) 124. pontját.
[89] Lásd a nyomozati hatáskörökről szóló, 2016. évi törvény 1. szakaszát.

területén sokkal tágabban kell értelmezni, mint a távközlési jogszabályokban, például az Európai Elektronikus Hírközlési Kódexben meghatározottak szerint[90]. Az Európai Adatvédelmi Testület megjegyzi, hogy a „távközlési szolgáltatásnak" és a „távközlési rendszernek" a törvényben szereplő meghatározásai szándékosan tágak, hogy továbbra is relevánsak maradjanak az új technológiák szempontjából. Hasonlóképpen a „távközlési szolgáltató" fogalommeghatározása is nagyon tág, és magában foglalhatja például a csevegőfunkcióval rendelkező online videojátékokat, vagy az ilyen csevegőablakokat tartalmazó egyéb online weboldalakat[91].

153. Ezenkívül, míg az adatgyűjtés és az adatokhoz való hozzáférés szükségességének és arányosságának értékelésére vonatkozó eljárások és felügyelet általában rendelkezésre állnak, az ilyen értékelés elvégzésének kritériumait maga a törvény nem határozza meg. További elemek találhatók más dokumentumokban, például a gyakorlati kódexekben.

154. Amint azonban az Európai Adatvédelmi Testületnek a megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról szóló, 02/2020. sz. ajánlásaiban is szerepel, az EUB kiemelte, hogy „*az a követelmény, miszerint e jog gyakorlása csak a törvény által korlátozható, magában foglalja, hogy a beavatkozást lehetővé tevő jogalapnak magának kell meghatároznia az érintett jog gyakorlásával kapcsolatos korlátozás terjedelmét*"[92]. Pontosabban az EUB tisztázta, hogy „*[a]z arányosság követelményének való megfelelés érdekében a szabályozásnak egyértelmű és pontos szabályokat kell tartalmaznia a szóban forgó intézkedés hatálya és alkalmazása tekintetében, és minimumkövetelményeket kell előírnia, oly módon, hogy azok a személyek, akiknek az adatait továbbították, elegendő garanciákkal rendelkezzenek, amelyek lehetővé teszik a személyes adataiknak a visszaélések veszélyeivel szembeni hatékony védelmét. E szabályozásnak a nemzeti jog szerint jogilag kötelező erejűnek kell lennie, és meg kell jelölnie különösen, hogy milyen körülmények között és milyen feltételek mellett lehet az ilyen adatok kezelését előíró intézkedést megtenni, biztosítva ezáltal, hogy a beavatkozás a szigorúan szükséges mértékre korlátozódjék.*"[93]

155. Az EJEB hangsúlyozta továbbá a jog egyértelműségének fontosságát annak érdekében, hogy az egyének „*megfelelő tájékoztatást kapjanak arról, hogy a közigazgatási szervek milyen körülmények között és milyen feltételek mellett jogosultak ilyen intézkedésekhez folyamodni*"[94].

156. **Az Európai Adatvédelmi Testület ezért felszólítja az Európai Bizottságot, hogy értékelje alaposabban a vonatkozó jogszabály pontosságával, egyértelműségével és teljeskörűségével kapcsolatos szempontokat, és nyújtson be további elemeket annak bizonyítására, hogy az a jogi**

---

[90] Lásd az Európai Elektronikus Hírközlési Kódex 2. cikkének 5. bekezdését, amely például úgy határozza meg a „személyközi hírközlési szolgáltatást", mint „*olyan, általában díjazás ellenében nyújtott szolgáltatás, amely elektronikus hírközlő hálózatokon keresztül lehetővé teszi a véges számú személy közötti közvetlen személyközi, interaktív információcserét, és amelyben a kommunikációt kezdeményező vagy abban részt vevő személyek határozzák meg a fogadó(ka)t, továbbá amely nem foglalja magában az olyan szolgáltatásokat, amelyek csupán egy másik szolgáltatáshoz szorosan kapcsolódó, csekély jelentőségű kiegészítő funkcióként teszik lehetővé a személyközi, interaktív kommunikációt*".

[91] Lásd brit Belügyminisztérium, A közlések lehallgatására vonatkozó gyakorlati kódex, 2018. március, 2.5. és azt követő pontok, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

[92] Lásd: Schrems II-ügy, 175. pont; és a hivatkozott ítélkezési gyakorlat, valamint az EUB C-623/17. sz., Privacy International kontra Secretary of State for Foreign and Commonwealth Affairs és társai ügyben 2020. október 6-án hozott ítéletének (ECLI:EU:C:2020:790, a továbbiakban: Privacy International ügy) 65. pontja.

[93] Lásd: Privacy International ügy, 68. pont.

[94] Lásd: EJEB, Zakharov kontra Oroszország, 2015. december 4., CE:ECHR:2015:1204JUD004714306, 229. pont.

jellemzők tekintetében az EU-ban biztosított védelemmel lényegében megegyező védelmet nyújt. Az Európai Adatvédelmi Testület azt is hangsúlyozza, hogy a tág fogalommeghatározásokat a lehallgatási intézkedések arányossága szempontjából is értékelni kell.

157. Ezen túlmenően, bár az illetékes hírszerzési közösségi hatóságok több belső kódexe részben továbbfejleszti ezen elemek némelyikét, például az adatgyűjtés szükségességének és arányosságának értékelését illetően, az Európai Adatvédelmi Testület hangsúlyozza, hogy az Európai Unió Bíróságának a jog jellegével kapcsolatos követelményei magukban foglalják, hogy az alapvető elemeket – többek között azt, hogy az egyének a jogorvoslat keretében hivatkozhassanak rájuk – a keresettel megtámadható jogokat előíró jogszabályokban kell meghatározni[95]. A nyomozati hatáskörökről szóló 2016. évi törvény 7. mellékletének 6. bekezdése megemlíti azt a tényt, hogy a bíróságok (és a felügyeleti hatóságok) *„figyelembe veszik, hogy valamely személy figyelmen kívül hagyja a kódexet az ilyen eljárások során egy kérdés meghatározása tekintetében*", azonban nem tisztázza, hogy az egyének hivatkozhatnak-e a kódex megsértésére a bíróságok (vagy a felügyeleti hatóságok) előtt. Ezenkívül a határozattervezetben eddig szereplő elemek vagy arra hivatkoznak, hogy az EJEB elismerte az e kódexekben foglalt szabályok előreláthatóságát[96], és nem arra, hogy az EUB által előírtak szerint a bíróság előtt „megtámadhatók"-e, vagy arra a tényre, hogy az Egyesült Királyság bíróságai néhány esetben kódexekre hivatkoztak, míg az említett ügyek egyike sem szemlélteti azt a lehetőséget, hogy az egyének felléphetnek a kódexekből eredő jogokkal szemben. **Amennyiben megállapítást nyer, hogy az Egyesült Királyság joga nem jelöli meg kellőképpen azokat a körülményeket és feltételeket, amelyek mellett egy intézkedést el lehet fogadni, és hogy ezeket az elemeket valójában a Hírszerző Közösség hatóságainak belső szabályzatai írják elő, az Európai Adatvédelmi Testület felkéri az Európai Bizottságot annak további értékelésére, hogy az egyének bíróság előtt felléphetnek-e a Hírszerzési Közösség hatóságainak különböző belső szabályzataiban foglalt korlátozásokkal és garanciákkal szemben, és azokat végre is hajthatják-e.**

158. A **második, figyelmet igénylő kérdés** arra a tényre vonatkozik, hogy egyrészt a kommunikációs adatok célzott megszerzésére és megőrzésére, másrészt a tömeges adatgyűjtésre vonatkozó rendelkezések – akár a nyomozati hatáskörökről szóló, 2016. évi törvényben, akár más jogszabályokban, például a hírszerző szolgálatokról szóló, 1994. évi törvényben vagy a nyomozati hatáskörök szabályozásáról szóló, 2000. évi törvényben – alkalmazandók lesznek az EU-ból az Egyesült Királyságba továbbított adatokra is. A tömeges adatgyűjtést illetően az Európai Adatvédelmi Testület hangsúlyozza, hogy az Egyesült Királyság jogának vonatkozó rendelkezései lehetővé teszik az Egyesült Királyságon kívüli adatgyűjtést; ami magában foglalja a megfelelőségi határozat alapján az EGT-ből az Egyesült Királyságba továbbított, átvitel alatt lévő adatokat is[97]. Ezenkívül az Európai Adatvédelmi Testület megemlíti, hogy az Európai Bizottság szerint *„[m]eg kell jegyezni, hogy a kommunikációs adatok megőrzése és gyűjtése általában nem uniós érintettek e határozat alapján az Egyesült Királyságba továbbított személyes adataira irányul. A kommunikációs adatok megőrzésére*

[95] E tekintetben az EUB például úgy ítélte meg, hogy a PPD 28 az Egyesült Államokban nem minősült megfelelőnek, bár a tömeges gyűjtés tekintetében is tartalmazott bizonyos korlátozásokat, lásd a Schrems II-ügyben hozott ítélet 181. pontját.

[96] Lásd: EJEB, Big Brother Watch és társai kontra Egyesült Királyság, 2018. szeptember 13., ECLI:ECHR:2018:0913JUD005817013 (a továbbiakban: Big Brother Watch ügy), 325. pont: *„Mivel az információs biztos kódexe nyilvános dokumentum, amelyet a Parlament mindkét háza jóváhagyott, és amelyet mind a lehallgatási feladatokat ellátók, mind a bíróságok figyelembe vesznek, a Bíróság kifejezetten elfogadta, hogy rendelkezéseit figyelembe lehet venni a nyomozati hatáskörök szabályozásáról szóló törvény szerinti rendszer előreláthatóságának értékelésekor*".

[97] Lásd a Schrems II. 183. és azt követő pontjait az EU és egy harmadik ország közötti, átvitel alatt lévő adatokhoz való hozzáférést előíró jogszabály megfelelőségi határozat keretében történő értékeléséről.

vagy közlésére vonatkozó kötelezettség a nyomozati hatáskörökről szóló, 2016. évi törvény 3. és 4. része szerint azokra az adatokra terjed ki, amelyeket az Egyesült Királyság telekommunikációs szolgáltatói közvetlenül a távközlési szolgáltatás felhasználóitól gyűjtenek"[98]. Mindazonáltal az Európai Adatvédelmi Testület kiemeli az egyértelműség hiányát azzal a ténnyel kapcsolatban, hogy kizárólag az Egyesült Királyságban található szolgáltatók telephelyei kaphatnak tájékoztatást az Egyesült Királyság illetékes hatóságaitól, mivel a távközlési szolgáltatónak a nyomozati hatáskörökről szóló 2016. évi törvény 261. szakaszának (10) bekezdésében szereplő meghatározása megköveteli, hogy a „távközlési szolgáltató olyan személy" legyen, „aki távközlési szolgáltatást kínál vagy nyújt az Egyesült Királyságban tartózkodó személyeknek, vagy *olyan távközlési rendszert irányít vagy biztosít, amely (teljes egészében vagy részben) az Egyesült Királyságban található, vagy amelyet onnan irányítanak*". Következésképpen az EGT-beli érintettek személyes adatai ténylegesen érintettek lehetnek, például egy egyesült királyságbeli távközlési szolgáltató EGT-n belüli telephelye által gyűjtött vagy generált adatok esetében, amelyeket ugyanannak a szolgáltatónak az Egyesült Királyságban található telephelyére továbbítanak a megfelelőségi határozat alapján (kereskedelmi célból), majd az Egyesült Királyságban az illetékes hatóságok gyűjtik őket.

159. **Az Európai Adatvédelmi Testület ezért azon a véleményen van, hogy e rendelkezések értékelése az Egyesült Királyság jogi kerete megfelelőségének értékelése szempontjából is releváns, és felszólítja az Európai Bizottságot, hogy tisztázza ezt a szempontot, és értékelje alaposabban ennek mértékét. Az Európai Adatvédelmi Testület különösen arra kéri az Európai Bizottságot, hogy tisztázza e jogszabály alkalmazási körét, beleértve azt is, hogy mit takar a „távközlési szolgáltatások felhasználói" fogalma, és hogy be lehet-e kérni az Egyesült Királyságon kívüli távközlési szolgáltatóktól származó adatokat, amennyiben azok az EGT-beli érintettek adatait érintik, tekintettel a távközlési szolgáltatók igen tág meghatározására.**

160. A **harmadik, figyelemre méltó pont** a „kettős zárolási" eljárásra vonatkozik. Az Európai Adatvédelmi Testület megjegyzi, hogy a nyomozati hatáskörökről szóló, 2016. évi törvény új „kettős zárolási" eljárást vezetett be. Mindazonáltal az Európai Adatvédelmi Testület úgy értelmezi, hogy még ha elvben nemzetbiztonsági vagy hírszerzési célokból történő adatgyűjtésre vagy adathozzáférésre csak igazságügyi biztos által jóváhagyott engedély mellett kerülhet is sor, a nyomozati hatáskörökről szóló, 2016. évi törvény szerint „*meghatározott, korlátozott esetekben az engedély nélküli jogszerű lehallgatás lehetséges, és csak maguknak az illetékes hatóságoknak az előzetes engedélye szükséges [lásd lentebb a felügyeletről szóló szakaszt], többek között a tengerentúli megkeresésekkel összhangban történő lehallgatáshoz (a nyomozati hatáskörökről szóló, 2016. évi törvény 52. szakasza)*". Amint azt az alábbiakban kiemeltük, ez az Európai Adatvédelmi Testületnek különösen a tengerentúli közzétételekkel kapcsolatos aggályaival is összhangban áll. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy a berendezésekkel végzett beavatkozás – akár célzott, akár tömeges beavatkozás – esetében a kettős zárolási eljárástól való eltérés is lehetséges, és az igazságügyi biztos legfeljebb hat hónapos kezdeti időszakot követően csak a tömeges engedélyek megújítását hagyhatja jóvá. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot annak további értékelésére és bizonyítására, hogy az Egyesült Királyság jogi kerete – többek között az egyének számára biztosított hatékony utólagos felügyeleti és jogorvoslati lehetőségek révén – még azokban az esetekben is megfelelő garanciákat ír-e elő, amikor a kettős zárolási eljárás nem alkalmazandó, annak biztosítása érdekében, hogy a védelem szintje lényegében megegyező legyen az EU-n belül biztosított védelemmel (lásd még a felügyeletről szóló 4.3.3. szakaszt).**

[98] Lásd a határozattervezet (196) preambulumbekezdését.

161. Ezen túlmenően, bár a nyomozati hatáskörökről szóló, 2016. évi törvény valóban bevezette a „kettős zárolási” eljárást, az Európai Adatvédelmi Testület továbbra is aggályosnak tartja az új jogszabály bizonyos jellemzőit. A határozattervezet megfelelő szakaszainak bemutatását követően az Európai Adatvédelmi Testület az adatgyűjtés és az adatokhoz való hozzáférés alábbi típusait elemezte az Európai Bizottság által ismertetett sorrendben. Az alábbiakban értékelt elemek sorrendje ezért nem tükrözi az Európai Adatvédelmi Testület aggodalmának szintjét.

4.3.1.2. A kommunikációs adatok célzott beszerzése és megőrzése

162. Az Európai Adatvédelmi Testület megjegyzi, hogy két tisztviselő adhat célzott engedélyt a kommunikációs adatok megszerzésére: a kommunikációs adatok engedélyezésével foglalkozó hivatal engedélyezésre jogosult tisztviselője (a továbbiakban: IPC), egy kijelölt vezető tisztviselő (az érintett hatóságban meghatározott tisztséget vagy pozíciót betöltő személy) a bírói biztos jóváhagyása mellett bizonyos esetekben. Az Európai Adatvédelmi Testület számára azonban továbbra sem világos, hogy a törvény és a vonatkozó kódex szerint pontosan mely tisztviselő engedélyezi a kommunikációs adatok célzott megszerzésének melyik típusát, és hogy a kijelölt tisztviselő milyen mértékben lenne kellően független[99].

163. **Az Európai Adatvédelmi Testület ezért felszólítja az Európai Bizottságot, hogy értékelje alaposabban ezt a szempontot, és adjon világosabb magyarázatot ezekről az elemekről.**

164. A kommunikációs adatok megőrzését előíró értesítéssel kapcsolatban az Európai Adatvédelmi Testület azt is megjegyzi, hogy az ilyen értesítéseket „a szolgáltatók leírásának” lehet címezni. Úgy tűnik, hogy ez a fogalom azt jelenti, hogy egyszerre több szolgáltatótól is meg lehet követelni az adatok megőrzését. A beszerzés célzott jellege ugyanis nem a szolgáltatók számához, hanem a „célt képező” személyek, szervezetek, személyek helyének vagy csoportjának nevéhez vagy leírásához, a vizsgálat jellegének leírásához és azon tevékenységek leírásához kapcsolódik, amelyekre a berendezést használják. Az Európai Adatvédelmi Testület ezért kiemeli, hogy az ilyen „szolgáltatók leírása” által érintett gazdasági szereplők számától függően az értesítés szélesebb körű lehet, mint amit a célzott megőrzési eljárás sugallhat. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy értékelje alaposabban ezt a szempontot, és nyújtson további garanciákat arra vonatkozóan, hogy még akkor is, ha az értesítéseket több szolgáltatónak címezték, azok továbbra is a feltétlenül szükséges és arányos mértékre korlátozódnak.**

4.3.1.3. A berendezésekkel végzett beavatkozás

165. Az Európai Adatvédelmi Testület megjegyzi, hogy a „berendezésekkel végzett beavatkozás” sürgős esetben eltérhet a kettős zárolási eljárástól[100]. Az Európai Adatvédelmi Testület ezért aggodalmát fejezi ki amiatt, hogy a berendezésekkel végzett beavatkozás céljai széles körűek, és hogy a sürgősség kritériumai (amely esetben az igazságügyi biztosnak nem kell előzetes engedélyt adnia a berendezésekkel végzett beavatkozás szükségességének és arányosságának értékelését követően) továbbra sem egyértelműek. Mivel ez utóbbi esetben „az engedély már nem érvényes és nem hosszabbodik meg” abban az esetben, ha az igazságügyi biztos utólag nem hagyja jóvá a berendezésekkel végzett beavatkozást, az Európai Adatvédelmi Testület úgy értelmezi, hogy az időközben gyűjtött adatok jogszerűen gyűjtött adatok maradnak. Ezen adatok törlése érdekében az igazságügyi biztos külön végzést adhat ki[101].

[99] Lásd még a kettős zárolási eljárás és az igazságügyi biztos függetlenségének értékelését.
[100] Lásd a nyomozati hatáskörökről szóló, 2016. évi törvény 109. szakaszát.
[101] Lásd a nyomozati hatáskörökről szóló, 2016. évi törvény 110. szakasza 3. alszakaszának b) pontját.

166. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy értékelje alaposabban azokat a feltételeket, amelyek mellett a sürgősségre lehet hivatkozni, és adjon felvilágosítást arról, hogy az érintettek milyen lehetséges módokon gyakorolhatják jogaikat, és milyen jogorvoslati lehetőségek állnak a rendelkezésükre a berendezésekkel végzett beavatkozási műveletekkel összefüggésben, különösen ha azokra a kettős zárolási eljárástól való eltéréshez vezető sürgősségi körülmények között kerül sor.**

4.3.1.4. A hordozóktól származó adatok tömeges lehallgatása

167. Ahogyan a tömeges hatáskörök felülvizsgálatáról szóló jelentésben[102] szerepel, „*[a] tömeges lehallgatás jellemzően a kommunikációs adatoknak az egyes hordozók közötti átvitel során történő gyűjtését foglalja magában (kommunikációs összeköttetések)*". A nyomozati hatáskörökről szóló, 2016. évi törvény szerinti hivatalos adatlap úgy írja le a „tömeges lehallgatást", mint „*bizonyos mennyiségű kommunikációs adat összegyűjtésének folyamatát, amelyek közül konkrét kommunikációs adatok kiválasztására kerül sor, amelyeket el kell olvasni, meg kell vizsgálni vagy meg kell hallgatni, amennyiben ez szükséges és arányos*". Az Európai Adatvédelmi Testület megjegyzi, hogy az adatok „tömeges lehallgatása" valójában az adatok gyűjtését jelenti a válogatók szerinti szűrés előtt (vagy egyszerű a már ismerten veszélyt jelentő személyek nyomon követése, vagy pedig összetett az új fenyegetések és a korábban nem ismert célszemélyek azonosítása esetén).

168. A tömeges kommunikációs adatok beszerzése szintén az egyik olyan kérdés volt, amelyet az EUB megvizsgált a Privacy International ügyben, aminek eredményeként a nagytanács 2020. október 6-án ítéletet hozott (annak megállapítása mellett, hogy az ilyen adatgyűjtésre akár nemzetbiztonsági célokból is sor került-e az uniós joggal összefüggésben). A nyomozati hatáskörökről szóló, 2016. évi törvény felváltotta a jelen ítélet tárgyát képező jogszabályt.

169. Az Európai Adatvédelmi Testület megjegyzi, hogy a nyomozati hatáskörökről szóló, 2016. évi törvény brit jogba való bevezetésével immár engedélyre van szükség az adatok tömeges lehallgatásához is. Ezen engedély kibocsátásának folyamata az „operatív célok" meghatározásán alapul. Ezen operatív célok listáját a hírszerző szolgálatok vezetői állítják össze, majd a külügyminiszter hagyja jóvá. Ezt a határozatot egy független igazságügyi biztos hagyja jóvá, akinek meg kell vizsgálnia, hogy az engedély szükséges-e és arányos-e az operatív célokkal. Az Európai Adatvédelmi Testület úgy értelmezi, hogy az igazságügyi biztos nem rendelkezik hatáskörrel arra, hogy magukat az operatív célokat értékelje, de hatásköre kiterjed annak vizsgálatára, hogy az engedély szükséges-e és az abban felsorolt operatív célokkal arányos-e. A Parlament Hírszerzési és Biztonsági Bizottsága háromhavonta megkapja a jegyzék egy példányát, és a miniszterelnök évente legalább egyszer felülvizsgálja ezen operatív célok listáját.

170. Az Európai Bizottság által a határozattervezetben megadott elemek alapján azonban nehéznek tűnik értékelni a listán szereplő ezen operatív célok körét, valamint azt, hogy az általuk lehetővé tett adatgyűjtés megfelel-e az EUB által meghatározott küszöbértéknek (például az adatgyűjtés földrajzi területe akár néhány utcára is korlátozódhat, azonban kiterjedhet az EGT egészéből származó adatok gyűjtésére).

171. Az Európai Adatvédelmi Testület hangsúlyozza továbbá, hogy a tömegesen gyűjtött adatokat hosszú ideig meg lehet őrizni (vizsgálat céljából való további hozzáférés érdekében). Az Európai Adatvédelmi Testület megjegyzi, hogy a nyomozati hatáskörökről szóló, 2016. évi törvény 150. szakaszának (5) és (6) bekezdése csak a gyűjtött adatok másolatainak megsemmisítését írja elő, és csak akkor, ha azok

[102] Lásd a tömeges hatáskörök felülvizsgálatáról szóló jelentést, Independent Review of Terrorism Legislation (a terrorizmus elleni küzdelemről szóló jogszabályok független felülvizsgálója), 2016. augusztus.

megőrzése nemzetbiztonsági okokból vagy a nyomozati hatáskörökről szóló, 2016. évi törvény 138. szakasza (2) bekezdésének hatálya alá tartozó bármely más okból nem szükséges vagy valószínűleg nem válik szükségessé, vagy ha a megőrzés több más célból nem szükséges[103]. Az Európai Adatvédelmi Testület hangsúlyozza, hogy ezek az indokok igen széles körűnek tűnnek, és csak a megszerzett adatok másolatai vannak megemlítve.

172. Az Európai Adatvédelmi Testület azt is megjegyzi, hogy sürgős esetekben a nyomozati hatáskörökről szóló, 2016. évi törvény lehetővé teszi az engedélyek igazságügyi biztos előzetes jóváhagyása nélküli módosítását is, és ebben az esetben, ha a megkérdezett igazságügyi biztos a módosítást követő három munkanapon belül utólag megtagadja a módosítás jóváhagyását, az engedélynek úgy kell érvényben maradnia, mintha a módosításra nem került volna sor, azonban az időközben gyűjtött adatok jogszerűen gyűjtött adatok maradnak[104]. Ezen adatok törlése érdekében az igazságügyi biztos külön végzést adhat ki[105].

173. **Az Európai Adatvédelmi Testület felszólítja az Európai Bizottságot a tömeges lehallgatások további tisztázására és értékelésére, különösen a tömeges lehallgatási eljárásokkal összefüggésben a válogatók kiválasztása és alkalmazása tekintetében annak tisztázása érdekében, hogy a személyes adatokhoz való hozzáférés milyen mértékben éri el az EUB által meghatározott küszöbértéket (lásd az alábbi 4.3.1.7. szakaszt, különösen a válogatók felügyeletével kapcsolatban), és milyen garanciák vannak érvényben az olyan egyének alapvető jogainak védelme érdekében, akiknek az adatait ebben az összefüggésben lefoglalták, többek közt az adatmegőrzési idővel kapcsolatban is. Különösen hasznos lenne az Egyesült Királyság illetékes felügyeleti hatóságainak független értékelése.**

174. **Az Európai Adatvédelmi Testület azt is hangsúlyozza, hogy annál is fontosabbnak tűnik, hogy a tömeges lehallgatási gyakorlatok körébe tartozó „tengerentúli kommunikáció" azt sugallja, hogy az Egyesült Királyság az EGT-n belül közvetlenül feltartóztathatja és tömegesen összegyűjtheti az adatokat, ideértve az EGT és az Egyesült Királyság közötti, átvitel alatt lévő adatokat is, amelyek a határozattervezet hatálya alá tartoznának (lásd az alábbi 4.3.2. szakaszt a nemzetbiztonsági célokból és tengerentúli közzététel céljából gyűjtött adatok további használatáról).**

4.3.1.5. A másodlagos adatok védelme és az azokra vonatkozó garanciák

175. Az Európai Adatvédelmi Testület aggodalmát fejezi ki továbbá amiatt, hogy a tömeges lehallgatásra vonatkozó egyesült királyságbeli jogszabályok nem biztosítanak azonos szintű védelmet valamennyi kommunikációs adat számára. A tömeges engedéllyel megszerezhető „másodlagos adatok" a nyomozati hatáskörökről szóló, 2016. évi törvény 137. szakaszával összhangban magukban foglalják a „rendszeradatokat", „*amelyek a kommunikációban szerepelnek, annak részét képezik, ahhoz vannak mellékelve vagy azzal logikailag összekapcsolódnak (a küldő részéről vagy egyéb módon)*"; valamint az „azonosító adatokat", „*amelyek a kommunikációban szerepelnek, annak részét képezik, ahhoz vannak mellékelve vagy azzal logikailag összekapcsolódnak (a küldő részéről vagy egyéb módon), logikailag elválaszthatók a kommunikáció többi részétől, és ha el lennének választva, akkor semmi olyat nem fednének fel, ami észszerűen a kommunikáció jelentésének tekinthető lenne (adott*

[103] Lásd a nyomozati hatáskörökről szóló, 2016. évi törvény 150. szakaszának 3. és 6. alszakaszát.
[104] Lásd a nyomozati hatáskörökről szóló, 2016. évi törvény 147. szakaszát (6. rész, I. fejezet).
[105] Lásd a nyomozati hatáskörökről szóló, 2016. évi törvény 181. szakasza 3. alszakaszának b) pontját.

esetben), figyelmen kívül hagyná a kommunikáció tényéből vagy a kommunikáció átvitelével kapcsolatos bármilyen adatból származó jelentést"[106].

176. Az Európai Adatvédelmi Testület megjegyzi, hogy úgy tűnik, hogy a tömegesen gyűjtött „másodlagos adatokra", más néven metaadatokra[107] nem ugyanazok a garanciák vonatkoznak, mint a célzott engedéllyel gyűjtött adatokra, hanem azok, amelyek az ömlesztve gyűjtött tartalmi adatokra. Az Európai Adatvédelmi Testület megjegyzi, hogy a lefoglalt tartalom bármelyikének kiválasztása több garanciát élvez[108], mint a másodlagos adatok kiválasztása[109].

177. Az Európai Adatvédelmi Testület hangsúlyozza továbbá, hogy mind az EJEB[110], mind az EUB[111] megkérdőjelezte ezen adatok más adatokhoz - különösen a tartalmi adatokhoz - képest érzékenyebb voltát. A lehallgatásokra vonatkozó gyakorlati kódex bemutatja a „másodlagos adatokra" vonatkozó példákat (mind a „rendszeradatokat", mint például a router-konfigurációk, e-mail-címek vagy felhasználói azonosítók; valamint alternatív fiókazonosítók, mind pedig az „azonosító adatokat", mint például a megbeszélés helyszíne a naptárban, a fényképre vonatkozó információk, például az időpont, a dátum és a kép készítésének helyszíne). **Az Európai Adatvédelmi Testület ezért hangsúlyozza az EJEB és az EUB következetes értékelését, és emlékeztet a másodlagos adatokkal kapcsolatban kifejezett aggályokra, amelyekre érzékeny jellegük miatt egyedi garanciákat kell nyújtani. Az Európai Adatvédelmi Testület ezért arra kéri az Európai Bizottságot, hogy gondosan mérje fel, hogy az Egyesült Királyság joga által a személyes adatok ilyen kategóriájára előírt garanciák az EU-ban biztosítottal lényegében megegyező védelmi szintet biztosítanak-e.**

---

[106] A „rendszeradatok" és az „azonosító adatok" meghatározása a nyomozati hatáskörökről szóló, 2016. évi törvény 263. szakaszában található.

[107] Lásd a tömeges hatáskörök felülvizsgálatáról szóló jelentést, Independent Review of Terrorism Legislation (a terrorizmus elleni küzdelemről szóló jogszabályok független felülvizsgálója), 2016. augusztus.

[108] Lásd a nyomozati hatáskörökről szóló, 2016. évi törvény 152. szakasza 1. alszakaszának c) pontját, valamint 3. és következő alszakaszait.

[108] Lásd a nyomozati hatáskörökről szóló, 2016. évi törvény 152. szakasza 1. alszakaszának c) pontját, valamint 3. és következő alszakaszait.

[109] Lásd a nyomozati hatáskörökről szóló, 2016. évi törvény 152. szakasza 1. alszakaszának a) és b) pontját.

[110] Lásd az EJEB nagytanács elé utalt Big Brother Watch ügyben hozott ítéletének 357. pontját: *„Következésképpen, bár a Bíróság nem vonja kétségbe, hogy a kapcsolódó kommunikációs adatok a hírszerző szolgálatok alapvető eszközei a terrorizmus és a súlyos bűncselekmények elleni küzdelemben, úgy véli, hogy a hatóságok nem teremtettek megfelelő egyensúlyt az egymással versengő köz- és magánérdekek között azáltal, hogy ezeket az adatokat teljes egészében mentesítették a tartalom keresésére és vizsgálatára alkalmazandó garanciák alól. Bár a Bíróság nem javasolja, hogy a kapcsolódó kommunikációs adatok csak annak meghatározása céljából legyenek hozzáférhetők, hogy egy adott személy a brit szigeteken tartózkodik-e, mivel ez azt jelentené, hogy szigorúbb szabványokat kellene alkalmazni a kapcsolódó kommunikációs adatokra, mint a tartalmi adatokra, elegendő garanciát kell biztosítani annak biztosítására, hogy a kapcsolódó kommunikációs adatoknak a nyomozati hatáskörök szabályozásáról szóló törvény 16. szakaszában foglalt követelmények alóli mentesítése arra a mértékre korlátozódjon, amely annak megállapításához szükséges, hogy egy adott személy pillanatnyilag a brit szigeteken tartózkodik-e.*"

[111] Lásd: az EUB Privacy International ügyben hozott ítéletének 71. pontját: *„A forgalmi és helymeghatározó adatoknak a biztonsági és hírszerző szolgálatok részére történő továbbítása által a Charta 7. cikkében biztosított jogba megvalósított beavatkozást 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).*"

4.3.1.6. A kommunikációs adatok automatikus kezelése

178. Az Európai Adatvédelmi Testület megjegyzi, hogy a Hírszerzési Közösség hatóságai nem csupán egyszerű vagy összetett válogatókat használnak az tömegesen szerzett adatok szűrésére, hanem más automatizált adatkezelési eszközökre is támaszkodhatnak *„nagy mennyiségű információ elemzése céljából, ami lehetővé teszi az ügynökségek számára, hogy olyan kapcsolatokat, mintákat, összefüggéseket vagy magatartásokat is találjanak, amelyek vizsgálatot igénylő súlyos fenyegetést igazolhatnak*" a Hírszerzési és Biztonsági Bizottság 2015. évi jelentése szerint[112]. **Az Európai Adatvédelmi Testület tisztában van azzal, hogy ez a nyilvános jelentés a korábbi jogi keret szerinti gyakorlatokra vonatkozik, amelyet később felváltott a nyomozati hatáskörökről szóló, 2016. évi törvény. Mindazonáltal úgy véli, hogy további független értékelésre és felügyeletre van szükség az automatizált adatkezelési eszközöknek az Egyesült Királyság illetékes felügyeleti hatóságai általi használata tekintetében, és felszólítja az Európai Bizottságot, hogy vizsgálja tovább ezt a kérdést és azokat a garanciákat, amelyeket az EGT-beli érintettek számára ebben az összefüggésben biztosítani lehetne és/vagy biztosítani kellene**.

4.3.1.7. A Hírszerzési Közösség illetékes hatóságainak megfelelési kockázatai és nem megfelelő gyakorlatai

179. Az Európai Adatvédelmi Testület tudomásul veszi, hogy részletes felügyeleti jelentések állnak rendelkezésre. Ezek értékes információkkal szolgálnak arra vonatkozóan, hogy mit értékeltek pozitív megfelelési gyakorlatként, valamint hogy milyen megfelelési kockázatokat és nem megfelelő gyakorlatokat lehet azonosítani.

180. E tekintetben az IPC 2019. évi jelentésében a jogi keret különböző illetékes hatóságok általi alkalmazásával kapcsolatos több elem is rámutatott az illetékes hatóságok általi meg nem felelésekre (vagy azok kockázataira).

181. Először is, az Európai Adatvédelmi Testület megállapította, hogy azok a kritériumok, amelyek alapján egy adatkészletet tömeges személyesadat-készletként vagy célzott adatkészletként sorolnak be, nem mindig egyértelműek az MI5 és a SIS számára sem, különösen az MI5 esetében, ami az adatokra alkalmazott megfelelő garanciák hiányához vezethet[113]. 2019. évi jelentésében az IPC azt javasolta, hogy *„ezt a kérdést prioritásként kell kezelni"*[114]. A tömeges személyesadat-készletek tekintetében az Európai Adatvédelmi Testület megjegyzi, hogy bár a Kormányzati Kommunikációs Központ esetében

---

[112] Lásd: a Parlament Hírszerzési és Biztonsági Bizottsága, Privacy and Security: A modern and transparent legal framework (Adatvédelem és Biztonság: modern és átlátható jogi keret, 2015, 18. bekezdés, 13. oldal, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf

[113] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 2020. december 15., 8.39. pont, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: *„A [tömeges felügyeletért felelős panel] pozitív fejlődését figyeltük meg, és megállapítottuk annak a belső megfelelés kezelésére gyakorolt hatását. Továbbra is arra törekszünk, hogy egyértelműbbé tegyük az MI5 azon eljárását, amelynek célja az új adatkészletek kezdeti vizsgálatának elvégzése annak érdekében, hogy jobban ,meg lehessen érteni az adatkészlet tömeges személyes adatként vagy például célzott adatként való besorolására vonatkozó döntéseket. Aggályosnak tartottuk, hogy a tömeges felügyeletért felelős panel jegyzőkönyveinek egyik megoldatlan intézkedése a tömeges személyes adatoknak az MI5 és a SIS közötti felosztásával kapcsolatos ellentmondások feloldása volt. Az adatok eltérő felhasználása és a tárolt adatok különböző csökkentése miatt lehetséges, hogy mindkét ügynökség ugyanazt az adatkészletet vagy annak változatait tárolja, és hogy azokat jogszerűen lehet az egyik által tömegesnek, a másik által pedig célzottnak minősíteni. Fennáll annak a kockázata, hogy ha valamelyik ügynökség helytelenül minősítette az adattárolást célzottnak, akkor az adatokat megfelelő engedély nélkül tárolják, és előfordulhat, hogy nem vonatkoznak rájuk megfelelő garanciák*."

[114] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 8.39. pont.

a tömeges személyesadat-készletek besorolása kielégítőnek tűnik (a tömeges adatkészletek besorolását azonban továbbra is az IPC ellenőrzi), 2019 márciusában a külön erre a célra létrehozott csoport súlyos aggályokat vetett fel az engedélyek belső megfelelési felülvizsgálata során, mivel a Kormányzati Kommunikációs Központ megfelelési csoportja által felülvizsgált, tömeges beszerzésre irányuló engedélyekre vonatkozó indokolások 50%-a nem felelt meg az előírt standardnak. Az IPC szerint a megfelelési csoport megkezdte a probléma kivizsgálását és a személyzet átképzését e standard javítása érdekében. A nyomozati hatáskörökről szóló, 2016. évi törvény rendelkezéseiről szóló, megújított képzés, valamint a szabályozói és megfelelési hálózatok által biztosított kiegészítő képzés javította a Kormányzati Kommunikációs Központ e területen való megfelelését. Az IPC várakozásai szerint a jövőbeli ellenőrzések során nem lesz probléma ezzel a standarddal, azonban továbbra is szorosan felülvizsgálja ezt a területet[115]. **Az Európai Adatvédelmi Testület ezért osztja azt a nézetet, hogy az említett elemeknek a védelmi szint értékelésének részeként az Európai Bizottság általi további felülvizsgálata és nyomon követése szükséges az e standard javításának biztosítása érdekében, amint azt az IPC jelentése is hangsúlyozza, és emlékeztet arra, hogy a jogi keret végrehajtását és konkrét alkalmazását az általános adatvédelmi rendelet 45. cikkében előírtak szerint szintén figyelembe kell venni a harmadik országok lényegi megegyezőségének értékelésekor.**

182. Átfogóbban az Európai Adatvédelmi Testület hangsúlyozza az IPC-vel közösen figyelemre méltónak tartott kérdéseket az MI5 tisztviselői által végzett „feladatalapú keresésekkel" kapcsolatban, amelyek lehetővé teszik, hogy a nyomozó a számára elérhető tömeges személyesadat-készleten belül egynél több keresést végezzen, valamint a „*az MI5 által használt, bizonyos technológiai környezetekkel kapcsolatos súlyos megfelelési kockázatokat*" azzal kapcsolatban, hogy az adatokat hol tárolták a környezetben, ki fért hozzá az adatokhoz, milyen mértékben került sor azok másolására vagy megosztására, valamint hogy milyen törlési eljárásokat és adatmegőrzési időt alkalmaztak az adatokkal kapcsolatban. Bár az IPC jelzi, hogy intézkedéseket hoztak és garanciákat vezettek be, amelyek némelyike továbbra is manuális marad, és egyéni, emberi alapon kerül rá sor, rámutat azonban arra, hogy kritikus fontosságú, hogy az „*MI5 továbbra is fenntartsa ezeket az új folyamatokat, és elegendő forrást biztosítson azok hatékony működéséhez. Ha az MI5 a nem megfelelő magatartás növekedését állapítja meg*"[116]. Az IPC arra számít, hogy ezekre a lehető leghamarabb felhívják a figyelmét. **Az Európai Adatvédelmi Testület ezért felszólítja az Európai Bizottságot, hogy a jövőben szorosan kövesse nyomon ezeket a szempontokat.**

183. Ami a Kormányzati Kommunikációs Központot illeti, az Európai Adatvédelmi Testület az IPC jelentéséből azt is megtudta, hogy a tömeges engedélyek alapján végzett műveletek esetében „*a belső jóváhagyás iránti kérelmek minősége változó volt, és megfigyeltük, hogy az ilyen alkalmazások meghatározásának módja még javításra szorul*"[117], valamint hogy a berendezésekkel végzett, célzott beavatkozás esetében az általános jellemzők használatának magyarázatai néha túl általánosak és pontatlanok voltak[118]. Az Európai Adatvédelmi Testület megállapította továbbá a berendezésekkel végzett, tömeges beavatkozással kapcsolatban, hogy az IPC azt javasolja, hogy „*az alkalmazásoknak folyamatosan és pontosan kell rögzíteniük a cél és a szabályozói cél, valamint a hírszerzési követelmények közötti kapcsolatot*"[119], „*az arányosság értékelésekor valamennyi alkalmazásnak egyértelműen foglalkoznia kell a járulékos behatolás lehetőségével és a vonatkozó mérséklési*

[115] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.48. pont.
[116] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 8.52. pont.
[117] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.2. pont.
[118] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.16. és 10.17. pont.
[119] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.23. pont.

lehetőségekkel"[120], és hogy az IPC hangsúlyozta, hogy az előrehaladás ellenére „*van még lehetőség fejlődésre*"[121], valamint a jövőben nagyobb figyelemre lesz szükség.

184. A nyomozati hatáskörökről szóló 2000. évi rendelet szerinti tömeges lehallgatási rendszerrel kapcsolatban – amelyet azóta felváltottak a nyomozati hatáskörökről szóló, 2016. évi törvényben foglalt rendelkezések – az Európai Adatvédelmi Testület emlékeztet arra, hogy a nem megfelelő felügyelet – mind a lehallgatásra alkalmas internetes hordozók kiválasztása, mind pedig a lefoglalt közlések szűrése, keresése és kiválasztása tekintetében – az egyik olyan alapvető szempont volt, amelyet az EJEB az EJEE 8. cikkével össze nem egyeztethetőnek ítélt az Egyesült Királyság hatóságainak a Wig nemzeti biztonsági kamarájának nyomozati hatáskörére vonatkozó korábbi jogszabályok tekintetében. **Az Európai Adatvédelmi Testület felszólítja az Európai Bizottságot, hogy ellenőrizze az eljárások aktuális helyzetét, vegye figyelembe ezeket a tényezőket, és pontosítsa őket a megfelelőségi határozatban, amennyiben az Európai Bizottság elfogadja azt.**

185. Ebben az ügyben az EJEB: „*nem volt meggyőződve arról, hogy a lehallgatással érintett hordozók kiválasztását és a lehallgatott anyagok vizsgálat céljából történő kiválasztását szabályozó garanciák kellően szilárdak ahhoz, hogy megfelelő garanciákat nyújtsanak a visszaélésekkel szemben. A legnagyobb aggodalom azonban a válogatók robusztus, független felügyeletének, valamint a lehallgatott kommunikáció szűrésére használt kritériumok hiánya*."[122] Ahogyan az IPC hangsúlyozza „*ez a megállapítás tükrözte a Hírszerzési és Biztonsági Bizottság „Privacy and Security: A modern and transparent legal framework report of March 2015" (Adatvédelem és Biztonság: Modern és átlátható jogi keretről szóló, 2015. márciusi jelentés") c. dokumentumában szereplő hasonló ajánlást*[123]. **Az Európai Adatvédelmi Testület továbbá üdvözli a tényt, hogy ennek következményeként az IPC 2019-ben felülvizsgálta a tömeges lehallgatás vizsgálatával kapcsolatos megközelítését, „*ami magában foglalta a tömeges lehallgatások tényleges végrehajtására vonatkozó, technikailag összetett módszerek gondos felülvizsgálatát*"[124], valamint kötelezettséget vállalt arra, hogy 2020-tól kezdve beépítse „*az EJEB által hivatkozott válogatók és keresési feltételek részletes vizsgálatát*"[125] a tömeges lehallgatások vizsgálatába. E szempont fontosságára tekintettel az Európai Adatvédelmi Testület aggodalmát fejezi ki amiatt, hogy az IPC még nem végezte el a válogatók és a keresési kritériumok részletes vizsgálatát, és felszólítja az Európai Bizottságot, hogy szorosan kövesse nyomon az ezzel kapcsolatos fejleményeket, különösen mivel e felügyelet konkrét formáját még tisztázni kell[126].**

4.3.2. Az összegyűjtött adatok további felhasználása nemzetbiztonsági célokra és tengerentúli közzététel céljából

186. Ami a nemzetbiztonsági célokból gyűjtött adatok további felhasználását illeti, az Európai Bizottság értékelésében a 2018. évi adatvédelmi törvény 87. cikkének (1) bekezdésére hivatkozik, amely kimondja, hogy „*az így gyűjtött személyes adatokat nem lehet az adatgyűjtés céljával összeegyeztethetetlen módon kezelni*". Az Európai Adatvédelmi Testület ugyanakkor rámutat arra, hogy ez a rendelkezés a 2018. évi adatvédelmi törvény 110. szakasza szerinti nemzetbiztonsági

[120] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.23. pont.
[121] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.23. pont.
[122] Lásd az EJEB Big Brother Watch ügyben hozott ítéletét, 347. pont.
[123] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.28. pont.
[124] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.28. pont.
[125] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.28. pont.
[126] Lásd a nyomozati hatáskörökért felelős biztos 2019. évi éves jelentését, 10.28. pont: „a vizsgálat pontos formátumáról még nem született megállapodás".

mentességek hatálya alá tartozhat. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy akár a célzott lehallgatás és vizsgálat, a kommunikációs adatok célzott beszerzése és megőrzése, a berendezésekkel végzett, célzott beavatkozás, akár a tömeges lehallgatás és a berendezésekkel végzett, tömeges beavatkozás esetén a jogszabály lehetővé teszi a „tengerentúli közzétételt".

4.3.2.1. További felhasználás, tengerentúli közzététel és az Egyesült Királyságban alkalmazandó jogi keret

187. Az Európai Bizottság a 2018. évi adatvédelmi törvény 4. részét és különösen annak 109. szakaszát jelölte meg releváns rendelkezésekként, amelyek konkrét követelményeket határoznak meg a gyűjtött információk további felhasználására, és különösen a személyes adatoknak a hírszerző szolgálatok által harmadik országokba vagy nemzetközi szervezetek részére történő nemzetközi továbbítására vonatkozóan. Az Európai Adatvédelmi Testület ugyanakkor megjegyzi, hogy a 2018. évi adatvédelmi törvény 110. szakasza nemzetbiztonsági mentességet ír elő, amely kimondja, hogy a 2018. évi adatvédelmi törvény egyes rendelkezései nem alkalmazandók, ha a nemzetbiztonság védelme érdekében az e rendelkezések alóli mentességre van szükség. Az érintett rendelkezések, amelyek esetleg nem alkalmazandók, magukban foglalják a 2018. évi adatvédelmi törvény 4. részének 2. fejezetét az adatvédelmi elvek tekintetében, ideértve a célhoz kötöttséget is, valamint a 2018. évi adatvédelmi törvény 4. részének az érintettek jogaira vonatkozó 3. fejezetét. A 2018. évi adatvédelmi törvény 109. szakasza a 2018. évi adatvédelmi törvény 110. szakaszával és alkalmazásának feltételeivel együtt értelmezve olyan esetekhez vezethet, amikor a személyes adatok hírszerző szolgálatok általi, harmadik országokba történő nemzetközi továbbítására az adatvédelmi elvekkel és az érintettek jogaival kapcsolatos rendelkezések alkalmazása nélkül kerül sor.

188. Amint azt az Európai Bizottság megállapította, ezt a mentességet eseti alapon kell értékelni, és csak akkor lehet alkalmazni, ha egy adott rendelkezés alkalmazása negatív következményekkel járna a nemzetbiztonságra nézve. Az Egyesült Királyság hírszerző szolgálatai számára kiállított nemzeti tanúsítvány célja annak igazolása, hogy mentességre van szükség bizonyos személyes adatok tekintetében, amelyeket a nemzetbiztonság védelme céljából kezelnek. Az Európai Adatvédelmi Testület ugyanakkor megjegyzi, hogy a 2018. évi adatvédelmi törvény szerinti nemzetbiztonsági tanúsítványra vonatkozó iránymutatásában az Egyesült Királyság Belügyminisztériuma egyértelművé teszi, hogy *„[a] kezdetektől fogva fontos megjegyezni, hogy a nemzetbiztonsági mentességre való hivatkozáshoz nincs szükség tanúsítványra*; *valójában a legtöbb esetben az adatkezelők maguk határozzák meg, hogy a nemzetbiztonsági mentesség alkalmazandó-e*." [127] Ezenkívül az Egyesült Királyság Belügyminisztériuma megjegyzi, hogy *„a nemzetbiztonsági tanúsítványok olyan személyes adatokra alkalmazhatók, amelyeket kifejezetten azonosítottak, vagy amelyek a személyes adatok szélesebb kategóriájára vonatkoznak. A tanúsítványok lehetnek előzetesek és utólagosak is.*" [128] A nemzetbiztonsági mentesség ezért nemzetbiztonsági tanúsítvány hiányában is alkalmazható a személyes adatok hírszerző szolgálatok általi, harmadik országok részére történő nemzetközi továbbításával kapcsolatban.

189. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy például a DPA/S27/Biztonsági Szolgálat nemzetbiztonsági tanúsítványa[129] úgy rendelkezik, hogy 2024. július 24-ig *„a Biztonsági Szolgálat*

[127] Lásd: Egyesült Királyság Belügyminisztériuma, a 2018. évi adatvédelmi törvény, Nemzetbiztonsági tanúsítványokról szóló útmutató, 2020. augusztus, 3. pont, 3. o.
[128] Lásd: Egyesült Királyság Belügyminisztériuma, a 2018. évi adatvédelmi törvény, Nemzetbiztonsági tanúsítványokról szóló útmutató, 2020. augusztus, 5. pont, 4. o.
[129] Lásd: DPA/S27/Biztonsági Szolgálat, a 2018. évi adatvédelmi törvény 27. szakasza, a külügyminiszter tanúsítványa, 2019. július 24., https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf

nevében, kérésére, segítségével vagy támogatásával kezelt" személyes adatok, „*amennyiben az adatkezelés a Biztonsági Szolgálatnak a Biztonsági Szolgálatról szóló, 1989. évi törvény 1. szakaszában ismertetett feladatok megfelelő ellátásának megkönnyítése érdekében szükséges*", mentességet élveznek az Egyesült Királyság jogának az általános adatvédelmi rendelet V. fejezetének megfelelő rendelkezései alól a személyes adatok harmadik országokba vagy nemzetközi szervezetekhez való továbbításával kapcsolatban. Míg a többi nyilvánosan hozzáférhető nemzetbiztonsági tanúsítvány nem biztosít mentességet a 2018. évi adatvédelmi törvény 109. szakaszának rendelkezései alól, emlékeztetni kell arra, hogy a nemzetbiztonsági tanúsítvány szövegének egy része vagy egésze visszatartható, ha annak közzététele nemzetbiztonsági érdekkel ellentétes lenne, közérdekbe ütközne, vagy bármely személy biztonságát veszélyeztetné.

190. Általánosságban elmondható, hogy az Európai Adatvédelmi Testület a határozattervezet e rendelkezésekkel kapcsolatos vizsgálata során megállapítja, hogy az e közzétételekre vonatkozó garanciák kizárólag azt a követelményt foglalják magukban, hogy az adatok címzettjének tiszteletben kell tartania az adatbiztonságra, a közzétételnek a szükséges mértékre korlátozódására, az adatmegőrzésre és az adatokhoz való hozzáférés korlátozott számú személyre történő korlátozására vonatkozó követelményeket. Ennek értelmében **az Európai Adatvédelmi Testület hangsúlyozza, hogy a tengerentúli közzétételek esetében az Egyesült Királyság joga által biztosított nemzetbiztonsági mentesség alkalmazása olyan helyzetekhez vezethet, amelyekben a célhoz kötöttség, a szükségesség és az arányosság elvének betartására vagy az egyének megfelelő jogainak, a felügyeletnek és a jogorvoslatnak a rendeltetési hely szerinti harmadik országban történő biztosítására vonatkozó garanciák nem teljes mértékben biztosítottak, vagy nincsenek betartva. Az Európai Adatvédelmi Testület ezért azt ajánlja az Európai Bizottságnak, hogy folytassa az Egyesült Királyság jogszabályai által a tengerentúli közzététel tekintetében biztosított általános garanciák vizsgálatát, különös tekintettel a nemzetbiztonsági mentességek alkalmazására.**

4.3.2.2. Tengerentúli közzététel és hírszerzések közötti megosztás nemzetközi együttműködés keretében

191. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az Európai Bizottság a megfelelőség értékelésének részeként nem vette figyelembe az Egyesült Királyság és harmadik országok vagy nemzetközi szervezetek között létrejött olyan meglévő nemzetközi megállapodásokat, amelyek konkrét rendelkezéseket írhatnak elő a személyes adatoknak a hírszerző szolgálatok által harmadik országokba történő nemzetközi továbbítására vonatkozóan.

192. Az Európai Adatvédelmi Testület azt is hangsúlyozza, hogy az Európai Bizottság értékelése főként a 2018. évi adatvédelmi törvény 4. részének értékelésén alapul, és különösen aggódik amiatt, hogy a nyomozati hatáskörökről szóló, 2016. évi törvény a hírszerzési információk külföldi partnerekkel való cseréjére irányuló „kérelmekre" összpontosít, azonban nem foglalkozik a hírszerzési információk megosztásának egyéb formáival. Az Európai Adatvédelmi Testület e tekintetben megjegyzi, hogy az Európai Bizottság határozattervezete nem hivatkozik az Egyesült Királyság jogalkotási kerete, valamint az Egyesült Királyság és az Egyesült Államok közötti távközlési felderítési megállapodás (a továbbiakban: az Egyesült Királyság és az Egyesült Államok közötti távközlési felderítési megállapodás) közötti kapcsolatra, és nem is értékeli azt. A megállapodás 75. évfordulója alkalmából nemrégiben született nyilatkozatban az Egyesült Államok Nemzetbiztonsági Ügynöksége (a továbbiakban NSA) megemlítette, hogy ez a partnerség „*a lehető legnagyobb mértékben, minimális korlátozásokkal teszi lehetővé a két ügynökség közötti információcserét*", és „*ez a korszakalkotó dokumentum szabályzatokat és eljárásokat hozott létre az Egyesült Királyság és az Egyesült Államok hírszerzési szakemberei számára a kommunikációs, fordítási, elemzési és kódfejtési információk*

megosztása terén."[130] Ez a megállapodás lett az alapja az Ausztráliával, Kanadával és Új-Zélanddal között egyéb hírszerzési partnerségeknek is.

193. E megállapodás és egyedi rendelkezései titkos jellege komoly kihívást jelent az Egyesült Királyság hatóságai által nemzetbiztonsági célokból gyűjtött információk további felhasználásával és tengeren túli közzétételével kapcsolatos jogszabályok egyértelműsége és előreláthatósága tekintetében. Ezzel összefüggésben az Európai Adatvédelmi Testület emlékeztet arra, hogy az EU-n belül biztosított védelem szintjét illetően az EUB hangsúlyozta, hogy a személyes adatok védelmére irányuló alapvető jogba való beavatkozást tartalmazó jognak „*egyértelmű és pontos szabályokat kell tartalmaznia az intézkedés hatálya és alkalmazása vonatkozásában, és minimális követelményeket kell előírnia annak érdekében, hogy azon személyek, akiknek a személyes adatai érintettek, elegendő olyan biztosítékokkal rendelkezzenek, amely lehetővé teszi az adataiknak a visszaélések veszélyeivel, valamint az ezen adatokat érintő minden jogellenes hozzáféréssel és felhasználással szembeni hatékony védelmét. Az ilyen biztosítékokkal való rendelkezés szükségessége még fontosabb abban az esetben, ha a személyes adatokat automatikusan kezelik és jelentős veszélye áll fenn az említett adatokhoz való jogellenes hozzáférésnek*"[131]. Az Európai Adatvédelmi Testület ezért úgy véli, hogy az Európai Bizottságnak a megfelelőségértékelés részeként figyelembe kell vennie az Egyesült Királyság és az Egyesült Államok közötti távközlési felderítési megállapodás hatását.

194. Az EJEB a Big Brother Watch ügyben 2018. szeptember 13-án hozott ítéletének első szakaszában értékelte az Egyesült Királyság hírszerzési információk megosztására vonatkozó rendszerét, és különösen az Egyesült Királyság és az Egyesült Államok közötti távközlési felderítési megállapodást. Az EJEB kijelentette, hogy „*[a] nyomozati hatáskörök szabályozásáról szóló törvény nem tartalmazza azt a jogszabályi keretet, amely lehetővé teszi az Egyesült Királyság hírszerző szolgálatai számára, hogy lefoglalt anyagot kérjenek külföldi hírszerzési ügynökségektől. Az Egyesült Királyság és az Egyesült Államok közötti, 1946. március 5-i távközlési felderítési megállapodás lehetővé teszi az Egyesült Államok és az Egyesült Királyság közötti információcserét*"[132], és úgy vélte, hogy „*létezik jogalap a külföldi hírszerzési ügynökségektől való hírszerzési információk kérésére, és ez a jogalap kellően elérhető*"[133]. Míg az EJEB megállapította, hogy nem került sor az EJEE 8. cikkének[134] megsértésére a hírszerzési információk megosztásának rendszerével kapcsolatban, az Európai Adatvédelmi Testület megjegyzi, hogy ezt az ítéletet a nagytanács elé utalták, amelynek határozata még folyamatban van. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az ítéletet részben egyetértő, részben eltérő véleményben Koskelo bíró, akihez csatlakozott Turković bíró is[135], arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét a hírszerzési információk megosztására vonatkozó rendszer tekintetében, és kijelentette, hogy „*[k]önnyen egyet lehet érteni azzal az elvvel, amely szerint minden olyan intézkedés, amely alapján a lefoglalt kommunikációból származó hírszerzési információkat külföldi hírszerző szolgálatokon keresztül szerzik be, függetlenül attól, hogy a lehallgatás végrehajtására vagy az eredmények továbbítására irányuló kérések alapján, nem engedélyezhető annak érdekében, hogy el lehessen kerülni a nemzeti hatóságok általi felügyeletre*

[130] Lásd az NSA sajtóközleményét, GCHQ és NSA Celebrate 75 Years of Partnership (A Kormányzati Kommunikációs Központ és az NSA partnerségük 75. évfordulóját ünnepli), 2021. február 5., https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/

[131] Lásd: Schrems I-ügy, 91. pont.

[132] Lásd az EJEB Big Brother Watch ügyben hozott ítéletét, 425. pont.

[133] Lásd az EJEB Big Brother Watch ügyben hozott ítéletét, 427. pont.

[134] Lásd az EJEB Big Brother Watch ügyben hozott ítéletét, 448. pont.

[135] Lásd: EJEB, Big Brother Watch ügy, Koskelo bíró részben egyetértő, részben eltérő véleménye, amelyhez csatlakozott Turković bíró is.

vonatkozóan előírt garanciákat (lásd a 216., 423. és 447. bekezdéseket). Minden más megközelítés valószínűtlen lenne".

195. Amint azt a média és a nem kormányzati szervezetek több jelentése is kiemelte[136][137], az Egyesült Királyság és az Egyesült Államok közötti távközlési felderítési megállapodás legutóbbi, nyilvánosságra hozott változata 1956-ból származik, és azóta a kommunikációs technológia és a jelfelderítés jellege jelentősen megváltozott. A médiában megjelenő beszámolók például feltárták, hogy az Egyesült Királyságban található, földfelszín alatti kábeleken áthaladó adatokat a Kormányzati Kommunikációs Központ lefoglalja, és hozzáférhetővé teszi az NSA számára[138].

196. Az Európai Adatvédelmi Testület számára a hírszerzési információk megosztásával kapcsolatban kulcsfontosságú kérdés, hogy a 2018. évi adatvédelmi törvény 109. szakasza és a nyomozati hatáskörökről szóló, 2016. évi törvény rendelkezései továbbra is alkalmazandók-e abban az esetben, ha az Egyesült Királyság hírszerző szolgálatai az Egyesült Királyság és az Egyesült Államok közötti távközlési felderítési megállapodással összhangban járnak el. Szintén vizsgálandó kulcsfontosságú elem az, hogy e megállapodás rendelkezései vagy tényleges alkalmazása hatással vannak-e az EGT-ből az Egyesült Királyságba irányuló, átvitel alatt álló személyes adatok védelmének szintjére, vagy lehetővé teszik-e a személyes adatokhoz való közvetlen hozzáférést és azok megszerzését más harmadik országbeli hírszerző szolgálatok számára.

197. Következésképpen a 2018. évi adatvédelmi törvény 4. része és az ahhoz kapcsolódó nemzetbiztonsági mentesség alapján tett „tengerentúli közzétételekkel" kapcsolatos fenntartások, valamint a nyomozati hatáskörökről szóló, 2016. évi törvény keretében benyújtott kérelmek mellett **az Európai Adatvédelmi Testület aggodalmát fejezi ki az egyéb eszközökön alapuló információmegosztás és -közlés egyéb formái, különösen az Egyesült Királyság által más harmadik országokkal kötött különböző nemzetközi megállapodások tekintetében, különösen ha ezek az eszközök továbbra sem hozzáférhetők a nyilvánosság számára, mint például az Egyesült Királyság és az Egyesült Államok közötti távközlési felderítési megállapodás. Az ilyen megállapodás hatása a személyes adatokhoz való, nemzetbiztonsági célú hozzáféréssel és az adatok felhasználásával kapcsolatban megállapított garanciák megkerüléséhez vezethet.**

198. Az Európai Adatvédelmi Testület osztja az ENSZ különmegbízottjának, Joe Cannataccinak a véleményét, amely szerint „*[a] hírszerzési információk megosztása nem eredményezhet kiskaput a tekintetben, hogy nemzeti garanciáktól mentesen hírszerzési információkat lehessen beszerezni vagy azt mások számára megkönnyíteni, sem pedig azt, hogy a magánélet (vagy más emberi jogok) védelmére vonatkozó alacsonyabb szintű normákkal rendelkező külföldi kormányok az Egyesült Királyság hírszerzési információiból olyan hírszerzési információkat szerezzenek be, amelyek az emberi jogok megsértésével járnak*"[139].

---

[136] Lásd BBC, Diary revealed of secret UK-US spy pact of Five Eyes, 2021. március 5., https://www.bbc.com/news/uk-56284453

[137] Lásd: Privacy International, Policy Briefing – UK Intelligence Sharing Arrangements, 2018. április, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf

[138] Lásd: The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, 2013. június 21., https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[139] A Nagy-Britannia és Észak-Írország Egyesült Királyságába irányuló missziójának küldetészáró nyilatkozata a magánélethez való joggal foglalkozó különleges előadó küldetésének befejezésekor, 2018. június 29., https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give

199. Ezenkívül az **Európai Adatvédelmi Testület úgy véli továbbá, hogy a hírszerzési együttműködés céljából harmadik országokkal kötendő, olyan két- vagy többoldalú megállapodások, amelyek jogalapot biztosítanak közvetlen lehallgatáshoz és a személyes adatok megszerzéséhez vagy a személyes adatok ezen országok részére történő továbbításához, szintén jelentősen érinthetik az összegyűjtött információk további használatának feltételeit, mivel ezek a megállapodások nagy valószínűséggel befolyásolhatják az Egyesült Királyság értékelt adatvédelmi jogi keretét.**

4.3.3. Felügyelet

200. Az Európai Adatvédelmi Testület hangsúlyozza a független felügyeleti hatóságok általi átfogó felügyelet fontosságát a megfelelő adatvédelmi szint biztosítása érdekében. Az Európai Unió Alapjogi Chartája 8. cikkének (3) bekezdése értelmében vett függetlenségi garancia célja a személyes adatok kezelése vonatkozásában az egyének védelmére vonatkozó szabályok betartásának hatékony és megbízható nyomon követése.

201. A személyes adatokhoz való hozzáférés és nemzetbiztonsági célú felhasználás esetén a felügyeleti funkciót elsősorban az IPC és az igazságügyi biztosok (a továbbiakban: igazságügyi biztosok) látják el.

202. **Az Európai Adatvédelmi Testület általánosságban jelentős előrelépésként ismeri el az igazságügyi biztosok fogalmának bevezetését a nyomozati hatáskörökről szóló, 2016. évi törvényben.** Egy fenti kéréssel összhangban felkérjük az Európai Bizottságot, hogy részletesebben értékelje **az igazságügyi biztosok függetlenségét, és különösen azt, hogy jogilag milyen mértékben biztosított az IPC és hivatala (a továbbiakban: IPCO) függetlensége, mivel ez nem szerepel a nyomozati hatáskörökről szóló, 2016. évi törvényben.** Ez annál is inkább fontos, mivel az IPC dönt a kormány általi fellebbezésről, amennyiben egy igazságügyi biztos **elutasította** a felügyeleti **intézkedés** iránti kérelmet.

203. Az IPC előzetes és utólagos felügyeleti feladatokat is ellát. Ami az előzetes felügyeletet illeti, az Európai Adatvédelmi Testület megérti, hogy az igazságügyi biztosok feladata, hogy egyedi esetekben különböző felügyeleti intézkedéseket hagyjanak jóvá, ideértve a kommunikációs adatok célzott lehallgatását és tömeges beszerzését. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy a felügyeleti intézkedések előzetes jóváhagyása nem vezethető le az EUB ítélkezési gyakorlatából a felügyeleti intézkedések arányosságának abszolút követelményeként.[140]

204. A felügyelet e szintje hatékonyságának értékelése érdekében az Európai Adatvédelmi Testület mindazonáltal úgy véli, hogy tovább kell pontosítani azokat a forgatókönyveket, amelyek esetében lehetséges az igazságügyi biztosok előzetes jóváhagyása nélküli jogszerű lehallgatás.

205. Határozattervezetében az Európai Bizottság a 201. és 266. lábjegyzetében a nyomozati hatáskörökről szóló, 2016. évi törvény 44–52. szakaszában a célzott lehallgatások tekintetében „különleges, korlátozott eseteket" említ. Az Európai Adatvédelmi Testület megjegyzi, hogy a nyomozati hatáskörökről szóló, 2016. évi törvény 45–51. szakaszai olyan mentességeket foglalnak magukban, amelyeket a hírszerző szolgálatok állítólag nem használnak rendszeresen. Az **Európai Adatvédelmi Testület továbbá úgy értelmezi**, hogy **azokban az esetekben, amikor a mentességek alkalmazandók** (pl. távközlési és postai szolgáltatók), az igazságügyi biztosok által végzett előzetes jóváhagyást abban az esetben kell elvégezni, ha a bűnüldöző hatóságok vagy a hírszerző szolgálatok hozzáférést **kérnek**

[140] Megjegyzi ugyanakkor, hogy az EUB az adatvédelmi pajzs Schrems II-ügyben való érvénytelenítésekor tudomásul vette, hogy az Egyesült Államok joga szerint az úgynevezett FISA-bíróság *„nem az egyéni megfigyelési intézkedéseket engedélyezi; hanem a megfigyelési programokat (mint a PRISM vagy az UPSTREAM) az éves tanúsítványok alapján*". (179. pont).

ezekhez az adatokhoz, és **felkéri az Európai Bizottságot, hogy határozatában erősítse meg, hogy ez helyes**.

206. Az Európai Adatvédelmi Testület elismeri, hogy a nyomozati hatáskörökről szóló, 2016. évi törvény 44. szakaszának (2) bekezdése lehetővé teszi a kommunikáció lehallgatását, ha az egyik fél (a feladó vagy a címzett) hozzájárult a kommunikációhoz, és a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény vagy a nyomozati hatáskörök szabályozásáról szóló rendeletről (Skócia) szóló, 2000. évi törvény (2000 asp 11), azaz az igazságügyi biztosok létrehozását megelőző korábbi jogi helyzet alapján van engedély. Az Európai Adatvédelmi Testület **felkéri** az Európai Bizottságot annak tisztázására, hogy ez azt jelenti-e, hogy azokban az esetekben, amikor létezik egyoldalú hozzájárulás, az előzetes jóváhagyási eljárás egyáltalán nem alkalmazandó.

207. Ami az utólagos felügyeletet illeti, fontos annak ellenőrzése is, hogy a hatékony független felügyeletet hiányosságok nélkül biztosítják–e, különösen, ha azt előzetesen nem irányozták elő.

208. Az Európai Adatvédelmi Testület megjegyzi, hogy a nyomozati hatáskörökről szóló, 2016. évi törvény 48–52. szakasza tekintetében az igazságügyi biztosok általi utólagos felülvizsgálatra kerül sor, **és felkéri az Európai Bizottságot annak tisztázására, hogy mely követelmények és kinek a kezdeményezése alapján kell elvégezni az utólagos felülvizsgálatot**.

209. A nyomozati hatáskörökről szóló, 2016. évi törvény 229. szakaszának (4) bekezdése szerint az IPC nem felügyeli bizonyos feladatkörök gyakorlását. E tekintetben az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy tisztázza a nyomozati hatáskörökről szóló, 2016. évi törvény 229. szakasza (4) bekezdésének d) és e) pontjában foglalt rendelkezéseket az IPC felülnyomozati hatáskörére gyakorolt gyakorlati hatása tekintetében. **Az Európai Adatvédelmi Testület értelmezése szerint az Információs Biztos Hivatala az illetékes felügyeleti hatóság, amely esetében a nyomozati hatáskörökről szóló, 2016. évi törvény 229. szakaszának (4) bekezdése szerinti mentességek alkalmazandók, és az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy határozatában erősítse meg, hogy ez így van-e.**

210. **Úgy tűnik, hogy az utólagos felügyelet során** az **IPC** feladata arra **korlátozódik**, hogy meg nem felelés esetén ajánlásokat tegyen, és értesítse az érintettet, ha a hiba súlyos, és az érintett tájékoztatása a közérdeket szolgálja. **Az Európai Adatvédelmi Testület felkéri az Európai Bizottságot annak tisztázására, hogy az IPCO hogyan tudja hatékonyan biztosítani a jogszabályoknak való megfelelést.**

211. **Végezetül az Európai Adatvédelmi Testület úgy értelmezi, hogy az érintett egyének nem fordulhatnak közvetlenül az IPCO-hoz, hanem az Információs Biztos Hivatalához kell panaszt benyújtaniuk, amely azonban korlátozott hatáskörrel rendelkezik a nemzetbiztonság területén. Az Európai Adatvédelmi Testület ezért felkéri az Európai Bizottságot, hogy pontosítsa, hogyan biztosítja jogilag, hogy az IPCO ezekben az esetekben kezelje a panaszokat.**

4.3.4. Jogorvoslat

212. Az EUB Schrems I és Schrems II-ügyben hozott ítéleteinek fényében egyértelmű, hogy a Charta 47. cikke értelmében vett hatékony bírói jogvédelem alapvető fontosságú a harmadik ország joga megfelelőségének vélelmezése szempontjából. Az ítéletek azt is megmutatták, hogy e tekintetben különös figyelmet kell fordítani a hatékony bírói jogvédelemre a nemzetbiztonság területén a személyes adatokhoz való hozzáférés terén.

213. **Az Európai Adatvédelmi Testület elismeri, hogy az Egyesült Királyság létrehozta az IPT-t. Az IPT hatásköre nemcsak arra terjed ki, hogy a bűnüldöző hatóságok nyomozati hatáskörének**

gyakorlásával kapcsolatos ügyekben hozzon ítéletet, hanem a hírszerző szolgálatok hatáskörével kapcsolatban is. Az Európai Adatvédelmi Testület úgy értelmezi, hogy az IPT az Európai Unió Alapjogi Chartájának 47. cikke értelmében megfelelő bíróságként működik. Ami a hatáskörét illeti, felkérjük az Európai Bizottságot annak megerősítésére, hogy az IPT rendelkezik-e a határozattervezet (262) preambulumbekezdésében említett valamennyi hatáskörrel, függetlenül attól, hogy milyen jogalap alapján nyújtották be a panaszt.

214. A hírszerzési ügynökségek általi leplezett figyelés gyakran azt jelenti, hogy a megfigyelés tárgya, az érintett a megfigyelésről nem tud és nem is fog tudni. Ezzel összefüggésben az Európai Adatvédelmi Testület az Egyesült Államok jogszabályainak elemzése során számos alkalommal aggodalmának adott hangot a megfigyelési ügyekben az Egyesült Államok joga szerint értelmezett „legitimáció" követelménye miatt. Mindezek alapján az Európai Adatvédelmi Testület megjegyzi, hogy az IPT-hez benyújtott panasz csak „feltételességi" tesztet ír elő, amely szerint a panaszosnak bizonyítania kell, hogy potenciálisan ki van téve az intézkedésnek.

215. Az IPT elemzése során az Európai Adatvédelmi Testület különös figyelmet fordít arra a tényre is, hogy az IPT működését többször is az EJEB értelmezése szerint az EJEE-vel összhangban lévőnek találták.