Az Európai Unió
Tanácsa

Brüsszel, 2020. június 29.
(OR. en)

9180/20
ADD 1

DATAPROTECT 57
JAI 536
FREMP 41
DIGIT 50
RELEX 482

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Jordi AYET PUIGARNAU igazgató
Az átvétel dátuma:	2020. június 25.
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	SWD(2020) 115 final
Tárgy:	BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM […] amely a következő dokumentumot kíséri A BIZOTTSÁG JELENTÉSE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK **A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve**

Mellékelten továbbítjuk a delegációknak az SWD(2020) 115 final számú dokumentumot.

Melléklet: SWD(2020) 115 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2020.6.24.
SWD(2020) 115 final

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

[…]

amely a következő dokumentumot kíséri

A BIZOTTSÁG JELENTÉSE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve

{COM(2020) 264 final}

Tartalom

1 HÁTTÉR

Az általános adatvédelmi rendelet[1] (a továbbiakban GDPR) nyolc év előkészítés, tervezés és intézményközi egyeztetés eredménye, amely kétéves (2016 májusától 2018 májusáig tartó) átmeneti időszakot követően 2018. május 25-én lépett hatályba. A GDPR 97. cikke előírja a Bizottság számára, hogy először a rendelet alkalmazásának első két éve után, majd négyévente jelentést készítsen a rendelet értékeléséről és felülvizsgálatáról.

Az értékelés továbbá egy többoldalú megközelítés része, amelyet a Bizottság már a GDPR hatálybalépése előtt is követett, és amelyet azóta is aktívan alkalmaz. E megközelítés részeként a Bizottság folyamatos, kétoldalú párbeszédeket folytat a tagállamokkal a nemzeti jogszabályok GDPR-nak való megfeleléséről, szakértelmével és tapasztalatával aktívan hozzájárul az Európai Adatvédelmi Testület (a továbbiakban a Testület) munkájához, támogatja az adatvédelmi hatóságokat, továbbá szoros kapcsolatot tart fenn az érdekelt felek széles körével a rendelet gyakorlati alkalmazásával összefüggésben.

Az értékelés arra a helyzetfelmérésre épít, amelyet a Bizottság a GDPR alkalmazásának első évében végzett, és amelyet a 2019. júliusi közleményben[2] foglalt össze. Ezenkívül a GDPR alkalmazásáról szóló, 2018. januári közleményre[3] is alapoz. A Bizottság továbbá elfogadta a 2018 szeptemberében közzétett, a személyes adatok választásokkal összefüggésben történő használatáról szóló iránymutatást, valamint a 2020 áprilisában közzétett, az adatvédelemmel összefüggésben a Covid19-világjárvány elleni küzdelmet támogató alkalmazásokról szóló iránymutatást.

Bár ez az értékelés a GDPR 97. cikkének (2) bekezdésében említett két kérdésre összpontosít, nevezetesen a nemzetközi adattovábbításokra, valamint az együttműködési és egységességi mechanizmusokra, szélesebb megközelítést alkalmaz annak érdekében, hogy foglalkozzon azokkal a problémákkal, amelyeket a különböző szereplők az elmúlt két évben felvetettek.

Az értékelés előkészítéséhez a Bizottság az alábbi forrásokból származó hozzájárulásokat vette figyelembe:

- a Tanács[4];
- az Európai Parlament (Állampolgári Jogi, Bel- és Igazságügyi Bizottság)[5];

---

[1] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (HL L 119., 2016.5.4., 1–88. o.).

[2] A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – Adatvédelmi szabályok: a bizalom alapja az Európai Unión belül és kívül – mérleg – COM(2019) 374 final, 2019.7.24.

[3] A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: Erősebb védelem, új lehetőségek – a Bizottság iránymutatása az általános adatvédelmi rendelet 2018. május 25-től történő közvetlen alkalmazásáról, COM/2018/043 final.

[4] Az általános adatvédelmi rendelet alkalmazásával kapcsolatos tanácsi álláspont és megállapítások – 14994/2/19 Rev2, 2020.1.15.: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/hu/pdf

[5] Az Európai Parlament Állampolgári Jogi, Bel- és Igazságügyi Bizottságának 2020. február 21-i levele Reynders biztos részére, Hiv.: IPOL-COM-LIBE D (2020)6525.

- a Testület[6] és az egyes adatvédelmi hatóságok[7], a Bizottság által küldött kérdőív alapján;
- a több érdekelt felet tömörítő, a GDPR alkalmazásának támogatásával foglalkozó szakértői csoport[8] tagjainak visszajelzése, szintén a Bizottság által küldött kérdőív alapján;
- valamint az érdekelt felektől kapott eseti hozzájárulások.

2 A GDPR VÉGREHAJTÁSA ÉS AZ EGYÜTTMŰKÖDÉSI ÉS EGYSÉGESSÉGI MECHANIZMUSOK MŰKÖDÉSE

A GDPR innovatív irányítási rendszert alakított ki, és létrehozta a valóban európai adatvédelmi kultúra alapjait, amelynek célja az összehangolt értelmezés mellett az adatvédelmi szabályok összehangolt alkalmazásának és végrehajtásának biztosítása. Pillérjei a független nemzeti adatvédelmi hatóságok és az újonnan létrehozott Testület.

Mivel az adatvédelmi hatóságok elengedhetetlenek az uniós adatvédelmi rendszer egészének működéséhez, a Bizottság gondosan nyomon követi a tényleges függetlenségüket, többek közt a megfelelő pénzügyi, emberi és technikai erőforrások tekintetében.

Az eddig szerzett kevés tapasztalat miatt még mindig túl korai lenne teljeskörűen értékelni az együttműködési és egységességi mechanizmusok működését[9]. Ezenkívül az adatvédelmi hatóságok még nem használták a GDPR által az együttműködésük további megerősítése céljából biztosított teljes eszköztárat.

2.1 Az adatvédelmi hatóságok megerősített jogköreinek alkalmazása

A GDPR független adatvédelmi hatóságokat hoz létre, és összehangolt és megerősített végrehajtási jogkörökkel ruházza fel őket. Amióta a GDPR alkalmazandó, a hatóságok a GDPR-ban előírt korrekciós jogkörök széles skáláját alkalmazták, úgy mint a közigazgatási bírságok (az EU/EGT 22 hatósága)[10], figyelmeztetések és megrovások (23), az érintettek kérelmeinek való megfelelésre irányuló utasítások (26), az adatvédelmi műveletek GDPR-ral való összehangolására irányuló utasítások

---

[6] A Testület hozzájárulása a GDPR 97. cikke szerinti értékeléséhez, elfogadás ideje: 2020. február 18.: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

[7] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_hu

[8] A Bizottság által létrehozott, a GDPR-ral foglalkozó, több felet tömörítő szakértői csoport a civil társadalom és a vállalkozások képviselőit, akadémikusokat és gyakorló szakértőket foglal magában: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=HU
A több érdekelt felet tömörítő szakértői csoport jelentése elérhető itt: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356

[9] Ezt a tényt többek közt kiemeli a Tanács a GDPR alkalmazásával kapcsolatos álláspontjában és megállapításaiban, valamint a Testület az értékeléshez való hozzájárulásában.

[10] A zárójelben megadott számok azoknak az EU-n/EGT-n belüli adatvédelmi hatóságoknak a számát jelölik, amelyek 2018 májusa és 2019 novemberének vége között alkalmazták a felsorolt jogköröket. Lásd a Testület hozzájárulásának 32–33. oldalát.

(27), valamint az adatok helyesbítésére, törlésére vagy az adatkezelés korlátozására irányuló utasítások (17). Körülbelül az adatvédelmi hatóságok fele (13) vezetett be ideiglenes vagy végleges adatkezelési korlátozásokat, beleértve a tilalmakat. Ez mutatja a GDPR-ban előírt valamennyi korrekciós intézkedés tudatos alkalmazását; az adatvédelmi hatóságok nem féltek attól, hogy közigazgatási bírságot szabjanak ki az egyéb korrekciós intézkedések mellett vagy helyett, az egyes ügyek körülményeitől függően.

Közigazgatási bírságok:

2018. május 25. és 2019. november 30. között 22, EU/EGT-n belüli adatvédelmi hatóság körülbelül 785 bírságot szabott ki. Csak néhány olyan hatóság van, amely még nem szabott ki közigazgatási bírságot, bár a jelenleg folyamatban lévő eljárások vezethetnek bírsághoz. A bírságok többsége az alábbiakkal kapcsolatos szabálysértésekkel volt összefüggésben: a jogszerűség elve; az érvényes hozzájárulás; az érzékeny adatok védelme; az átláthatóságra vonatkozó kötelezettség, az érintettek jogai; és az adatvédelmi incidensek.

Az adatvédelmi hatóságok által kiszabott bírságokra példák többek közt az alábbiak[11]:

- 200 000 EUR a közvetlen üzletszerzéssel szembeni tiltakozáshoz való jog megszegéséért Görögországban;
- 220 000 EUR egy lengyelországi adatkereskedő céggel szemben, amiért elmulasztotta tájékoztatni a természetes személyeket az adataik kezeléséről;
- 250 000 EUR egy spanyol labdarúgó-bajnoksággal, a LaLigával szemben, amiért az okostelefonos alkalmazásuk kialakításában nem volt biztosított az átláthatóság;
- 14,5 millió EUR az adatvédelmi elveknek egy német ingatlancég általi megszegéséért, különös tekintettel a jogellenes tárolásra;
- 18 millió EUR az adatok különleges kategóriáinak az osztrák postai szolgáltatások általi, nagy számban történő jogellenes kezeléséért;
- 50 millió EUR a Google-lel szemben Franciaországban, a hozzájárulás felhasználóktól való megszerzésének feltételei miatt.

A GDPR sikere nem mérhető a kiszabott bírságok számában, mivel a GDPR a korrekciós jogkörök szélesebb skáláját kínálja. A körülményektől függően például az adatkezelés tilalmának vagy az adatáramlások felfüggesztésének az elrettentő hatása jóval erősebb lehet.

A közszektor tekintetében felmerülő kérdések

A GDPR lehetővé teszi a tagállamok számára, hogy meghatározzák, hogy a nemzeti hatóságokra és testületekre ki lehet-e szabni közigazgatási bírságokat, és ha igen, milyen mértékben. Ahol a tagállamok élnek ezzel a lehetőséggel, ez nem fosztja meg az adatvédelmi hatóságokat attól a jogtól, hogy az összes többi korrekciós jogkört is alkalmazzák a nemzeti hatóságokkal és testületekkel szemben[12].

[11] A bírságot kiszabó határozatok közül sok jelenleg bírósági felülvizsgálat tárgyát képezi.
[12] A GDPR 83. cikkének (7) bekezdése.

Egy másik konkrét kérdés a bíróságok felügyelete: bár a GDPR a bíróságok tevékenységeire is kiterjed, ők mentesülnek az adatvédelmi hatóságok általi felügyelet alól, ha az igazságszolgáltatási feladatkörükben járnak el. Mindazonáltal a Charta és az EUMSZ arra kötelezi a tagállamokat, hogy az igazságügyi rendszerükön belül egy független szervet bízzanak meg az ilyen jellegű adatkezelési műveletek felügyeletével[13].

Együttműködés más szabályozókkal

Ahogyan 2019. júliusi közleményében bejelentette, a Bizottság támogatja a más szabályozókkal való interakciót, a vonatkozó hatáskörök teljes körű betartása mellett. Az együttműködés ígéretes területei magukban foglalják a fogyasztóvédelmet és a versenyt. A Testület jelezte, hogy hajlandó együttműködni más szabályozókkal, különösen a digitális piacokon tapasztalható koncentrációval kapcsolatban[14]. A Bizottság felismerte a magánélet és az adatvédelem mint a verseny minőségi paraméterének jelentőségét[15]. A Testület tagjai a fogyasztóvédelmi együttműködési hálózattal közös, az uniós fogyasztóvédelmi és adatvédelmi jogszabályok hatékonyabb végrehajtásáról szóló munkaértekezleteken vettek részt. E megközelítés alkalmazása a kölcsönös megértés előmozdítása és a fogyasztók által különösen a digitális gazdaság terén tapasztalt konkrét problémák leküzdésére irányuló gyakorlati módszerek kialakítása érdekében folytatódik.

A magánélet és adatok védelmére irányuló, összehangolt megközelítés biztosítása érdekében és az elektronikus adatvédelemről szóló rendelet elfogadásának függvényében elengedhetetlen a szoros együttműködés az elektronikus kommunikáció területén lex specialisnak minősülő, az elektronikus adatvédelemről szóló irányelv[16] végrehajtásáért felelős hatóságokkal. A kiberbiztonsági irányelv[17] alapján illetékes hatóságokkal, valamint a hálózat- és információbiztonsággal foglalkozó együttműködési csoporttal való szorosabb együttműködés kölcsönösen előnyös lenne e hatóságok és az adatvédelmi hatóságok számára is.

2.2 Az együttműködési és egységességi mechanizmusok

A GDPR létrehozta az együttműködési mechanizmust (a vállalkozások számára biztosított egyablakos ügyintézési rendszerek, az adatvédelmi hatóságok együttes műveletei és egymás közötti kölcsönös segítségnyújtás) és az egységességi mechanizmust annak érdekében, hogy a hatóságok közötti esetleges viták egységes értelmezésén és Testület általi rendezésén keresztül támogassa az adatvédelmi szabályok egységes alkalmazását.

---

[13] A Charta 8. cikkének (3) bekezdése; Az EUMSZ 16. cikkének (2) bekezdése; a GDPR (20) preambulumbekezdése.

[14] Vö. a Testületnek a gazdasági koncentráció adatvédelmi hatásairól szóló nyilatkozatával, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_hu.pdf

[15] Lásd a COMP M. 8124. számú, Microsoft/LinkedIn ügyet.

[16] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv), HL L 201., 2002.7.31., 37–47. o.

[17] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, HL L 194., 2016.7.19., 1–30. o.

A valamennyi adatvédelmi hatóságot magában foglaló Testület jogi személyiséggel rendelkező uniós szervként jött létre, és teljeskörűen működőképes, munkáját titkárság támogatja[18]. A fent említett két mechanizmus működéséhez elengedhetetlen. 2019 végére a Testület 67 dokumentumot fogadott el, beleértve 10 új iránymutatást[19] és 43 véleményt[2021].

A Testület fontos szerepe akkor mutatkozott meg, amikor gyorsan kellett biztosítani a GDPR egységes értelmezését, és uniós szinten meg kellett találni az azonnal alkalmazható megoldásokat. Például a Covid19-világjárvány kitörése tekintetében 2020 márciusában a Bizottság a személyes adatok kezeléséről szóló nyilatkozatot fogadott el, amely többek közt az adatkezelés jogszerűségével és a mobil helymeghatározó adatok e tekintetben történő használatával foglalkozik[22], 2020 áprilisában pedig az egészségügyi adatoknak a Covid19-járvánnyal összefüggésben végzett tudományos kutatás céljából történő kezeléséről szóló iránymutatást [23], valamint a Covid19-járvánnyal összefüggésben a helymeghatározási adatok és a kontaktkövető eszközök használatáról szóló iránymutatást[24] fogadott el. A Testület ezenkívül jelentős mértékben hozzájárult a kontaktkövető alkalmazásokhoz való uniós megközelítés Bizottság és tagállamok általi kialakításához.

Az adatvédelmi hatóságok közötti napi együttműködés, függetlenül attól, hogy saját nevükben vagy a Testület tagjaként járnak-e el, a hatóságok által elindított ügyekre vonatkozó információk és értesítések cseréjén alapul. A hatóságok közötti kommunikáció megkönnyítése érdekében a Bizottság jelentős támogatást adott azáltal, hogy információcserére irányuló rendszert bocsátott a rendelkezésükre[25]. A legtöbb hatóság úgy véli, hogy a rendszer megfelel az együttműködési és egységességi mechanizmusok szükségleteinek, bár további finomhangolásra még sor kerülhetne, például azzal, ha a rendszer felhasználóbarátabbá válna.

Bár még korai szakaszban vagyunk, számos eredmény és kihívás azonosítható, amelyeket az alábbiakban ismertetünk. Ezek rámutatnak arra, hogy az adatvédelmi hatóságok eddig hatékonyan alkalmazták az együttműködési eszközöket, és a rugalmasabb megoldásokat részesítik előnyben.

Egyablakos ügyintézés

---

[18] A titkársági tevékenységekre vonatkozó részletekért lásd a Testület hozzájárulásának 24–26. oldalát.

[19] A 29. cikk alapján létrehozott munkacsoport által a GDPR hatálybalépését megelőző időszakban elfogadott és a Testület által jóváhagyott 10 iránymutatás mellett. Ezenkívül a Testület 4 további iránymutatást fogadott el 2020 januárja és májusának vége között, valamint egyet frissített.

[20] E vélemények közül 42-t a GDPR 64. cikke alapján, egyet pedig a GDPR 70. cikke (1) bekezdésének s) pontja alapján fogadtak el, és a Japánnal kapcsolatos megfelelőségi határozatra vonatkozott.

[21] A Testület tevékenységeinek teljes körű áttekintéséért lásd a Testület hozzájárulásának 18–23. oldalát.

[22] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[23] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_hu.

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_hu.pdf

[25] Belső piaci információs rendszer („IMI”).

Főszabályként elmondható, hogy határokon átívelő ügyekben az adott tagállam adatvédelmi hatósága (i) vezető hatóságként járhat el, ha a vállalkozás üzleti tevékenységének fő helye abban a tagállamban található; vagy (ii) érintett hatóságként léphet fel, ha a vállalkozás rendelkezik tevékenységi hellyel a tagállamban, ha a tagállamban élő természetes személyek jelentős mértékben érintettek, vagy ha panaszt nyújtottak be hozzá.

Az ilyen szoros együttműködés napi gyakorlat lett: a GDPR alkalmazásának kezdőnapjától valamennyi tagállam adatvédelmi hatóságai voltak már vezető vagy érintett hatóságként azonosítva a határokon átívelő ügyekben, bár eltérő mértékben.

2018 májusától 2019 végéig az írországi adatvédelmi hatóság járt el a legtöbb, határokon átívelő ügyben vezető hatóságként (127), őt követte Németország (92), Luxemburg (87), Franciaország (64) és Hollandia (45). Ez a rangsor tükrözi többek közt a számos nemzetközi technológiai társaságnak helyet adó Írország és Luxemburg különleges helyzetét.

A rangsor az érintett adatvédelmi hatóságként való fellépés tekintetében eltérő; a németországi hatóságok vettek részt a legtöbb ügyben (435), őket követte Spanyolország (337), Dánia (327), Franciaország (332) és Olaszország (306)[26].

2018. május 25. és 2019. december 31. között 141 határozattervezetet nyújtottak be az egyablakos ügyintézési eljáráson keresztül, amelyből 79 eredményezett végleges határozatot. Az e jelentés közzétételének idején számos fontos, határokon átívelő dimenzióval rendelkező határozat és egyablakos ügyintézési eljárás van folyamatban. A határozatok közül néhány nagy nemzetközi technológiai vállalatokra vonatkozik[27]. Ezek várhatóan további pontosítást adnak, és hozzájárulnak a GDPR értelmezésének nagyobb fokú összehangolásához.

Kölcsönös segítségnyújtás

Az adatvédelmi hatóságok széles körben alkalmazzák a kölcsönös segítségnyújtási eszközt.

2019 végére 115 kölcsönös segítségnyújtási[28] eljárásra került sor, különösen vizsgálatok elvégzése céljából, amelyek közül a legtöbbet a spanyol (26), a német (20), a dán (13), a lengyel (12) és a cseh (10) adatvédelmi hatóságok indítottak. Ezzel párhuzamosan Írország (19), Franciaország (11), Ausztria (10), Németország (10) és Luxemburg (9) kapta a legtöbb kérelmet[29].

A hatóságok jelentős többsége az együttműködés rendkívül hasznos eszközének tartja a kölcsönös segítségnyújtást, és nem szembesült semmilyen akadállyal a kölcsönös segítségnyújtási eljárás alkalmazása során. Az önkéntes kölcsönös segítségnyújtást,

---

[26] Lásd a Testület hozzájárulásának 8. oldalát.

[27] 2020. május 22-én például az ír adatvédelmi hatóság a Twitter nemzetközi vállalatnak az adatvédelmi incidensek bejelentésére vonatkozó vizsgálatával kapcsolatos határozattervezetet nyújtott be más érintett hatóságok részére a rendelet 60. cikkével összhangban. Ugyanezen a napon az ír adatvédelmi hatóság bejelentette, hogy a WhatsApp Ireland Limitedre vonatkozó határozattervezet 60. cikk szerinti benyújtása áll előkészítés alatt, az átláthatósággal kapcsolatban, beleértve az általa a Facebookkal megosztott információk átláthatóságát.

[28] A GDPR 61. cikke.

[29] Lásd a Testület hozzájárulásának 12–14. oldalát.

amely esetében nem áll fenn jogszabályi határidő vagy szigorú válaszadási kötelezettség, gyakrabban alkalmazták, 2 427 eljárás során. Írország adatvédelmi hatósága küldte és fogadta a legnagyobb számban a kölcsönös segítségnyújtásra irányuló kérelmeket (527 elküldött és 359 beérkező kérelem), őt követték a német hatóságok (260 elküldött és 356 beérkező kérelemmel).

Másrészről még nem került sor közös műveletekre[30], amelyek lehetővé tennék, hogy számos tagállam adatvédelmi hatósága már vizsgálati szinten részt vegyen a határokon átívelő ügyekben. A Testület folyamatosan vizsgálja ennek az eszköznek a gyakorlati végrehajtását és alkalmazásának előmozdítását.

Az egységességi mechanizmus

Eddig csak az egységességi mechanizmus első pillérjét vették igénybe, nevezetesen a Testület véleményeinek elfogadását[31]. Másrészről eddig még nem került sor testületi szintű vitarendezésre[32] vagy sürgősségi eljárásra[33].

2018. május 25. és 2019. december 31. között a Testület 36 véleményt adott ki a valamely tagja által bevezetett intézkedések elfogadása kapcsán[34]. A legtöbb vélemény (31) az adatvédelmi hatásvizsgálatot igénylő adatkezelési műveletek nemzeti jegyzékeinek elfogadására vonatkozott. Két vélemény a kötelező erejű vállalati szabályokkal volt kapcsolatos, két másik a magatartási kódex ellenőrző szervére vonatkozó akkreditációs követelmények tervezetére, egy pedig az általános szerződési feltételekre vonatkozott[35].

A Testület továbbá hat véleményt fogadott el kérésre[36]. Ezek közül három az adatvédelmi hatásvizsgálatot nem igénylő adatkezelési műveleteket azonosító nemzeti jegyzékekre vonatkozott. A többi pedig egy, a személyes adatoknak az EGT és nem EGT-beli pénzügyi felügyeleti hatóságok közötti továbbítására vonatkozó közigazgatási intézkedésre, az elektronikus adatvédelemről szóló irányelv és a GDPR közötti kölcsönhatásra, valamint egy felügyeleti hatóságnak a fő vagy egyetlen tevékenységi központtal kapcsolatos körülmények változása esetén fennálló hatáskörére vonatkozott[37].

A kezelendő kihívások

Bár az adatvédelmi hatóságok rendkívül aktívan dolgoztak együtt a Testülettel, és már intenzíven használják a kölcsönös segítségnyújtás együttműködési eszközét, a valóban közös adatvédelmi kultúra kialakítása még folyamatban van.

A határokon átívelő ügyek kezeléséhez különösen hatékonyabb és összehangoltabb megközelítésre és a GDPR-ban meghatározott valamennyi együttműködési eszköz hatékony alkalmazására van szükség. Ebben a pontban rendkívül széles körű a konszenzus, mivel ezt különböző módokon az Európai Parlament, a Tanács, az

[30] A GDPR 62. cikke.
[31] A GDPR 64. cikke alapján.
[32] A GDPR 65. cikke.
[33] A GDPR 66. cikke.
[34] A GDPR 64. cikkének (1) bekezdése értelmében.
[35] A GDPR 28. cikkének (8) bekezdése.
[36] A GDPR 64. cikkének (2) bekezdése értelmében.
[37] Lásd a Testület hozzájárulásának 15. oldalát.

európai adatvédelmi biztos, az érdekelt felek (a több érdekelt felet tömörítő szakértői csoporton belül és azon kívül), valamint az adatvédelmi hatóságok is felvetették.

A legfontosabb megoldandó problémák e tekintetben az alábbiak terén fennálló különbségeket foglalják magukban:

- nemzeti közigazgatási eljárások, különös tekintettel az alábbiakra: panaszkezelési eljárások, a panaszok elfogadhatósági feltételei, az eljárások időtartama a különböző időkeretek vagy a határidők hiánya miatt, az a pont az eljárásban, amikor megadják a meghallgatáshoz való jogot, a panaszosok tájékoztatása és bevonása az eljárás során;
- az együttműködési mechanizmussal kapcsolatos fogalmak értelmezései, például a releváns információ, a „késedelem nélkül" fogalma, a „panasz", a vezető adatvédelmi hatóság „határozattervezeteként" definiált dokumentum, a békés vitarendezés (különös tekintettel a békés vitarendezéshez vezető eljárásra és a vitarendezés jogi formájára); valamint
- az a megközelítés, hogy mikor kell együttműködési eljárást indítani, bevonni az érintett adatvédelmi hatóságokat és tájékoztatást nyújtani számukra. A panaszosok nincsenek tájékoztatva arról, hogy miként kezelik az ügyüket határokon átívelő helyzetekben, ahogyan ezt a több érdekelt félt tömörítő szakértői csoport számos tagja kiemelte. Ezenkívül a vállalkozások megemlítik, hogy egyes esetekben a nemzeti adatvédelmi hatóságok nem utalták az ügyeket a vezető adatvédelmi hatósághoz, hanem helyi ügyekként kezelték őket.

A Bizottság üdvözli a Testület bejelentését arról, hogy megkezdte az ezen aggodalmak kezelésére vonatkozó vizsgálatot. A Testület jelezte, hogy egyértelműsíteni fogja a vezető adatvédelmi hatóság és az érintett adatvédelmi hatóságok közötti együttműködéssel kapcsolatos eljárási lépéseket, elemezni fogja a közigazgatási eljárásokra vonatkozó nemzeti jogszabályokat, a kulcsfogalmak közös értelmezésén fog dolgozni, és meg fogja erősíteni a kommunikációt és együttműködést (beleértve a közös műveleteket). A Testület vizsgálata és elemzése azt fogja eredményezni, hogy a határokon átívelő ügyekben hatékonyabb munkafeltételeket alakítsanak ki[38], többek közt a tagjainak szakértelmére alapozva és a titkársága részvételét megerősítve. Ezenkívül megjegyzendő, hogy a Testületnek a GDPR egységes értelmezésének biztosítása terén fennálló felelőssége nem merül ki a legkisebb közös nevező megtalálásában.

Végezetül uniós szervként a Testületnek az uniós közigazgatási jogot is alkalmaznia kell, és biztosítania kell az átláthatóságot a döntéshozatali folyamat során.

2.3 Tanácsadás és iránymutatások

Tájékoztatás és tanácsadás az adatvédelmi hatóságok részéről

Számos adatvédelmi hatóság új eszközöket hozott létre, például a természetes személyeknek és vállalkozásoknak szóló segélyvonalakat és a vállalkozásoknak szóló eszköztárakat[39]. Számos vállalkozó üdvözli az e hatóságok pragmatizmusát, amelyet a

[38] Ahogyan arra a Tanács álláspontja és megállapításai is rámutatnak.
[39] Lásd alább a 7. pontban.

GDPR alkalmazásában nyújtott segítség során mutattak. Sokan közülük aktívan és szorosan együttműködtek és kommunikáltak az adatvédelmi tisztviselőkkel, többek az adatvédelmi tisztviselők szövetségein keresztül. Számos hatóság iránymutatásokat adott ki, amelyek az adatvédelmi tisztviselők szerepére terjedtek ki, valamint arra, hogy az adatvédelmi tisztviselőket támogatni kell a napi tevékenységeik során, és kifejezetten nekik szóló szemináriumokat kell tartani. Mindazonáltal nem minden adatvédelmi hatóság esetében ez a helyzet.

Az érdekelt felektől kapott visszajelzések számos problémára rámutatnak az iránymutatásokkal és tanácsadással kapcsolatban is:

- a nemzeti adatvédelmi hatóságok közötti egységes megközelítés és iránymutatás hiánya bizonyos kérdésekben (pl. a sütikkel[40], a jogos érdek alkalmazásával, az adatvédelmi incidensek bejelentésével vagy az adatvédelmi hatásvizsgálatokkal kapcsolatban) vagy az ugyanazon tagállamon belüli adatvédelmi hatóságok közötti egységes megközelítés és iránymutatás hiánya (pl. Németországban az adatkezelő és adatfeldolgozó fogalma kapcsán);
- a nemzeti szinten elfogadott és a Testület által elfogadott iránymutatások közötti egységesség hiánya;
- a nemzeti szinten elfogadott egyes iránymutatásokra vonatkozó nyilvános konzultációk hiánya;
- az érdekelt felek bevonásának eltérő szintjei az adatvédelmi hatóságok körében;
- késedelmek a tájékoztatásra irányuló kérelmekre adott válaszok kézbesítése során;
- nehézségek azon a téren, hogy gyakorlati és értékelhető tanácsot lehessen kapni az adatvédelmi hatóságoktól;
- egyes adatvédelmi hatóságoknál az ágazati szakértelem szintje növelésének szükségessége (pl. az egészségügyi és gyógyszerészeti ágazat).

E problémák közül sok a számos adatvédelmi hatóságnál fennálló erőforráshiánnyal is összefügg.

Különböző gyakorlatok az adatvédelmi incidensek bejelentése terén[41]

Míg a Tanács kiemeli az ilyen bejelentések okozta terhet, jelentős ellentmondások állnak fenn a tagállamok között a bejelentések terén: míg 2018 májusa és 2019 novemberének vége között a legtöbb tagállamban az adatvédelmi incidensek bejelentésének teljes száma 2000 alatt, 7 tagállamban pedig 2000 és 10 000 között volt, a holland és a német adatvédelmi hatóságok 37 400 és 45 600 bejelentésről számoltak be[42].

[40] Az elektronikus adatvédelemről szóló rendelet elfogadásának függvényében az elektronikus adatvédelemről szóló irányelv végrehajtásáért felelős, tagállamokon belüli illetékes hatóságok szoros együttműködésére van szükség. Az irányelvvel összhangban egyes tagállamokban az elektronikus adatvédelemről szóló irányelv 5. cikke (3) bekezdésének (amely meghatározza azokat a feltételeket, amelyek alapján „sütik" állíthatók be és érhetők el a felhasználó végberendezésén) végrehajtásáért felelős hatóságok nem ugyanazok, mint a GDPR szerinti felügyeleti hatóságok.

[41] A GDPR 33. cikke.

[42] Lásd a Testület hozzájárulásának 35. oldalát.

Ez az egységes értelmezés és végrehajtás hiányára mutathat rá, annak ellenére, hogy léteznek uniós szintű iránymutatások az adatvédelmi incidensek bejelentésével kapcsolatban.

Az Európai Adatvédelmi Testület iránymutatásai

Napjainkig a Testület több mint 20 iránymutatást fogadott el, amelyek a GDPR fő aspektusaival foglalkoznak[43]. Az iránymutatások a GDPR egységes alkalmazásának elengedhetetlen eszközei, ezért azokat az érdekelt felek jelentős mértékben üdvözölték. Az érdekelt felek nagyra értékelték a (6–8 hetes) nyilvános konzultációt. Mindazonáltal több párbeszédet szeretnének a Testülettel. E tekintetben folytatni és bővíteni kell az iránymutatások elkészítése előtti, a célzott témákról szóló munkaértekezletek szervezésének gyakorlatát, hogy biztosítani lehessen a Testület munkájának átláthatóságát, inkluzivitását és relevanciáját. Az érdekelt felek ezenkívül azt kérik, hogy a legvitatottabb kérdések értelmezése az iránymutatásokban szerepeljen, mivel ezek nyilvános konzultáció tárgyát képezik, és ne a GDPR 64. cikkének (2) bekezdése szerinti véleményekben. Egyes érdekelt felek ezenkívül gyakorlatiasabb irányelveket kérnek, amelyek részletezik a GDPR fogalmainak és rendelkezéseinek alkalmazását[44]. A több érdekelt felet tömörítő szakértői csoport tagjai hangsúlyozták, hogy konkrétabb problémákra van szükség annak érdekében, hogy a lehető legnagyobb mértékben csökkenteni lehessen az adatvédelmi hatóságok közötti eltérő értelmezések terét. Ugyanakkor a GDPR alkalmazásának egyértelműsítésére és a jogbiztonság biztosítására irányuló kérelmek nem vezethetnek további követelményekhez, vagy nem csökkenthetik a kockázatalapú megközelítés és az elszámoltathatósági elv előnyeit.

Az érdekelt felek részéről a Testület további iránymutatását igénylő témák többek közt az alábbiak: az érintettek jogainak alkalmazási köre (beleértve a foglalkoztatás tekintetében); a jogos érdek alapján végzett adatkezelésről szóló vélemény módosításai; az adatkezelő, a közös adatkezelő és az adatfeldolgozó fogalma, valamint a felek közötti szükséges intézkedések[45]; a GDPR alkalmazása új technológiák esetén (például blokklánc vagy mesterséges intelligencia); adatkezelés tudományos kutatások keretében (többek közt a nemzetközi együttműködéssel kapcsolatban); gyermekek adatainak kezelése; álnevesítés és anonimizálás; valamint az egészségre vonatkozó adatok kezelése.

A Testület már jelezte, hogy e témák közül számos tekintetében fog kiadni iránymutatást, és már többel kapcsolatban megkezdődött a munka (pl. a jogos érdeknek az adatkezelés jogalapjaként történő alkalmazásáról).

Az érdekelt felek arra kérik a Testületet, hogy szükség esetén módosítsák és vizsgálják felül a meglévő iránymutatásokat, figyelembe véve a közzétételük óta szerzett gyakorlatot, és kihasználva a lehetőséget, hogy, ha szükséges, még részletesebbé tegyék azokat.

---

[43] Az iránymutatásokra vonatkozó munka a GDPR alkalmazásának 2018. május 25-i kezdő időpontja előtt megkezdődött a 29. cikk alapján létrehozott munkacsoport keretében. Az iránymutatások teljes jegyzékét lásd a https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_hu oldalon.

[44] Ezt az Európai Parlament és a Tanács is kiemelte.

[45] A Testület adatkezelőkre és adatfeldolgozókra vonatkozó iránymutatásának elkészítése jelenleg folyamatban van.

2.4 Az adatvédelmi hatóságok erőforrásai

A feladatok hatékony elvégzése és a jogkörök gyakorlása érdekében elengedhetetlen, és ezért a függetlenségük alapvető feltétele, hogy az egyes adatvédelmi hatóságok számára biztosítottak legyenek a szükséges emberi, technikai és pénzügyi erőforrások, helyszínek és infrastruktúra[46].

A legtöbb adatvédelmi hatóságnál a GDPR 2016. évi hatálybalépése óta nőtt a személyzet és az erőforrások mennyisége[47]. Mindazonáltal közülük többen továbbra is arról számolnak be, hogy nem áll a rendelkezésükre elegendő erőforrás[48].

A nemzeti adatvédelmi hatóságoknál dolgozó személyek száma

Az EGT figyelembe vett adatvédelmi hatóságainál dolgozó személyek teljes száma 42 %-kal nőtt 2016 és 2019 között (62 %-kal, ha figyelembe vesszük a 2020. évi előrejelzést).

Ezen időszak alatt a legtöbb hatóságnál nőtt a személyzet száma, a legnagyobb mértékben (százalékos arányban mérve) Írországban (+169 %-kal), Hollandiában (+145 %-kal), Izlandon (+143 %-kal), Luxemburgban (+126 %-kal) és Finnországban (+114 %-kal). Másrészről számos adatvédelmi hatóságnál csökkent a személyzet száma, a legnagyobb mértékben Görögországban (–15 %-kal), Bulgáriában (–14 %-kal), Észtországban (–11 %-kal), Lettországban (–10 %-kal) és Litvániában (–8 %-kal). Egyes hatóságoknál a személyzet számának csökkentése azzal is magyarázható, hogy az adatvédelmi szakértők a kedvezőbb feltételeket kínáló magánszektorba mentek át.

Általánosságban a 2020-ra szóló előrejelzés 2019-hez képest nagyobb számú személyzetet jelez, kivéve az Ausztriában, Bulgáriában, Olaszországban, Svédországban és Izlandon (ahol a személyzet száma várhatóan stabil marad), valamint Cipruson és Dániában található hatóságok esetében (ahol a személyzet száma várhatóan csökkenni fog).

A német adatvédelmi hatóságok[49] közösen rendelkeznek a legnagyobb számú személyzettel (888 2019-ben/1002 a 2020. évi előrejelzés szerint), őket követik a lengyel (238/260), a francia (215/225), a spanyol (170/220), a holland (179/188), az olasz (170/170) és az ír (140/176) adatvédelmi hatóságok.

A legkisebb számú személyzettel rendelkező adatvédelmi hatóságok Ciprusban (24/22), Lettországban (19/31), Izlandon (17/17), Észtországban (16/18) és Máltán (13/15) találhatók.

A nemzeti adatvédelmi hatóságok költségvetése

Az EGT figyelembe vett adatvédelmi hatóságainak költségvetése 49 %-kal nőtt 2016 és 2019 között (64 %-kal, ha figyelembe vesszük a 2020. évi előrejelzést).

---

[46] Lásd a GDPR 52. cikkének (4) bekezdését.

[47] A rendelet 2016 májusában lépett hatályba, és alkalmazásának kezdete 2018 májusa volt, egy kétéves átmeneti időszakot követően.

[48] Lásd a Testület hozzájárulásának 26–30. oldalát.

[49] 18 hatóság van Németországban, közülük egy szövetségi hatóság, 17 pedig regionális hatóság (beleértve kettőt Bajorországban).

Ezen időszak alatt a legtöbb hatóságnál nőtt a költségvetés, a legnagyobb mértékben (százalékos arányban mérve) Írországban (+223 %-kal), Izlandon (+167 %-kal), Luxemburgban (+165 %-kal), Hollandiában (+130 %-kal) és Cipruson (+114 %-kal). Másrészről egyes hatóságoknál csak kis mértékű költségvetési növekedés volt tapasztalható, a legkisebb növekedést az észt (7 %), a lett (4 %), a román (3 %) és a belga (1 %) adatvédelmi hatóságoknál mérték, Franciaországban pedig csökkent a hatóság költségvetése (–2 %-kal).

Általánosságban a 2020-ra szóló előrejelzés költségvetési növekedést vetít előre 2019-hez képest, kivéve Ausztria, Bulgária, Észtország és Hollandia hatósága tekintetében (amelyeknél a költségvetés várhatóan stabil marad).

A legnagyobb költségvetéssel rendelkező adatvédelmi hatóságok Németországban (76,6 millió EUR 2019-ben/85,8 millió EUR a 2020-as előrejelzés szerint), Olaszországban (29,1/30,1), Hollandiában (18,6/18,6), Franciaországban (18,5/20,1) és Írországban (15,2/16,9) találhatók.

A legkisebb költségvetéssel rendelkező adatvédelmi hatóságok Horvátországban (1,2 millió EUR 2019-ben/1,4 millió EUR a 2020-as előrejelzés szerint), Romániában (1,1/1,3), Lettországban (0,6/1,2), Cipruson (0,5/0,5) és Máltán (0,5/0,6) találhatók.

A II. mellékletben található táblázat áttekintést nyújt a nemzeti adatvédelmi hatóságok emberi és költségvetési erőforrásairól.

Azon túl, hogy kihat a szabályok nemzeti szintű végrehajtására irányuló kapacitásra, az erőforrások hiánya korlátozza az adatvédelmi hatóságok azon kapacitását is, hogy részt vegyenek az együttműködési és egységességi mechanizmusokban és a Testület által végzett munkában, valamint hogy azokhoz hozzájáruljanak. Ahogyan a Testület kiemeli, az egyablakos mechanizmus sikere attól függ, hogy az adatvédelmi hatóságok mennyi időt és erőfeszítést tudnak az egyes, határokon átívelő ügyek kezelésére és az azokkal kapcsolatos együttműködésre szentelni. Az erőforrás-probléma összefügg azzal is, hogy a hatóságok egyre nagyobb szerepet játszanak a nagy méretű, jelenleg fejlesztés alatt álló IT-rendszerek felügyeletében. Ezenkívül az írországi és luxemburgi adatvédelmi hatóságok speciális erőforrás-szükségletekkel rendelkeznek, mivel vezető hatóságként járnak el a GDPR végrehajtása terén a nagy technológiai vállalatok esetében, amelyek főképp ezekben a tagállamokban találhatók.

Míg a Tanács az együttműködési mechanizmus és határidőinek az adatvédelmi hatóságok munkájára gyakorolt hatását emeli ki[50], a GDPR arra kötelezi a tagállamokat, hogy biztosítsanak megfelelő emberi, pénzügyi és technikai erőforrásokat a nemzeti adatvédelmi hatóságaik részére[51].

A Testület titkársága, amelyet az európai adatvédelmi biztos biztosít[52], jelenleg 20 személyből áll, beleértve jogi, IT-s és kommunikációs szakértőket. Értékelni kell, hogy ennek a számnak a jövőben változnia kell-e annak érdekében, hogy a titkárság hatékonyan teljesíteni tudja az elemzői, adminisztratív és logisztikai támogatást a

[50] A GDPR 60. cikke.
[51] A GDPR 52. cikkének (4) bekezdése.
[52] A GDPR 75. cikke.

Testületnek és az alcsoportjainak, többek közt az információcserére irányuló rendszer irányításán keresztül.

3 ÖSSZEHANGOLT SZABÁLYOK, AZONBAN TOVÁBBRA IS BIZONYOS FOKÚ SZÉTTÖREDEZETTSÉG ÉS ELTÉRŐ MEGKÖZELÍTÉSEK

A GDPR az adatvédelmi szabályokkal kapcsolatban EU-szerte egységes megközelítést ír elő, amely az 1995. évi adatvédelmi irányelv szerint fennálló különböző nemzeti rendszerek helyébe lép.

3.1 A GDPR tagállamok általi végrehajtása

A GDPR 2018. május 25. óta közvetlenül alkalmazandó minden tagállamban. Jogalkotásra kötelezte a tagállamokat, különösen arra, hogy nemzeti adatvédelmi hatóságokat hozzanak létre, és alakítsák ki a tagjaikra vonatkozó általános feltételeket annak érdekében, hogy biztosítsák, hogy mindegyik hatóság a GDPR-ral összhangban teljes körű függetlenséggel járjon el a feladatai végrehajtása és a hatáskörei gyakorlása során. A jogi kötelezettségek és a közfeladatok csak akkor tekinthetők a személyesadat-kezelés jogalapjának, ha azokat az (uniós vagy) nemzeti jog határozza meg. Ezenkívül a tagállamoknak meg kell határozniuk a büntetésekre vonatkozó szabályokat, különös tekintettel a közigazgatási bírsággal nem érintett szabálysértésekre, és össze kell egyeztetniük a személyes adatok védelméhez való jogot a véleménynyilvánítás és a tájékozódás szabadságához való joggal. A nemzeti jog továbbá jogalapot adhat a személyes adatok különleges kategóriái kezelésének általános tilalmától való eltérésre, például a népegészségügy területét érintő jelentős közérdek miatt, beleértve a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelmet. Ezenkívül a tagállamoknak biztosítaniuk kell a tanúsító szervek akkreditációját.

A Bizottság nyomon követi a GDPR nemzeti jogszabályokban történő végrehajtását. E jelentés készítésekor Szlovénia kivételével valamennyi tagállam új adatvédelmi jogszabályokat fogadott el, vagy módosította az e területen fennálló törvényeit. A Bizottság ezért felkérte Szlovéniát, hogy adjon tájékoztatást az eddig megvalósított előrehaladásról, és sürgette, hogy zárja le ezt a folyamatot[53].

Ezenkívül a nemzeti jogszabályok adatvédelmi szabályoknak való, a schengeni vívmányokkal kapcsolatos megfelelésének értékelésére is sor kerül a Bizottság által koordinált schengeni értékelési mechanizmus keretében. A Bizottság és a tagállamok együttesen értékelik, hogy az országok miként hajtják végre és alkalmazzák a schengeni vívmányokat számos területen; az adatvédelem tekintetében ez a nagy méretű IT-rendszereket érinti, mint amilyen például a Schengeni Információs Rendszer és a Vízuminformációs Rendszer, és kiterjed az adatvédelmi hatóságoknak az e rendszereken belüli személyesadat-kezelés felügyeletében játszott szerepére.

Az ágazati jogszabályok módosítására irányuló munka jelenleg is folyamatban van nemzeti szinten. A GDPR-nak az Európai Gazdasági Térségről szóló megállapodásba való beépítését követően a rendelet alkalmazási köre Norvégiára, Izlandra és

[53] Megjegyzendő, hogy a szlovéniai nemzeti adatvédelmi hatóságot a jelenlegi nemzeti adatvédelmi törvény alapján hozták létre, és az felügyeli a GDPR végrehajtását a tagállamban.

Liechtensteinre is kiterjed. Ezek az országok szintén elfogadták a nemzeti adatvédelmi jogszabályaikat.

A Bizottság a rendelkezésére álló valamennyi eszközt – ezen belül a kötelezettségszegési eljárásokat is – alkalmazni fogja, hogy biztosítsa a tagállamok GDPR-nak való megfelelését.

A nemzeti végrehajtással kapcsolatos fő problémák

A nemzeti jogszabályok folyamatban lévő értékelésének és a tagállamokkal folytatott kétoldalú információcsere részeként eddig azonosított fő problémák az alábbiakat foglalják magukban:

- A GDPR alkalmazására vonatkozó korlátozások: egyes tagállamok például teljes mértékben kizárják a nemzeti parlament tevékenységeit;
- Különbségek a vonatkozó nemzeti jogszabályok alkalmazhatósága terén. Egyes tagállamok a nemzeti jogszabályaik alkalmazhatóságát ahhoz kapcsolják, hogy hol kerül sor az áruk vagy szolgáltatások forgalmazására, míg mások ahhoz, hogy hol található az adatkezelő vagy az adatfeldolgozó székhelye. Ez ellentétes a GDPR-ban foglalt jogharmonizációs céllal;
- Nemzeti jogszabályok, amelyek kérdéseket vetnek fel az adatvédelemhez való jogba történő beavatkozás arányossága terén. A Bizottság például kötelezettségszegési eljárást indított egy tagállam ellen, amely olyan jogszabályt vezetett be, amely arra kötelezte a bírákat, hogy közöljenek bizonyos információkat a nem szakmai tevékenységeikről, ami nem összeegyeztethető a magánélet tiszteletben tartásához való joggal és a személyes adatok védelméhez való joggal[54];
- Az igazságszolgáltatási feladatkörükben eljáró bíróságok által végzett adatkezelés felügyeletéért felelős független szervezet hiánya[55].
- A teljes mértékben a GDPR által szabályozott területeken az előírásokra vagy korlátozásokra meghatározott mozgástéren túlmutató jogszabályok. Különösen ez a helyzet, ahol a nemzeti rendelkezések az adatkezelő és az érintett természetes személyek érdekei egyensúlyának biztosításával meghatározzák a jogos érdeken alapuló adatkezelés feltételeit, míg a GDPR arra kötelez minden adatkezelőt, hogy ezt az egyensúlyt egyedi alapon határozzák meg, és ezt a jogalapot egyedi alapon alkalmazzák.
- Előírások és további követelmények a jogi kötelezettségnek való megfelelés vagy közfeladat ellátása céljából végzett adatkezelésen túl (pl. videófelügyelet a magánágazatban vagy közvetlen üzletszerzés esetén); valamint a GDPR-ban használt fogalmak (pl. „nagymértékű” vagy „törlés”) tekintetében.

---

[54] Ez a kötelezettségszegési eljárás a bíróságról szóló, 2019. december 20-i lengyel törvényre vonatkozik, amely a bírák függetlenségét érinti, és többek közt a bírák nem szakmai tevékenységekben való részvételének közlésével foglalkozik: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_772.

[55] Lásd a Charta 8. cikkének (3) bekezdését; az EUMSZ 16. cikke; a GDPR (20) preambulumbekezdése.

E problémák közül néhányat a Bíróság pontosíthat olyan ügyekben, amelyek jelenleg folyamatban vannak[56].

A személyes adatok védelméhez való jog, valamint a véleménynyilvánítás és tájékozódás szabadságához való jog összeegyeztetése

Az egyik konkrét probléma a tagállamok azon kötelezettségének teljesítésére vonatkozik, amely szerint össze kell egyeztetniük a személyes adatok védelméhez való jogot a véleménynyilvánítás és tájékozódás szabadságával[57]. Ez a probléma rendkívül összetett, mivel az e két alapvető jog közötti egyensúly értékelése során figyelembe kell venni a sajtóra és médiára vonatkozó jogszabályokban foglalt rendelkezéseket és garanciákat.

A tagállami jogszabályok értékelése azt mutatja, hogy a személyes adatok védelméhez való jog, valamint a véleménynyilvánítás és tájékozódás szabadságához való jog összeegyeztetését különböző módokon közelítik meg:

- Egyes tagállamok előírják, hogy a véleménynyilvánítás szabadsága elsőbbséget élvez, vagy elvben mentesítenek a GDPR 85. cikkének (2) bekezdésében foglalt teljes szakasz alól, ha újságírás céljából kerül sor adatkezelésre, vagy ha akadémiai, művészi és irodalmi véleménynyilvánításról van szó. A médiára vonatkozó törvények bizonyos mértékben meghatároznak néhány garanciát az érintettek jogai tekintetében.
- Egyes tagállamok a személyes adatok védelmének elsőbbségét írják elő, csak bizonyos helyzetekben mentesítenek az adatvédelmi szabályok alkalmazása alól, például ha közszereplőről van szó.
- Más tagállamok a jogalkotó általi egyensúlyozást írják elő, és/vagy eseti alapú értékelést tesznek kötelezővé a GDPR bizonyos rendelkezéseitől való eltérések tekintetében.

A Bizottság továbbra is értékelni fogja a nemzeti jogszabályokat a Charta követelményei alapján. Az összeegyeztetést jogszabályban kell előírni, annak be kell tartania az alapvető jogokat, valamint arányosnak és szükségesnek kell lennie (a Charta 52. cikkének (1) bekezdése). Az adatvédelmi szabályok nem hathatnak ki a véleménynyilvánítás és tájékozódás szabadságának gyakorlására, különös tekintettel arra, ha visszatartó hatást hoznak létre, vagy úgy értelmezik őket, mintha az újságírókra nyomást gyakorolnának, hogy közzétegyék forrásaikat.

[56] Például egy parlamenti bizottságnak a GDPR alkalmazása alóli felmentése előzetes döntéshozatalra vonatkozó, folyamatban lévő bírósági ügy tárgyát képezi (C-272/19).

[57] A GDPR 85. cikke.

3.2 Fakultatív előírások és azok korlátai

A GDPR lehetőséget biztosít a tagállamok számára, hogy tovább pontosítsák annak alkalmazását néhány területen. Ez a nemzeti jogalkotás számára biztosított mozgástér elkülönítendő attól a kötelezettségtől, hogy a GDPR fentiekben említett bizonyos egyéb rendelkezéseit végre kell hajtani. A fakultatív előírásokra vonatkozó rendelkezések az I. mellékletben találhatók.

A tagállami jog számára biztosított mozgástér a GDPR-ban meghatározott feltételek és korlátozások tárgyát képezi, és nem teszi lehetővé a párhuzamos nemzeti adatvédelmi rendszereket[58]. A tagállamok kötelesek módosítani vagy hatályon kívül helyezni az adatvédelmi jogszabályokat, beleértve az adatvédelmi aspektusokkal rendelkező ágazati jogszabályokat.

Ezenkívül a vonatkozó tagállami jogszabályok nem foglalhatnak magukban olyan rendelkezéseket, amelyek félreértést eredményezhetnek a GDPR közvetlen alkalmazásával kapcsolatban. Ezért ahol a GDPR lehetővé teszi a szabályainak tagállami jog általi specifikációját vagy korlátozásait, a tagállamok olyan mértékben építhetik be a GDPR elemeit a nemzeti jogukba, amely az egységesség biztosításához és ahhoz szükséges, hogy érintett személyek számára érthetővé váljanak a nemzeti rendelkezések[59].

Az érdekelt felek úgy vélik, hogy a tagállamoknak csökkenteniük kell a fakultatív előírásokat, vagy tartózkodniuk kell azoktól, mivel azok nem járulnak hozzá a harmonizációhoz. A jogszabályok végrehajtása és azoknak az adatvédelmi hatóságok általi értelmezése terén fennálló nemzeti különbségek jelentősen növelik a jogi megfelelés költségeit EU-szerte.

A fakultatív előírások használatával kapcsolatos széttöredezettség

- A gyermekek hozzájárulására vonatkozó korhatár az információs társadalommal összefüggő szolgáltatások esetében

Számos tagállam élt a lehetőséggel, hogy 16 éves kornál alacsonyabb korhatárt írjon elő az információs társadalommal összefüggő szolgáltatásokkal kapcsolatos hozzájárulás tekintetében (a GDPR 8. cikkének (1) bekezdése). Míg kilenc tagállam a 16 éves korhatárt alkalmazza, nyolc tagállam a 13 éves kort választotta, hat a 14 éves kort, míg három a 15 éves életkort[60].

Ennek következményeként az EU-szerte kiskorúaknak az információs társadalommal összefüggő szolgáltatásokat nyújtó vállalatnak különbséget kell tennie a potenciális felhasználók életkora között attól függően, hogy melyik tagállamban tartózkodnak. Ez ellentétes a GDPR kulcsfontosságú célkitűzésével, hogy ugyanolyan szintű védelmet

---

[58] A széles körben alkalmazott „bevezető szakaszok” kifejezés fakultatív szakaszokra történő alkalmazása félrevezető, mivel azt a benyomást keltheti, hogy a tagállamoknak lehetőségük van arra, hogy a rendelet rendelkezéseit megkerüljék.

[59] A GDPR (8) preambulumbekezdése.

[60] 13 éves kor Belgium, Dánia, Észtország, Finnország, Lettország, Málta, Portugália és Svédország esetében; 14 éves kor Ausztria, Bulgária, Ciprus, Spanyolország, Olaszország és Litvánia esetében; 15 éves kor a Cseh Köztársaság, Görögország és Franciaország esetében; 16 éves kor Németország, Magyarország, Horvátország, Írország, Luxemburg, Hollandia, Lengyelország, Románia és Szlovákia esetében.

nyújtson a természetes személyeknek, és ugyanolyan szintű üzleti lehetőségeket biztosítson minden tagállamban.

Ezek a különbségek olyan helyzeteket eredményeznek, amelyekben az a tagállam, amelyikben az adatkezelő székhellyel rendelkezik, más életkori határt ír elő, mint azok a tagállamok, amelyekben az érintettek tartózkodnak.

- Egészségügy és kutatás

A személyes adatok különleges kategóriái kezelésének általános tilalma[61] alóli eltérések végrehajtása során a tagállami jogszabályok különböző megközelítéseket alkalmaznak az előírások és garanciák szintjével kapcsolatban, beleértve az egészségügyi és kutatási célokat. A legtöbb tagállam további feltételeket vezetett be vagy tart fenn a genetikai adatok, a biometrikus adatok és az egészségre vonatkozó adatok kezelése tekintetében. Ugyanez elmondható az érintettek jogaitól való, kutatási célokkal összefüggő eltérések[62] esetén, mind az eltérések mértéke és a kapcsolódó garanciák tekintetében.

A Testületnek a személyes adatok tudományos kutatási területen történő használatára vonatkozó, jövőbeli iránymutatása hozzá fog járulni ahhoz, hogy ezen a területen is összehangolt megközelítés legyen érvényben. A Bizottság információt fog nyújtani a Testületnek, különös tekintettel az egészségügyi kutatással kapcsolatban, többek közt a kutatói közösségtől kapott konkrét kérdések és a konkrét forgatókönyvek elemzése formájában. Hasznos lenne, ha ezeket az iránymutatásokat az Európai horizont kutatási és innovációs keretprogram elindítása előtt el lehetne fogadni annak érdekében, hogy össze lehessen hangolni az adatvédelmi gyakorlatokat, és meg lehessen könnyíteni a kutatások előmozdítása céljából végzett adatmegosztást. Szintén hasznos lenne a Testület iránymutatása a személyes adatok egészségügy területén történő kezelésével kapcsolatban.

A GDPR széles körű keretet biztosít a nemzeti jogalkotás számára a népegészségügy területén, és kifejezetten magában foglalja a határokon átívelő egészségügyi fenyegetéseket, valamint a járványok és azok terjedésének nyomon követését[63], ami releváns volt a Covid19-világjárvány elleni küzdelem során.

Uniós szinten 2020. április 8-án a Bizottság elfogadta az e tekintetben szükséges technológia és adatok, különösen a mobilalkalmazások és az anonimizált mobilitási adatok használatára szolgáló eszköztárról szóló ajánlást[64], 2020. április 16-án pedig az adatvédelemmel összefüggésben a világjárvány elleni küzdelmet támogató alkalmazásokról szóló iránymutatást[65]. A Testület 2020. március 19-én közzétette az e tekintetben végzett adatkezelésről szóló nyilatkozatát[66], amelyet 2020. április 21-én a kutatási célokból végzett adatkezelésről és a helymeghatározási adatok és kontaktkövető alkalmazások e tekintetben történő használatáról szóló iránymutatás[67] követett. Ezek az ajánlások és iránymutatások pontosítják, hogy a személyes adatok védelmére vonatkozó elvek és szabályok miként alkalmazandók a járvány elleni küzdelem keretében.

- Az érintettek jogainak széles körű korlátozása

---

61 A GDPR 9. cikke.
62 A GDPR 89. cikkének (2) bekezdése.
63 Lásd a GDPR 9. cikke (2) bekezdésének i) pontját és a (46) preambulumbekezdést.
64 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf
65 https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=HU
66 https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en
67 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_hu

A legtöbb nemzeti adatvédelmi jogszabály, amely korlátozza az érintettek jogait, nem határozza meg az e korlátozásokkal védett általános közérdekű célkitűzéseket, és/vagy nem felel meg kellő mértékben a GDPR 23. cikkének (2) bekezdésében előírt feltételeknek és garanciáknak[68]. Számos tagállam nem hagy teret az arányossági vizsgálatnak, vagy a korlátozásokat a GDPR 23. cikkének (1) bekezdésében foglalt alkalmazási körön túlra terjeszti. Egyes nemzeti jogszabályok például megtagadják a hozzáféréshez való jogot, mivel ez aránytalan erőfeszítés az adatkezelő részéről, az olyan személyes adatok tekintetében, amelyeket a megőrzési kötelezettség alapján tárolnak, vagy amelyek közfeladat ellátásával kapcsolatosak, és nem korlátozzák ezt a korlátozást az általános közérdekű célkitűzésekre.

- A vállalatokra vonatkozó további előírások

Bár a kötelező adatvédelmi tisztviselőre vonatkozó előírás a kockázatalapú megközelítésen alapul[69], az egyik tagállam[70] azt kvantitatív kritériumokra is kiterjesztette, és arra kötelezte a 20 vagy annál több munkavállalóval rendelkező vállalatokat, amelyek állandó jelleggel végeznek automatizált személyesadat-kezelést, hogy az adatkezelési tevékenységeikkel kapcsolatos kockázatoktól függetlenül jelöljenek ki adatvédelmi tisztviselőt[71]. Ez további terheket eredményezett.

4 A TERMÉSZETES SZEMÉLYEK FELHATALMAZÁSA ARRA, HOGY RENDELKEZZENEK AZ ADATAIK FELETT

A GDPR érvényesíti az alapjogokat, különös tekintettel a személyes adatok védelméhez való jogra, valamint a Charta által elismert egyéb alapjogokra, beleértve a magánélet és a családi élet tiszteletét, a véleménynyilvánítás és tájékozódás szabadságát, a diszkriminációmentességet, a gondolat, lelkiismeret és vallás szabadságát, a vállalkozás szabadságát és a hatékony jogorvoslathoz való jogot. Ezeket a jogokat az arányosság elvével összhangban egyensúlyba kell hozni[72].

A GDPR érvényesíthető jogokat biztosít a természetes személyeknek, például a hozzáféréshez, a helyesbítéshez, a törléshez, az adatkezeléssel szembeni tiltakozáshoz, az adathordozhatósághoz és a nagyobb átláthatósághoz való jogot. Ezenkívül feljogosítja a természetes személyeket arra, hogy panaszt nyújtsanak be az adatvédelmi hatósághoz, többek közt képviseleti kereseten keresztül, valamint hogy bírósági jogorvoslatért folyamodjanak.

A természetes személyek egyre inkább tisztában vannak a jogaikkal, ahogyan az a 2019. júliusi Eurobarométerből[73] és az Alapjogi Ügynökség által végzett felmérésből[74] is látszik.

Az Alapjogi Ügynökség által végzett alapjogi felmérés szerint:

[68] Például azért, mert egyszerűen megismétlik a GDPR 23. cikkének (1) bekezdésében szereplő megfogalmazást.
[69] A GDPR 37. cikkének (1) bekezdése.
[70] Németország.
[71] A GDPR 37. cikkének (4) bekezdésében szereplő fakultatív előírás alkalmazásával.
[72] Vö. a GDPR (4) preambulumbekezdésével.
[73] https://ec.europa.eu/commission/presscorner/detail/hu/IP_19_2956
[74] Az Európai Unió Alapjogi Ügynöksége (FRA) (2020): 2019. évi alapjogi felmérés. Adatvédelem és technológia: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

- az EU-ban a 16 éves kor feletti lakosság 69 %-a hallott a GDPR-ról;
- az EU-ban a válaszadók 71 %-a hallott a nemzeti adatvédelmi hatóságáról; ez a szám a csehországi 90 % és a belgiumi 44 % között alakul;
- az EU-ban a válaszadók 60 %-a ismer olyan jogszabályt, amely lehetővé teszi számára, hogy hozzáférjen a közigazgatásban tárolt személyes adataihoz; mindazonáltal ez a százalékos arány a magánvállalatok esetében csupán 51 %;
- az EU-ban több mint minden ötödik válaszadó (23 %) nem akarja megosztani a személyes adatait (például a címét, állampolgárságát vagy születési idejét) a közigazgatással, és 41 % nem akarja megosztani ezeket az adatokat a magánvállalatokkal.

A természetes személyek egyre inkább élnek azzal a joggal, hogy panaszt nyújtsanak be az adatvédelmi hatóságokhoz, akár egyénileg, akár képviseleti kereset révén[75]. Csak néhány tagállam engedélyezte a nem kormányzati szervezetek számára, hogy megbízás nélkül keresetet indítsanak, a GDPR-ban megadott lehetőséggel összhangban. A fogyasztók kollektív érdekeinek védelmére irányuló képviseleti eljárásokról szóló, javasolt irányelv[76] az elfogadását követően várhatóan az adatvédelem terén is megerősíti a képviseleti eljárások keretét.

Panaszok

A 2018 májusa és 2019 novembere közötti panaszok teljes száma a Testület jelentése szerint 275 000 körül van[77]. Mindazonáltal ezt a számot óvatosan kell kezelni, mivel a panasz definíciója nem azonos a hatóságok körében. Az adatvédelmi hatósághoz beérkezett panaszok abszolút száma[78] rendkívül eltérő az egyes tagállamok között. A legtöbb panaszt Németországban (67 000), Hollandiában (37 000), Spanyolországban és Franciaországban (mindkettőnél 18 000), Olaszországban (14 000), Lengyelországban és Írországban (mindkettőnél 12 000) regisztrálták. A hatóságok kétharmada 8 000 és 600 közötti számú panaszról számolt be. A legkevesebb panaszt Észtországban és Belgiumban (mindkettőnél 500), Máltán és Izlandon (mindkettőnél kevesebb, mint 200) nyújtották be.

A panaszok száma nem feltétlenül egyenesen arányos a lakosság méretével vagy a GDP-vel, például közel kétszer annyi panasz született Németországban, mint Hollandiában, és négyszer annyi, mint Spanyolországban és Franciaországban.

A több érdekelt felet tömörítő szakértői csoporttól származó visszajelzések alapján a szervezetek számos intézkedést vezettek be, hogy megkönnyítsék az érintettek jogainak gyakorlását, beleértve az olyan eljárások végrehajtását, amelyek biztosítják a kérelmek egyedi felülvizsgálatát és az adatkezelő válaszát, a különböző csatornák használatát (levél, külön e-mail-cím, weboldal stb.), a módosított belső eljárásokat és szabályzatokat a kérelmek időben történő belső kezeléséről, valamint a személyzet képzését. Az érintettek jogai gyakorlásának megkönnyítése érdekében egyes vállalatok digitális portálokat vezettek be, amelyek elérhetők a vállalat weboldalán keresztül (vagy a munkavállalók számára a vállalat intranetes felületén keresztül).

---

75 A GDPR 80. cikke.
76 COM/2018/0184 final – 2018/089 (COD).
77 Mind a GDPR 77. és 80. cikke értelmében.
78 Lásd a Testület hozzájárulásának 31–32. oldalát.

Mindazonáltal további előrehaladásra van szükség az alábbi pontok tekintetében:

- Nem minden adatkezelő tesz eleget azon kötelezettségének, hogy megkönnyítse az érintetti jogok gyakorlását[79]. Biztosítaniuk kell, hogy az érintettek rendelkezésére álljon egy hatékony kapcsolattartó, akinek elmagyarázhatják a problémájukat. Ez lehet az adatvédelmi tisztviselő, akinek elérhetőségeit proaktív módon kell az érintett rendelkezésére bocsátani[80]. Az elérhetőségeket nem lehet az e-mailre korlátozni, lehetővé kell tenni az érintett számára, hogy más módokon is kapcsolatba léphessen az adatkezelővel.
- A természetes személyek továbbra is nehézségekbe ütköznek, amikor hozzáférést kérnek az adataikhoz, például platformoktól, adatbrókerektől vagy hirdetéstechnológiai vállalatoktól.
- Az adathordozhatósághoz való jog nincs teljes mértékben kihasználva. A 2020. február 19-én a Bizottság által elfogadott európai adatstratégia (a továbbiakban adatstratégia)[81] hangsúlyozta, hogy e jog minden lehetséges használatát meg kell könnyíteni (pl. a [közel] valós idejű adathordozhatóságot lehetővé tévő technikai interfészek és géppel olvasható formátumok engedélyezésével). A vállalkozások megjegyzik, hogy néha nehézségek merülnek fel az adatok strukturált, széles körben használt, géppel olvasható formátumban történő biztosításában (a szabványok hiánya miatt). Csak bizonyos ágazatok, például a banki, telekommunikációs, víz- és fűtésmérő ágazatok szervezetei számoltak be arról, hogy bevezették a szükséges interfészeket[82]. Új technológiai eszközöket alakítottak ki, hogy megkönnyítsék az érintettek GDPR szerinti jogainak gyakorlását, és ezek nem korlátozódnak az adathordozhatóságra (pl. személyesadat-terek és személyes adatok kezelésére irányuló szolgáltatások).
- A gyermekek jogai: A több érdekelt felet tömörítő szakértői csoport számos tagja hangsúlyozta a gyermekeknek nyújtott tájékoztatás szükségességét és azt a tényt, hogy számos szervezet figyelmen kívül hagyja, hogy az adatkezelésük gyermekeket is érinthet. A Tanács hangsúlyozta, hogy a magatartási kódexek elkészítésekor külön figyelmet lehetne szentelni a gyermekek védelmének. A gyermekek védelme az adatvédelmi hatóságok számára is központi kérdés[83].
- A tájékoztatáshoz való jog: egyes vállalatok rendkívül jogszabályi megközelítést alkalmaznak, és az adatvédelmi értesítéseket jogi gyakorlatnak veszik, a tájékoztatást meglehetősen összetetten, nehezen érthetően vagy hiányosan végzik, míg a GDPR azt írja el, hogy a tájékoztatásnak tömörnek kell lennie, és azt világos és közérthető nyelven kell megfogalmazni[84]. Úgy tűnik, hogy egyes

---

79 A GDPR 12. cikkének (2) bekezdése.

80 A GDPR 13. cikke (1) bekezdésének b) pontja, valamint 14. cikke (1) bekezdésének b) pontja.

81 https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

82 Lásd a több érdekelt felet tömörítő szakértői csoport jelentését.

83 Lásd a gyermekek adatvédelmi jogairól szóló nyilvános konzultációt, amelyet az ír adatvédelmi hatóság végzett: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf A francia adatvédelmi hatóság szintén indított nyilvános konzultációt 2020 áprilisában: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique

84 A GDPR 12. cikkének (1) bekezdése.

vállalatok nem követik a Testület ajánlásait, például azon jogi személyek nevének felsorolása tekintetében, amelyekkel megosztják az adatokat.

- Számos tagállam széles körben korlátozta az érintettek jogait a nemzeti jogán keresztül, és néhány még a GDPR 23. cikkében meghatározott mozgásteret is meghaladta.
- Az érintettek személyes jogainak gyakorlását bizonyos esetekben néhány nagyobb digitális szereplő gyakorlatai akadályozzák, amelyek megnehezítik a természetes személyek számára, hogy a magánéletüket leginkább védő beállításokat válasszák (ez ellentétes a beépített és alapértelmezett adatvédelem követelményével[85])[86].

A Testület adatvédelmi jogokról szóló iránymutatását izgatottan várják az érdekelt felek.

5 A SZERVEZETEK, KÜLÖNÖSEN A KIS ÉS KÖZÉPVÁLLALKOZÁSOK ELŐTT ÁLLÓ LEHETŐSÉGEK ÉS KIHÍVÁSOK

A szervezetek lehetőségei

A GDPR előmozdítja a versenyt és az innovációt. A nem személyes adatok szabad áramlásáról szóló rendelettel[87] együtt biztosítja az adatok EU-n belüli szabad áramlását, és a nem uniós székhelyű vállalatokéval egyenlő feltételeket teremt. A személyes adatok védelmére vonatkozó harmonizált keret létrehozásával a GDPR biztosítja, hogy a belső piac valamennyi szereplőjére ugyanazon szabályok vonatkozzanak, és ugyanazokból a lehetőségekből részesüljenek, függetlenül attól, hol található a székhelyük, és hol kerül sor az adatkezelésre. A GDPR technológiasemlegessége adatvédelmi keretet biztosít az új technológiai fejlemények tekintetében. A beépített és alapértelmezett adatvédelem elvei innovatív megoldásokra ösztönöznek, amelyek a kezdetektől magukban foglalják az adatvédelmi szempontokat, és csökkenthetik az adatvédelmi szabályoknak való megfelelés költségeit.

Ezenkívül a magánélet védelme fontos versenytényező, amelyet a természetes személyek egyre inkább figyelembe vesznek a szolgáltatásaik megválasztásakor. Azok, akik tájékozottabbak és az adatvédelmi szempontokra érzékenyebbek, olyan termékeket és szolgáltatásokat keresnek, amelyek biztosítják a személyes adatok hatékony védelmét. Az adathordozhatósághoz való jog végrehajtásában van potenciál

---

85 A GDPR 25. cikke.

86 Lásd a Norvég Fogyasztói Tanács „Deceived by Design” című jelentését, amely rámutat azokra a „sötét mintákra”, alapértelmezett beállításokra, valamint egyéb funkciókra és technikákra, amelyeket a vállalatok annak érdekében használnak, hogy a felhasználókat a magánéletbe behatoló opciók felé tereljék: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/
Lásd továbbá a transzatlanti fogyasztói párbeszéd és a Heinrich-Böll-Stiftung Brussels European Union által 2019 decemberében közzétett kutatást, amely a három legnagyobb globális platform gyakorlatait elemzi: https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms

87 Az Európai Parlament és a Tanács (EU) 2018/1807 rendelete (2018. november 14.) a nem személyes adatok Európai Unióban való szabad áramlásának keretéről, HL L 303., 2018.11.28., 59–68. o.

arra, hogy csökkenjenek az innovatív, adatvédelmi szempontból kedvező szolgáltatásokat nyújtó vállalkozások belépésének akadályai. Nyomon kell követni, hogy milyen hatásokkal jár, ha ezt a jogot a különböző ágazatok piacain szélesebb körben alkalmazzák. Az adatvédelmi szabályoknak való megfelelés és azok átlátható alkalmazása bizalmat szül a személyes adatok használatával kapcsolatban, és ezáltal új lehetőségeket teremt a vállalkozásoknak.

Minden rendelkezéshez hasonlóan az adatvédelmi szabályoknak való megfelelés is költségekkel jár a vállalkozások számára. Mindazonáltal ezeken a költségeken túlmutatnak a digitális innovációba vetett, megerősödött bizalommal járó előnyök és lehetőségek, valamint az alapjogok betartásából eredő társadalmi előnyök. Az egyenlő versenyfeltételek és annak biztosításával, hogy az adatvédelmi hatóságok rendelkezzenek a szabályok hatékony végrehajtásához szükséges eszközökkel, a GDPR megakadályozza, hogy a nem megfelelő vállalatok kihasználják azt a bizalmat, amelyet a szabályokat betartó vállalatok alakítottak ki.

A kis és középvállalkozásokat (kkv-kat) érő speciális kihívások

Az érdekelt felek, valamint az Európai Parlament, a Tanács és az adatvédelmi hatóságok általános benyomása, hogy a GDPR alkalmazása különösen nehéz a mikro-, kis és középvállalkozások, valamint a kisebb önkéntes és jótékonysági szervezetek számára.

A kockázatalapú megközelítés szerint nem lenne megfelelő eltéréseket biztosítani a vállalkozások mérete alapján, mivel önmagában a méretük nem irányadó az általuk végzett személyesadat-kezeléssel járó, a természetes személyeket érő kockázatok tekintetében. A kockázatalapú megközelítés a rugalmasságot a hatékony védelemmel párosítja. Figyelembe veszi azon kkv-k szükségleteit, amelyek nem fő tevékenységként végeznek adatkezelést, és kötelezettségeiket kifejezetten az alapján határozza meg, hogy mekkora a valószínűsége és súlya azoknak a kockázatoknak, amelyek az általuk végzett adatkezeléssel járnak[88].

A kis mértékű és alacsony kockázatú adatkezelést nem lehet ugyanúgy kezelni, mint a magas kockázatú és gyakori adatkezelést – függetlenül az adatkezelést végző vállalat méretétől. Ezért a Testület megállapította, hogy „mindenesetre a szövegben a jogalkotó által előmozdított kockázatalapú megközelítést fenn kell tartani, mivel az érintettre vonatkozó kockázatok nem az adatkezelők méretétől függnek”[89]. Az adatvédelmi hatóságoknak teljes mértékben alkalmazniuk kell ezt az elvet a GDPR végrehajtása során, lehetőleg a közös európai megközelítésnek megfelelően, hogy ne hozzanak létre akadályokat a közös piacon.

Az adatvédelmi hatóságok számos eszközt kialakítottak, és hangsúlyozták azon szándékukat, hogy azokat továbbfejlesszék. Egyes hatóságok tájékoztató kampányokat indítottak, és még ingyenes „GDPR-kurzusokat” is tartanak a kkv-k számára.

Példák az adatvédelmi hatóságok által kifejezetten a kkv-k számára biztosított iránymutatásra és eszközökre

- a kkv-knak szóló tájékoztatás közzététele;

[88] A GDPR 24. cikkének (1) bekezdése.
[89] Lásd a Testület hozzájárulásának 35. oldalát.

- szemináriumok az adatvédelmi tisztviselők részére, valamint rendezvények azon kkv-k részére, amelyeknek nem kell adatvédelmi tisztviselőt kinevezniük;
- interaktív útmutatók a kkv-k részére;
- konzultációs forróvonalak;
- minták az adatkezelési szerződésekhez és az adatkezelési tevékenységek nyilvántartásához.

Az adatvédelmi hatóságok által végzett tevékenységek ismertetése megtalálható a Tanács hozzájárulásában[90].

A kifejezetten a kkv-kat támogató számos intézkedés részesült uniós finanszírozásban. A Bizottság három támogatási hullám keretében nyújtott pénzügyi támogatást összesen 5 millió EUR értékben, amelyek közül a két legutóbbi kifejezetten arra irányult, hogy segítse a nemzeti adatvédelmi hatóságokat abban, hogy elérjék a természetes személyeket és a kkv-kat. Ennek eredményeként 2018-ban 2 millió EUR-t különítettek el kilenc adatvédelmi hatóság részére a 2018–2019 során végzett tevékenységekre (Belgium, Bulgária, Dánia, Magyarország, Litvánia, Lettország, Hollandia, Szlovénia és Izland)[91], 2019-ben pedig 1 millió EUR-t négy adatvédelmi hatóság részére a 2020-ban végzett tevékenységekre (Belgium, Málta, Szlovénia és Horvátország Írországgal partnerséggel)[92]. További 1 millió EUR-t fognak elkülöníteni 2020-ban.

E kezdeményezések ellenére a kkv-k és induló innovatív vállalkozások gyakran arról számolnak be, hogy nehézségekbe ütköznek a GDPR-ban előírt elszámoltathatósági elv végrehajtása során[93]. Nevezetesen azt mondják, hogy nem mindig kapnak elegendő iránymutatást és gyakorlati tanácsot a nemzeti adatvédelmi hatóságoktól, vagy hogy túl sok időbe telik, hogy iránymutatást és tanácsot kapjanak. Voltak olyan esetek is, ahol a hatóságok nem akartak jogi ügyekben részt venni. Ilyen helyzetekben a kkv-k gyakran külső tanácsadókhoz és ügyvédekhez fordulnak az elszámoltathatósági elv és a kockázatalapú megközelítés végrehajtásával kapcsolatban (beleértve az átláthatósági követelményeket, az adatkezelési nyilvántartást és az adatvédelmi incidensek bejelentését). Ez szintén további költségekkel járhat számukra.

Az egyik konkrét probléma az adatkezelési tevékenységek nyilvántartása, amelyet a kkv-k és a kis szervezetek súlyos adminisztratív tehernek tartanak. Az ezen kötelezettség tekintetében a GDPR 30. cikkének (5) bekezdésében biztosított kivétel valóban rendkívül szűkkörű. Mindazonáltal az e kötelezettségnek való megfeleléssel kapcsolatos erőfeszítéseket nem szabad túlbecsülni. Ha a kkv-k fő üzleti tevékenysége nem jár személyes adatok kezelésével, akkor ez a nyilvántartás lehet egyszerű és nem terhes. Ugyanez alkalmazandó az önkéntes és egyéb szervezetekre. Az ilyen

[90] Lásd a Testület hozzájárulásának 35–45. oldalát.
[91] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017
[92] https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en
[93] Lásd a több érdekelt felet tömörítő szakértői csoport jelentését.

egyszerűsített nyilvántartásokat megkönnyítik a nyilvántartási minták, amely gyakorlatot néhány adatvédelmi hatóság már bevezette. Mindenesetre mindenkinek, aki személyes adatot kezel, az elszámoltathatósági elv alapkövetelményeként rendelkeznie kell az adatkezeléseire vonatkozó áttekintéssel.

A gyakorlati eszközök uniós szintű, Testület általi kialakítása, mint az adatvédelmi incidensekre és az adatkezelési tevékenységek egyszerűsített nyilvántartására vonatkozó összehangolt űrlapok segíthetnek a kötelezettségeik teljesítésében a kkv-knak és kis szervezeteknek[94], amelyek fő tevékenysége nem a személyes adatok kezelésére irányul.

Számos iparági szervezet tett erőfeszítéseket annak érdekében, hogy növelje a tudatosságot és tájékoztassa a tagjait, például konferenciákon és szemináriumokon keresztül, a vállalkozásokat tájékoztassa az elérhető iránymutatásról, vagy adatvédelmi segítőszolgálatot alakítson ki a tagjai számára. Ezenkívül egyre több szemináriumról, megbeszélésről és rendezvényről számolnak be, amelyeket szellemi műhelyek és kkv-szervezetek rendeztek a GDPR-ral kapcsolatos témákkal összefüggésben.

Annak érdekében, hogy az EU-n belül növelni lehessen minden adat szabad áramlását, és ki lehessen alakítani a GDPR és a nem személyes adatok szabad áramlásáról szóló rendelet egységes alkalmazását, a Bizottság kifejezetten a kkv-kat célzó gyakorlati iránymutatást adott ki a személyes és nem személyes adatokból álló vegyes adatkészletek kezeléséről[95].

Eszköztár a vállalkozások számára

A GDPR olyan eszközöket biztosít, amelyek segítenek a megfelelés igazolásában, többek közt magatartási kódexeket, tanúsítási mechanizmusokat és általános szerződési feltételeket.

- Magatartási kódexek

A Testület iránymutatást[96] adott ki, hogy támogassa a „kódexek felelőseit”, és megkönnyítse számukra a kódexek elkészítését, módosítását vagy kibővítését, valamint hogy gyakorlati iránymutatást és értelmezési segítséget nyújtson számukra. Ezek az iránymutatások a szükséges minimumkritériumok meghatározásával pontosítják a kódexek nemzeti és uniós szintű benyújtását, jóváhagyását és közzétételét is.

Az érdekelt felek a magatartási kódexeket rendkívül hasznos eszközöknek tartják. Bár számos kódexet nemzeti szinten hajtanak végre, jelenleg előkészület alatt áll több, EU-szerte alkalmazandó magatartási kódex is (például az egészségügyi mobilalkalmazásokkal, a genomikai egészségügyi kutatással, a felhőtechnológiával, a közvetlen üzletszerzéssel, a biztosítással, a gyermekek számára nyújtott megelőző és tanácsadó szolgáltatások általi adatkezeléssel kapcsolatban)[97]. A vállalkozások úgy

---

94 Lásd a Tanács hozzájárulását.

95 A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – Iránymutatás a nem személyes adatok Európai Unióban való szabad áramlásának keretéről szóló rendeletről, COM/2019/250 final.

96 https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_hu

97 Lásd a több érdekelt felet tömörítő szakértői csoport jelentését.

vélik, hogy az EU-szintű magatartási kódexeket nagyobb mértékben kellene támogatni, mivel azok elősegítik a GDPR egységes alkalmazását minden uniós tagállamban.

Mindazonáltal a magatartási kódexek időt és befektetést igényelnek a vállalkozások részéről mind a fejlesztésük, mind pedig a szükséges független ellenőrző szervek létrehozása terén. A kkv-k képviselői hangsúlyozzák az olyan magatartási kódexek jelentőségét és hasznosságát, amelyek a helyzetükhöz igazodnak, és nem járnak aránytalan költségekkel.

Ennek következményeként számos ágazatban a vállalkozások más önszabályozó eszközöket vezettek be, például a bevált gyakorlatokra vonatkozó kódexeket vagy iránymutatásokat. Míg ezek az eszközök hasznos információkat nyújthatnak, azokat az adatvédelmi hatóságok nem hagyták jóvá, és nem szolgálhatnak a GDPR-nak való megfelelés igazolását segítő eszközként.

A Tanács hangsúlyozza, hogy a magatartási kódexeknek külön figyelmet kell szentelniük a gyermekek adatainak és az egészségre vonatkozó adatoknak a kezelésére. A Bizottság az olyan magatartási kódexeket támogatja, amelyek összehangolják az egészségügy és kutatás terén alkalmazott megközelítést, és megkönnyítik a személyes adatok határokon átívelő kezelését[98]. A Testület jelenleg azon dolgozik, hogy jóváhagyja az egyes adatvédelmi hatóságok által előterjesztett, a magatartási kódexek ellenőrzéséért felelős szervezetekre vonatkozó akkreditációs követelmények tervezetét[99]. Ha a nemzetközi vagy uniós magatartási kódexek készen állnak arra, hogy azokat benyújtsák az adatvédelmi hatóságoknak jóváhagyásra, a Testület elé kerülnek konzultáció céljából. A nemzetközi magatartási kódexek bevezetése különösen fontos az olyan területeken, amelyek jelentős adatmennyiségek (pl. felhőtechnológia) vagy érzékeny adatok (pl. egészségügy/kutatás) kezelésével járnak.

- Tanúsítás

A tanúsítás hasznos eszköz lehet a GDPR egyes követelményeinek való megfelelés igazolására. Növelheti a vállalkozások jogbiztonságát, és általánosságban előmozdíthatja a GDPR-t.

Ahogyan a tanúsításról szóló, 2019. áprilisban közzétett tanulmány[100] rámutat, a cél az, hogy meg lehessen könnyíteni a vonatkozó rendszerek bevezetését. A tanúsítási rendszerek EU-n belüli kialakítását a Testület által a tanúsítási kritériumokkal kapcsolatban kiadott iránymutatás[101] és a tanúsító szervek akkreditációjáról szóló iránymutatás[102] fogja támogatni.

---

98 Lásd a bejelentett intézkedéseket az európai adatstratégia 30. oldalán.

99 A GDPR 41. cikkének (3) bekezdése értelmében. Lásd az Európai Adatvédelmi Testület véleményeit itt: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_hu

100 https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en

101 https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_hu

102 https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_hu Számos felügyeleti hatóság már benyújtotta az Európai Adatvédelmi Testület számára az akkreditációs követelményeit, mind a magatartási kódexek ellenőrzéséért felelős szervezetek, mind pedig a tanúsító szervezetek tekintetében. Lásd az áttekintést itt: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_hu

A biztonság és a beépített adatvédelem kulcsfontosságú tényezők, amelyeket figyelembe kell venni a GDPR szerinti tanúsítási rendszerek tekintetében, és amelyeket közös és ambiciózus megközelítéssel kell kezelni EU-szerte. A Bizottság továbbra is támogatja az Európai Uniós Kiberbiztonsági Ügynökség (ENISA), az adatvédelmi hatóságok és a Testület közötti jelenlegi kapcsolatot.

A kiberbiztonsággal kapcsolatban a kiberbiztonsági jogszabály elfogadását követően a Bizottság felkérte az ENISA-t, hogy készítsen két tanúsítási rendszert, beleértve egyet a felhőszolgáltatások tekintetében[103]. A fogyasztóknak szóló szolgáltatások és termékek kiberbiztonságával foglalkozó további rendszerek jelenleg megfontolás tárgyát képezik. Bár ezek a kiberbiztonsági jogszabály alapján létrehozott tanúsítási rendszerek nem kifejezetten az adatvédelemmel és magánélettel foglalkoznak, hozzájárulnak ahhoz, hogy nőjön a fogyasztók digitális szolgáltatásokba és termékekbe vetett bizalma. Ezek a rendszerek bizonyítékot adhatnak a beépített biztonság elveinek való megfelelésre, valamint a személyes adatok kezelésének biztonságával kapcsolatos, megfelelő technikai és szervezési intézkedések végrehajtására.

- Általános szerződési feltételek

A Bizottság jelenleg az adatkezelők és az adatfeldolgozók közötti általános szerződési feltételeken[104] dolgozik, többek közt a nemzetközi adattovábbításokra vonatkozó általános szerződési feltételek modernizációjának fényében (lásd a 7.2. szakaszt). A Bizottság által elfogadott uniós jogszabálynak EU-szerte kötelező ereje lesz, ami biztosítani fogja a teljes körű harmonizációt és jogbiztonságot.

6 A GDPR ALKALMAZÁSA ÚJ TECHNOLÓGIÁKRA

Az új technológiákra nyitott, technológiasemleges keret

A GDPR technológiasemleges, bizalomkeltő és elveken alapul[105]. Ezek az elvek, beleértve a jogszerű és átlátható adatkezelést, a célhoz kötöttséget és az adattakarékosságot, szilárd alapot adnak a személyes adatok védelmére, függetlenül az alkalmazott adatkezelési műveletekről és technikáktól.

A több érdekelt felet tömörítő szakértői csoport tagjai arról számolnak be, hogy általánosságban a GDPR-nak pozitív hatása van az új technológiák fejlesztésére, és jó alapot nyújt az innovációra. A GDPR-t az új technológiák alapjogokkal összhangban történő kialakításának biztosítása szempontjából alapvető és rugalmas eszköznek tekintik. Az alapvető elveinek végrehajtása különösen elengedhetetlen az intenzív adatkezeléshez. A GDPR kockázatalapú és technológiasemleges megközelítése olyan szintű adatvédelmet biztosít, amely megfelelő az adatkezeléssel járó kockázat kezelése szempontjából, beleértve a kialakulóban lévő technológiákat.

Az érdekelt felek különösen azt említik, hogy a GDPR-nak a célhoz kötöttségre és a további összeegyeztethető adatkezelésre, az adattakarékosságra, a tárolás korlátozására, az átláthatóságra, az elszámoltathatóságra vonatkozó elvei, valamint

[103] https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe
[104] A GDPR 28. cikkének (7) bekezdése.
[105] Ahogyan a Tanács, az Európai Parlament és a Testület emlékeztet az értékeléshez való hozzájárulásaikban.

azok a feltételek, amelyek alapján automatizált döntéshozatali folyamatokat lehet jogszerűen végezni nagy mértékben[106], foglalkoznak a mesterséges intelligencia használatával kapcsolatos aggodalmakkal is.

A GDPR jövőbiztos és kockázatalapú megközelítését fogják alkalmazni a mesterséges intelligenciára vonatkozó lehetséges jövőbeli keret és az adatstratégia végrehajtása során is. Az adatstratégia célja, hogy előmozdítsa az adatokhoz való hozzáférhetőséget és a külső felhőinfrastruktúra-szolgáltatások által támogatott közös európai adatterek létrehozását. A személyes adatokkal kapcsolatban a GDPR előírja a fő jogi keretet, amelyen belül hatékony megoldásokat lehet kialakítani eseti alapon, az egyes adatterek jellegétől és tartalmától függően.

A GDPR növelte a személyes adatok védelmével kapcsolatos tudatosságot mind az EU-n belül és azon kívül, és arra kötelezte a vállalatokat, hogy gyakorlataikat az adatvédelmi elvek figyelembevételével módosítsák az innovációk során. Mindazonáltal a civil társadalmi szervezetek megjegyzik, hogy bár a GDPR új technológiák fejlesztésére gyakorolt hatása pozitívnak tűnik, a fő digitális szereplők gyakorlatait még nem módosították lényegesen a magánéletet nagyobb mértékben tiszteletben tartó adatkezelés irányába. A GDPR erőteljes és hatékony végrehajtása a nagy digitális platformokkal és integrált vállalatokkal szemben, beleértve az olyan területeket, mint az online hirdetés és mikrotargetálás, elengedhetetlen a természetes személyek védelme szempontjából.

A Bizottság elemzi a nagy digitális szereplők piaci magatartásával kapcsolatos, szélesebb körű problémákat a digitális szolgáltatásokról szóló jogszabályi csomag tekintetében[107]. A közösségi média terén végzett kutatásokkal kapcsolatban a Bizottság emlékeztet, hogy a közösségi platformok nem használhatják a GDPR-t kifogásként arra, hogy korlátozzák a kutatók és tényellenőrzők olyan nem személyes adatokhoz való hozzáférését, mint a statisztikák arról, hogy milyen célzott hirdetéseket mely személyek kategóriáinak továbbítottak, az e targetálás kialakítására irányuló kritériumok, a hamis fiókokra vonatkozó információk stb.

A Covid19-világjárvány próbára tette a GDPR technológiasemleges és jövőbiztos megközelítését, és az sikeresnek bizonyult. Az elveken alapuló szabályai támogatták a vírus terjedése elleni küzdelemre és annak nyomon követésére irányuló eszközök kialakítását.

A kezelendő kihívások

Az új technológiák kialakítása és alkalmazása nem kérdőjelezi meg ezeket az elveket. A kihívások annak pontosításában rejlenek, hogy ezeket a bevált elveket hogyan kell alkalmazni az egyes technológiák alkalmazása során, például a mesterséges intelligencia, a blokkláncok, az Internet of Things, az arcfelismerés vagy a kvantumszámítás tekintetében.

Ezzel kapcsolatban az Európai Parlament és a Tanács hangsúlyozta, hogy folyamatos nyomon követésre van szükség annak pontosításához, hogy a GDPR miként alkalmazandó az új technológiákra és a nagy technológiai vállalatokra. Ezenkívül az

[106] Mindazonáltal az érdekelt felek megállapítják, hogy a mesterséges intelligencia tekintetében végzett automatizált döntéshozatali folyamatok közül nem mind esik a GDPR 22. cikkének hatálya alá.

[107] https://ec.europa.eu/commission/presscorner/detail/hu/ip_20_962

érdekelt felek figyelmeztetnek, hogy annak értékeléséhez, hogy a GPDR a célnak megfelelő-e, szintén folyamatos nyomon követésre van szükség.

Az iparági érdekelt felek hangsúlyozzák, hogy az innováció szükségessé teszi, hogy a GDPR alkalmazása elveken alapuló módon történjen, annak kialakításával összhangban, nem pedig szigorú és formális módon. Úgy vélik, hogy a Testületnek a GDPR elveinek, fogalmainak és szabályainak olyan új technológiákra történő alkalmazásáról szóló iránymutatása, mint a mesterséges intelligencia, a blokkláncok vagy az Internet of Things, a kockázatalapú megközelítés figyelembevételével segítene az egyértelműség és a nagyobb jogbiztonság biztosításában. Az ilyen puha jogi eszközök remekül kiegészítik a GDPR új technológiákra történő alkalmazását, mivel nagyobb jogbiztonságot biztosítanak, és a technológiai fejleményekkel összhangban felülvizsgálhatók. Egyes érdekelt felek továbbá úgy vélik, hogy a GDPR új technológiákra történő alkalmazásáról szóló ágazati iránymutatás hasznos lehetne.

A Testület kijelentette, hogy továbbra is figyelembe fogja venni a kialakulóban lévő technológiáknak a személyes adatok védelmére gyakorolt hatását.

Az érdekelt felek továbbá hangsúlyozzák annak jelentőségét, hogy a szabályozók alaposan megértsék, hogyan használják a technológiát, és hogyan lehet párbeszédet folytatni az ágazattal a kialakulóban lévő technológiák fejlesztéséről. Úgy vélik, hogy a „szabályozási kötöttség” megközelítés – a szabályok alkalmazására vonatkozó iránymutatás megszerzésének eszközeként – érdekes opció lehet az új technológiák tesztelésére, és segíthet a vállalkozásoknak abban, hogy alkalmazzák a beépített és alapértelmezett adatvédelmet az új technológiák során.

A további szakpolitikai intézkedések tekintetében az érdekelt felek azt javasolják, hogy a mesterséges intelligenciáról szóló jövőbeli szakpolitikai javaslatoknak a meglévő jogi keretre kell építeniük, és azokat össze kell hangolni a GDPR-ral. Az esetleges konkrét problémákat gondosan kell értékelni, a vonatkozó bizonyítékok alapján, mielőtt új előíró szabályokat javasolnának.

A mesterséges intelligenciáról szóló bizottsági fehér könyv számos szakpolitikai opciót terjeszt elő, amelyekkel kapcsolatban 2020. június 14-ig várták az érdekelt felek véleményeit. A természetes személyek jogait jelentősen befolyásoló arcfelismeréssel kapcsolatban a fehér könyv emlékeztetett a jelenlegi jogi keretre, és nyilvános vitát indított az esetleges konkrét körülményekről, amelyek indokolhatják a mesterséges intelligencia arcfelismerés és egyéb biometrikus azonosítás céljából történő használatát a közterületeken, valamint a közös garanciákról.

7 NEMZETKÖZI ADATTOVÁBBÍTÁSOK ÉS GLOBÁLIS EGYÜTTMŰKÖDÉS

7.1 A magánélet védelme: globális kérdés

A személyes adatok védelme iránti igényaz országhatároktól független kérdés, mivel a természetes személyek világszerte egyre fontosabbnak tartják a magánélet védelmét és az adataik biztonságát.

Ugyanakkor megkerülhetetlen tény, hogy kölcsönösen összekapcsolt világunkban az adatáramlások nagy jelentőséggel bírnak a természetes személyek, a kormányok, a vállalatok és általánosabb szinten a társadalom egésze számára. Az adatáramlások a kereskedelem, a nemzeti hatóságok közötti együttműködés és a szociális interakciók

elengedhetetlen részét képezik. E tekintetben a jelenlegi Covid19-világjárvány szintén rámutat arra, mennyire fontos a személyes adatok továbbítása és cseréje számos alapvető tevékenység esetén, legyen szó akár a kormányzati tevékenységek és az üzleti műveletek folytonosságának biztosításáról – az információs és kommunikációs technológiára jelentős mértékben támaszkodó távmunka és egyéb megoldások lehetővé tételével –, akár a diagnosztikára, kezelésekre és vakcinákra vonatkozó tudományos kutatásokkal összefüggő együttműködés kialakításáról, akár a kiberbűncselekmények olyan új formái elleni küzdelemről, mint a Covid19 megelőzése vagy gyógyítása tekintetében hatásosnak mondott, hamis gyógyszereket kínáló online csalások.

Ezzel a háttérrel a magánélet védelmének és az adatáramlások megkönnyítésének minden eddiginél nagyobb mértékben kéz a kézben kell járnia. Az EU a nemzetközi adattovábbításokra való nyitottságot a természetes személyek magas szintű védelmével összehangoló adatvédelmi rendszerének köszönhetően rendkívül jó helyzetben van ahhoz, hogy előmozdítsa a biztonságos és megbízható adatáramlásokat. A GDPR már nemzetközi szinten is referenciapontot jelent, és a modern adatvédelmi szabályok bevezetése terén katalizátorként kezdett működni világszerte számos országban.

Ez valóban globális tendencia, amely – csak néhány példát említve – Chilétől Dél-Koreáig, Brazíliától Japánig, Kenyától Indiáig, Tunéziától Indonéziáig és Kaliforniától Tajvanig terjed. Ezek a fejlemények nemcsak kvantitatív, hanem kvalitatív szempontból is kiemelkedőek: a nemrégiben elfogadott vagy az elfogadás előtt álló adatvédelmi szabályok közül számos az EU által megosztott közös garanciák, jogok és végrehajtási mechanizmusok alapvető készletén alapul. A túl sokszor különböző, ha nem ellentétes szabályozási megközelítésekkel jellemezhető világunkban ez a globális konvergencia felé vezető tendencia rendkívül pozitív fejlemény, amely új lehetőségeket teremt a természetes személyek védelmének növelésére Európában, miközben megkönnyíti az adatáramlásokat és csökkenti a vállalkozások tranzakciós költségeit.

Annak érdekében, hogy kihasználja ezeket a lehetőségeket, és végrehajtsa „A személyes adatok cseréje és védelme a globalizált világban” c. 2017. évi közleményében[108] meghatározott stratégiát, a Bizottság az alábbiakban ismertetett, rendelkezésre álló adattovábbítási „eszköztár” teljes körű kihasználásával jelentősen fokozta az adatvédelem nemzetközi dimenziójával összefüggő munkáját. Ez magában foglalta a kulcsfontosságú partnerekkel folytatott aktív párbeszédet, amelynek célja a „megfelelőségi megállapítás” elérése volt, és fontos eredményeket hozott, például létrejött a világ legnagyobb, szabad és biztonsági adatáramlási terület az EU és Japán között.

A megfelelőségre vonatkozó munka mellett a Bizottság szorosan együttműködött a Testületen belüli adatvédelmi hatóságokkal, valamint más érdekelt felekkel, hogy a GDPR nemzetközi adattovábbításokra vonatkozó rugalmas szabályaiban rejlő teljes potenciált kiaknázza. Ez magában foglalja az olyan eszközök modernizálását, mint az

[108] A Bizottság közleménye az Európai Parlament és a Tanács részére – „A személyes adatok cseréje és védelme a globalizált világban”, 2017.1.10., (COM(2017) 7 final).

általános szerződési feltételek, a tanúsítási rendszerek, a magatartási kódexek vagy a nemzeti hatóságok közötti adatcserékre vonatkozó adminisztratív intézkedések kialakítását, valamint például az EU adatvédelmi szabályainak területi hatályával vagy a személyes adatok továbbítására vonatkozó, úgynevezett „eltérések” használatával kapcsolatos fő fogalmak tisztázását.

Végezetül a Bizottság fokozta a párbeszédet számos kétoldalú, regionális és multilaterális fórumon, hogy elősegítse a magánélet iránti tisztelet általános kultúráját, és a különböző adatvédelmi rendszerek között egységességi elemeket alakítson ki. Erőfeszítéseiben a Bizottság számíthatott az Európai Külügyi Szolgálat, valamint a harmadik országokban található uniós delegációk és a nemzetközi szervezeteknél lévő küldöttségek hálózatának aktív támogatására. Ez biztosította az egységességet és az uniós szakpolitikák külső dimenziójának különböző aspektusai közötti komplementaritást – a kereskedelemtől az Afrika és EU közötti új partnerségig.

7.2 A GDPR adattovábbítási eszközkészlete

Mivel egyre több magán- és állami vállalat alkalmaz rutinműveletei részeként nemzetközi adatáramlásokat, egyre nagyobb az igény a rugalmas eszközök iránt, amelyek a különböző ágazatokhoz, üzleti modellekhez és továbbítási helyzetekhez igazíthatók. E szükségleteket tükrözve a GDPR modernizált eszköztárat kínál, amely megkönnyíti a személyes adatok EU-ból harmadik országba vagy nemzetközi szervezethez történő továbbítását, miközben biztosítja, hogy az adatok továbbra is magas szintű védelmet élvezzenek. A védelem folytonossága fontos, mivel napjaink világában az adatok gyorsan mozognak a határokon át, és a GDPR által biztosított védelem nem lenne teljes körű, ha az kizárólag az EU-n belüli adatkezelésre korlátozódna.

A GDPR V. fejezetével a jogalkotó megerősítette a 95/46/EK irányelv alapján korábban már létező adattovábbítási szabályok szerkezetét: akkor kerülhet sor adattovábbításokra, ha a Bizottság megfelelőségi megállapítást tett az adott harmadik országgal vagy nemzetközi szervezettel kapcsolatban, vagy ennek hiányában ha az uniós adatkezelő vagy adatfeldolgozó („adatátadó”) megfelelő garanciákat biztosított, például a címzettel („adatátvevő”) kötött szerződésen keresztül. Ezenkívül az adattovábbításokra vonatkozó törvényi alapok (az úgynevezett eltérések) továbbra is rendelkezésre állnak bizonyos helyzetekben, amelyekben a jogalkotó úgy határozott, hogy az érdekek egyensúlya bizonyos körülmények között lehetővé teszi az adattovábbítást. Ugyanakkor a reform egyértelműsítette és egyszerűsítette a meglévő szabályokat, például a megfelelőségi megállapításra vagy a kötelező erejű vállalati szabályokra vonatkozó feltételek részletes előírásával, az engedélyezési követelmények rendkívül kevés, konkrét ügyre korlátozásával, valamint a bejelentési követelmények teljes eltörlésével. Ezenkívül új továbbítási eszközök, például magatartási kódexek vagy tanúsítási rendszerek bevezetésére került sor, és a meglévő eszközök (pl. általános szerződési feltételek) használatára irányuló lehetőségek kibővültek.

Napjaink digitális gazdasága lehetővé teszi a külföldi vállalkozások számára, hogy (ugyan távolról, de) közvetlenül részt vegyenek az uniós belső piacon, és versenyezzenek az uniós fogyasztókért és személyes adataikért. Ha az áruk vagy szolgáltatások nyújtásával kifejezetten európaiakat céloznak, vagy az ő viselkedésüket követik nyomon, ugyanúgy meg kell felelniük az uniós jognak, mint az uniós

vállalkozásoknak. Ezt tükrözi a GDPR 3. cikke, amely kiterjeszti az uniós adatvédelmi szabályok közvetlen alkalmazhatóságát az EU-n kívüli adatkezelők vagy adatfeldolgozók bizonyos adatkezelési műveleteire. Ez biztosítja a szükséges garanciákat, valamint az egyenlő versenyfeltételeket az uniós piacon működő valamennyi vállalat számára.

Széles körű elérése az egyik oka annak, hogy a GDPR hatásai a világ más részein is érződnek. A Testület által a GDPR területi hatályával kapcsolatos, átfogó nyilvános konzultációt követően kiadott részletes iránymutatás azért fontos, hogy segíteni lehessen a külföldi vállalkozásoknak abban, hogy meghatározzák, hogy az adatkezelési tevékenységek közvetlenül a GDPR garanciáinak hatálya alá esnek-e, és ha igen, melyek ezek, beleértve a konkrét példákat[109].

Az uniós adatvédelmi jog alkalmazási körének kibővítése azonban önmagában nem elegendő a gyakorlati betartásának biztosításához. Ahogyan azt a Tanács is kiemeli[110], elengedhetetlen biztosítani a külföldi vállalkozások megfelelését és a velük szembeni hatékony végrehajtást. E tekintetben kulcsszerepe lehet az EU-n belüli képviselő kinevezésének (a GDPR 27. cikkének (1) és (2) bekezdése), akit a természetes személyek és a felügyeleti hatóságok a külföldről eljáró felelős vállalat mellett vagy helyett felkereshetnek[111]. Ez a más kontextusokban is egyre inkább megjelenő[112] megközelítés szigorúbban alkalmazandó annak érdekében, hogy egyértelmű üzenetet lehessen küldeni azzal kapcsolatban, hogy az EU-n belüli székhely hiánya nem mentesíti a külföldi vállalkozásokat a GDPR szerinti felelősségük alól. Ha a vállalkozások nem felelnek meg a képviselő kinevezésére irányuló kötelezettségüknek[113], a felügyeleti hatóságoknak a GDPR 58. cikkében foglalt, teljes végrehajtási eszköztárat alkalmazniuk kell (pl. nyilvános figyelmeztetések, ideiglenes vagy végleges tilalom az EU-n belüli adatkezelés tekintetében, az EU-n belül található, közös adatkezelőkkel szembeni végrehajtás).

Végezetül nagyon fontos, hogy a Testület véglegesítse a munkáját a GDPR közvetlen alkalmazásáról szóló 3. cikk és az V. fejezetben szereplő, nemzetközi

---

[109] Európai Adatvédelmi Testület, 2/2018. számú iránymutatás a GDPR területi hatályáról, 2019.11.12. Az iránymutatás a nyilvános konzultáció során felmerült számos kérdéssel foglalkozik, például a targetálásra és nyomon követésre vonatkozó kritériumok értelmezésével.

[110] Lásd a Tanács álláspontjának és megállapításainak 34., 35. és 38. bekezdését.

[111] Lásd a GDPR 27. cikkének (4) bekezdését és (80) preambulumbekezdését („Meg nem felelés esetén, a kijelölt képviselővel szemben az adatkezelő vagy az adatfeldolgozó kikényszerítési eljárásokat indíthat”).

[112] Javaslat – Az Európai Parlament és a Tanács irányelve a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályok meghatározásáról (COM/2018/226 final), 3. cikk; Javaslat – Az Európai Parlament és a Tanács rendelete az online terrorista tartalom terjesztésének megelőzéséről (COM(2018)640 final), 16. cikk (2) és (3) bekezdés.

[113] A nyilvános konzultációra beküldött egyik beadvány szerint az egyik fő kezelendő kérdés „a hatékony végrehajtás és a valós következmények azok számára, akik úgy döntenek, hogy ignorálják ezt a követelményt […]. Különösen észben kell tartani, hogy ez versenyhátrányba hozza az EU-ban bejegyzett vállalkozásokat azokhoz a nem megfelelő vállalkozásokhoz képest, amelyek nem az EU-ban vannak bejegyezve, és az EU-ban kereskednek.” Lásd az EU Business Partners 2020. április 29-i beadványát.

adattovábbításokra vonatkozó szabályok közötti kapcsolat pontosításával kapcsolatban[114].

Megfelelőségi határozatok

Az érdekelt felektől kapott észrevételek megerősítik, hogy a megfelelőségi határozatok továbbra is elengedhetetlen eszközök az uniós vállalkozások számára a személyes adatok harmadik személyek részére történő biztonságos továbbítása terén[115]. Ezek a határozatok nyújtják a leginkább átfogó, egyenes és költséghatékony megoldást az adattovábbításokra, mivel azok az EU-n belüli adattovábbításokhoz hasonlatossá válnak, ezáltal biztosítva a személyes adatok biztonságos és szabad áramlását anélkül, hogy további feltételekre vagy engedélyre lenne szükség. A megfelelőségi határozatok ezért kereskedelmi csatornákat nyitnak meg az uniós vállalkozások számára, és megkönnyítik a nemzeti hatóságok közötti együttműködést, miközben kiváltságos hozzáférést biztosítanak az uniós belső piachoz. Az 1995. évi irányelv szerinti gyakorlatra építve a GDPR kifejezetten lehetővé teszi, hogy egy harmadik ország adott területével vagy a harmadik országon belüli adott ágazattal vagy iparággal kapcsolatban megfelelőségi határozat szülessen (úgynevezett „részleges" megfelelés).

A GDPR a korábbi évek tapasztalatára és a Bíróság által megadott magyarázatokra épít, amikor meghatározza azon elemek részletes jegyzékét, amelyeket a Bizottságnak figyelembe kell vennie az értékelés során. A megfelelőségi szabvány olyan szintű védelmet ír elő, amely összehasonlítható (vagy „lényegében megegyező") azzal, amely az EU-n belül biztosított[116]. Ez magában foglalja a harmadik ország rendszere egészének átfogó értékelését, beleértve az adatvédelem tartalmát, annak hatékony végrehajtását és érvényesítését, valamint a nemzeti hatóságok személyes adatokhoz való hozzáférésére vonatkozó szabályokat, különös tekintettel a bűnüldözésre és a nemzeti biztonsági célokra[117].

Ez tükröződik továbbá a korábbi, 29. cikk alapján létrehozott munkacsoport által elfogadott (és a Testület által jóváhagyott) iránymutatásban, különös tekintettel az úgynevezett „megfelelőségi referenciára", amely tovább pontosítja azokat az elemeket, amelyeket a Bizottságnak figyelembe kell vennie a megfelelőségi értékelés elvégzése során, beleértve a nemzeti hatóságok személyes adatokhoz való hozzáférésére vonatkozó „alapvető garanciák" áttekintésének biztosítását[118]. Utóbbi

---

[114] A nyilvános konzultációra küldött számos beadvány felvetette ezt a kérdést, például a személyes adatok EU-n kívüli, azonban a GDPR alkalmazási körébe tartozó címzetteknek történő továbbítása tekintetében.

[115] A Tanács álláspontja és megállapításai, 17. bekezdés; A Testület hozzájárulásának 5–6. oldala. A nyilvános konzultációra érkezett számos beadvány, beleértve számos üzleti szervezettől (például a Nagyvállalatok Francia Szövetsége, a Digitális Európa, a Globális Adatszövetség/BSA, a Computer & Communication Industry Association [CCIA] az Egyesült Államok kereskedelmi kamarája) érkezőt, arra szólított fel, hogy fokozni kell a megfelelőségi megállapításokkal összefüggő munkát, különösen a fontos kereskedelmi partnerekkel.

[116] Az Európai Unió Bíróságának 2015. október 6-i ítélete, Maximillian Schrems kontra adatvédelmi biztos („*Schrems*"), C-362/14, 73., 74. és 96. pont. Lásd továbbá a GDPR (104) preambulumbekezdését, amely a lényegi megegyezőség szabványára hivatkozik.

[117] A GDPR 45. cikkének (2) bekezdése és (104) preambulumbekezdése. Lásd továbbá a *Schrems* ítélet 75., 91–91. pontját.

[118] Megfelelőségi referencia, WP 254 rev. 01., 2018. február 6. (elérhető itt: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

különösen az Emberi Jogok Európai Bíróságának ítélkezési gyakorlatára épít. Bár a „lényegi megegyezés” normája nem az uniós szabályok pontról pontra történő lemásolását („fénymásolatát”) jelenti, mivel a hasonló szintű védelem biztosításának eszközei a különböző adatvédelmi rendszerek között eltérőek lehetnek, és gyakran a különböző jogi hagyományokat tükrözik, azonban szigorú védelmi szintet ír elő.

Ezt a normát az a tény indokolja, hogy a megfelelőségi határozat az adatok szabad áramlása tekintetében lényegében kiterjeszti a harmadik országokra a belső piac előnyeit. Mindazonáltal ez azt is jelenti, hogy néha az adott harmadik országban biztosított védelmi szint és a GDPR között releváns különbségek lesznek, amelyeket át kell hidalni, például a további garanciákkal kapcsolatos egyeztetésen keresztül. Ezeket a garanciákat pozitívan kell tekinteni, mivel azok tovább erősítik az EU-ban a természetes személyek számára elérhető védelmet. Ugyanakkor a Bizottság egyetért a Testülettel a gyakorlati alkalmazásuk folyamatos nyomon követésének jelentősége kapcsán, beleértve azoknak a harmadik ország adatvédelmi hatósága általi hatékony végrehajtását[119].

A GDPR egyértelművé teszi, hogy a megfelelőségi határozatok „élő eszközök”, amelyeket folyamatosan nyomon kell követni és rendszeresen felül kell vizsgálni[120]. E követelményekkel összhangban a Bizottság rendszeresen párbeszédet folytat az illetékes hatóságokkal, hogy proaktívan nyomon kövesse az új fejleményeket. Például az EU–USA adatvédelmi pajzs 2016. évi elfogadása óta[121] a Bizottság a Testület képviselőivel együtt három éves felülvizsgálatot végzett, hogy értékelje a keret működésének minden aspektusát[122]. Ezek a felülvizsgálatok az Egyesült Államok hatóságaival végzett tapasztalatcserén keresztül szerzett információkra, valamint más érdekelt felek, például az uniós adatvédelmi hatóságok, a civil társadalom és a kereskedelmi szervezetek észrevételeire alapoztak. Lehetővé tették a keret számos eleme gyakorlati működésének fejlesztését. Szélesebb tekintetben pedig az éves

---

[119] A Testület hozzájárulásának 5–6. oldala.

[120] A GDPR 45. cikkének (4) és (5) bekezdése előírja a Bizottság számára, hogy folyamatosan kövessék nyomon a harmadik országokban bekövetkező fejleményeket, és rendszeresen – legalább négyévente – vizsgálják felül a megfelelőségi megállapítást. Ezenkívül felhatalmazzák a Bizottságot arra, hogy hatályon kívül helyezze, módosítsa vagy felfüggessze a megfelelőségi határozatot, ha úgy ítéli meg, hogy az adott ország vagy nemzetközi szervezet már nem biztosít megfelelő szintű védelmet. A GDPR 97. cikke (2) bekezdésének a) pontja emellett előírja, hogy a Bizottság 2020-ig nyújtson be értékelő jelentést az Európai Parlamentnek és a Tanácsnak. Lásd továbbá az Európai Unió Bíróságának 2015. október 6-i ítéletét, *Maximillian Schrems* kontra *adatvédelmi biztos*, C-362/14, 76. pont.

[121] A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről. Ez a megfelelőségi határozat különleges helyzet, amely az Egyesült Államok általános adatvédelmi jogszabályainak hiányában a részt vevő vállalatok által vállalt, az ezen megállapodásban meghatározott adatvédelmi szabványok alkalmazására irányuló kötelezettségeken alapul (amelyek az USA jogszabályai szerint végrehajthatók). Emellett az adatvédelmi pajzs az Egyesült Államok által a nemzetbiztonsági célú adathozzáférés tekintetében adott konkrét nyilatkozatokra és biztosítékokra épül, amelyek alátámasztják a megfelelőség megállapítását.

[122] A felülvizsgálatokra 2017-ben (a Bizottság jelentése az Európai Parlamentnek és a Tanácsnak az EU–USA adatvédelmi pajzs működésének első éves felülvizsgálatáról, COM(2017) 611 final), 2018-ban (a Bizottság jelentése az Európai Parlamentnek és a Tanácsnak az EU–USA adatvédelmi pajzs működésének második éves felülvizsgálatáról, COM(2018) 860 final), valamint 2019-ben került sor (a Bizottság jelentése az Európai Parlamentnek és a Tanácsnak az EU-USA adatvédelmi pajzs működésének harmadik éves felülvizsgálatáról, COM(2019) 495 final).

felülvizsgálatok hozzájárultak ahhoz, hogy szélesebb körű párbeszédet lehessen kialakítani az Egyesült Államok kormányával általánosságban az adatvédelemről és különösen a nemzetbiztonsággal kapcsolatos korlátozásokról és garanciákról.

A GDPR első értékelésének részeként a Bizottság továbbá köteles felülvizsgálni az 1995. évi irányelv alapján elfogadott megfelelőségi határozatokat is[123]. A bizottsági szolgálatok intenzív párbeszédet kezdtek mind a 11 érintett országgal és területtel, hogy értékeljék, miként alakultak a személyes adatok védelmére irányuló rendszereik a megfelelőségi határozat elfogadása óta, és hogy megfelelnek-e a GDPR által meghatározott szabványoknak. Mivel e határozatok a kereskedelem és nemzetközi együttműködés kulcsfontosságú eszközei, a folytonosságuk biztosítása iránti szükséglet az egyik legfontosabb tényező, amely ezen országok és területek közül sokat arra sarkallt, hogy modernizálja és megerősítse adatvédelmi jogszabályait. Ezek mindenképpen üdvözlendő fejlemények. Néhány országgal és területtel tárgyalások folynak a további garanciákról, hogy meg lehessen oldani a védelemben fennálló különbségeket.

Mindazonáltal mivel a Bíróság július 16-án meghozandó ítéletében olyan pontosításokkal szolgálhat, amelyek relevánsak lehetnek a megfelelőségi szabvány egyes elemeivel kapcsolatban, a Bizottság a Bíróság ezen ügyben hozott ítéletét követően külön jelentést fog készíteni az említett 11 megfelelőségi határozat értékeléséről[124].

„A személyes adatok cseréje és védelme a globalizált világban” című 2017. évi közleményében meghatározott stratégia végrehajtásával a Bizottság új megfelelőségi párbeszédeket is elindított[125]. Ez a munka már jelentős eredményeket hozott, amelyekben az EU kulcsfontosságú partnerei is részt vettek. 2019 januárjában a Bizottság elfogadta a Japánra vonatkozó megfelelőségi határozatát, amely magas szintű konvergencián alapul – ezt olyan eszközök biztosítják, mint a többek között az újbóli adattovábbítások területére vonatkozó konkrét garanciák és a természetes személyek által a személyes adatok bűnüldözési és nemzetbiztonsági célokból történő, kormányzati hozzáféréssel kapcsolatban benyújtott panaszok vizsgálatára és

[123] E meglévő határozatok olyan országokat érintenek, amelyek az Európai Unióval és annak tagállamaival szoros kapcsolatot ápolnak (Svájc, Andorra, Feröer-szigetek, Guernsey, Jersey, Man-sziget), jelentős kereskedelmi partnerek (pl. Argentína, Kanada, Izrael), vagy az adatvédelmi jogszabályok fejlesztése szempontjából úttörő szerepet töltöttek be térségükben (Új-Zéland, Uruguay).

[124] A C-311/18. számú, adatvédelmi biztos kontra Facebook Ireland Limited, Maximillian Schrems („Schrems II”) ügy az úgynevezett általános szerződési feltételekre vonatkozó, előzetes döntéshozatalra irányuló hivatkozást érint. Mindazonáltal a megfelelőségi szabvány bizonyos elemeit a Bíróságnak tovább kell pontosítania. Az ügyben a tárgyalásra 2019. július 9-én került sor, és az ítéletet 2020. július 16-án tervezik bejelenteni.

[125] Lásd fent a 109. lábjegyzetet. A Bizottság kifejtette, hogy az alábbi kritériumokat fogja figyelembe venni, amikor értékeli, mely harmadik országokkal kell párbeszédet folytatni a megfelelőségről: (i) az adott harmadik országgal (ténylegesen vagy esetlegesen) fennálló uniós kereskedelmi kapcsolatok terjedelme, ideértve a szabadkereskedelmi megállapodás meglétét, illetve arra vonatkozóan folyamatban lévő tárgyalásokat; (ii) a személyes adatok Európai Unióból kifelé irányuló áramlásának mértéke, tükrözve a földrajzi és/vagy kulturális kapcsolatokat; (ii) az ország által a magánélet és az adatok védelme terén betöltött úttörő szerep, amellyel példát mutathat az adott térség többi országa számára; valamint (iv) az országgal fennálló általános politikai kapcsolat, különösen a közös értékek és célkitűzések nemzetközi szintű előmozdítása terén.

megoldására szolgáló mechanizmusok létrehozása.

A GDPR szerint elfogadott első megfelelőségi megállapításként a Japánnal elfogadott keretrendszer hasznos precedenst teremt a jövőbeli határozatokhoz[126]. Ez magában foglalja a tényt, hogy azt a japán oldalon egy EU-ra vonatkozó „megfelelőségi" megállapítással viszonozták. Együttesen ezek a kölcsönös megfelelőségi megállapítások a világon a legnagyobb, biztonságos és szabad személyesadat-áramlási területet hozzák létre, kiegészítve ezáltal az EU és Japán közötti gazdasági partnerségi megállapodást. Az intézkedés körülbelül 124 milliárd EUR értékű árukereskedelmet és 42,5 milliárd EUR értékű szolgáltatáskereskedelmet támogat évente.

A megfelelőségi folyamat Dél-Koreával is előrehaladott állapotban van. Annak fontos eredménye Dél-Korea nemrégiben elfogadott jogalkotási reformja, amely egy független, erős végrehajtási jogkörrel rendelkező adatvédelmi hatóság létrehozásához vezetett. Ez mutatja, hogy a megfelelőségről szóló párbeszéd miként tud hozzájárulni az uniós adatvédelmi szabályok és a külföldi országok szabályai közötti megnövekedett konvergenciához.

A Bizottság teljes mértékben egyetért az érdekelt felek azon felszólításával, miszerint az új megfelelőségi megállapítások céljából fokozni kell a párbeszédet a kiválasztott harmadik országokkal[127]. Aktívan keresi ezt a lehetőséget más partnerekkel Ázsiában, Dél-Amerikában és a szomszédságban, és az adatvédelmi szabványok felfelé irányuló globális konvergenciájára irányuló, jelenlegi tendenciára alapoz. Például átfogó adatvédelmi jogszabályt fogadtak el, vagy a jogalkotási folyamat előrehaladott szakaszban van Dél-Amerikában (Brazília, Chile), és ígéretesek a fejlemények Ázsiában (pl. India, Indonézia, Malajzia, Srí Lanka, Tajvan és Thaiföld), Afrikában (pl. Etiópia, Kenya), valamint az európai keleti és déli szomszédságban (pl. Grúzia, Tunézia). Ahol lehetséges, a Bizottság folytatja a munkát annak érdekében, hogy átfogó megfelelőségi határozatok szülessenek, amelyek mind a magán-, mind pedig az állami ágazatra kiterjednek[128].

Ezenkívül a GDPR bevezette a Bizottság számára azt a lehetőséget, hogy nemzetközi szervezetekkel kapcsolatban is elfogadjon megfelelőségi megállapításokat. Most, amikor néhány nemzetközi szervezet átfogó szabályok, valamint a független felügyeletet és jogorvoslatot biztosító mechanizmusok bevezetésével modernizálja az adatvédelmi rendszerét, ezzel a lehetőséggel először lehet élni.

---

[126] Az Európai Parlament 2018. december 13-i állásfoglalása a személyes adatok Japán által biztosított védelmének megfelelőségéről (2018/2979(RSP)), 27. pont; A Testület hozzájárulásának 5–6. oldala.

[127] Lásd az Európai Parlament 2017. december 12-i, „A digitális kereskedelmi stratégia felé" c. állásfoglalását (2017/2065(INI)), 8. és 9. pont; Az általános adatvédelmi rendelet (GDPR) alkalmazásával kapcsolatos tanácsi álláspont és megállapítások – 2019.12.19. (14994/1/19), 17. bekezdés; A Testület hozzájárulásának 5. oldala.

[128] A Tanács is kérelmezte, lásd az általános adatvédelmi rendelet (GDPR) alkalmazásával kapcsolatos tanácsi álláspont és megállapítások – 2019.12.19. (14994/1/19), 17. és 40. bekezdését. Mindazonáltal ehhez elengedhetetlen, hogy a nemzeti hatóságok felé történő adattovábbításokra vonatkozó megfelelőségi megállapításra irányuló feltételek teljesüljenek, beleértve a független felügyeletet.

A megfelelőség fontos szerepet játszik az Egyesült Királysággal a Brexit után fennálló kapcsolat tekintetében is, feltéve, hogy a szükséges feltételek teljesülnek. A megfelelőség a kereskedelmet elősegítő tényező, beleértve a digitális kereskedelmet, és alapvető előfeltétele a bűnüldözés és biztonság terén tanúsított szoros és nagyratörő együttműködésnek[129]. Ezenkívül figyelembe véve az Egyesült Királysággal fennálló adatáramlások jelentőségét és az Egyesült Királyság uniós piachoz való közelségét, az egyenlő versenyfeltételek megteremtése érdekében a Csatorna két oldalán fennálló adatvédelmi szabályok közötti magas szintű konvergencia is fontos elem. Az EU és az Egyesült Királyság jövőbeli kapcsolatáról szóló politikai nyilatkozattal összhangban a Bizottság jelenleg végzi a megfelelőségi értékelést mind a GDPR, mind pedig a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv[130] alapján. A megfelelőségi értékelés autonóm és egyoldalú jellegét figyelembe véve ezek a megbeszélések az EU és az Egyesült Királyság közötti jövőbeli kapcsolatra vonatkozó megállapodásról szóló tárgyalásoktól külön zajlanak.

Végezetül a Bizottság üdvözli, hogy más országok a megfelelőségi megállapításhoz hasonló adattovábbítási mechanizmusokat vezetnek be. Ennek során gyakran az adattovábbítás biztonságos céljaként ismerik el az EU-t és azokat az országokat, amelyek tekintetében a Bizottság megfelelőségi határozatot fogadott el[131]. Egyrészről az uniós megfelelőségi határozatokkal rendelkező országok növekvő számában, másrészről pedig a más országok általi elismerés e formájában megvan a potenciál arra, hogy a szabad és biztonságos adatáramlást biztosító országok hálózata jöjjön létre. A Bizottság úgy véli, hogy ez pozitív fejlemény, amely tovább fogja növelni a harmadik országokra vonatkozó megfelelőségi határozat előnyeit, és hozzá fog járulni a globális konvergenciához. A szinergiák e típusa szintén hasznosan hozzájárulhat a biztonságos és szabad adatáramlásokra vonatkozó keretrendszer kialakításához, például a „bizalmon alapuló szabad adatáramlási” kezdeményezés keretében (lásd alább).

Megfelelő garanciák

A GDPR a megfelelőségi megállapítás átfogó megoldása mellett számos más adattovábbítási eszközt is előír. Ezen „eszköztár” rugalmasságát a GDPR 46. cikke igazolja, amely az adattovábbításokat „megfelelő garanciák” alapján szabályozza, beleértve a végrehajtható érintetti jogokat és a hatékony jogorvoslatot. A megfelelő garanciák biztosítása érdekében különböző eszközök állnak rendelkezésre, hogy ki lehessen szolgálni mind a kereskedelmi vállalkozások, mind pedig az állami szervek adattovábbítási szükségleteit.

- Általános szerződési feltételek

[129] Lásd a Nagy-Britannia és Észak-Írország Egyesült Királyságával való új partnerségről folytatandó tárgyalások megkezdésére való felhatalmazásról szóló tanácsi határozathoz mellékelt tárgyalási irányelveket (ST 5870/20 ADD 1 REV 3), 13. és 118. bekezdés.

[130] Lásd az Európai Unió és az Egyesült Királyság közötti jövőbeli kapcsolatok keretének meghatározásáról szóló politikai nyilatkozat felülvizsgált szövegét, amelyről tárgyalói szinten született megállapodás 2019. október 17-én, 8–10. bekezdés (elérhető itt: https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf).

[131] Például Argentína, Kolumbia, Izrael, Svájc vagy Uruguay.

Ezen eszközök első csoportja a szerződéses eszközökre vonatkozik, amelyek lehetnek egyedi, eseti adatvédelmi feltételek, amelyeket az uniós adatátadó és az EU-n kívüli adatátvevő fogad el, és az illetékes adatvédelmi hatóság engedélyez (a GDPR 46. cikke (3) bekezdésének a) pontja), vagy a Bizottság által előzetesen jóváhagyott mintafeltételek (a GDPR 46. cikke (2) bekezdésének c) és d) pontja[132]). Ezen eszközok közül a legfontosabb az úgynevezett általános szerződési feltételek, azaz az adatvédelmi mintafeltételek, amelyeket az adatátadó és az adatátvevő önkéntes alapon be tud építeni a szerződéses megállapodásukba (például a személyes adatok továbbításával járó szolgáltatási szerződés), és amelyek meghatározzák a megfelelő garanciákkal kapcsolatos követelményeket.

Az általános szerződési feltételek messze a legszélesebb körben használt adattovábbítási mechanizmusnak minősülnek[133]. Több ezer uniós vállalat alkalmazza az általános szerződési feltételeket annak érdekében, hogy szolgáltatások széles körét nyújtsa ügyfeleinek, szállítóinak, partnereinek és munkavállalóinak, beleértve a gazdaság működése szempontjából alapvető szolgáltatásokat. Széles körű alkalmazásuk jelzi, hogy azok rendkívül hasznosak a vállalkozások számára a megfelelőségi erőfeszítéseik tekintetében, és különösen előnyösek azon vállalkozások számára, amelyek nem rendelkeznek a szükséges erőforrásokkal ahhoz, hogy minden kereskedelmi partnerükkel külön szerződéseket fogadjanak el. A szabványosításukon és előzetes jóváhagyásukon keresztül az általános szerződési feltételek könnyen végrehajtható eszközt nyújtanak a vállalatoknak annak érdekében, hogy az adattovábbítással összefüggésben megfeleljenek az adatvédelmi követelményeknek.

Az általános szerződési feltételek meglévő készletét[134] az 1995. évi irányelv alapján fogadták el és hagyták jóvá. Ezek az általános szerződési feltételek addig maradnak hatályban, amíg egy bizottsági határozat nem módosítja, cseréli vagy szükség esetén hatályon kívül nem helyezi azokat (a GDPR 46. cikkének (5) bekezdése). A GDPR mind az EU-n belüli, mind pedig a nemzetközi adattovábbításokra kiterjeszti az általános szerződési feltételek alkalmazására irányuló lehetőségeket. A Bizottság az érdekelt felekkel közösen azon dolgozik, hogy kihasználja ezeket a lehetőségeket, és

---

[132] A nemzetközi adattovábbításokra vonatkozó általános szerződési feltételekhez minden esetben szükséges a Bizottság jóváhagyása, azonban azokat akár a Bizottság, akár a nemzeti adatvédelmi hatóság is elkészítheti. Valamennyi létező általános szerződési feltétel az első kategóriába tartozik.

[133] Az IAPP-EY magánélet kezelésére vonatkozó, 2019. évi éves jelentése szerint „ezen [adattovábbítási] eszközök közül – évről évre – túlnyomórészt az általános szerződési feltételek a legnépszerűbbek: az idei felmérés válaszadóinak 88 %-a számolt be arról, hogy az általános szerződési feltételeket alkalmazzák elsődlegesen a területen kívüli adattovábbítások során, ezt követi az EU–USA adatvédelmi pajzs (60 %). Az EU-ból az Egyesült Királyságba adatokat exportáló válaszadók közül 52 %) 91 % arról számolt be, hogy a Brexit után az adattovábbítási megfelelőség érdekében az általános szerződési feltételeket kívánja alkalmazni.

[134] Jelenleg a Bizottság az általános szerződési feltételek három készletét fogadta el a személyes adatok harmadik országokba történő továbbítása tekintetében: kettő az EGT-n belüli adatkezelő által egy EGT-n kívüli adatkezelő részére történő adattovábbításra, egy pedig egy EGT-n belüli adatkezelő által egy EGT-n kívüli adatfeldolgozó részére történő adattovábbításra vonatkozik. Ezek módosítására 2016-ban került sor, a *Schrems I* ügyben (C-362/14) a Bíróság által hozott ítéletet követően, hogy megszüntessék az illetékes felügyeleti hatóságoknak az adattovábbítások felügyeletére vonatkozó jogkörére irányuló korlátozásokat. Lásd itt: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

frissítse a meglévő feltételeket[135]. Annak biztosítása érdekében, hogy az általános szerződési feltételek jövőbeli kialakítása a célnak megfelelő legyen, a Bizottság a GDPR-ral foglalkozó, több érdekelt felet tömörítő szakértői csoport és egy 2019 szeptemberében külön ebből a célból tartott munkaértekezlet keretében, valamint az általános szerződési feltételeket alkalmazó vállalatokkal és civil társadalmi szervezetekkel fennálló több kapcsolat révén visszajelzést gyűjtött az érdekelt felek általános szerződési felekkel kapcsolatos tapasztalatairól. A Testület ezenkívül számos iránymutatást módosít, amely releváns lehet az általános szerződési feltételek felülvizsgálata szempontjából, például az adatkezelő és az adatfeldolgozó fogalmával kapcsolatban.

A kapott visszajelzések alapján a bizottsági szolgálatok jelenleg az általános szerződési feltételek felülvizsgálatán dolgoznak. E tekintetben számos fejlesztendő terület azonosítására került sor, különösen az alábbi szempontokkal összefüggésben:

1. Az általános szerződési feltételek módosítása a GDPR által bevezetett új követelmények fényében, például a GDPR 28. cikke szerint az adatkezelő és az adatfeldolgozó kapcsolatára vonatkozó követelmények (különös tekintettel az adatfeldolgozó kötelezettségeire), az adatátvevő átláthatósággal kapcsolatos kötelezettségei (az érintett számára biztosítandó szükséges információ fényében) stb.
2. A jelenlegi általános szerződési feltételekkel nem érintett adattovábbítási forgatókönyvek kezelése, például az EU-n belüli adatfeldolgozó által egy EU-n kívüli (további) adatfeldolgozó részére történő adattovábbítás, vagy például az olyan helyzetek, ahol az adatkezelő az EU-n kívül található[136].
3. Az adatkezelési műveletek realitásának hatékonyabb tükrözése a modern digitális gazdaságon belül, ahol ezek a műveletek gyakran több adatátvevőt és adatátadót, hosszú és gyakran összetett adatkezelési láncokat, változó üzleti kapcsolatokat stb. foglalnak magukban. Az ilyen helyzetek rendezése érdekében a kialakított megoldások között szerepel például az a lehetőség, hogy az általános szerződési feltételeket több fél írja alá, vagy a szerződés időtartama alatt ahhoz új felek is csatlakozzanak.

E pontok rendezése során a Bizottság vizsgálja azt is, hogy az általános szerződési feltételek jelenlegi struktúráját miképpen lehetne felhasználóbarátabbá tenni, például azzal, ha az általános szerződési feltételek különböző készleteit egyetlen átfogó dokumentum helyettesítené. A kihívás abban rejlik, hogy megfelelő egyensúlyt kell találni az egyértelműség iránti szükséglet és a standardizáció bizonyos foka, valamint a szükséges rugalmasság között, amely lehetővé teszi, hogy a feltételeket számos

[135] Lásd továbbá a Testület hozzájárulásának 6–7. oldalát. Hasonlóképpen a Tanács felszólította a Bizottságot, hogy „a közeljövőben vizsgálják felül és módosítsák [az általános szerződési feltételeket], hogy figyelembe vegyék az adatkezelők és adatfeldolgozók szükségleteit”. Lásd a Tanács álláspontját és megállapításait.

[136] A nyilvános konzultációra érkezett számos beadványban szerepelt az utóbbi forgatókönyv, és gyakran felmerültek aggodalmak azzal kapcsolatban, hogy amennyiben az uniós adatfeldolgozókat arra kötelezik, hogy a nem uniós adatkezelőkkel fennálló kapcsolatukban biztosítsák a megfelelő garanciákat, az versenyhátrányt jelent számukra a hasonló szolgáltatásokat kínáló külföldi adatfeldolgozókkal szemben.

vállalkozás használni tudja különböző követelmények, különböző helyzetek és az adattovábbítások különböző típusai esetén.

A Bíróság előtt jelenleg zajló pereskedés fényében[137] szintén fontos tényező, amelyet figyelembe kell venni, a garanciák további pontosítása iránti esetleges szükséglet a külföldi nemzeti hatóságok által az általános szerződési feltételek alapján továbbított adatokhoz való hozzáférés tekintetében, különös tekintettel a nemzetbiztonsági célokra. Ez magában foglalhatja az adatátvevő vagy az adatátadó vagy mindkettő kötelezését arra, hogy lépéseket tegyen, és tisztázza az adatvédelmi hatóság e tekintetben játszott szerepét. Bár az általános szerződési feltételek felülvizsgálata előrehaladott állapotban van, meg kell várni a Bíróság ítéletét, hogy be lehessen építeni a felülvizsgált feltételekbe az esetleges további követelményeket, mielőtt az új általános szerződési feltételek készletéről szóló határozattervezetet be lehetne nyújtani a Testület részére véleményezésre, majd „bizottsági eljáráson" keresztül javasolni lehetne annak elfogadását[138].

Ezzel párhuzamosan a Bizottság kapcsolatban áll a hasonló eszközöket kialakító nemzetközi partnerekkel is[139]. Ez a párbeszéd, amely lehetővé teszi a tapasztalatok és bevált gyakorlatok cseréjét, jelentős mértékben hozzájárulhat a „helyszíni" konvergencia további fejlesztéséhez, és e tekintetben megkönnyítheti a határokon átívelő adattovábbításokra vonatkozó szabályoknak való megfelelést a világ különböző térségeiben működő vállalatok számára.

- Kötelező erejű vállalati szabályok

A másik fontos eszköz az úgynevezett kötelező erejű vállalati szabályok. Ezek kötelező erejű szabályzatok és intézkedések, amelyek a vállalatcsoport tagjaira alkalmazandók, beleértve a munkavállalókat (a GDPR 46. cikke (2) bekezdésének b) pontja, 47. cikke). A kötelező erejű vállalati szabályok használata lehetővé teszi, hogy a személyes adatok világszerte szabadon mozogjanak a csoport tagjai között – anélkül, hogy minden egyes vállalati szervezet között szerződéses megállapodást kellene kötni, valamint biztosítja, hogy a csoporton belül a személyes adatok védelme ugyanolyan magas szintű legyen. A szabályok különösen jó megoldást kínálnak az összetett és nagy vállalatcsoportok számára, valamint szoros együttműködést biztosítanak a különböző joghatóságokon átívelően adatokat cserélő vállalatok között. Az 1995. évi irányelvvel ellentétben a GDPR szerint a kötelező erejű vállalati szabályokat alkalmazhatja olyan vállalatok csoportja is, amelyek közös gazdasági tevékenységet folytatnak, azonban nem ugyanazon vállalatcsoport részét képezik.

---

[137] Lásd a Schrems II ügyet.

[138] A GDPR 46. cikke (2) bekezdésének c) pontjával összhangban az általános szerződési feltételeket a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról szóló, 2011. február 16-i 182/2011/EU európai parlamenti és tanácsi rendelet (HL L 55., 2011.2.28., 13–18. o.) 5. cikkében foglalt vizsgálati eljáráson keresztül kell elfogadni. Ez magában foglalja különösen a tagállamok képviselőiből álló bizottság pozitív határozatát.

[139] Ez például magában foglalja az ASEAN tagállamai által jelenleg végzett munkát, amely az „ASEAN szerződéses mintafeltételeinek" kialakítására irányul. Lásd az ASEAN-nek az ASEAN határokon átívelő adatáramlásokra irányuló mechanizmusára vonatkozó fő megközelítéseket (elérhető itt: https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf).

Eljárásilag a kötelező erejű vállalati szabályokat az illetékes adatvédelmi hatóságoknak kell jóváhagyniuk a Testület nem kötelező erejű véleménye alapján[140]. E folyamat irányítása érdekében a Testület a GDPR fényében felülvizsgálta a kötelező erejű vállalati szabályok adatkezelőkre[141] és adatfeldolgozókra[142] vonatkozó referenciáit (amelyek meghatározzák a lényeges standardokat), és folytatja e dokumentumok módosítását a felügyeleti hatóságok által szerzett gyakorlati tapasztalatok alapján. Ezenkívül számos iránymutatást fogadott el, hogy segítse a kérelmezőket, és korszerűsítse a kötelező erejű vállalati szabályokra vonatkozó kérelmezési és jóváhagyási folyamatot[143]. A Testület szerint jelenleg több mint 40 kötelező erejű vállalati szabálycsomag vár jóváhagyásra, amelyek felét várhatóan 2020 végéig fogják jóváhagyni[144]. Fontos, hogy az adatvédelmi hatóságok továbbra is azon dolgoznak, hogy korszerűsítsék a jóváhagyási folyamatot, mivel az eljárások hosszát az érdekelt felek gyakran megemlítik a kötelező erejű vállalati szabályok széles körű alkalmazása terén felmerülő gyakorlati akadályként.

Végezetül kifejezetten az Egyesült Királyság adatvédelmi hatósága – az Information Commissioner Office – által jóváhagyott kötelező erejű vállalati szabályok tekintetében a vállalatok azokat a GDPR szerinti érvényes adattovábbítási mechanizmusként továbbra is használhatják az EU és az Egyesült Királyság közötti, a kilépésről rendelkező megállapodás szerinti átmeneti időszak végéig, azonban csak akkor, ha azokat úgy módosítják, hogy az Egyesült Királyság jogrendjét az EU-n belüli vállalati szervezetekre és illetékes hatóságokra vonatkozó megfelelő referenciákkal helyettesítik. Az új, kötelező erejű vállalati szabályok jóváhagyását az EU-n belüli felügyeleti hatóságok valamelyikétől kell kérni.

- Tanúsítási mechanizmusok és magatartási kódexek

A már létező adattovábbítási eszközök alkalmazásának modernizálása és szélesítése mellett a GDPR új eszközöket is bevezetett, ezáltal szélesítve a nemzetközi adattovábbításokra irányuló lehetőségek körét. Ez magában foglalja bizonyos feltételek mellett a jóváhagyott magatartási kódexek és tanúsítási mechanizmusok (például adatvédelmi bélyegzők vagy jelölések) alkalmazását a megfelelő garanciák biztosítása érdekében. Ezek alulról építkező eszközök, amelyek lehetővé teszik az egyedi megoldásokat – általános elszámoltathatósági mechanizmusként (lásd a GDPR 40. és 42. cikkét), és különösen a nemzetközi adattovábbítások tekintetében tükrözik például az adott ágazat vagy iparág vagy adott adatáramlások egyedi jellemzőit és szükségleteit. A kötelezettségek kockázatokkal való összehangolásával a magatartási kódexek szintén rendkívül hasznos és költséghatékony megoldást kínálnak a kis és középvállalkozások számára a GDPR szerinti kötelezettségeiknek való megfelelés tekintetében.

---

[140] Az Európai Adatvédelmi Testület eddig kiadott véleményeinek áttekintését lásd itt: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_hu

[141] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109

[142] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110

[143] E dokumentumoknak (a korábbi 29. cikk alapján létrehozott munkacsoport általi) elfogadására a GDPR hatálybalépését követően, azonban az átmeneti időszak vége előtt került sor. Lásd: WP263 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056); WP264 (https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf); WP265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848).

[144] A Testület hozzájárulásának 7. oldala.

A tanúsítási mechanizmusok tekintetében, bár a Testület elfogadta az EU-n belüli használatuk ösztönzésére irányuló iránymutatásokat, a tanúsítási mechanizmusok nemzetközi adattovábbítási eszközökként való jóváhagyására irányuló kritériumok kialakítása jelenleg is folyamatban van. Ugyanez elmondható a magatartási kódexekre is, amelyek tekintetében a Testület jelenleg dolgozik az azoknak az adattovábbítás eszközeként történő használatára irányuló iránymutatáson.

Figyelembe véve, hogy mennyire fontos, hogy a vállalkozások számára az igényeikre szabott adattovábbítási eszközök széles skálája álljon rendelkezésre, valamint hogy mekkora potenciál rejlik az egyes tanúsítási mechanizmusokban az adattovábbítások megkönnyítése és a magas szintű adatvédelem biztosítása terén, a Bizottság arra ösztönzi a Testületet, hogy a lehető leghamarabb véglegesítse az ezzel összefüggő iránymutatását. Ez mind a tartalmi (kritériumok), mind pedig az eljárási aspektusokra (jóváhagyás, nyomon követés stb.) kiterjed. Az érdekelt felek rendkívül érdeklődőnek bizonyultak az adattovábbítási mechanizmusokkal kapcsolatban, és képesnek kell lenniük arra, hogy a GDPR eszköztárát teljes mértékben kihasználják. A Testület iránymutatása hozzájárulna ahhoz is, hogy globálisan is elő lehessen mozdítani az uniós adatvédelmi modellt, és fokozni lehessen a konvergenciát, mivel más adatvédelmi rendszerek hasonló eszközöket használnak.

Értékes tanulságok vonhatók le az adatvédelem területén jelenleg fennálló standardizációs törekvésekből mind európai, mind pedig nemzetközi szinten. Az egyik érdekes példa a nemrégiben közzétett ISO 27701 nemzetközi szabvány[145], amely célja, hogy segítsen a vállalkozásoknak az adatvédelmi követelményeknek való megfelelésben, és az „adatvédelmi információkezelési rendszereken" keresztül kezelje a személyes adatokkal kapcsolatos kockázatokat. Bár a szabvány szerinti tanúsítási mechanizmusok nem tesznek eleget a GDPR 42. és 43. cikkében foglalt követelményeknek, az adatvédelmi információkezelési rendszerek alkalmazása hozzájárulhat az elszámoltathatósághoz, többek közt a nemzetközi adattovábbítások tekintetében.

- Nemzetközi megállapodások és közigazgatási megállapodások

A GDPR lehetővé teszi továbbá, hogy a nemzeti hatóságok vagy szervek közötti adattovábbításra vonatkozó megfelelő garanciákat nemzetközi megállapodások (a GDPR 46. cikke (2) bekezdésének a) pontja) vagy közigazgatási megállapodások (a GDPR 46. cikke (3) bekezdésének b) pontja) alapján biztosítsák. Bár mindkét eszköznek ugyanazt az eredményt kell biztosítania a garanciák tekintetében, beleértve a végrehajtható érintetti jogokat és a tényleges jogorvoslati lehetőségeket, jogi jellegüket és az elfogadási eljárást tekintve eltérnek egymástól.

A nemzetközi jog szerint kötelező erejű kötelezettségeket létrehozó nemzetközi megállapodásokkal ellentétben a közigazgatási megállapodások (pl. egyetértési megállapodás formájában) jellemzően nem kötelező erejűek, és ezért az illetékes adatvédelmi hatóság előzetes engedélyéhez kötöttek (lásd továbbá a GDPR (108) preambulumbekezdését). Egy korai példa az Értékpapír-felügyeletek Nemzetközi Szervezetének (IOSCO) keretében az EGT-n belüli és EGT-n kívüli pénzügyi felügyelők közötti személyesadat-továbbításra vonatkozó közigazgatási

[145] Az ISO szabvány konkrét követelményeinek jegyzéke elérhető itt: https://www.iso.org/standard/71670.html

megállapodást érinti, amelyről a Testület 2019 elején adott véleményt[146]. Azóta a Testület tovább pontosította a „minimális garanciák” értelmezését, amelyeket a nemzetközi (együttműködési) megállapodásoknak és a nemzeti hatóságok vagy szervek (beleértve a nemzetközi szervezeteket) közötti közigazgatási megállapodásoknak biztosítaniuk kell a GDPR 46. cikkében foglalt követelményeknek való megfelelés érdekében. 2020. január 18-án elfogadta az iránymutatás tervezetét[147], amelyben foglalkozott a tagállamok azon kérésével, hogy további pontosítást és útmutatót nyújtson a tekintetben, hogy mi tekinthető megfelelő garanciának a nemzeti hatóságok közötti adattovábbítások esetén[148]. A Testület határozottan javasolja, hogy a nemzeti hatóságok referenciapontként használják ezeket az iránymutatásokat a harmadik felekkel folytatott tárgyalások során[149].

Az iránymutatás rámutat az ezen eszközök tervezésében rejlő rugalmasságra, beleértve az olyan fontos szempontokat, mint a felügyelet[150] és a jogorvoslat[151]. Ez lehetővé fogja tenni a nemzeti hatóságok számára, hogy legyőzzék a nehézségeket, amelyek például a végrehajtható érintetti jogok nem kötelező erejű megállapodásokon keresztüli biztosításával kapcsolatosak. E megállapodások fontos eleme azoknak az illetékes adatvédelmi hatóságok általi folyamatos nyomon követése – amelyet az információs és nyilvántartásra vonatkozó követelmények támogatnak –, valamint az

---

[146] Európai Adatvédelmi Testület, 4/2019. számú vélemény a személyes adatoknak az Európai Gazdasági Térségen belül (a továbbiakban: EGT) és az EGT-n kívül működő pénzügyi felügyeleti hatóságai közötti továbbításáról szóló közigazgatási megállapodás tervezetéről szóló, 2019.2.12.

[147] Európai Adatvédelmi Testület, 2/2020. számú iránymutatás az (EU) 2016/679 rendeletnek a személyes adatoknak az EGT-n belüli és EGT-n kívüli nemzeti hatóságok és szervek közötti továbbításáról szóló 46. cikke (2) bekezdésének a) pontjáról és 46. cikke (3) bekezdésének b) pontjáról (a tervezet elérhető itt: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en). Az Európai Adatvédelmi Testület szerint „[a]z illetékes [felügyeleti hatóság] a vizsgálatát az ezen irányelvben meghatározott általános ajánlásokra fogja alapozni, azonban a konkrét ügytől függően kérhet további garanciákat is.” Az Európai Adatvédelmi Testület a 2020. május 18-án lezárult nyilvános konzultációra nyújtotta be ezt az iránymutatás-tervezetet.

[148] A Tanács álláspontja és megállapításai, 20. bekezdés.

[149] A Testület ugyanakkor egyértelműsíti, hogy a nemzeti hatóságok továbbra is „szabadon használhatnak egyéb releváns eszközöket, amelyek a GDPR 46. cikkével összhangban megfelelő garanciákat biztosítanak.” Az eszköz kiválasztásával kapcsolatban az Európai Adatvédelmi Testület hangsúlyozza, hogy „[a]laposan meg kell vizsgálni, hogy az adatkezelés célját és az adatok jellegét figyelembe véve jogilag kötelező erejű közigazgatási megállapodásokat kell-e igénybe venni a közszektorban a garanciák biztosításához. Ha az EGT-n belüli személyek adatvédelemhez és jogorvoslathoz való jogai nem biztosítottak a harmadik ország nemzeti jogában, a jogilag kötelező erejű megállapodást kell előnyben részesíteni. Az elfogadott eszköztől függetlenül a bevezetett intézkedéseknek hatékonynak kell lenniük a megfelelő végrehajtás, érvényesítés és felügyelet biztosítása terén (67. bekezdés).

[150] Ez magában foglalhatja például a belső ellenőrzések (nem megfelelés esetén a másik fél értesítésének vállalásával) és a külső vagy legalább funkcionálisan önálló mechanizmusokon keresztüli független felügyelet összehangolását, valamint a továbbító nemzeti szerv számára azon lehetőség biztosítását, hogy felfüggessze vagy megszüntesse a továbbítást.

[151] Ez magában foglalhatja például a kvázi bírósági, kötelező erejű mechanizmusokat (pl. választottbíráskodás) vagy az alternatív vitarendezési mechanizmusokat azzal a lehetőséggel kombinálva, hogy a továbbító nemzeti hatóság felfüggessze vagy megszüntesse a személyes adatok továbbítását, ha a felek nem tudják békésen rendezni a vitát, valamint a fogadó nemzeti hatóság azon kötelezettségvállalásával, hogy visszajuttatja vagy törli a személyes adatokat. Abban az esetben, ha nincs lehetőség a hatékony jogorvoslat biztosítására, és emiatt alternatív jogorvoslati mechanizmusokat kell választani a kötelező erejű és végrehajtható eszközökben, a Testület azt javasolja, hogy az eszközök megkötése előtt érdemes az illetékes felügyeleti hatóság tanácsát kérni.

adatáramlások felfüggesztése, ha a megfelelő garanciák már nem biztosítottak a gyakorlatban.

Eltérések

Végezetül a GDPR pontosítja az úgynevezett „eltérések” alkalmazását. Ezek a jogban elismert, adattovábbításra vonatkozó konkrét jogalapok (pl. kifejezett hozzájárulás[152], szerződés teljesítése vagy fontos közérdekű okok), amelyekre a szervezetek más továbbítási eszközök hiányában és bizonyos körülmények között támaszkodhatnak.

Annak érdekében, hogy e kötelező jogalapok használatát tisztázza, a Testület külön iránymutatást[153] adott ki, és számos ügyben értelmezte a 49. cikket az adott adattovábbítási forgatókönyvre vonatkozóan[154]. Kivételes jellegük miatt a Testület úgy véli, hogy az eltéréseket korlátozó módon, eseti alapon kell értelmezni. Szigorú értelmezésük ellenére ezek a jogalapok az adattovábbítási forgatókönyvek széles skáláját lefedik. Ez különösen magában foglalja mind a nemzeti hatóságok, mind pedig a magánszervezetek által „fontos közérdekből” végzett adattovábbításokat, például a verseny-, pénzügyi, adó- vagy vámhatóságok, a társadalombiztosítási ügyekért vagy közegészségügyért felelős szolgálatok között (például fertőző betegségeknél kontaktkövetés esetén, vagy a sportban a doppingolás megszüntetése érdekében)[155]. Egy másik terület a bűnüldözési célokból folytatott, határokon átívelő együttműködés, különös tekintettel a súlyos bűncselekményekre[156].

A Testület egyértelműsítette, hogy bár az adott közérdeket el kell ismernie az uniós vagy tagállami jognak, ez megállapítható az alábbiak szerint is: „a 49. cikk (1) bekezdésének d) pontja szerinti közérdek fennállásának értékelése során erre való jelzés lehet az, ha olyan nemzetközi megállapodás vagy egyezmény irányul egy bizonyos célkitűzésre, és rendelkezik e célkitűzés érdekében nemzetközi együttműködésről, amelynek az EU vagy a tagállamok részes felei”[157].

---

[152] Ez a 95/46/EK irányelvhez képest változás, ugyanis az pusztán „egyértelmű” hozzájárulást írt elő. Ezenkívül a GDPR 4. cikkének (11) bekezdése szerinti, hozzájárulásra vonatkozó általános követelmények alkalmazandók.

[153] Európai Adatvédelmi Testület, 2/2018. számú iránymutatás az (EU) 2016/679 rendelet 49. cikke szerinti eltérésekről, 2018.5.25. (elérhető itt: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_hu.pdf).

[154] Ez magában foglalja például az egészségre vonatkozó adatok kutatási célokból végzett nemzetközi továbbítását a Covid19-világjárvánnyal összefüggésben. Lásd az Adatvédelmi Testület 03/2020. számú iránymutatását az egészségügyi adatoknak a Covid19-járvánnyal összefüggésben végzett tudományos kutatás céljából történő kezeléséről, 2020.4.21. (elérhető itt: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_hu.pdf).

[155] Lásd az (112) preambulumbekezdést.

[156] Lásd az Európai Bizottságnak az Európai Unió nevében *amicus curiae* minőségben küldött levelét, amelyben egyik felet sem támogatja az *USA kontra Microsoft* ügyben, 15. o.: „Általánosságban az uniós és a tagállami jog elismeri a súlyos bűncselekmények elleni küzdelem – és ezáltal a bűnüldözés és az e tekintetben folytatott együttműködés – mint közérdekű célkitűzés fontosságát. […] Az EUMSZ 83. cikke a bűncselekmények számos olyan területét azonosítja, amelyek különösen súlyosak és határokon átívelő dimenzióval rendelkeznek, mint például a tiltott kábítószer-kereskedelem.” (elérhető itt: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

[157] Európai Adatvédelmi Testület, az eltérésekről szóló iránymutatás (fent a 153. lábjegyzet), 10. o. A Testület továbbá pontosította, hogy bár a közérdeken alapuló adattovábbításokra vonatkozó „eltérések nem lehetnek „nagymértékűek” vagy „szisztematikusak”, „hanem konkrét helyzetekre

Külföldi bíróságok vagy hatóságok határozatai: nem jogalap az adattovábbításokra

Az adattovábbítások jogalapjának pozitív meghatározása mellett a GDPR V. fejezete a 48. cikkben pontosítja továbbá, hogy az EU-n kívüli bíróságok végzései és közigazgatási hatóságok határozatai *önmagukban* nem jelentenek ilyen jogalapot, kivéve, ha azokat nemzetközi megállapodás (pl. kölcsönös jogsegélyszerződés) alapján elismerik és végrehajthatóvá teszik. Az ilyen végzésre vagy határozatra adott válaszként az EU-n belüli felkért szervezet által a külföldi bíróság vagy hatóság számára történő közlés nemzetközi adattovábbításnak minősül, amelynek az említett adattovábbítási eszközök egyikén kell alapulnia[158].

A GDPR nem minősül „blokkoló intézkedésekről szóló rendeletnek", és bizonyos feltételek mellett lehetővé teszi a harmadik ország megfelelő bűnüldözési kérelmére válaszként végzett adattovábbítást. Ebben az a fontos, hogy az uniós jognak kell meghatároznia, hogy ez-e a helyzet, és hogy mely garanciák alapján kerülhet sor az ilyen adattovábbításokra.

A Bizottság a *Microsoft* ügyben az Egyesült Államok legfelsőbb bírósága előtt ismertette a külföldi bűnüldöző hatóság általi, közlésre kötelező határozat (végrehajtási parancs) tekintetében a GDPR 48. cikkének működését[159]. Beadványában a Bizottság hangsúlyozta, hogy az EU annak biztosításában érdekelt, hogy a bűnüldözési együttműködésre „olyan jogi kereten belül kerüljön sor, amely elkerüli a kollíziót, és az egymás alapvető adatvédelmi és bűnüldözési érdekeinek tiszteletén alapul"[160]. Különösen „a nemzetközi közjog szempontjából amikor egy nemzeti hatóság a joghatóságán belül bejegyzett vállalatot arra kötelez, hogy egy külföldi joghatóságban található szerveren tárolt elektronikus adatokat nyújtson be, a területiség és a nemzetközi közjog szerinti udvariasság elve alkalmazandó"[161].

Ez tükröződik a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és

---

kell korlátozni alkalmazásukat, és [ki kell állniuk] a szigorú szükségességi próbát", nincs arra vonatkozó követelmény, hogy „alkalomszerűek" legyenek.

158 Ezt egyértelművé tette a GDPR 48. cikkének megfogalmazása („az adattovábbítás e fejezet szerinti egyéb okainak sérelme nélkül"), és az azt kísérő (115) preambulumbekezdés („[a]z adattovábbítás csak akkor engedélyezhető, ha az e rendeletben a harmadik országokba történő adattovábbítás tekintetében meghatározott feltételek teljesülnek. Ez többek között akkor állhat fenn, ha az adatközlés olyan, az uniós jogban vagy azon tagállam jogában elismert fontos közérdekből szükséges, amelynek az adatkezelő a hatálya alá tartozik"). Ezt a Testület is elismeri, lásd az eltérésekről szóló iránymutatást (a fenti 153. lábjegyzet), 5. o. Mint minden adatkezelési művelet esetében, a rendelet szerinti egyéb garanciáknak is meg kell felelni (pl. az adatokat konkrét célból kell továbbítani, azoknak relevánsnak kell lenniük, és a kérelem céljához szükségesre kell korlátozódniuk, stb.).

159 Microsoft beadvány (fent a 156. lábjegyzet) Ahogy a Bizottság kifejtette, a GDPR ezáltal a kölcsönös jogsegélyszerződést tekinti az „előnyben részesített opciónak" az adattovábbítások esetén, mivel ezek a szerződések „előírják a bizonyítékok hozzájárulás útján történő gyűjtését, és a különböző államok érdekei között gondosan megtárgyalt egyensúlyt testesítenek meg, amelynek célja, hogy mérsékelje az egyébként adott esetben előforduló joghatósági konfliktusokat." Lásd továbbá az Európai Adatvédelmi Testület eltérésekről szóló iránymutatását (fent a 153. lábjegyzet), 5. o. („Azokban az esetekben, amelyekre nemzetközi megállapodás – például kölcsönös jogsegélyről szóló megállapodás – vonatkozik, az uniós vállalkozásoknak általában el kell utasítaniuk a közvetlen kéréseket, és a kérelmező harmadik országbeli hatóság számára a hatályban lévő, kölcsönös jogsegélyről szóló vagy egyéb megállapodás alkalmazását kell ajánlaniuk").

160 Microsoft beadvány (fent a 156. lábjegyzet), 4. o.

161 Microsoft beadvány (fent a 156. lábjegyzet), 6. o.

megőrzésre kötelező európai határozatokról szóló rendeletre irányuló bizottsági javaslatban[162] is, amely „udvariassági záradékot" tartalmaz, amely lehetővé teszi a közlésre kötelező határozat elleni kifogás benyújtását, ha az annak való megfelelés ellentétes lenne egy harmadik ország jogszabályaival, amelyek a közzétételt kifejezetten tiltják azon az alapon, hogy ez az érintett természetes személyek alapjogainak védelme érdekében szükséges[163].

Az udvariasság biztosítása fontos, mivel a bűnüldözés – a bűncselekményekhez és különösen a kiberbűncselekményekhez hasonlóan – egyre inkább határokon átívelő, és ezáltal gyakran joghatósági kérdéseket vet fel, és potenciális kollíziót okoz[164]. Nem meglepő módon e problémákat a leghatékonyabban a nemzetközi megállapodásokon keresztül lehet kezelni, amelyek előírják a személyes adatokhoz való, határokon átívelő hozzáférésre vonatkozó szükséges korlátozásokat és garanciákat, többek közt azzal, hogy biztosítják a magas szintű adatvédelmet a kérelmező hatóság oldalán.

Az EU nevében eljáró Bizottság jelenleg többoldalú tárgyalásokat folytat az Európa Tanács számítástechnikai bűnözésről szóló Budapesti Egyezményének az elektronikus bizonyítékokhoz való hozzáférésre vonatkozó második kiegészítő jegyzőkönyvéről, amelynek célja, hogy fokozza a bűnügyi nyomozások során az elektronikus bizonyítékokhoz való, határokon átívelő hozzáférés megszerzésére irányuló jelenlegi szabályokat, és a jegyzőkönyv részeként biztosítsa a megfelelő adatvédelmi garanciákat[165]. Hasonlóképpen kétoldalú tárgyalások kezdődtek az EU és az Egyesült Államok közötti, az elektronikus bizonyítékokhoz a büntetőügyekben

---

[162] Európai Bizottság Javaslat – Az Európai Parlament és a Tanács rendelete a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról, 2018.4.17. (COM(2018) 225 final). A Tanács 2018. december 7-én elfogadta a javasolt rendeletre vonatkozó általános megközelítését (elérhető itt: https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-eevidence-council-agrees-its-position/#). Lásd továbbá az európai adatvédelmi biztos 7/19. számú véleményét a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló javaslatokról (elérhető itt: https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en).

[163] Az indokolás 21. oldala egyértelművé teszi, hogy a harmadik felek szuverén érdekeivel összefüggő udvariasság biztosítása, az érintett természetes személyek védelme és a kollízió szolgáltatók általi elkerülése mellett az udvariassági záradék egyik fontos motivációja a kölcsönösség, azaz az uniós szabályok betartásának biztosítása, többek közt a személyes adatok védelmével kapcsolatban (a GDPR 48. cikke). Lásd továbbá a 29. cikk alapján létrehozott munkacsoport 2017. november 29-i, „ Az elektronikus bizonyítékokhoz való, határokon átívelő hozzáférés adatvédelmi és magánélet-védelmi aspektusai" című nyilatkozatát (WP29-nyilatkozat) (elérhető itt: file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINALpdf%20(1).pdf), 9. o.

[164] Lásd a WP29-nyilatkozatot (a fenti 163. lábjegyzet), 6. o.

[165] Lásd az Európai Tanács számítástechnikai bűnözésről szóló egyezményének (185. sz. CETS) második kiegészítő jegyzőkönyvére vonatkozó tárgyalásokon való részvétel engedélyezéséről szóló tanácsi határozatra irányuló ajánlást, 2019.2.5. (COM(2019) 71 final). Lásd továbbá az Európai Adatvédelmi Testület 3/2019. számú véleményét a számítástechnikai bűnözésről szóló Budapesti Egyezmény második kiegészítő jegyzőkönyvére vonatkozó tárgyalásokon való részvételről, 2019.4.2. (elérhető itt: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf); az Európai Adatvédelmi Testület hozzájárulását a számítástechnikai bűnözésről szóló egyezmény (Budapesti Egyezmény) második kiegészítő jegyzőkönyvének tervezetére vonatkozó konzultációról, 2019.11.13. (elérhető itt: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf).

folytatott bírósági együttműködés céljából történő, határokon átívelő hozzáférésről szóló megállapodásról[166]. A Bizottság e tárgyalások során számít az Európai Parlament és a Tanács támogatására, valamint az Európai Adatvédelmi Testület iránymutatására.

Még általánosabban fontos biztosítani, hogy amikor az európai piacon aktív vállalatokat jogos érdek alapján felszólítják az adatok bűnüldözési célokból történő megosztására, ezt megtehessék az uniós alapjogok teljes körű betartása mellett és anélkül, hogy kollízióval szembesüljenek. Az ilyen adattovábbítások javítása érdekében a Bizottság elkötelezett az iránt, hogy megfelelő jogi kereteket alakítson ki a nemzetközi partnerekkel közösen a kollízió elkerülése, valamint az együttműködés hatékony formáinak támogatása céljából, nevezetesen a szükséges adatvédelmi garanciák előírásával, és hogy ezáltal hozzájáruljon a bűncselekmények elleni hatékonyabb küzdelemhez.

7.3 Nemzetközi együttműködés az adatvédelem területén

A különböző adatvédelmi rendszerek közötti konvergencia fokozása továbbá azzal is jár, hogy az ismeretek, tapasztalatok és bevált gyakorlatok cseréjén keresztül egymástól lehet tanulni. Ezek a cserék elengedhetetlenek az új kihívások leküzdéséhez, amelyek egyre inkább globálisak jellegüket és hatályukat tekintve. Ezért a Bizottság fokozta az adatvédelemről és az adatáramlásokról szóló, a szereplők széles körével és különböző fórumokon folytatott, kétoldalú, regionális és multilaterális párbeszédet.

A kétoldalú dimenzió

A GDPR elfogadását követően egyre nagyobb lett az érdeklődés a modern adatvédelmi szabályok kialakítása, tárgyalása és végrehajtása terén szerzett uniós tapasztalat iránt. A hasonló folyamatokon áteső országokkal folytatott párbeszédek különböző formákat öltöttek.

A bizottsági szolgálatok beadványokat nyújtottak be az adatvédelem terén jogalkotást tervező, külföldi kormányzatok által szervezett nyilvános konzultációkon, például az Egyesült Államokban[167], Indiában[168], Malajziában és Etiópiában. Egyes harmadik

---

[166] Lásd az Európai Unió és az Amerikai Egyesült Államok közötti, a büntetőügyekben folytatott igazságügyi együttműködésre vonatkozó elektronikus bizonyítékokhoz való határon átnyúló hozzáférésről szóló megállapodásra irányuló tárgyalások megkezdésére való felhatalmazásról szóló tanácsi határozatra irányuló ajánlást, 2019.2.5. (COM(2019) 70 final). Lásd továbbá az európai adatvédelmi biztos 2/2019. számú véleményét az elektronikus bizonyítékokhoz való határon átnyúló hozzáférésről szóló EU–USA megállapodásra vonatkozó tárgyalási felhatalmazásról (elérhető itt: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf).

[167] Lásd a Jogérvényesülési és Fogyasztópolitikai Főigazgatóság 2018. november 9-i beadványát, amelyet az USA Nemzeti Távközlési és Információs Kormányhivatala által a fogyasztók adatvédelmére vonatkozó, javasolt megközelítésre irányuló nyilvános észrevételek iránti kérelmére [Iktatási szám: 180821780-8780-01] nyújtott be (elérhető itt: https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf)

[168] Lásd a Jogérvényesülési és Fogyasztópolitikai Főigazgatóságnak az Elektronikai és Információtechnológiai Minisztérium részére címzett 2018. november 19-i beadványát a 2018. évi indiai személyesadat-védelmi törvényről (elérhető itt:

országokban a bizottsági szolgálatoknak lehetőségük nyílt arra, hogy beszámolót tartsanak az illetékes parlamenti szervek előtt, például Brazíliában[169], Chilében[170], Ecuadorban és Tunéziában[171].

Ezenkívül az adatvédelmi jogszabályok folyamatban lévő reformjának keretében külön megbeszélésekre került sor a világ számos térségének kormányzati képviselőivel vagy parlamenti küldöttségeivel (pl. Grúzia, Kenya, Tajvan, Thaiföld, Marokkó). Ez magában foglalta a szemináriumok és tanulmányutak szervezését, például az indonéz kormány képviselőivel és az Egyesült Államok kongresszusa tagjainak küldöttségével. Ez lehetőséget teremtett a GDPR fontos fogalmainak tisztázására, az adatvédelmi ügyek kölcsönös megértésének fejlesztésére, valamint az érintetti jogok védelme, a kereskedelem és az együttműködés magas szintjének biztosítására irányuló konvergencia előnyeinek bizonyítására. Bizonyos esetekben lehetővé tette az adatvédelem egyes olyan félreértelmezéseivel szembeni elővigyázatosságot, amelyek protekcionista intézkedésekhez, például kényszerített lokalizációs követelményekhez vezethetnek.

A GDPR elfogadása óta a Bizottság számos nemzetközi szervezettel kapcsolatba lépett, többek közt az e szervezetekkel különböző szakpolitikai területeken folytatott adatcserék jelentőségének fényében. Nevezetesen külön párbeszéd jött létre az Egyesült Nemzetekkel annak érdekében, hogy meg lehessen könnyíteni az összes érintett féllel folytatott párbeszédet, amely a zavartalan adattovábbítások biztosítására és az érintett adatvédelmi rendszerek közötti további konvergencia kialakítására irányul. E párbeszéd részeként a Bizottság szorosan együtt fog működni az Európai Adatvédelmi Testülettel, hogy tovább pontosítsa, hogy az uniós állami és magánvállalkozások miként tudnak megfelelni a GDPR szerinti kötelezettségeiknek, amikor olyan nemzetközi szervezettel cserélnek adatokat, mint az ENSZ.

A Bizottság készen áll arra, hogy folytassa a reformfolyamatából eredő tapasztalatok megosztását az érdekelt országokkal és nemzetközi szervezetekkel ugyanolyan módon, ahogyan más rendszerekből tanult, amikor kialakította az új uniós adatvédelmi szabályokra irányuló javaslatát. Az ilyen típusú párbeszéd kölcsönösen kedvező az EU és partnerei számára, mivel lehetővé teszi a gyorsan változó

---

https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en).

[169] Lásd a brazil szenátus 2018. április 17-i plenáris ülését (https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384), a brazil kongresszus 869/2018. számú ideiglenes intézkedésével foglalkozó közös bizottság 2019. április 10-i ülését (https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=15392), valamint a brazil képviselőház különleges bizottságának 2019. november 26-i ülését (https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/).

[170] Lásd a 2018. május 29-i (https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsesion=12513&idpunto=15909&sesion=29/05/2018&listado=1), 2019. április 24-i (https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2) üléseket és a chilei szenátus alkotmányos, jogalkotói és igazságügyi bizottságának ülését.

[171] Lásd a tunéziai népképviselők gyűlésének jogokkal, szabadságokkal és külső kapcsolatokkal foglalkozó bizottságának 2018. november 2-i ülését (https://www.facebook.com/1515094915436499/posts/2264094487203201/).

adatvédelmi környezet jobb megértését, valamint a kialakulóban lévő jogi és technológiai megoldásokra vonatkozó vélemények cseréjét.

A Bizottság ebben a szellemben hozza létre az „adatvédelmi akadémiát”, hogy fokozza az európai és harmadik országok szabályozói közötti cserét, és ezáltal javítsa a „helyszíni” együttműködést.

Ezenkívül ki kell alakítani az együttműködés és kölcsönös segítségnyújtás szorosabb formáira irányuló, megfelelő jogi eszközöket, beleértve a vizsgálatok során végzett, szükséges információcsere lehetővé tételét. A Bizottság ezért élni fog a GDPR 50. cikke által e tekintetben rá ruházott jogkörökkel, és különösen engedélyt kér arra, hogy tárgyalásokat indítson a végrehajtási együttműködési megállapodások adott harmadik országokkal való megkötésével összefüggésben. E tekintetben a Bizottság figyelembe fogja venni a Testület véleményét is azzal kapcsolatban, hogy az adattovábbítások mennyiségének tükrében mely országokat kell előnyben részesíteni, valamint a harmadik országokban fennálló adatvédelmi végrehajtó szerepét és jogköreit és a közös érdekű ügyek megoldására irányuló végrehajtási együttműködés iránti igényt.

A multilaterális dimenzió

A kétoldalú párbeszédek mellett a Bizottság aktívan részt vesz számos multilaterális fórumon, hogy előmozdítsa a közös értékeket, és kialakítsa a regionális és globális szintű konvergenciát.

Az adatvédelem területén fennálló egyetlen jogilag kötelező, többoldalú eszköz, az Európa Tanács 108. Egyezményének egyre növekvő egyetemes tagsága egyértelmű jele a (felfelé irányuló) konvergenciára irányuló tendenciának[172]. Az Egyezményt, amely azok előtt is nyitott, akik nem tagjai az Európa Tanácsnak, 55 ország ratifikálta, beleértve számos afrikai és dél-amerikai államot[173]. A Bizottság jelentős mértékben hozzájárult az Egyezmény modernizációjáról szóló tárgyalások sikeréhez[174], és biztosította, hogy az ugyanazokat az elveket tükrözze, amelyek az uniós adatvédelmi szabályokban szerepelnek. A legtöbb uniós tagállam aláírta a módosításról szóló jegyzőkönyvet, azonban Dánia, Málta és Románia aláírása még hiányzik. Eddig csak négy tagállam (Bulgária, Horvátország, Litvánia és Lengyelország) ratifikálta a módosításról szóló jegyzőkönyvet. A Bizottság sürgeti a fennmaradó három tagállamot, hogy írja alá a modernizált Egyezményt, és valamennyi tagállamot, hogy mihamarabb végezze el a ratifikálást, és tegye lehetővé annak hatálybalépését a

[172] Fontos megjegyezni, hogy a modernizált Egyezmény nem csupán szerződés, amely szigorú adatvédelmi garanciákat határoz meg, hanem létrehozza a végrehajtási együttműködésre irányuló eszközökkel rendelkező felügyeleti hatóságok hálózatát és az egyezményi bizottsággal egy olyan fórumot, amely alkalmas a megbeszélésekre, a bevált gyakorlatok cseréjére és a nemzetközi szabványok kialakítására.

[173] Lásd a tagok teljes listáját: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures Az afrikai országok között szerepel a Zöld-foki-szigetek, Mauritius, Marokkó, Szenegál és Tunézia, a latin-amerikai országok között pedig Argentína, Mexikó és Uruguay. Burkina Faso meghívást kapott, hogy csatlakozzon az Egyezményhez.

[174] Lásd a modernizált Egyezmény szövegét itt: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

közeljövőben[175]. Ezenkívül folytatni fogja a harmadik országok csatlakozásának ösztönzésére irányuló proaktív munkát.

Az adatáramlásokkal és az adatvédelemmel nemrégiben a G20- és a G7-csoport is foglalkozott. A globális vezetők először 2019-ben támogatták azt a gondolatot, hogy az adatvédelem hozzájárul a digitális gazdaságba vetett bizalomhoz, és megkönnyíti az adatáramlásokat. A Bizottság aktív támogatásával[176] a vezetők elfogadták a „bizalmon alapuló szabad adatáramlás" koncepcióját, amelyet eredetileg Japán javasolt a G20-ak oszakai nyilatkozatában[177] és a biarritzi G7-csúcson[178]. Ez a megközelítés tükröződik az európai adatstratégiáról szóló, 2020. évi bizottsági közleményben[179] is, amely hangsúlyozza a Bizottság azon szándékát, hogy folytatni kívánja a megbízható partnerekkel történő adatmegosztás előmozdítását, miközben küzd a visszaélésekkel, például az adatokhoz való, (külföldi) nemzeti hatóságok általi aránytalan hozzáféréssel szemben.

Ennek során az EU számos eszközre támaszkodhat majd az adatvédelemre gyakorolt hatást egyre inkább figyelembe vevő különböző szakpolitikai területeken: például a külföldi befektetések átvilágítására irányuló első uniós keret, amely 2020 októberében válik teljes mértékben alkalmazandóvá, lehetőséget teremt az EU és a tagállamai számára, hogy átvilágítsák azokat a befektetési tranzakciókat, amelyek hatással vannak az „érzékeny adatokhoz való hozzáférésre, beleértve a személyes adatokat, vagy az ilyen információk feletti rendelkezésre irányuló képességre", ha azok kihatnak a biztonságra vagy a közrendre[180].

A Bizottság számos multilaterális fórumon együttműködik a hasonló gondolkodású országokkal, hogy aktívan előmozdítsa az értékeit és standardjait. Az egyik fontos fórum az OECD által nemrégiben létrehozott, adatokkal kapcsolatos irányítással és

---

[175] A módosításról szóló jegyzőkönyvre vonatkozó, 2018. május 18-i határozata alapján a Miniszteri Bizottság „sürgette a tagállamokat és az Egyezmény egyéb feleit, hogy késedelem nélkül tegyék meg azokat az intézkedéseket, amelyek ahhoz szükségesek, hogy a jegyzőkönyv az aláírásra való megnyitástól számított három éven belül hatályba lépjen, és haladéktalanul, azonban legkésőbb a jegyzőkönyv aláírásra való megnyitásától számított egy éven belül indítsák el a nemzeti joguk szerinti folyamatot, amely a ratifikáláshoz vezet (...)" Ezenkívül „arra utasította a képviselőit, hogy kétévente és először a jegyzőkönyv aláírásra való megnyitásától számított egy év elteltével vizsgálják meg a ratifikálás irányába tett teljes folyamatot az egyes tagállamok és az Egyezmény egyéb felei által a főtitkár számára legkésőbb a vizsgálat előtt egy hónappal benyújtott információk alapján." Lásd: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016808a3c9f

[176] A 2019. áprilisi, EU és Japán közötti csúcstalálkozó alkalmával Juncker elnök támogatását fejezte ki Japán „bizalmon alapuló szabad adatáramlására" vonatkozó kezdeményezésével és az „Oszaka-pálya" elindításával kapcsolatban, és felszólította a Bizottságot, hogy „mindkét kezdeményezésben játsszon aktív szerepet".

[177] Lásd a G20-ak oszakai vezetői nyilatkozatát: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf

[178] Lásd a G7-ek nyitott, szabad és biztonságos digitális átalakulásról szóló biarritzi stratégiájának szövegét: https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf

[179] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Európai adatstratégia, 2020.2.19. (COM(2020) 66 final) (https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf), 23–24. o.

[180] Az Unióba irányuló közvetlen külföldi befektetések átvilágítási keretének létrehozásáról szóló, 2019. március 19-i (EU) 2019/452 európai parlamenti és tanácsi rendelet (HL L 79. I, 2019.3.21.) 4. cikke (1) bekezdésének d) pontja.

magánélettel foglalkozó munkacsoport (DGP), amely az adatvédelemmel, az adatmegosztással és az adattovábbításokkal kapcsolatos számos fontos kezdeményezést kíván megvalósítani. Ez magában foglalja az OECD 2013. évi adatvédelmi iránymutatásának értékelését. Ezenkívül a Bizottság aktívan hozzájárult az OECD Tanácsának mesterséges intelligenciáról szóló ajánlásához[181], és biztosította, hogy az EU emberközpontú megközelítése, azaz az, hogy az MI-alkalmazásoknak meg kell felelniük az alapjogoknak és különösen az adatvédelem szabályainak, tükröződjön a végleges szövegben. Fontos megjegyezni, hogy a mesterséges intelligenciáról szóló ajánlás –amelyet később beépítettek a G20-ak mesterséges intelligenciáról szóló, a G20-ak oszakai vezetői nyilatkozatához mellékelt elveibe[182] – előírja az átláthatóság és megmagyarázhatóság elvét annak érdekében, hogy „lehetővé tegye az MI-rendszer által negatívan érintettek számára, hogy vitassák annak eredményét az előrejelzés, ajánlás vagy határozat alapjául szolgáló tényezőkre és logikára vonatkozó, egyszerű és könnyen érthető információk alapján”, ezáltal szorosan tükrözi a GDPR automatizált döntéshozatallal kapcsolatos elveit[183].

A Bizottság továbbá fokozza a párbeszédet a regionális szervezetekkel és hálózatokkal, amelyek egyre inkább központi szerepet játszanak a közös adatvédelmi szabványok formálásában[184], előmozdítják a bevált gyakorlatok cseréjét, és támogatják a végrehajtók közötti együttműködést. Ez alkalmazandó többek közt a Délkelet-ázsiai Nemzetek Szövetségére (ASEAN) – beleértve az adattovábbítási eszközökre vonatkozó, folyamatban lévő munkája kapcsán –, az Afrikai Unióra, az Ázsiai és Csendes-óceáni Adatvédelmi Hatóságok (APPA) fórumára, valamint az Ibéramerikai Adatvédelmi Hálózatra, amelyek közül mind fontos kezdeményezéseket indított ezen a területen, és fórumot kínál az adatvédelmi szabályozók és egyéb érdekelt felek közötti gyümölcsöző párbeszédre.

Afrika jó példa az adatvédelem nemzeti, regionális és globális dimenzióinak komplementer jellegére. A digitális technológiák gyorsan és mélyrehatóan alakítják át az afrikai kontinenst. Ebben van potenciál arra, hogy a gazdasági növekedés ösztönzésével, a szegénység csökkentésével és az emberek életének javításával felgyorsítsa a fenntartható fejlesztési célok elérését. Ezen átalakulás kulcsfontosságú eleme, hogy legyen olyan modern adatvédelmi keret, amely vonzza a beruházást, és előmozdítja a versenypiaci tevékenységet, miközben hozzájárul az emberi jogok, a demokrácia és a jogállamiság betartásához. Az adatvédelmi szabályok Afrika-szerte történő harmonizálása lehetővé tenné a digitális piac integrációját, miközben a globális standardokkal fennálló konvergencia megkönnyítené az EU-val folytatott adatcseréket. Az adatvédelem

[181] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[182] A G20-ak miniszteri nyilatkozata a kereskedelemről és a digitális gazdaságról: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf

[183] Lásd a GDPR 13. cikke (2) bekezdésének f) pontját, 14. cikke (2) bekezdésének g) pontját és 22. cikkét.

[184] Lásd például az Afrikai Unió *kiberbiztonságról és a személyes adatok védelméről szóló egyezményét* („Malabo-egyezmény”), valamint az *ibéramerikai államok adatvédelmi szabványait*, amelyeket az Ibéramerikai Adatvédelmi Hálózat alakított ki.

különböző dimenziói egymáshoz kapcsolódnak, és kölcsönösen erősítik egymást.

Jelenleg számos afrikai országban egyre nagyobb az érdeklődés az adatvédelem iránt, és egyre nő[185] azon afrikai országok száma, amelyek modern adatvédelmi szabályokat fogadtak el vagy fogadnak el jelenleg, ratifikálták a 108. Egyezményt[186] vagy a Malabo-egyezményt[187]. Ugyanakkor a szabályozói keret továbbra is egyenlőtlen és széttöredezett az afrikai kontinensen belül. Számos ország továbbra is kevés adatvédelmi garanciát kínál, vagy egyáltalán nem kínál. Az adatáramlásokat korlátozó intézkedések széles körben elterjedtek, és akadályozzák a regionális digitális gazdaság kialakítását.

Az egységes adatvédelmi szabályok kölcsönös előnyeinek kiaknázása érdekében a Bizottság kapcsolatba fog lépni az afrikai partnereivel mind kétoldalú módon, mind pedig a regionális fórumokon[188]. Ez az EU és az AU közötti, digitális gazdasággal foglalkozó munkacsoportnak az Afrika és Európa közötti, új digitális gazdasági partnerség keretében végzett munkájára épít[189]. Az is előmozdítja e célok megvalósítását, hogy a Bizottság „megnövekedett adatvédelemre és adatáramlásokra” vonatkozó partnerségi eszközének alkalmazási körét Afrikára is kiterjesztették. A projekt mozgósítására fog sor kerülni, hogy a képzéseken, tudásmegosztáson és a bevált gyakorlatok cseréjén keresztül támogatni lehessen azokat az afrikai országokat, amelyek modern adatvédelmi keretrendszereket kívánnak kialakítani, vagy meg akarják erősíteni a szabályozó hatóságaik kapacitását.

---

[186] Az Európa Tanács egyezménye a személyes adatok gépi felhasználása során az egyének védelméről https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD

[187] Az Afrikai Unió egyezménye a kiberbiztonságról és a személyes adatok védelméről https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection Ezenkívül számos regionális gazdasági közösség alakított ki adatvédelmi szabályokat, például a Nyugat-afrikai Államok Gazdasági Közössége (ECOWAS) és a Dél-afrikai Fejlesztési Közösség (SADC). Lásd itt: http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf és itt: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf

[188] Többek közt a digitális Afrikára irányuló szakpolitikai és szabályozói kezdeményezésen (PRIDA) keresztül, az információkat lásd itt: https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida

[189] Lásd az Európai Bizottság és az Unió külügyi és biztonságpolitikai főképviselőjének a „Átfogó afrikai stratégia felé” c. közös közleményét (elérhető itt: https://ec.europa.eu/international-partnerships/system/files/communication-eu-africa-strategy-join-2020-4-final_en.pdf); Digitális gazdaságért felelős munkacsoport, az Afrika és Európa közötti, új digitális gazdasági partnerség: A fenntartható fejlesztési célok elérésének felgyorsítása (elérhető itt: https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf).

Végezetül az adatvédelmi standardok nemzetközi szintű konvergenciájának – az adatáramlások és ezáltal a kereskedelem megkönnyítését célzó – előmozdítása mellett a Bizottság elkötelezett aziránt is, hogy szembeszálljon a digitális protekcionizmussal, ahogyan arra nemrégiben rámutatott az adatstratégiában[190]. Ebből a célból külön rendelkezéseket határozott meg az adatáramlásokkal és az adatvédelemmel kapcsolatban a kereskedelmi megállapodásokban, amelyeket rendszeresen előterjeszt a kétoldalú – legutóbb Ausztráliával, Új-Zélanddal és az Egyesült Királysággal folytatott – és multilaterális tárgyalásokon, így például a WTO jelenlegi e-kereskedelmi megbeszélésein. Ezek a horizontális rendelkezések kizárják az indokolatlan korlátozásokat, például a kényszerített adatlokalizációs követelményeket, miközben az adatvédelemhez való alapvető jog védelme érdekében megőrzik a felek szabályozói autonómiáját.

Bár az adatvédelemről folytatott párbeszédeknek és a kereskedelmi tárgyalásoknak külön pályán kell haladniuk, kiegészíthetik egymást. Valójában a szigorú standardokon alapuló és hatékony végrehajtással támogatott konvergencia nyújtja a legerősebb alapot a személyes adatok cseréjéhez, és ezt egyre inkább elismerik a nemzetközi partnereink. Mivel a vállalatok egyre inkább határokon átívelően működnek, és világszerte minden üzleti tevékenységük során hasonló szabálykészleteket szeretnének inkább alkalmazni, ez a konvergencia hozzájárul egy olyan környezet kialakításához, amely elősegíti a közvetlen befektetést, megkönnyíti a kereskedelmet és előmozdítja a kereskedelmi partnerek közötti bizalmat. A kereskedelmi és adatvédelmi eszközök közötti szinergiákat ennek értelmében még inkább fel kell tárni, hogy biztosítani lehessen a szabad és biztonságos nemzetközi adatáramlásokat, amelyek napjaink egyre inkább digitalizált gazdaságában elengedhetetlenek az európai vállalatok, többek közt a kkv-k üzleti tevékenységeihez, versenyképességéhez és növekedéséhez.

[190] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, 23. o.

I. MELLÉKLET – A nemzeti jogszabályok általi fakultatív előírásokra vonatkozó rendelkezések

Tárgy	Alkalmazási kör	A GDPR cikkei
A jogi kötelezettségek és a közfeladat meghatározása	A jogi kötelezettséggel vagy közfeladattal összhangban végzett adatkezelésre vonatkozó rendelkezések alkalmazásának módosítása, beleértve a IX. fejezet szerinti egyes adatkezelési helyzeteket	a 6. cikk (2) bekezdése és a 6. cikk (3) bekezdése
Hozzájárulásra vonatkozó korhatár az információs társadalommal összefüggő szolgáltatások esetében	A minimális életkör meghatározása 13 és 16 éves kor között	a 8. cikk (1) bekezdése
Különleges adatkategóriák kezelése	További feltételek – köztük korlátozások – hatályban tartása, illetve bevezetése a genetikai adatok, a biometrikus adatok és az egészségre vonatkozó adatok kezelése kapcsán.	a 9. cikk (4) bekezdése
Eltérések a tájékoztatási követelményektől	Az adat jogban kifejezetten előírt vagy jogban előírt szakmai titoktartási kötelezettség alapján történő megszerzése vagy közlése	a14. cikk (5) bekezdésének c) és d) pontja
Automatizált döntéshozatal egyedi ügyekben	Az automatizált döntéshozatal engedélyezése az általános tilalomtól eltérő módon	a 22. cikk (2) bekezdésének b) pontja
Az érintettek jogainak korlátozásai	A 12–22. cikk, a 34. cikk korlátozásai és az 5. cikk vonatkozó rendelkezései, ha a teljeskörűen felsorolt fontos célkitűzések biztosítása érdekében szükséges és arányos	a 23. cikk (1) bekezdése
Konzultációs és engedélyezési követelmény	Az adatkezelők azon követelménye, hogy konzultáljanak az adatvédelmi hatósággal, vagy megszerezzék az engedélyét a közérdekű feladat elvégzéséhez szükséges adatkezeléssel összefüggésben	a 36. cikk (5) bekezdése
Adatvédelmi tisztviselő kinevezése további esetekben	Adatvédelmi tisztviselő kinevezése a 37. cikk (1) bekezdésében foglaltaktól eltérő esetekben	a 37. cikk (4) bekezdése
Az adattovábbításokra vonatkozó korlátozások	A személyes adatok speciális kategóriáinak továbbítására vonatkozó korlátozások	a 49. cikk (5) bekezdése
A szervezetek saját jogon benyújtott panaszai és	Adatvédelmi szervezeteknek az érintettek megbízásától független	a 80. cikk

keresetindításai	panaszbenyújtásra és keresetindításra vonatkozó felhatalmazása	(2) bekezdése
Közokiratokhoz való hozzáférés	A közokiratokhoz való nyilvános hozzáférés összehangolása a személyes adatok védelméhez való joggal	86. cikk
A nemzeti azonosító számok kezelése	A nemzeti azonosító számok kezelésére vonatkozó speciális feltételek	87. cikk
A foglalkoztatással összefüggő adatkezelés	A munkavállalók személyes adatainak kezelésére vonatkozó pontosabb szabályok	88. cikk
Eltérések a közérdekű archiválás, kutatás érdekében vagy statisztikai célokból történő adatkezeléssel összefüggésben	Eltérések a meghatározott érintetti jogoktól, amennyiben ezek a jogok vélhetőleg lehetetlenné teszik vagy súlyosan károsítják a kifejezett célok elérését	a 89. cikk (2) és (3) bekezdése
Az adatvédelem összehangolása a titoktartási kötelezettségekkel	Az adatvédelmi hatóságok vizsgálati jogkörére vonatkozó speciális szabályok a szakmai titoktartási kötelezettségekkel érintett adatkezelőkkel vagy adatfeldolgozókkal kapcsolatban	90. cikk

II. MELLÉKLET – Az adatvédelmi hatóságok erőforrásainak áttekintése

Az alábbi táblázat ismerteti az adatvédelmi hatóságok (személyzeti és költségvetési) erőforrásainak áttekintését EU-/EGT-tagállamonként[191].

A tagállamok számainak összehasonlításakor fontos figyelembe venni, hogy a hatóságoknak lehetnek a GDPR-ban meghatározottakon túl egyéb feladataik is, és ezek tagállamonként változóak lehetnek. A hatóságok által foglalkoztatott, egymillió lakosra jutó személyek aránya, valamint a hatóságok egymillió euró GDP-re jutó költségvetésének aránya csak azért szerepel a táblázatban, hogy további összehasonlító elemek legyenek elérhetők a hasonló méretű tagállamok között, és azokat nem érdemes külön vizsgálni. Az abszolút számokat, arányokat és az elmúlt évek változását együttesen kell vizsgálni, amikor az adott hatóság erőforrásait értékeljük.

	SZEMÉLYZET (teljes munkaidős egyenérték)					KÖLTSÉGVETÉS (EUR)				
EU-/EGT-tagállamok	2019	Előrejelzés 2020-ra	2016 és 2019 közötti növekedés (%)	2016 és 2020 közötti növekedés (%) (előrejelzés)	Személyzet aránya egymillió lakosonként (2019)	2019	Előrejelzés 2020-ra	2016 és 2019 közötti növekedés (%)	2016 és 2020 közötti növekedés (%) (előrejelzés)	A költségvetés egymillió EUR GDPR-re eső aránya (2019)
Ausztria	34	34	48 %	48 %	3,8	2 282 000	2 282 000	29 %	29 %	5,7
Belgium	59	65	9 %	20 %	5,2	8 197 400	8 962 200	1 %	10 %	17,3
Bulgária	60	60	–14 %	–14 %	8,6	1 446 956	1 446 956	24 %	24 %	23,8
Horvátország	39	60	39 %	114 %	9,6	1 157 300	1 405 000	57 %	91 %	21,5
Ciprus	24	22	n.a.	n.a.	27,4	503 855	n.a.	114 %	n.a.	23,0
Cseh Köztársaság	101	109	0 %	8 %	9,5	6 541 288	6 720 533	10 %	13 %	29,7
Dánia	66	63	106 %	97 %	11,4	5 610 128	5 623 114	101 %	101 %	18,0
Észtország	16	18	–11 %	0 %	12,1	750 331	750 331	7 %	7 %	26,8
Finnország	45	55	114 %	162 %	8,2	3 500 000	4 500 000	94 %	150 %	14,6
Franciaország	215	225	9 %	14 %	3,2	18 506 734	20 143 889	–-2 %	7 %	7,7
Németország	888	1002	52 %	72 %	10,7	76 599 800	85 837 500	48 %	66 %	22,3
Görögország	33	46	–15 %	18 %	3,1	2 849 000	3 101 000	38 %	50 %	15,2
Magyarország	104	117	42 %	60 %	10,6	3 505 152	4 437 576	102 %	155 %	24,4
Izland	17	17	143 %	143 %	47,6	2 272 490	2 294 104	167 %	170 %	105,2
Írország	140	176	169 %	238 %	28,5	15 200 000	16 900 000	223 %	260 %	43,8
Olaszország	170	170	40 %	40 %	2,8	29 127 273	30 127 273	46 %	51 %	16,3
Lettország	19	31	–10 %	48 %	9,9	640 998	1 218 978	4 %	98 %	21,0
Litvánia	46	52	–8 %	4 %	16,5	1 482 000	1 581 000	40 %	49 %	30,6
Luxemburg	43	48	126 %	153 %	70,0	5 442 416	6 691 563	165 %	226 %	85,7
Málta	13	15	30 %	50 %	26,3	480 000	550 000	41 %	62 %	36,3
Hollandia	179	188	145 %	158 %	10,4	18 600 000	18 600 000	130 %	130 %	22,9
Norvégia	49	58	2 %	21 %	9,2	5 708 950	6 580 660	27 %	46 %	15,9
Lengyelország	238	260	54 %	68 %	6,3	7 506 345	9 413 381	66 %	108 %	14,2
Portugália	25	27	–4 %	4 %	2,4	2 152 000	2 385 000	67 %	86 %	10,1
Románia	39	47	–3 %	18 %	2,0	1 103 388	1 304 813	3 %	22 %	4,9
Szlovákia	49	51	20 %	24 %	9,0	1 731 419	1 859 514	47 %	58 %	18,4
Szlovénia	47	49	42 %	48 %	22,6	2 242 236	2 266 485	68 %	70 %	46,7

[191] Kivéve Liechtensteint.

Spanyolország	170	220	13 %	47 %	3,6	15 187 680	16 500 000	8 %	17 %	12,2
Svédország	87	87	81 %	81 %	8,5	8 800 000	10 300 000	96 %	129 %	18,5
ÖSSZESEN	**2 966**	**3 372**	**42 %**	**62 %**	**6,6**	**249 127 139**	**273 782 870**	**49 %**	**64 %**	**17,4**

A nyers adatok forrása: a Testület hozzájárulása. A Bizottság számításai.