EURÓPAI
BIZOTTSÁG

Brüsszel, 2020.6.24.
COM(2020) 264 final

A BIZOTTSÁG KÖZLEMÉNYE 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

{SWD(2020) 115 final}

A BIZOTTSÁG KÖZLEMÉNYE 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

1 A POLGÁROK SZEREPE ERŐSÍTÉSÉNEK ÉS AZ EU DIGITÁLIS ÁTÁLLÁSSAL KAPCSOLATOS MEGKÖZELÍTÉSÉNEK PILLÉRÉT KÉPEZŐ ADATVÉDELMI SZABÁLYOK

Ez az első jelentés az általános adatvédelmi rendelet[1] (a továbbiakban GDPR) értékeléséről és felülvizsgálatáról a GDPR 97. cikke szerint, különös tekintettel a személyes adatok harmadik országok és nemzetközi szervezetek felé történő továbbításáról szóló szabályok, valamint az együttműködésről és az egységességről szóló szabályok alkalmazására és működésére.

A GDPR, amely 2018. május 25. óta alkalmazandó, az adatvédelemhez való alapvető jogot biztosító uniós keretrendszer[2] középpontja, ahogyan az az Európai Unió Alapjogi Chartájában (8. cikk) és a Szerződésekben szerepel (az Európai Unió működéséről szóló szerződés, „EUMSZ” 16. cikke). A GDPR megerősítette az adatvédelmi garanciákat, erősebb jogokat és megnövekedett átláthatóságot nyújt a természetes személyeknek, valamint biztosítja, hogy mindazok, akik a hatályán belül személyes adatokat kezelnek, elszámoltathatók és felelősek legyenek. A független adatvédelmi hatóságokat erősebb és összehangoltabb végrehajtási jogkörökkel ruházza fel, és új irányítási rendszert hoz létre. Ezenkívül egyenlő versenyfeltételeket teremt az uniós piacon működő valamennyi vállalat számára, függetlenül attól, hol jöttek létre, továbbá biztosítja az adatok szabad áramlását az EU-n belül, ezáltal is megerősítve a belső piacot.

A GDPR a technológiára és digitális átállásra irányuló, uniós szakpolitikai döntéshozatalra jellemző emberközpontú megközelítés fontos eleme, és iránytűként szolgál a technológia használatához az uniós politikai döntéshozatalt jellemző kettős zöld és digitális átmenet során. Legutóbb a mesterséges intelligenciáról szóló fehér könyv[3], valamint az európai adatstratégiáról (a továbbiakban adatstratégia) szóló, 2020. februári közlemény[4] foglalkozott a kérdéssel.

---

[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. o.

[2] Az Európai Gazdasági Térségről (EGT) szóló megállapodásba való beépítése óta a rendelet Norvégiára, Izlandra és Liechtensteinre is vonatkozik.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_hu

Az egyre inkább az adatkezelésen, többek közt a személyes adatok kezelésén alapuló gazdaságban a GDPR elengedhetetlen eszköz annak biztosításához, hogy a természetes személyek nagyobb mértékben rendelkezhessenek a személyes adataik felett, és hogy ezeket az adatokat jogos célból kezeljék, jogszerű, tisztességes és átlátható módon. Emellett a GDPR segít a megbízható innováció előmozdításában, nevezetesen a kockázatalapú megközelítésével és az olyan elveivel, mint a beépített és az alapértelmezett adatvédelem. A Bizottság azt javasolta, hogy az adatvédelemre és a magánélet védelmére vonatkozó meglévő jogi keret[5] egészüljön ki az elektronikus adatvédelemről szóló rendelettel[6], amelynek célja a jelenlegi, elektronikus hírközlési adatvédelmi irányelv helyettesítése[7]. Ezt a javaslatot jelenleg vizsgálják a társjogalkotók, és rendkívül fontos annak gyors elfogadása.

A „Digitális korra felkészült Európával”[8] és az „Európai zöld megállapodással”[9] kapcsolatos fő bizottsági prioritások részeként új kezdeményezések kialakítására kerülhet sor annak érdekében, hogy a polgárok aktívabb szerepet játszhassanak a digitális átállásban és a digitális eszközök használatának kiaknázásában a klímasemleges társadalom és a fenntarthatóbb fejlődés megvalósítása érdekében. A GDPR keretet határoz meg e kezdeményezések tekintetében, és biztosítja, hogy azok kialakítása a természetes személyek hatékony ösztönzésére irányuljon.

Az adatstratégia[10] valódi egységes adatpiac, azaz az „egységes európai adattér”, valamint tíz ágazati közös európai adattér létrehozására szólít fel, amelyek fontosak az zöld és digitális kettős átállás szempontjából[11]. Mindezen prioritások tekintetében kulcsfontosságú a biztonságos adatmegosztásra és az adatok fokozott rendelkezésre állására vonatkozó egyértelmű és működőképes szabályozás. Az adatstratégia bejelentette a Bizottság azon szándékát is, hogy a jövőbeli jogalkotásban feltárja, hogyan lehet lehetővé tenni a nyilvános adatbázisokban tárolt adatok tudományos kutatási célokra történő felhasználását a GDPR-nak megfelelő módon. Az adattereket európai felhőszövetségnek kell támogatnia, amely a GDPR-nak megfelelő adatkezelési és felhő-infrastruktúrával kapcsolatos szolgáltatásokat nyújt. A GDPR biztosítja a személyes adatok magas szintű védelmét, valamint a természetes személyek központi

---

[5] Ez a jogi keret magában foglalja a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet ((EU) 2016/680 irányelv) és a személyes adatok uniós intézmények, szervek általi kezelése tekintetében való védelméről szóló rendeletet ((EU) 2018/1725) is.

[6] Az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről szóló európai parlamenti és tanácsi rendeletre (elektronikus hírközlési adatvédelmi rendelet) irányuló javaslat, COM(2017) 010 final, 2017/03 (COD).

[7] Az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv („elektronikus hírközlési adatvédelmi irányelv”), HL L 201., 2002.7.31., 0037. o.

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_hu

[9] A Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az európai zöld megállapodás – COM/2019/640 final.

[10] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Európai adatstratégia – COM/2020/66 final.

[11] Ez a tíz ágazati közös európai adattér a következő célokat szolgálja: egészségügy, feldolgozóipar, energia, mobilitás, mezőgazdaság, pénzügyi adatok, közigazgatás, közös európai adatkészség-adattér, európai zöld megállapodás adattér és európai nyílt tudományosadat-felhő.

szerepét valamennyi adattérben, továbbá megadja a különböző megközelítések megvalósításához szükséges rugalmasságot.

A bizalom biztosítása és a személyes adatok védelme iránti igény minden bizonnyal nem korlátozódik az EU-ra. A természetes személyek világszerte egyre inkább értékelik a magánélet és az adataik biztonságának értékét. Ahogyan egy nemrégiben készített nemzetközi felmérés[12] rávilágít, ezt fontos tényezőnek tartják, amely befolyásolja a vásárlással kapcsolatos döntéseiket és az online viselkedésüket. Egyre több vállalat reagál erre az adatvédelmi igényre többek közt azzal, hogy kiterjeszti a GDPR-ban előírt jogok és garanciák egy részét a nem uniós ügyfeleire is. Számos vállalkozás ezenkívül versenyelőnyt jelentő, megkülönböztető elemként és a nemzetközi piacon ütőkártyaként alkalmazza a természetes adatok tiszteletben tartásának előmozdítását azáltal, hogy innovatív termékeket és szolgáltatásokat kínál új adatvédelmi vagy adatbiztonsági megoldásokkal. Ezenkívül a magán- és állami ágazati szereplők nagymértékű adatgyűjtés és -kezelés iránti megnövekedett képessége fontos és összetett kérdéseket vet fel, amelyek egyre inkább a nyilvános vita középpontjába emelik a magánélet védelmét a világ különböző pontjain.

A GDPR elfogadása a világ számos régiójában arra ösztönzött más országokat, hogy kövessék a példát. Ez valóban globális tendencia, amely Chilétől Dél-Koreáig, Brazíliától Japánig, Kenyától Indiáig és Kaliforniától Indonéziáig terjed. Az EU adatvédelemmel kapcsolatos vezető szerepe rámutat arra, hogy az EU képes arra, hogy nemzetközi standardalkotóvá váljon a digitális gazdaság szabályozásában, és ezt a nemzetközi közösség fontos szereplői üdvözölték, úgymint az ENSZ főtitkára, António Guterres, aki megjegyezte, hogy a GDPR miként „*állít példát* […] *abban, hogy hasonló intézkedéseket inspiráljon máshol*” és „*arra ösztönözze az EU-t és tagállamait, hogy folytassák a digitális kor formálásának vezetését, és álljanak a technológiai innováció és szabályozás élvonalában*”.[13]

A Covid19-világjárvánnyal kapcsolatos jelenlegi válság remek példa az adatvédelmi vita globalizációjára mind a válság, mind pedig az abból való felépülés során. Az EU-ban számos tagállam hozott vészhelyzeti intézkedéseket annak érdekében, hogy megóvja a közegészséget. A GDPR egyértelmű a tekintetben, hogy minden korlátozásnak tiszteletben kell tartania az alapvető jogok és szabadságok lényegét, valamint a közérdek, nevezetesen a közegészség megóvása érdekében szükséges és arányos intézkedésnek kell lennie a demokratikus társadalomban. A kijárási korlátozások megszüntetésével a döntéshozóknak szembe kell nézniük a polgárok azon elvárásával, hogy olyan digitális megoldásokat kapjanak, amelyek megbízhatóak és tiszteletben tartják a magánélet és a személyes adatok védelméhez való jogokat.

Számos országban a beépített adatvédelmi óvintézkedéseket, mint a felhasználók önkéntes feliratkozása, az adattakarékosság és -biztonság, valamint a földrajzi helymeghatározás kizárása, elengedhetetlennek tartják annak érdekében, hogy biztosított legyen a vírus terjedésének nyomon követését és korlátozását, a közrendi

---

[12] Lásd például a Cisco 2019. évi fogyasztói adatvédelmi tanulmányát (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). A világszerte 2600 fogyasztót megszólaltató tanulmány szerint számos fogyasztó már tett intézkedéseket annak érdekében, hogy megvédje a magánéletét, például vállalatot vagy szolgáltatót váltott azok adatvédelmi szabályzatai vagy adatmegosztási gyakorlatai miatt.

[13] Az ENSZ-főtitkár olasz szenátusnak címzett beszéde, 2019. december 18. (elérhető itt: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

ellenintézkedések meghatározását, a betegek segítését vagy az enyhítési stratégiák végrehajtását célzó, adatokon alapuló megoldások megbízhatósága és társadalmi elfogadottsága. Az EU-ban az adatvédelemre és a magánélet védelmére vonatkozó jogi keret[14] kellően rugalmas eszköznek bizonyult a tekintetben, hogy a személyes adatok magas szintű védelmének biztosítása mellett ki lehessen alakítani gyakorlati megoldásokat (pl. kontaktkövető alkalmazásokat). Ezzel kapcsolatban 2020. április 16-án a Bizottság iránymutatást tett közzé az adatvédelemmel összefüggésben a világjárvány elleni küzdelmet támogató alkalmazásokról.[15]

A személyes adatok védelme szintén fontos szerepet játszik a polgárok által hozott döntések manipulációjának megelőzésében, különösen a választók jogszerűtlen személyesadat-kezelésen alapuló, specifikus tartalommal történő célzásán keresztül, a demokratikus folyamatokba való beavatkozás elkerülésében és a demokráciában elengedhetetlen nyílt vita, tisztességesség és átláthatóság megőrzésében. Emiatt 2018 szeptemberében a Bizottság közzétette az uniós adatvédelmi szabályok választásokkal összefüggésben történő alkalmazásáról szóló iránymutatásait[16].

Ehhez az értékeléshez és felülvizsgálathoz a Bizottság figyelembe vette a Tanácstól[17], az Európai Parlamenttől[18], az Európai Adatvédelmi Testülettől (a továbbiakban a „Testület")[19], valamint az egyes adatvédelmi hatóságoktól[20], a több érdekelt felet tömörítő szakértői csoporttól[21] és más érdekelt felektől kapott hozzájárulásokat, beleértve az ütemtervvel kapcsolatban nyújtott visszajelzéseket[22].

Az általános vélekedés szerint az általános adatvédelmi rendelet alkalmazásának megkezdése után két évvel sikeresen megvalósította az egyén személyes adatok

---

[14] Ez a keret a GDPR mellett magában foglalja az elektronikus hírközlési adatvédelmi irányelvet (2002/58/EK irányelv), amely szabályokat ír elő többek közt a felhasználó végberendezésére vonatkozó információkhoz való hozzáféréssel és azok tárolásával kapcsolatban.

[15] Az adatvédelemmel összefüggésben a Covid19-világjárvány elleni küzdelmet támogató alkalmazásokról szóló bizottsági iránymutatásra vonatkozó közlemény, 2020/C 124 I/01 – C/2020/2523 – HL C 124I., 2020.4.17., 1–9. o., 2020 április 16-án az uniós tagállamok a Bizottság támogatásával a koronavírus-világjárványra válaszként uniós eszköztárat hoztak létre a kontaktkövető és figyelmeztető mobilalkalmazások használatára. Ez a kijárási korlátozások fokozatos feloldásának támogatására irányuló, közös összehangolt megközelítés része. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[16] A Bizottság iránymutatása az uniós adatvédelmi szabályok választásokkal összefüggésben történő alkalmazásáról – Az Európai Bizottság hozzájárulása a 2018. szeptember 19–20-i salzburgi vezetői üléshez – COM/2018/638 final.

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

[18] Az Európai Parlament LIBE Bizottságának 2020. február 21-i levele Reynders biztos részére, hiv.: IPOL-COM-LIBE D (2020)6525.

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

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

[21] A több érdekelt felet tömörítő, a rendelettel kapcsolatban a Bizottság által létrehozott szakértői csoport a civil társadalmat és a vállalkozások képviselőit, akadémikusokat és gyakorló szakembereket foglal magában: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437

védelméhez való joga védelmének megerősítésére és a személyes adatok EU-n belüli szabad áramlásának biztosítására irányuló célkitűzéseit[23]. Mindazonáltal azonosíthatók olyan területek, amelyek a jövőben további fejlesztésre várnak. A legtöbb érdekelt félhez és adatvédelmi hatósághoz hasonlóan a Bizottság úgy véli, ebben a szakaszban korai lenne végleges következtetéseket levonni a GDPR alkalmazásával kapcsolatban. Valószínű, hogy a tagállamok és az érdekelt felek által feltárt legtöbb problémára kedvező hatással lesznek a GDPR alkalmazásával kapcsolatban a következő években születő tapasztalatok. Mindenesetre ez a jelentés rámutat a GDPR alkalmazásával kapcsolatban eddig azonosított kihívásokra, és meghatározza azok leküzdésének lehetséges módjait.

Annak ellenére, hogy az értékelés és felülvizsgálat a GDPR 97. cikkének (2) bekezdésében kiemelt két kérdésre, nevezetesen a nemzetközi adattovábbításokra, valamint az együttműködési és egységességi mechanizmusokra összpontosít, szélesebb megközelítést alkalmaz, hogy azokkal a problémákkal is foglalkozzon, amelyeknek az elmúlt két évben számos szereplő hangot adott.

2 FŐBB MEGÁLLAPÍTÁSOK

A GDPR végrehajtása és az együttműködési és egységességi mechanizmusok működése

A GDPR innovatív irányítási rendszert hozott létre, amely a tagállamok független adatvédelmi hatóságain és a köztük határokon átnyúló ügyekben és az Európai Adatvédelmi Testületen (a „Testület”) belül folytatott együttműködésen alapul. Az általános vélemény szerint az adatvédelmi hatóságok kiegyensúlyozottan használták megerősített korrekciós hatáskörüket, beleértve a figyelmeztetéseket és elmarasztalásokat, a bírságokat, valamint az ideiglenes vagy végleges adatkezelési korlátozásokat[24]. A Bizottság megjegyzi, hogy a hatóságok néhány ezer eurótól több millió euróig terjedő közigazgatási bírságokat alkalmaztak a szabálysértés súlyosságától függően. Az egyéb szankcióknak, mint az adatkezelés tilalmának legalább ugyanakkora, ha nem nagyobb elrettentő hatása lehet, mint a bírságoknak. A GDPR végső célja a kultúra és az összes érintett szereplő viselkedésének a természetes személyek számára kedvező átalakítása. Az adatvédelmi hatóságok korrekciós hatáskörének alkalmazásával kapcsolatos részletesebb információk megtalálhatók a kísérő bizottsági szolgálati munkadokumentumban.

Bár még korai teljes körűen értékelni az új együttműködési és egységességi mechanizmusok működését, az adatvédelmi hatóságok az egységességi mechanizmuson[25] és a kölcsönös segítségnyújtás[26] nagymértékű alkalmazásán keresztül kialakították az együttműködésüket. Az egységességi mechanizmust, amely a belső piac kulcsfontosságú eszköze, számos, határokon átnyúló ügyben

[23] Lásd például a tanácsi álláspontot és megállapításokat, valamint a Testület hozzájárulását.
[24] Lásd a bizottsági szolgálati munkadokumentum 2.1. pontját.
[25] Ha egy vállalat határokon átívelő módon kezel adatokat, az abban a tagállamban lévő hatóság minősül illetékes adatvédelmi hatóságnak, amelyben a vállalat üzleti tevékenységeinek fő helye található.
[26] Lásd a bizottsági szolgálati munkadokumentum 2.2. pontját.

alkalmazzák[27]. Jelenleg függőben vannak határokon átívelő dimenzióval rendelkező fontos döntések, amelyekre az egységességi mechanizmus alkalmazandó lesz. Ezek a döntések, amelyek gyakran multinacionális, nagy technológiai vállalatokra vonatkoznak, számos tagállamban jelentős hatással lesznek a természetes személyek jogaira.

Mindazonáltal az adatvédelmi hatóságok közötti, valóban közös európai adatvédelmi kultúra kialakításának folyamat továbbra sem fejeződött be. Az adatvédelmi hatóságok még nem használták ki teljes mértékben a GDPR által nyújtott eszközöket, például a közös műveleteket, amelyek közös vizsgálatokhoz vezethetnek. Néha a közös megközelítés megtalálása egyet jelentett a legkisebb közös nevező felé való elmozdulással, és ennek eredményeként a nagyobb harmonizáció előmozdítására irányuló lehetőségek nem lettek kiaknázva[28].

További előrehaladásra van szükség annak érdekében, hogy a határokon átnyúló ügyek kezelése hatékonyabb és EU-szerte összehangoltabb legyen, többek közt eljárási szempontból, például az olyan kérdésekkel kapcsolatban, mint a panaszkezelési eljárások, a panaszok elfogadhatóságára vonatkozó kritériumok, az eljárások időtartama a nemzeti közigazgatási eljárásjogban meghatározott különböző határidők vagy azok hiánya miatt, az a pont az eljárás során, amikor a meghallgatáshoz való jogot megadják, vagy a panaszt benyújtók tájékoztatása és bevonása az eljárás során. A Testület által ezzel kapcsolatban elindított gondolkodási folyamat üdvözlendő, és a Bizottság is részt vesz ezeken a megbeszéléseken[29].

A Testület tevékenységei és iránymutatása kulcsfontosságúak a Testület és az érdekelt felek közötti tapasztalatcserék folyamatos továbbfejlesztése szempontjából[30]. 2019 végéig a Testület 67 dokumentumot fogadott el, beleértve 10 új iránymutatást[31] és 43 véleményt[32]. Az érdekelt felek általánosságban üdvözlik a Testület iránymutatásait, és továbbiakat kérnek a GDPR kulcsfogalmaival kapcsolatban, azonban rámutatnak a nemzeti iránymutatások és a Testület iránymutatásai közötti ellentmondásokra is. Hangsúlyozzák a gyakorlatibb jellegű tanácsadás iránti igényt, különösen a konkrétabb példák tekintetében, valamint az adatvédelmi hatóságok azon igényét, hogy rendelkezzenek a feladataik hatékony ellátásához szükséges emberi, műszaki és pénzügyi erőforrásokkal.

A Bizottság rendszeresen hangsúlyozta a tagállamok azon kötelességét, miszerint elegendő emberi, pénzügyi és műszaki erőforrást kell biztosítaniuk a nemzeti

[27] 2018. május 25. és 2019. december 31. között 141 határozattervezetet nyújtottak be az egységességi mechanizmuson keresztül, amelyek közül 79 esetben született jogerős határozat.

[28] Például jobban össze lehetett volna hangolni az olyan adatkezelési műveleteket felsoroló nemzetközi listákat, amelyek a GDPR 35. cikke alapján adatvédelmi hatásvizsgálatot tesznek szükségessé.

[29] Lásd a bizottsági szolgálati munkadokumentum 2.2. pontját.

[30] Különösen a vállalkozások és a civil társadalom képviselői. Lásd a bizottsági szolgálati munkadokumentum 2.3. pontját.

[31] Ezek kiegészítik azt a 10 iránymutatást, amelyeket a 29. cikk szerinti munkacsoport fogadott el a rendelet hatálybalépését megelőző időszakban, és amelyeket a Testület támogatott. A Testület ezenkívül 4 további iránymutatást fogadott el 2020. január és május vége között, és egy meglévőt módosított.

[32] E vélemények közül 42 elfogadására a GDPR 64. cikke alapján, egy elfogadására pedig a GDPR 70. cikke (1) bekezdésének s) pontja alapján került sor, és utóbbi a Japánnal kapcsolatos megfelelőségi határozatot érintette.

adatvédelmi hatóságok számára[33]. A legtöbb hatóságnál 2016 és 2019 között nőtt a személyzet száma és a költségvetés[34], az ír, a holland, az izlandi, a luxemburgi és a finn hatóságok részesültek a legnagyobb személyzeti bővülésben. Mivel a legnagyobb technológiai multinacionális cégek Írországban és Luxemburgban rendelkeznek tevékenységi központtal, ezen országok adatvédelmi hatóságai számos, határokon átnyúló ügyben vezető hatóságként járnak el, és nagyobb erőforrásokat igényelhetnek a lakosságuk alapján elvárhatóhoz képest. Mindazonáltal a helyzet továbbra is egyenlőtlen a tagállamok között, és összességében egyáltalán nem kielégítő. Az adatvédelmi hatóságok elengedhetetlen szerepet játszanak abban, hogy a GDPR végrehajtása biztosított legyen nemzeti szinten, és hogy a Testületen belüli együttműködési és egységességi mechanizmusok hatékonyan működjenek, beleértve különösen a határokon átívelő ügyekben alkalmazott egységességi mechanizmust. A tagállamoknak ezért biztosítaniuk kell számukra a GDPR-ban előírt megfelelő erőforrásokat[35].

Összehangolt szabályok, azonban továbbra is bizonyos fokú széttagoltság és eltérő megközelítések

A Bizottság nyomon követi a GDPR nemzeti jogalkotásban történő végrehajtását. E jelentés idején Szlovénia kivételével valamennyi tagállam új jogszabályt fogadott el, vagy módosította nemzeti adatvédelmi törvényét. Szlovénia[36] felszólítást kapott arra, hogy tájékoztatást nyújtson a Bizottságnak a folyamat véglegesítéséről[37].

A GDPR előírja, hogy EU-szerte összehangolt módon kell megközelíteni az adatvédelmi szabályokat. Mindazonáltal arra kötelezi a tagállamokat, hogy egyes területeken jogszabályokat alkossanak[38], és biztosítja számukra azt a lehetőséget, hogy más területeken tovább pontosítsák a GDPR-t[39]. Ennek eredményeként továbbra is fennáll bizonyos fokú széttagoltság, ami nevezetesen a fakultatív előírásokból fakad. Például a tagállamok között az információs társadalommal összefüggő szolgáltatásokkal kapcsolatban a gyermekek beleegyezési korhatára tekintetében fennálló különbség elbizonytalanítják a gyermekeket és szüleiket adatvédelmi jogaik egységes piacon történő alkalmazását illetően. Ez a széttagoltság kihívásokat is teremt a határokon átívelő üzletvitel és innováció terén, különös tekintettel az új technológiai fejleményekre és kiberbiztonsági megoldásokra. A belső piac hatékony működése és a vállalatokra nehezedő, szükségtelen terhek elkerülése érdekében továbbá elengedhetetlen, hogy a nemzeti jogszabályok ne haladják meg a GDPR által meghatározott kereteket, vagy ne vezessenek be további követelményeket ott, ahol nincsenek keretek.

A nemzeti jogalkotás számára külön kihívás a személyes adatok védelméhez való jog és a véleménynyilvánítás és a tájékozódás szabadságának egyeztetése, valamint az e

[33] 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.
[34] 2016 és 2019 között a személyzet terén összesen 42 %-os, a költségvetés terén pedig 49 %-os növekedés volt megfigyelhető az EGT-n belüli nemzeti adatvédelmi hatóságoknál.
[35] Lásd a bizottsági szolgálati munkadokumentum 2.4. pontját.
[36] Legutóbb 2020 márciusában Reynders biztos levelén keresztül.
[37] Megjegyzendő, hogy a szlovén nemzeti adatvédelmi hatóság a jelenlegi nemzeti adatvédelmi törvény alapján jött létre, és felügyeli a tagállamban a GDPR alkalmazását.
[38] Lásd a bizottsági szolgálati munkadokumentum 3.1. pontját.
[39] Lásd a bizottsági szolgálati munkadokumentum 3.2. pontját.

jogok közötti megfelelő egyensúly kialakítása. Egyes nemzeti jogszabályok a véleménynyilvánítás szabadsága elsőbbségének elvét határozzák meg, míg mások a személyes adatok védelmének elsőbbségét, és az adatvédelmi szabályok alól csak bizonyos helyzetekben mentenek fel, például amikor közszereplőről van szó. Végezetül más tagállamok a jogalkotó általi egyensúlyteremtést és/vagy eseti alapú értékelést írnak elő a GDPR egyes rendelkezéseitől való eltérés tekintetében.

A Bizottság folytatni fogja a nemzeti jogalkotás értékelését. Az egyeztetést jogszabálynak kell előírnia, be kell tartania az alapvető jogokat, és arányosnak és szükségesnek kell lennie[40]. Az adatvédelmi szabályok (valamint azok értelmezése és alkalmazása) nem hathatnak ki a véleménynyilvánítás és tájékozódás szabadságának gyakorlására, például azzal, hogy elrettentő hatást hoznak létre vagy nyomást gyakorolnak az újságírókra, hogy megosszák forrásaikat. Az e két jog közötti egyensúly nemzeti jogszabályok általi megteremtésének keretét a Bíróság és az Emberi Jogok Európai Bíróságának ítélkezési gyakorlatának kell adnia[41].

A tagállami jogalkotások a feltételek és a garanciák szintje terén, beleértve az egészségügyi és kutatási célokat, különböző megközelítéseket alkalmaznak, amikor végrehajtják a személyes adatok különleges kategóriáinak kezelésére vonatkozó általános tilalomtól való eltérést. E probléma kezelése érdekében a Bizottság első lépésként feltérképezi a tagállamok különböző megközelítéseit[42], következő lépésként pedig támogatni fogja a magatartási kódex(ek) létrehozását, amelyek hozzájárulnának az e tekintetben alkalmazandó egységesebb megközelítéshez, és megkönnyítenék a személyes adatok határokon átívelő kezelését[43]. Ezenkívül a Testületnek a személyes adatok tudományos kutatás terén való felhasználásáról szóló jövőbeli iránymutatásai is hozzá fognak járulni az összehangolt megközelítéshez. A Bizottság információkat fog nyújtani a Testületnek, különösen az egészségügyi kutatásokkal kapcsolatban, többek közt konkrét kérdések és a kutatói közösségtől kapott egyes forgatókönyvek elemzésének formájában.

[40] A Charta 52. cikkének (1) bekezdése.
[41] Lásd a bizottsági szolgálati munkadokumentum 3.1. pontját: A személyes adatok védelméhez való jog és a véleménynyilvánítás és a tájékozódás szabadságának egyeztetése.
[42] A Bizottság kutatást indított „A GDPR fényében a tagállamok egészségügyi adatokra vonatkozó szabályainak értékeléséről”, Chafea/2018/Health/3, egyedi szerződés száma: 2019 70 01.
[43] Lásd az európai adatstratégiában bejelentett intézkedéseket, 30. o.

A természetes személyek felhatalmazása arra, hogy rendelkezzenek saját adataik felett

Egy alapjogi felmérés[44] szerint a 16 éves kor feletti uniós lakosság 69 %-a hallott a GDPR-ról, és az uniós lakosság 71 %-a tud a nemzeti adatvédelmi hatóságáról.

A természetes személyek egyre inkább tisztában vannak jogaikkal: a személyes adataikhoz való hozzáférés jogával, a helyesbítéshez, a törléshez, a személyes adatok hordozhatóságához való joggal, az adatkezelés elleni tiltakozáshoz való joggal, valamint a nagyobb átláthatósággal. A GDPR megerősítette az eljárási jogokat, és magában foglalja az adatvédelmi hatóságnál való panasztétel jogát, többek közt képviseleti kereset útján, valamint a bírósági jogorvoslathoz való jogot. A természetes személyek egyre inkább használják ezeket a jogokat, azonban meg kell könnyíteni azok gyakorlását és teljes körű érvényesítését. A Testület által vezetett gondolkodás egyértelműsíteni fogja és meg fogja könnyíteni a természetes személyek jogainak gyakorlását, míg a képviseleti eljárásokról szóló irányelv[45] elfogadását követően várhatóan lehetővé teszi a természetes személyek számára, hogy kollektív keresetet nyújtsanak be bármely tagállamban, és csökkenteni fogja a határokon átívelő keresetek költségeit.

Az adathordozhatósághoz való jogban egyértelmű potenciál rejlik, azonban továbbra sincs teljes mértékben kiaknázva annak érdekében, hogy az adatgazdaság középpontjába a természetes személyek kerüljenek azáltal, hogy lehetővé válik számukra a különböző szolgáltatók közötti váltás, a különböző szolgáltatások egyesítése, az innovatív szolgáltatások igénybevétele, valamint a leginkább adatvédelem-barát szolgáltatások választása. Ez közvetve elő fogja segíteni a versenyt és támogatni fogja az innovációt. E potenciál kiaknázása a Bizottság egyik prioritása, különösen mivel az „Internet of Things" eszközök megnövekedett használatával a fogyasztók egyre több adatot generálnak, és ezáltal a tisztességtelen gyakorlatok és „bezártsági hatások" veszélyével kell szembenézniük. A hordozhatóság jelentős előnyökkel járhat az egészséggel és a jóléttel, a csökkentett ökológiai lábnyommal, valamint az állami és magánszolgáltatásokhoz való hozzáféréssel, a megnövekedett gyártási termelékenységgel és a jobb termékminőséggel és -biztonsággal kapcsolatban.

Az adatstratégia kiemelte, hogy le kell küzdeni az olyan akadályokat, mint az adatok géppel olvasható formátumban történő rendelkezésre bocsátását lehetővé tévő standardok hiánya, és növelni kell az adathordozhatósághoz való jog hatékony alkalmazását, amely jelenleg csak néhány ágazatra korlátozódik (pl. banki és telekommunikációs ágazat). Ezt nevezetesen a megfelelő eszközök, a standardizált formátum és interfészek kialakításán keresztül lehet megvalósítani[46]. Ez a megnövekedett használat a technikai interfészek és géppel olvasható formátumok engedélyezésével érhető el, ami lehetővé teszi az adatok valós idejű hordozhatóságát. Az adathordozhatósághoz való jog megnövekedett alkalmazása többek között megkönnyítheti a természetes személyek számára, hogy lehetővé tegyék az adataik

[44] Az Európai Unió Alapjogi Ügynöksége (FRA) (2020): 2019. évi alapjogi kutatás. Adatvédelem és technológia: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

[45] A fogyasztók kollektív érdekeinek védelmére irányuló képviseleti eljárásokról szóló javasolt irányelv (COM/2018/0184 final – 2018/089 (COD)) az elfogadását követően várhatóan az adatvédelem terén is megerősíti a képviseleti keresetek keretét.

[46] Ezek az eszközök magukban foglalhatják a hozzájárulás-kezelő eszközöket, valamint a személyes adatok kezelésére szolgáló alkalmazásokat.

közjó érdekében történő felhasználását (például az egészségügyi kutatások előmozdítása érdekében), ha ezzel élni kívánnak („adataltruizmus”). A digitális szolgáltatásokról szóló jogszabálycsomag[47] előkészítése során a Bizottság szélesebb körben fogja feltárni az adatok és az adatokkal kapcsolatos gyakorlatok platform-ökoszisztémában játszott szerepét.

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

A szervezetek, különösen a kis- és középvállalkozások előtt álló lehetőségek és kihívások

A GDPR a nem személyes adatok szabad áramlásáról szóló rendelettel[48] együtt a verseny és innováció előmozdításával, az adatok EU-n belüli szabad áramlásának biztosításával és az EU-n kívül létrehozott vállalatokkal egyenlő versenyfeltételek megteremtésével lehetőségeket kínál a vállalatok számára[49]. Az adathordozhatósághoz való jog az adatvédelem-barát megoldásokat kereső természetes személyek egyre nagyobb számával kiegészülve alkalmas arra, hogy csökkentse a vállalkozás elindításának akadályait, és lehetővé tegye a bizalmon és innováción alapuló növekedést. Egyes érdekelt felek arról számolnak be, hogy a GDPR alkalmazása különösen a kis- és középvállalkozások (kkv-k) számára kihívásokkal teli. A kockázatalapú megközelítés szerint nem lenne helyénvaló a gazdasági szereplők méretén alapuló eltéréseket biztosítani, mivel azok mérete önmagában nem mutatja, hogy az személyes adatok e gazdasági szereplő általi feldolgozása milyen kockázatokkal jár az egyének számára. Számos adatvédelmi hatóság gondoskodott gyakorlati eszközökről, hogy megkönnyítse az általános adatvédelmi rendelet alacsony kockázatú adatfeldolgozási tevékenységet folytató kkv-k általi végrehajtását. Ezeket az erőfeszítéseket fokozni és széles körben alkalmazni kell, lehetőleg egy közös európai megközelítés keretében, hogy ne gördítsenek akadályokat az egységes piac elé.

Az adatvédelmi hatóságok számos tevékenységet alakítottak ki, hogy segítsenek a kkv-nak abban, hogy megfeleljenek a GDPR-nak, például az adatfeldolgozási megállapodásokra és az adatkezelési tevékenységek nyilvántartására vonatkozó minták, szemináriumok és konzultációs forrónvonalak biztosításán keresztül. E kezdeményezések közül számos részesült uniós finanszírozásban[50]. További tevékenységeket kell fontolóra venni a GDPR kkv-k általi alkalmazásának megkönnyítése érdekében.

A GDPR minden típusú vállalat és szervezet számára eszköztárt tesz elérhetővé, hogy segítse őket a megfelelés igazolásában, például magatartási kódexeket, tanúsítási mechanizmusokat és általános szerződési feltételeket. Ezt az eszköztárat teljes mértékben alkalmazni kell. A kkv-k különösen a magatartási kódexek jelentőségét és hasznosságát hangsúlyozzák, amelyek a saját helyzetükre vannak szabva, és nem járnak aránytalan költségekkel. A tanúsítási rendszerek tekintetében a biztonság (beleértve a kiberbiztonságot) és a beépített adatvédelem kulcsfontosságú elemek, amelyeket a GDPR alapján figyelembe kell venni, és amelyek számára kedvező lenne

[48] 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. o.

[49] Lásd a bizottsági szolgálati munkadokumentum 5. pontját. Lásd továbbá a nem személyes adatok Európai Unióban való szabad áramlásának keretéről szóló rendeletről szóló COM/2019/250 final iránymutatást, amely ismerteti a személyes és nem személyes adatokból álló vegyes adatkészletek kezelésére vonatkozó szabályokat, amelyek praktikussá teszik azt a vállalkozások számára, beleértve a kkv-kat.

[50] A Bizottság három támogatási hullámon keresztül nyújtott pénzügyi támogatást összesen 5 millió EUR értékben, amelyek közül a két legutóbbi kifejezetten azt célozta, hogy segítse a nemzeti adatvédelmi hatóságokat abban, hogy eljussanak a természetes személyekhez és a kis- és középvállalkozásokhoz: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_hu. 2020-ban további 1 millió EUR kerül elkülönítésre

az EU-n átívelő közös és ambiciózus megközelítés. A Bizottság jelenleg az adatkezelők és adatfeldolgozók közötti általános szerződési feltételeken dolgozik[51], és a nemzetközi adattovábbításokra vonatkozó általános szerződési feltételek modernizációjára irányuló, folyamatban lévő munkára alapoz[52].

A GDPR alkalmazása új technológiák esetén

A GDPR technológiailag semleges módon jött létre, és elveken alapul, ezért úgy van kialakítva, hogy az új technológiákra is alkalmazandó legyen azok fejlődésével.

Elengedhetetlen és rugalmas eszköz, amely biztosítja, hogy az új technológiák fejlesztése összhangban legyen az alapvető jogokkal. Az adatvédelemre és a magánélet védelmére vonatkozó jogi keret a Covid19-világjárvány során bizonyította jelentőségét és rugalmasságát, nevezetesen a kontaktkövető alkalmazások és a világjárvány leküzdésére irányuló egyéb technológiai megoldások kialakítása terén. További kihívások állnak fenn a tekintetben, hogy a bizonyított elveket hogyan kell alkalmazni az egyes technológiákra, mint a mesterséges intelligencia, a blokkláncok, az „Internet of Things" vagy az arcfelismerés, amelyek folyamatos nyomon követést igényelnek. A Bizottság mesterséges intelligenciáról szóló fehér könyve[53] például nyilvános vitát indított bizonyos, esetlegesen fennálló körülményekről, amelyek indokolhatják a mesterséges intelligencia használatát a távoli biometrikus azonosítási célok (például arcfelismerés) érdekében nyilvános helyeken, valamint a közös garanciákról. E tekintetben az adatvédelmi hatóságoknak készen kell állniuk arra, hogy korai szakaszban nyomon kövessék a technikai tervezési folyamatokat.

Ezenkívül a GDPR nagy digitális platformokkal és integrált vállalatokkal szembeni erős és hatékony érvényesítése, többek közt olyan területeken mint az online hirdetés és mikrocélzás, a természetes személyek védelmének elengedhetetlen eleme.

Modern nemzetközi adattovábbítási eszköztár kialakítása

A GDPR modernizált eszköztárat kínál annak érdekében, hogy megkönnyítse a személyes adatoknak az EU-ból harmadik ország vagy nemzetközi szervezet felé történő továbbítását, és biztosítsa, hogy az adatok továbbra is magas szintű védelmet élvezzenek. Az elmúlt két évben a Bizottság fokozta a GDPR szerint elérhető eszközökben rejlő teljes potenciál kiaknázására irányuló erőfeszítéseit.

Ez magában foglalta a kulcsfontosságú partnerekkel való aktív kapcsolattartást a „megfelelőségi határozat" meghozatala érdekében. Az ilyen határozat joghatása, hogy lehetővé válik a személyes adatok biztonságos és szabad áramlása az adott harmadik országba anélkül, hogy az adatátadónak további garanciákat kellene biztosítania vagy valamilyen engedélyt be kellene szereznie. Az EU és Japán közötti kölcsönös megfelelőségi határozatok, amelyek 2019 februárjában léptek hatályba, létrehozták a világ legnagyobb, szabad és biztonságos adatáramlási területét. Emellett a Koreai Köztársasággal is előrehaladott szakaszban tart a megfelelőségi folyamat, és más fontos ázsiai és latin-amerikai partnerekkel is folyamatban vannak a tájékozódási célú megbeszélések.

[51] A GDPR 28. cikke értelmében.
[52] A GDPR 46. cikke értelmében.
[53] Fehér könyv a mesterséges intelligenciáról – A kiválóság és bizalom európai megközelítése – COM/2020/65 final.

A megfelelőség fontos szerepet játszik az Egyesült Királysággal fennálló jövőbeli kapcsolat tekintetében is, feltéve, hogy az alkalmazandó feltételek teljesülnek. A megfelelőség a kereskedelmet lehetővé tévő egyik tényező, beleértve a digitális kereskedelmet, valamint elengedhetetlen előfeltétele a jogérvényesítés és biztonság területén folytatott szoros és ambiciózus együttműködésnek. Ezenkívül az adatvédelem terén fennálló konvergencia magas foka fontos elem a tekintetben, hogy biztosítani lehessen a két szorosan integrált gazdaság közötti egyenlő versenyfeltételeket. Az EU és az Egyesült Királyság jövőbeli kapcsolatáról szóló politikai nyilatkozattal összhangban a Bizottság jelenleg a GDPR és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv[54] szerinti megfelelőségi értékelést végez.

A GDPR első értékelésének részeként a Bizottság köteles felülvizsgálni azokat a megfelelőségi határozatokat, amelyeket a korábbi szabályok alapján fogadtak el[55]. A bizottsági szolgálatok intenzív párbeszédet folytatnak a 11 érintett harmadik ország és terület[56] mindegyikével annak érdekében, hogy értékeljék, hogy az adatvédelmi rendszereik hogyan alakultak a megfelelőségi határozat elfogadása óta, és megfelelnek-e a GDPR által meghatározott normáknak. A kereskedelem és nemzetközi együttműködés kulcsfontosságú eszközeinek minősülő határozatok folytonossága biztosításának szükségessége az egyik tényező, amely ezen országok és területek közül számosat arra ösztönzött, hogy modernizálja és megerősítse az adatvédelmi jogszabályait. Egyes országokkal és területekkel további garanciák megvitatása zajlik a védelem vonatkozó nehézségeinek leküzdése érdekében. Mindazonáltal mivel a Bíróság egy július 16-án meghozandó ítéletben pontosításokat adhat, amelyek relevánsak lehetnek a megfelelőségi standard bizonyos elemei szempontjából, a Bizottság a Bíróság adott ügyre vonatkozó ítéletének meghozatalát követően külön jelentést fog készíteni a meglévő megfelelőségi határozatok értékeléséről.[57]

A megfelelőséggel kapcsolatos munka mellett a Bizottság jelenleg az általános szerződési feltételek átfogó modernizációján dolgozik, hogy frissítse azokat a GDPR által bevezetett új követelmények fényében. A cél az, hogy jobban tükröződjön a modern digitális gazdaságban végzett adatkezelési műveletek valósága, és hogy fontolóra lehessen venni a Bíróság leendő ítélkezési gyakorlatának fényében az egyes garanciák további pontosítása iránti igényt.[58] A feltételek messze a legszélesebb körben használt adattovábbítási mechanizmust jelentik, amelyre uniós vállalatok ezrei

---

[54] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, HL L 119., 2016.5.4., 89. o.

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

[56] Ezek az országok és területek az alábbiak: Andorra, Argentína, Kanada, Feröer-szigetek, Guernsey, Jersey, Man-sziget, Izrael, Új-Zéland, Svájc és Uruguay.

[57] Lásd a C-311/18. számú, az adatvédelmi biztos kontra Facebook Ireland Limited, Maximilian Schrems („Schrems II") ügyet, amely az úgynevezett általános szerződési feltételekre vonatkozó előzetes döntéshozatallal kapcsolatos referenciát érint. Mindazonáltal a megfelelőségi standard egyes elemeit szintén tovább pontosíthatja a Bíróság.

[58] Lásd a Schrems II ügyet.

támaszkodnak annak érdekében, hogy széles körű szolgáltatásokat kínáljanak ügyfeleiknek, partnereiknek és munkavállalóiknak.

A Testület ezenkívül aktív szerepet játszott a GDPR nemzetközi aspektusainak kialakításában is. Ez magában foglalja a meglévő adattovábbítási mechanizmusokról, például a kötelező erejű vállalati szabályokról és az úgynevezett „eltérésekről" szóló iránymutatás frissítését, valamint a GDPR által bevezetett új eszközök, azaz a magatartási kódexek és a tanúsítás alkalmazására vonatkozó jogi infrastruktúra kialakítását.

Annak érdekében, hogy az érdekelt felek teljes mértékben ki tudják használni a GDPR továbbítási eszköztárát, fontos, hogy a Testület fokozza a különböző továbbítási mechanizmusokkal kapcsolatos munkát, beleértve a kötelező erejű vállalati szabályok jóváhagyására irányuló folyamat további korszerűsítését, a magatartási kódexekre és tanúsításra mint az adattovábbítás eszközeire vonatkozó iránymutatás véglegesítését, valamint a nemzetközi adattovábbítások szabályai (V. fejezet) és a GDPR területi hatálya (3. cikk) közötti kölcsönhatás egyértelműsítését.

Az uniós adatvédelmi szabályok nemzetközi dimenziójának másik fontos aspektusa a GDPR kiterjesztett területi hatálya, amely magában foglalja az uniós piacon aktív, külföldi gazdasági szereplők adatkezelési tevékenységeit is. A GDPR-nak való hatékony megfelelés és a valóban egyenlő versenyfeltételek biztosítása érdekében elengedhetetlen, hogy ez a kiterjesztés megfelelően tükröződjön az adatvédelmi hatóságok végrehajtási intézkedésein. Szükség esetén be kell vonniuk az adatkezelő vagy az adatfeldolgozó uniós képviselőjét, akihez az EU-n kívüli vállalkozás mellett vagy helyett lehet fordulni. Ezt a megközelítést szigorúan kell alkalmazni annak érdekében, hogy egyértelmű üzenetet lehessen küldeni azzal kapcsolatban, hogy az EU-n belüli tevékenységi központ hiánya nem mentesíti a külföldi gazdasági szereplőket a GDPR szerinti felelősségeik alól.

Az egységesség és a nemzetközi együttműködés előmozdítása az adatvédelem terén

A GDPR kulcsfontosságú referenciaponttá nőtte ki magát nemzetközi szinten, és katalizátorként működik világszerte számos országban a modern adatvédelmi szabályok bevezetése terén. Ez a globális egységesség felé vezető tendencia rendívül pozitív fejlemény, amely új lehetőségeket kínál az EU-n belüli természetes személyek hatékonyabb védelme terén az adataik külföldre továbbítása esetén, ugyanakkor megkönnyíti az adatáramlást.

E tendenciára építve a Bizottság fokozta a párbeszédet számos kétoldalú, regionális és multilaterális fórumon, hogy előmozdítsa a magánélet védelmének globális kultúráját, és kialakítsa a különböző adatvédelmi rendszerek közötti egységesség elemeit. Ezen erőfeszítéseiben a Bizottság az Európai Külügyi Szolgálat és a harmadik országokban található uniós küldöttségek és nemzeti szervezetek melletti képviseletek hálózatának aktív támogatására támaszkodott és fog támaszkodni a jövőben. Ez lehetővé tette az uniós szakpolitikák külső dimenziójának különböző aspektusai közötti nagyobb egységességet és komplementaritást – a kereskedelemtől kezdve az EU és Afrika közötti új partnerségig. A G20 és a G7 nemrégiben szintén elismerte, hogy az

adatvédelem hozzájárul a digitális gazdaságba és az adatok áramlásába vetett bizalomhoz, különösen az eredetileg a japán G20 elnökség által javasolt „Szabad adatáramlás bizalommal” koncepción keresztül.[59] Az adatstratégia rámutat arra, hogy a Bizottság továbbra is elő kívánja mozdítani a megbízható partnerekkel folytatott adatmegosztást, miközben küzd a visszaélések ellen, például a (külföldi) nemzeti hatóságok személyes adatokhoz való aránytalan hozzáférése ellen.

Az adatvédelmi standardok nemzetközi szintű egységességének előmozdítása során az adatáramlások és ezáltal a kereskedelem megkönnyítésének módjaként a Bizottság elkötelezett aziránt, hogy szembeszálljon a digitális protekcionizmussal, ahogyan arra az adatstratégia nemrégiben rámutatott.[60] Ennek érdekében a kereskedelmi megállapodásokban külön rendelkezéseket alakított ki az adatáramlásokról és az adatvédelemről[61], amelyeket rendszeresen előterjeszt a kétoldalú – legutóbb Ausztráliával, Új-Zélanddal és az Egyesült Királysággal folytatott – és multilaterális tárgyalások során, például a jelenlegi WTO e-kereskedelmi megbeszéléseken[62]. Ezek a horizontális rendelkezések kizárják az indokolatlan korlátozásokat, például a kényszerített adatlokalizációs követelményeket, miközben megőrzik a felek szabályozói autonómiáját az adatvédelemhez való alapvető jog védelme érdekében.

A kereskedelmi és adatvédelmi eszközök közötti szinergiákat ezért tovább kell fejleszteni, hogy biztosítottak legyenek a szabad és biztonságos nemzetközi adatáramlások, amelyek az egyre inkább digitalizált gazdaságban elengedhetetlenek az európai vállalatok üzleti műveleteihez, versenyképességéhez és növekedéséhez, beleértve a kkv-kat.

Hasonlóképpen fontos annak biztosítása, hogy amennyiben az európai piacon aktív vállalatokhoz bűnüldözési célú adatmegosztásra irányuló jogos kérelmet intéznek, ez jogi kollízió nélkül és az uniós alapvető jogok teljes körű tiszteletben tartása mellett történhessen. Az ilyen adattovábbítások javítása céljából Bizottság elkötelezett amellett, hogy megfelelő jogi kereteket alakítson ki nemzetközi partnereivel, hogy elkerülje a kollíziót és támogassa az együttműködés tényleges formáit, nevezetesen azáltal, hogy előírja a szükséges adatvédelmi garanciákat, és ezáltal hozzájárul a bűnözés elleni hatékonyabb küzdelemhez.

Végezetül ezekben az időkben, amikor az adatvédelmi megfelelőségi kérdések vagy adatbiztonsági incidensek egyszerre számos természetes személyt érintenek számos joghatóságban, az európai és nemzetközi szabályozók közötti „helyszíni” együttműködést tovább kell erősíteni. Ez különösen szükségessé teszi a megfelelő jogi eszközök kialakítását az együttműködés és kölcsönös segítségnyújtás szorosabb formái terén, beleértve a vizsgálatok során a szükséges információcsere lehetővé

---

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

[60] Adatstratégia, 23. o.

[61] Lásd a határokon átívelő adatáramlásokra és a személyes adatok védelmére vonatkozó horizontális rendelkezéseket (az uniós kereskedelmi és beruházási megállapodásokban): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf

[62] A WTO 84 tagja vesz részt jelenleg az e-kereskedelemről szóló többoldalú tárgyalásokban, valamint a 2019. január 25-én Davosban a miniszterek által elfogadott, közös nyilatkozatra irányuló kezdeményezésben. E folyamat részeként az EU 2019. május 3-án előterjesztette az e-kereskedelemre vonatkozó jövőbeli szabályokra és kötelezettségekre vonatkozó javaslatát. A javaslat magában foglalja az adatáramlásokra és a személyes adatok védelmére vonatkozó horizontális rendelkezéseket: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf

tételét. Szintén ebben a szellemben a Bizottság létrehozza az „adatvédelmi akadémiát”, amely olyan platform, ahol az uniós és külföldi adatvédelmi hatóságok tudást, tapasztalatot és bevált gyakorlatokat oszthatnak meg, hogy megkönnyítsék és támogassák az adatvédelmi végrehajtók közötti együttműködést.

3 A KÖVETKEZŐ LÉPÉSEK

A GDPR-ban rejlő teljes potenciál kiaknázása érdekében fontos összehangolt megközelítést és egységes európai adatvédelmi kultúrát létrehozni, valamint előmozdítani a határokon átívelő ügyek hatékonyabb és összehangoltabb kezelését. Ezt várják a természetes személyek és a vállalkozások, és ez az uniós adatvédelmi szabályok reformjának alapvető célkitűzése. Ugyanilyen fontos biztosítani, hogy a GDPR-ban elérhető valamennyi eszközt teljes mértékben használják annak érdekében, hogy biztosított legyen a hatékony alkalmazás a természetes személyek és vállalkozások számára.

A Bizottság folytatni fogja a tagállamokkal folytatott kétoldalú tapasztalatcseréket a GDPR végrehajtásáról, és szükség esetén továbbra is kihasználja a rendelkezésére álló valamennyi eszközt annak érdekében, hogy előmozdítsa a tagállamok GDPR szerinti kötelezettségeiknek való megfelelését.

A nemzeti jogszabályok folyamatban lévő értékelése, a GDPR hatálybalépése óta a gyakorlati tapasztalatszerzéssel eltelt rövid idő, valamint amiatt a tény miatt, hogy az ágazatspecifikus jogszabályok számos tagállamban még felülvizsgálat alatt állnak, túl korai végleges következtetéseket levonni a széttagoltság szintjéről. Az egyes rendelkezések tagállamok általi végrehajtásából fakadó lehetséges kollízió tekintetében először jobban meg kell érteni az adatkezelőkre és adatfeldolgozókra vonatkozó következményeket[63].

E kérdések nyomon követése során a nemzeti bíróságok és a Bíróság vonatkozó ítélkezési gyakorlata segít az adatvédelmi szabályok egységes értelmezésének megteremtésében. A nemzeti bíróságok nemrégiben olyan ítéleteket adtak ki, amelyek érvénytelenítik a nemzeti jogszabályok GDPR-tól eltérő rendelkezéseit[64].

A nemzetközi dimenzió tekintetében a Bizottság továbbra is az adatvédelmi szabályok konvergenciájának előmozdítására összpontosít a biztonságos adatáramlások biztosításának zálogaként. Ez magában foglalja a „felfelé irányuló” munka számos formáját, például az új vagy módosított adatvédelmi jogszabályok folyamatban lévő reformja vagy a „Szabad adatáramlás bizalommal” elképzelés többoldalú fórumokon való népszerűsítése tekintetében. Kiterjed továbbá a megfelelőséggel kapcsolatos számos párbeszédre, valamint az adattovábbítási eszköztárunk modernizációjára és bővítésére az általános szerződési feltételek módosításán és a tanúsítási mechanizmusok alapjainak lefektetésén keresztül. Ez a munka magában foglalja ezenkívül a nemzetközi tárgyalásokat, például az elektronikus bizonyítékokhoz való, határokon átnyúló hozzáférés terén, annak biztosítása érdekében, hogy az adattovábbításokra megfelelő adatvédelmi garanciák mellett kerüljön sor. Végezetül

[63] Vö. a GDPR alkalmazásáról szóló tanácsi állásponttal és megállapításokkal.
[64] Ez történt Németországban és Spanyolországban vagy Ausztriában, megszüntetve egy hiányosságot a nemzeti jogszabályokban.

az adatvédelmi végrehajtók közötti nemzetközi együttműködésre és kölcsönös segítségnyújtásra vonatkozó tárgyalásokon való részvétellel a Bizottság törekedni fog a konvergencia „gyakorlati megvalósítására".

A GDPR 2018 májusa óta történő alkalmazásának értékelése alapján az alábbiakban felsorolt intézkedések szükségesek az alkalmazásának támogatásához. A Bizottság nyomon fogja követni azok végrehajtását a 2024-ben következő értékelési jelentés fényében is.

A jogi keret végrehajtása és kiegészítése

A tagállamok feladata:

- az ágazati jogszabályok GDPR-ral való összehangolásának befejezése;
- az adott esetben széttagoltságot létrehozó és az adatok EU-n belüli szabad áramlását veszélyeztető specifikációs előírások használata korlátozásának fontolóra vétele;
- annak értékelése, hogy a GDPR-t végrehajtó nemzeti jog minden tekintetben a tagállami jogszabályok számára előírt kereteken belül van-e.

A Bizottság:

- folytatja a tagállamokkal folytatott kétoldalú tárgyalásokat a nemzeti jogszabályok GDPR-nak való megfeleléséről, ideértve a nemzeti adatvédelmi hatóságok függetlenségét és erőforrásait; kihasználja a rendelkezésére álló valamennyi eszközt, beleértve a kötelezettségszegés megállapítására irányuló eljárást, hogy biztosítsa a tagállamok GDPR-nak való megfelelését;
- támogatja a vélemények és nemzeti gyakorlatok tagállamok közötti további cseréjét olyan témákkal kapcsolatban, amelyek további nemzeti szintű pontosítást igényelnek az egységes piac széttöredezettségének csökkentése érdekében, például az egészségüggyel és kutatással kapcsolatos személyesadat-kezelés, vagy amelyek esetében más jogokkal, például a véleménynyilvánítás szabadságával való egyensúlyra kell törekedni;
- támogatja az adatvédelmi keret egységes alkalmazását az új technológiákkal kapcsolatban, hogy segítse az innovációt és a technológiai fejlődést;
- igénybe veszi a GDPR-ral foglalkozó tagállami szakértői csoportot (amely a GDPR hatálybalépése előtti átmeneti időszak alatt jött létre), hogy megkönnyítse a tagállamok és a Bizottság közötti megbeszéléseket és tapasztalatcserét;
- feltárja, hogy a további tapasztalatok és a vonatkozó ítélkezési gyakorlat fényében célszerű-e a GDPR egyes rendelkezései esetleges jövőbeli célzott módosításának javaslata, különös tekintettel a személyes adatok kezelését nem fő üzleti tevékenységként végző (alacsony kockázatú)[65] kkv-k által végzett adatkezelés nyilvántartására, és az információs társadalommal összefüggő szolgáltatások tekintetében a gyermekek hozzájárulási életkorának esetleges összehangolására.

[65] A GDPR 30. cikkének (5) bekezdése.

Az új irányítási rendszerben rejlő teljes potenciál kiaknázásának biztosítása

A Testület és az adatvédelmi hatóságok felszólítást kapnak az alábbiakra:

- hatékony megállapodások kialakítása az adatvédelmi hatóságok között az együttműködési és egységességi mechanizmus működésével kapcsolatban, beleértve az eljárási szempontokat, a tagok szakértelmére építve és a titkársága bevonásának megerősítésével;
- a GDPR alkalmazása és végrehajtása összehangolásának támogatása minden rendelkezésre álló eszköz igénybevételével, beleértve a GDPR kulcsfontosságú fogalmainak további együttműködését, valamint annak biztosítását, hogy a nemzeti iránymutatások teljes mértékben összhangban legyenek a Testület által elfogadott iránymutatásokkal;
- a GDPR-ban előírt valamennyi eszköz használatának ösztönzése a GDPR egységes alkalmazásának biztosítása érdekében;
- az adatvédelmi hatóságok közötti együttműködés fokozása, például közös vizsgálatok lefolytatásával.

A Bizottság:

- továbbra is szorosan nyomon követi a nemzeti adatvédelmi hatóságok tényleges és teljes körű függetlenségét;
- előmozdítja az együttműködést a szabályozók között (különösen az olyan területeken, mint a verseny, az elektronikus kommunikáció, a hálózat és az információs rendszerek biztonsága és a fogyasztóvédelmi politika);
- támogatja a Testületen belüli gondolkodást a nemzeti adatvédelmi hatóságok által alkalmazott eljárásokról annak érdekében, hogy fejlessze a határokon átnyúló ügyekben végzett együttműködést.

A tagállamok

- biztosítják az adatvédelmi hatóságok számára a feladataik ellátásához szükséges erőforrásokat.

Az érdekelt felek támogatása

A Testület és az adatvédelmi hatóságok felszólítást kapnak az alábbiakra:

- fogadjanak el gyakorlati jellegű és könnyen érthető további iránymutatásokat, amelyek egyértelmű válaszokat adnak és mellőzik a kétértelműséget a GDPR alkalmazásával kapcsolatos kérdések tekintetében, például a gyermekek adatainak kezelésével és az érintettek jogaival kapcsolatban, beleértve a hozzáféréshez és az adatok törléséhez való jog gyakorlását, valamint az érdekelt felekkel való konzultációt a folyamat során;
- vizsgálják felül az iránymutatásokat, ha az új tapasztalatok és fejlemények fényében, beleértve a Bíróság ítélkezési gyakorlatát további egyértelműsítésre van szükség;
- dolgozzanak ki gyakorlati eszközök – például az adatsértésekre vonatkozó harmonizált formanyomtatványt és a feldolgozási tevékenységek

egyszerűsített nyilvántartását – annak érdekében, hogy segítsék az alacsony kockázatú kkv-kat kötelezettségeik teljesítésében.

A Bizottság:

- mind a nemzetközi adattovábbítások, mind pedig az adatkezelő és adatfeldolgozó közötti kapcsolat tekintetében rendelkezésre bocsátja az általános szerződési feltételeket;
- olyan eszközöket bocsát rendelkezésre, amelyek egyértelműsítik/segítik az adatvédelmi szabályok gyermekek esetében történő alkalmazását[66];
- az adatstratégiával összhangban gyakorlati eszközöket alakít ki az adathordozhatósághoz való jog természetes személyek általi megnövekedett igénybevételének megkönnyítése érdekében, például nagyobb rendelkezést biztosítva számukra afelett, hogy ki férhet hozzá a géppel létrehozott adatokhoz, és ki használhatja azokat;
- Támogassák a szabványosítást/tanúsítást különösen a kiberbiztonsági szempontokra vonatkozóan az Európai Uniós Kiberbiztonsági Ügynökség (ENISA), az adatvédelmi hatóságok és a Testület közötti együttműködés révén;
- adott esetben él azzal a jogával, hogy felszólítsa a Testületet arra, hogy iránymutatásokat és véleményeket készítsen az érdekelt felek számára fontos témákról;
- szükség esetén iránymutatást ad, miközben teljes mértékben tiszteletben tartja a Testület szerepét;
- támogassák az adatvédelmi hatóságok azon tevékenységeit, amelyek pénzügyi támogatás révén megkönnyítik a GDPR-kötelezettségek kkv-k általi végrehajtását, különösen a más tagállamokban megismételhető gyakorlati útmutatások és digitális eszközök tekintetében.

Az innováció ösztönzése

A Bizottság:

- nyomon követi a GDPR új technológiákra történő alkalmazását, figyelembe véve a mesterséges intelligenciával kapcsolatos és az adatstratégia szerinti esetleges jövőbeli kezdeményezéseket is;
- többek közt pénzügyi támogatáson keresztül ösztönzi az uniós magatartási kódexek készítését az egészségügy és a kutatás területén;
- szorosan nyomon követi a Covid19-világjárvánnyal kapcsolatos alkalmazások fejlesztését és használatát.

A Bizottság felkéri a Testületet, hogy:

[66] Az életkor-azonosítási eszközökre vonatkozó bizottsági projekt – kísérleti projekt, amelynek célja egy kölcsönösen átjárható műszaki infrastruktúra kialakítása a gyermekek védelme érdekében, beleértve az életkor-ellenőrzést és a szülői hozzájárulást. Ez várhatóan támogatni fogja a gyermekek online védelmével kapcsolatban fennálló uniós jogszabályokon alapuló gyermekvédelmi mechanizmusok végrehajtását.

- adjon ki iránymutatásokat a GDPR tudományos kutatás, mesterséges intelligencia, blokkláncok és egyéb lehetséges technológiai fejlődések terén történő alkalmazásáról;
- vizsgálja felül az iránymutatásokat, ha további pontosításra van szükség a technológiai fejlemények fényében.

Az adattovábbításokra vonatkozó eszköztár továbbfejlesztése

A Bizottság:

- megfelelőségi párbeszédeket folytat az érdekelt harmadik országokkal „A személyes adatok cseréje és védelme a globalizált világban” című, 2017. évi közleményében meghatározott stratégiával összhangban, beleértve adott esetben (a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv szerint) a bűnüldöző hatóságok és egyéb nemzeti hatóságok részére történő adattovábbítást; ez magában foglalja a Koreai Köztársasággal folytatott megfelelőségi folyamat mihamarabbi véglegesítését;
- véglegesíti a meglévő megfelelőségi határozatok folyamatban lévő értékelését, és jelentést tesz az Európai Parlamentnek és a Tanácsnak;
- véglegesíti az általános szerződési feltételek modernizációját annak érdekében, hogy azokat a GDPR fényében frissítse, kitérve valamennyi vonatkozó továbbítási forgatókönyvre és jobban tükrözve a modern üzleti gyakorlatokat.

A Bizottság felkéri a Testületet, hogy:

- egyértelműsítse a nemzetközi adattovábbításokra vonatkozó szabályok (V. fejezet) és a GDPR területi hatálya (3. cikk) közötti kölcsönhatást;
- biztosítsa a GDPR területi hatályán belüli harmadik országokban székhellyel rendelkező gazdasági szereplőkkel szembeni hatékony végrehajtást, beleértve adott esetben egy képviselő kinevezését (27. cikk);
- korszerűsítse a kötelező erejű vállalati szabályok értékelését és esetleges jóváhagyását annak érdekében, hogy felgyorsítsa a folyamatot;
- végezze el az adattovábbítás eszközeiként szolgáló magatartási kódexek és tanúsítási mechanizmusok kialakítására, eljárásaira és értékelési kritériumaira vonatkozó munkát.

A konvergencia előmozdítása és a nemzetközi együttműködés kialakítása

A Bizottság:

- a tapasztalatok és bevált gyakorlatok megosztásával támogatni fogja a harmadik országokban folyamatban lévő, az új vagy modernizált adatvédelmi szabályokkal kapcsolatos reformokat;
- az EU és Afrika közötti új partnerség digitális fejezetének részeként kapcsolatba lép az afrikai partnerekkel a szabályozói konvergencia előmozdítása és a felügyeleti hatóságok kapacitásépítésének támogatása érdekében;

- értékeli, hogy miként lehetne megkönnyíteni a magánszereplők és a bűnüldöző hatóságok közötti együttműködést, többek között kétoldalú és multilaterális adattovábbítási keretekről állapodik meg a külföldi bűnüldöző hatóságok elektronikus bizonyítékokhoz való hozzáférése tekintetében, hogy elkerülje a kollíziót és biztosítsa a megfelelő adatvédelmi garanciákat;
- kapcsolatba lép nemzetközi és regionális szervezetekkel, például az OECD-vel, az ASEAN-nal vagy a G20-szal, hogy előmozdítsa a szigorú adatvédelmi standardokon alapuló, megbízható adatáramlásokat, többek közt az „Adatáramlás bizalommal” kezdeményes keretében;
- „adatvédelmi akadémiát” hoz létre, hogy megkönnyítse és támogassa az európai és nemzetközi szabályozók közötti tapasztalatcserét;
- előmozdítja a nemzetközi végrehajtási együttműködést a felügyeleti hatóságok között, többek közt az együttműködési és kölcsönös segítségnyújtási megállapodásokról szóló tárgyalásokon keresztül.