Az Európai Unió
Tanácsa

Brüsszel, 2024. január 22.
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Címzett:	Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2024) 7 final
Tárgy:	A BIZOTTSÁG JELENTÉSE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK a 95/46/EK irányelv 25. cikkének (6) bekezdése alapján elfogadott megfelelőségi határozatok végrehajtásának első felülvizsgálatáról

Mellékelten továbbítjuk a delegációknak a következő dokumentumot: COM(2024) 7 final.

Melléklet: COM(2024) 7 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2024.1.15.
COM(2024) 7 final

A BIZOTTSÁG JELENTÉSE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

a 95/46/EK irányelv 25. cikkének (6) bekezdése alapján elfogadott megfelelőségi határozatok végrehajtásának első felülvizsgálatáról

{SWD(2024) 3 final}

1. AZ ELSŐ FELÜLVIZSGÁLAT – HÁTTÉR

Ez a jelentés a 95/46/EK irányelv[1] (adatvédelmi irányelv) 25. cikkének (6) bekezdése alapján elfogadott megfelelőségi határozatok első felülvizsgálatára vonatkozó bizottsági megállapításokat tartalmazza.

Ezekben a határozatokban a Bizottság megállapította, hogy az alábbi tizenegy ország vagy terület megfelelő szintű védelmet biztosít az Európai Unióból (EU)[2] továbbított személyes adatok tekintetében: Andorra[3], Argentína[4], Kanada (kereskedelmi szereplők esetében)[5], Feröer szigetek[6], Guernsey[7], Man-sziget[8], Izrael[9], Jersey[10], Új-Zéland[11], Svájc[12] és Uruguay[13]. Ennek eredményeként az EU-ból ezen országokba vagy területekre irányuló adattovábbításra további követelmények nélkül kerülhet sor.

Az (EU) 2016/679 rendelet[14] (GDPR) 2018. május 25-i hatálybalépésével az adatvédelmi irányelv alapján elfogadott megfelelőségi határozatok hatályban maradtak[15]. Ugyanakkor az általános adatvédelmi rendelet egyértelművé tette, hogy a megfelelőségi megállapítások „élő

[1]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.).

[2] Az Európai Gazdasági Térségről (EGT) szóló megállapodásba való beépítése óta a GDPR Norvégiára, Izlandra és Liechtensteinre is vonatkozik. Ebben a jelentésben az EU-ra való hivatkozásokat úgy kell értelmezni, hogy azok az EGT-államokra is vonatkoznak.

[3] A Bizottság 2010/625/EU határozata (2010. október 19.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok Andorrában biztosított megfelelő védelméről (HL L 277., 2010.10.21., 27. o.).

[4] A Bizottság 2003/490/EK határozata (2003. június 30.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok Argentínában biztosított megfelelő védelméről (HL L 168., 2003.7.5., 19. o.).

[5]A Bizottság 2002/2/EK határozata (2001. december 20.) a 95/46/EK európai parlamenti és tanácsi határozat értelmében a személyes adatoknak a személyes információk védelméről és az elektronikus dokumentumokról szóló kanadai törvény által biztosított megfelelő védelméről (HL L 2., 2002.1.4., 13. o.).

[6]A Bizottság 2010/146/EU határozata (2010. március 5.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatoknak a személyes adatok feldolgozásáról szóló Feröer szigeteki törvény által biztosított megfelelő védelméről (HL L 58., 2010.3.9., 17. o.).

[7]A Bizottság 2003/821/EK határozata (2003. november 21.) a személyes adatok Guernseyben biztosított megfelelő védelméről (HL L 308., 2003.11.25., 27. o.).

[8]A Bizottság 2004/411/EK határozata (2004. április 28.) a személyes adatok Man-szigeten biztosított megfelelő szintű védelméről (HL L 151., 2004.4.30., 48. o.).

[9]A Bizottság 2011/61/EU határozata (2011. január 31.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok Izrael Állam által biztosított megfelelő védelméről a személyes adatok automatizált feldolgozása tekintetében (HL L 27., 2011.2.1., 39. o.).

[10] A Bizottság 2008/393/EK határozata (2008. május 8.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok Jerseyn biztosított megfelelő védelméről (HL L 138., 2008.5.28., 21. o.).

[11] A Bizottság 2013/65/EU végrehajtási határozata (2012. december 19.) a személyes adatok védelmének Új-Zéland által biztosított szintje megfelelőségének a 95/46/EK európai parlamenti és tanácsi irányelv alapján történő megállapításáról (HL L 28., 2013.1.30., 12. o.).

[12] A Bizottság 2000/518/EK határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, a személyes adatok Svájcban biztosított megfelelő védelméről (HL L 215., 2000.8.25., 1. o.).

[13] A Bizottság 2012/484/EU végrehajtási határozata (2012. augusztus 21.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatoknak az Uruguayi Keleti Köztársaság által biztosított megfelelő védelméről a személyes adatok automatizált feldolgozása tekintetében (HL L 227., 2012.8.23., 11. o.).

[14] 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 rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

[15] Lásd az általános adatvédelmi rendelet 45. cikkének (9) bekezdését, amely előírja, hogy a Bizottság által a 95/46/EK irányelv 25. cikkének (6) bekezdése alapján elfogadott határozatok mindaddig hatályban maradnak, amíg azokat a 45. cikk (3) vagy (5) bekezdésével összhangban elfogadott bizottsági határozat nem módosítja, nem váltja fel vagy nem helyezi hatályon kívül.

eszközök", és előírja, hogy a Bizottságnak folyamatosan figyelemmel kell kísérnie a harmadik országokban végbement azon fejleményeket, amelyek érinthetik a meglévő megfelelőségi határozatok végrehajtását[16]. Ezenkívül az általános adatvédelmi rendelet 97. cikke előírja a Bizottság számára, hogy rendszeresen, négyévente felül kell vizsgálnia ezeket a határozatokat annak megállapítása érdekében, hogy továbbra is megfelelő szintű védelmet biztosítanak-e a személyes adatok tekintetében azok az országok és területek, amelyek esetében megfelelőségi megállapításra került sor.

A korábbi uniós adatvédelmi keret alapján elfogadott megfelelőségi határozatok első felülvizsgálatának kezdeményezésére az általános adatvédelmi rendelet alkalmazásának és végrehajtásának szélesebb körű értékelése keretében került sor, amellyel kapcsolatban a Bizottság „A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve" című közleményében ismertette megállapításait[17]. A felülvizsgálat e vonatkozását érintő következtetést azonban elhalasztották, hogy figyelembe vegyék a Bíróság Schrems II-ügyben hozott ítéletét[18], amelyben a Bíróság fontos pontosításokkal szolgált a megfelelőségi előírás kulcsfontosságú elemeivel, valamint egyéb kapcsolódó fejleményekkel kapcsolatban. Ez viszont részletes eszmecseréket eredményezett az érintett országokkal és területekkel a jogi keretük, felügyeleti mechanizmusaik és végrehajtási rendszerük releváns szempontjairól[19]. Ez a jelentés teljes mértékben figyelembe veszi ezeket a fejleményeket mind az EU-ban, mind az érintett harmadik országokban és területeken.

Fontos megjegyezni, hogy erre az első felülvizsgálatra a digitális technológiák exponenciális fejlődésével összefüggésben kerül sor. Az elmúlt évtizedekben jelentősen megnőtt a megfelelőségi határozatok jelentősége, mivel az adatáramlás immár a társadalom digitális átalakulásának és a gazdaság globalizációjának szerves része. Az adatok határokon átnyúló továbbítása minden ágazatban a különböző méretű európai vállalatok napi működésének részévé vált. A magánélet tiszteletben tartása minden eddiginél nagyobb mértékben a stabil, biztonságos és versenyképes kereskedelmi forgalom feltétele. Ebben az összefüggésben a megfelelőségi határozatok számos szempontból egyre fontosabb szerepet játszanak. Annak biztosításával, hogy a védelem az adatok továbbításával is megmaradjon, lehetővé teszik a biztonságos adatáramlást, tiszteletben tartva az egyének jogait, összhangban a digitális átalakulás emberközpontú uniós megközelítésével. Annak elismerésével, hogy a harmadik országok adatvédelmi keretrendszere az uniós védelemmel lényegében egyenértékű védelmi

[16]A GDPR 45. cikkének (4) bekezdése. Lásd még az Európai Unió Bíróságának 2015. október 6-i ítéletét a C-362/14. számú, Maximillian Schrems kontra adatvédelmi biztos ügyben (Schrems I), ECLI:EU:C:2015:650, 76. pont.

[17] A közlemény közzétételére 2020 júniusában került sor, és a következő linken érhető el: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en

[18] Az Európai Unió Bíróságának 2020. július 16-i ítélete a C-311/18. sz., adatvédelmi biztos kontra Facebook Ireland Ltd. és Maximillian Schrems ügyben (Schrems II), ECLI:EU:C:2020:559.

[19] A Japánra vonatkozó megfelelőségi határozat elfogadására az általános adatvédelmi rendelet alapján került sor, és külön időszakos felülvizsgálatot ír elő. Az első felülvizsgálat 2023 áprilisában zárult le a Japánra vonatkozó megfelelőségi határozat működésének első felülvizsgálatáról szóló, az Európai Parlamentnek és a Tanácsnak címzett bizottsági jelentéssel (COM(2023) 275 final), amely a következő linken érhető el: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=COM:2023:275:FIN

szintet biztosít, elősegítik a magas szintű védelmen alapuló adatvédelmi rendszerek konvergenciáját. Továbbá, amint azt e jelentés kifejti, a megfelelőségi határozatok ahelyett, hogy „végpontként” szolgálnának, lefektették az EU és a hasonlóan gondolkodó partnerek közötti szorosabb együttműködés és a további szabályozási konvergencia alapjait. A személyes adatok szabad áramlásának lehetővé tételével ezek a határozatok kereskedelmi csatornákat nyitottak meg az uniós gazdasági szereplők számára, többek között azáltal, hogy kiegészítették és bővítették a kereskedelmi megállapodások előnyeit, valamint megkönnyítették a külföldi partnerekkel való együttműködést számos szabályozási területen. Azáltal, hogy egyszerű és átfogó megoldást biztosítanak az adattovábbításra anélkül, hogy az adatátadónak további biztosítékokat kellene nyújtania vagy engedélyt kellene szereznie, elősegítik, hogy különösen a kis- és középvállalkozások megfeleljenek az általános adatvédelmi rendelet nemzetközi adattovábbítási követelményeinek. Végezetül, az Európai Bizottság által elfogadott megfelelőségi határozatok a „hálózati hatásuknak” köszönhetően az EU-n kívül is egyre fontosabbak, mivel nemcsak az EU 30 gazdasága számára teszik lehetővé az adatok szabad áramlását, hanem világszerte[20] sokkal több olyan joghatóság között is, amelyek saját adatvédelmi szabályaik értelmében „biztonságos célként” ismerik el azokat az országokat, amelyekre vonatkozóan uniós megfelelőségi határozat született.

Mindezen okok miatt, amint azt az érintett harmadik országokkal/területekkel folytatott, ezt a felülvizsgálatot alátámasztó intenzív és gyümölcsöző párbeszéd is megerősíti, a megfelelőségi határozatok az EU és e külföldi partnerek közötti általános kapcsolat stratégiai elemévé váltak, és számos területen elismerten jelentősen támogatják az együttműködés elmélyítését. Ezért különösen fontos, hogy ezek a határozatok kiállhassák az idő próbáját, és figyelembe vehessék az új fejleményeket és kihívásokat.

2. A FELÜLVIZSGÁLAT CÉLJA ÉS MÓDSZERTANA

Az e felülvizsgálat tárgyát képező megfelelőségi határozatok elfogadására az általános adatvédelmi rendeletet megelőző uniós adatvédelmi keret alapján került sor. Míg a legutóbbi határozatok körülbelül egy évtizedre nyúlnak vissza (például az Új-Zélandra és az Uruguayra vonatkozó, 2012-ben elfogadott határozatok), mások már több mint húsz éve hatályban vannak (például a Kanadára vonatkozó, 2001-ben, illetve a Svájcra vonatkozó, 2000-ben elfogadott határozat). Azóta mind a tizenegy országban és területen fejlődtek az adatvédelmi keretek, például a jogalkotási vagy szabályozási reformok, az adatvédelmi hatóságok jogérvényesítési gyakorlatának fejlődése vagy az ítélkezési gyakorlat révén.

A Bizottság ezért az értékelés során az érintett országok és területek adatvédelmi keretrendszerében a megfelelőségi határozat elfogadása óta bekövetkezett fejleményekre összpontosított. Értékelte, hogy ezek a fejlemények hogyan alakították tovább az adott ország vagy terület adatvédelmi rendszerét, és hogy e fejlemények fényében a különböző rendszerek továbbra is megfelelő szintű védelmet biztosítanak-e.

E célból teljes mértékben figyelembe vette az EU saját adatvédelmi rendszerének alakulását, különösen az általános adatvédelmi rendelet hatálybalépésével. Mindenekelőtt e megfelelőségi

[20] Például Argentína, Izrael, Kolumbia, Marokkó, Svájc és Uruguay.

határozatok elfogadása óta a Bíróság ítélkezési gyakorlata, valamint a 29. cikk alapján létrehozott munkacsoport és utódja, az Európai Adatvédelmi Testület[21] által elfogadott iránymutatás tovább pontosította az ilyen határozatokra alkalmazandó jogi normákat, valamint az annak értékelése szempontjából releváns elemeket, hogy egy külföldi rendszer megfelelő szintű védelmet biztosít-e.

A Bíróság a Schrems I-ügyben 2015. október 6-án hozott ítéletében megállapította, hogy bár egy harmadik ország nem kötelezhető arra, hogy az EU-ban biztosított védelmi szinttel azonos védelmi szintet biztosítson, a megfelelőségi vizsgálatot úgy kell értelmezni, hogy az „lényegében azonos" védelmi szintet követel meg[22]. A Bíróság különösen egyértelművé tette, hogy a harmadik ország által a személyes adatok védelme céljából igénybe vett eszközök különbözhetnek az Unióban alkalmazott eszközöktől, amennyiben – a gyakorlatban – ténylegesen megfelelő szintű védelmet biztosítanak[23]. A megfelelőségi vizsgálat ezért szükségessé teszi a harmadik ország teljes rendszerének átfogó értékelését, beleértve a magánélet védelmének tartalmát, valamint e védelem hatékony végrehajtását és érvényesítését.

A Bíróság továbbá egyértelművé tette, hogy a Bizottság értékelése nem korlátozódhat a harmadik ország általános adatvédelmi keretrendszerére, hanem ki kell terjednie a közigazgatási szervek személyes adatokhoz való – különösen bűnüldözési és nemzetbiztonsági célú – hozzáférésére vonatkozó szabályokra is[24]. Az Alapjogi Chartát viszonyítási alapként használva a Bíróság számos olyan követelményt azonosított, amelyeknek e szabályoknak meg kell felelniük ahhoz, hogy teljesítsék a „lényegében vett egyenértékűség" követelményét. Például az e területre vonatkozó jogszabályoknak egyértelmű és pontos szabályokat kell meghatározniuk az intézkedések hatálya és alkalmazása tekintetében, és ezeknek a szabályoknak minimális biztosítékokat kell előírniuk annak érdekében, hogy azon személyek, akiknek a személyes adatai érintettek, elegendő olyan biztosítékkal rendelkezzenek, amely lehetővé teszi az adataiknak a visszaélések veszélyeivel, valamint az ezen adatokat érintő minden jogellenes hozzáféréssel és felhasználással szembeni hatékony védelmét[25]. Lehetővé kell tenniük továbbá az egyének számára a jogorvoslati lehetőséget abból a célból, hogy a rájuk vonatkozó személyes adatokhoz hozzáférést kapjanak, vagy azokat helyesbíttessék, illetve töröltessék[26].

Az általános adatvédelmi rendelet a Bíróság által nyújtott pontosításokra építve részletes jegyzéket állított össze azokról az elemekről, amelyeket a Bizottságnak figyelembe kell vennie a megfelelőségi értékelés során[27]. Ezenkívül a Bíróság a Schrems II-ügyben 2020. július 16-án hozott ítéletében tovább részletezte a „lényegében vett egyenértékűség" előírását, különös tekintettel a közigazgatási szervek személyes adatokhoz való, bűnüldözési és nemzetbiztonsági

[21] Az Európai Adatvédelmi Testület összefogja a tagállamok adatvédelmi felügyeleti hatóságait és az európai adatvédelmi biztost.
[22] A Schrems I-ügyben hozott ítélet 73., 74. és 96. pontja. Lásd még az (EU) 2016/679 rendelet (104) preambulumbekezdését, amely hivatkozik a lényegében vett egyenértékűség követelményére.
[23] Schrems I-ügy, 74. pont.
[24] Schrems I-ügy, 90. pont.
[25] Schrems I-ügy, 91. pont.
[26] Schrems I-ügy, 95. pont.
[27] A GDPR 45. cikkének (2) bekezdése.

célú hozzáférésére vonatkozó szabályokra. Különösen azt tisztázta, hogy a „lényegében vett egyenértékűség” előírása megköveteli, hogy az érintett harmadik országok és területek közigazgatási szerveire nézve kötelező jogi keretek tartalmazzanak olyan minimális biztosítékokat, amelyek biztosítják, hogy az ilyen közigazgatási szervek ne férhessenek hozzá az adatokhoz a jogszerű célok eléréséhez szükséges és arányos mértéken túl, és az érintetteket az ilyen közigazgatási szervekkel szemben tényleges és érvényesíthető jogok illessék meg[28].

A megfelelőségi előírás alakulását a 29. cikk alapján létrehozott munkacsoport által eredetileg elfogadott, majd az Európai Adatvédelmi Testület által jóváhagyott iránymutatás is tükrözi[29]. Ez az iránymutatás és különösen az úgynevezett „megfelelőségi referencia” tovább pontosítja azokat az elemeket, amelyeket a Bizottságnak figyelembe kell vennie a megfelelőségi értékelés elvégzésekor, többek között azáltal, hogy áttekintést nyújt a közigazgatási szervek személyes adatokhoz való hozzáférésére vonatkozó „alapvető garanciákról”. Ez utóbbi különösen az Emberi Jogok Európai Bíróságának ítélkezési gyakorlatára épül, és azt az Európai Adatvédelmi Testület aktualizálta annak érdekében, hogy figyelembe vegye a Bíróság által a Schrems II-ügyben hozott ítéletben nyújtott pontosításokat[30]. Fontos megjegyezni, hogy a megfelelőségi referencia azt is elismeri, hogy a „lényegében vett egyenértékűség” előírása nem foglalja magában az uniós szabályok pontról pontra történő leképezését („lemásolását”), mivel a hasonló szintű védelem biztosításának eszközei eltérőek lehetnek a különböző adatvédelmi rendszerek esetében, és gyakran eltérő jogi hagyományokat tükröznek.

Ezért annak megállapításához, hogy a korábbi szabályok alapján elfogadott tizenegy megfelelőségi határozat továbbra is megfelel-e az általános adatvédelmi rendeletben meghatározott előírásnak, a Bizottság nemcsak az adott országokban és területeken alkalmazott adatvédelmi keretek alakulását vette figyelembe, hanem magának a megfelelőségi előírásnak az uniós jog szerinti értelmezése szerinti alakulását is. Ez magában foglalja az EU-ból továbbított személyes adatokhoz való, azon országok vagy területek közigazgatási szervei általi hozzáférést és az ezen adatok felhasználását szabályozó jogi keret értékelését is, amelyekről megállapítást nyert, hogy az adatvédelmi irányelv 25. cikkének (6) bekezdése alapján megfelelő szintű védelmet biztosítanak.

3. A FELÜLVIZSGÁLATI FOLYAMAT

A fentiekben leírtak szerint a meglévő megfelelőségi határozatok értékelése minden egyes érintett ország vagy terület tekintetében kiterjed az adatvédelmi keretre és az e jogi kerettel kapcsolatban a megfelelőségi megállapítás elfogadása óta bekövetkezett fejleményekre, továbbá az adatokhoz – különösen bűnüldözési és nemzetbiztonsági célokból – való kormányzati hozzáférésre vonatkozó szabályokra. Az elmúlt években a Bizottság szolgálatai

[28] Schrems II-ügy, 180–182. pont.
[29] Megfelelőségi referencia, WP 254 rev. 01., 2018. február 6. (elérhető a következő internetcímen: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).
[30] A megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról szóló 02/2020. számú ajánlás (elérhető a következő internetcímen: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_hu).

számos lépést tettek az értékelés elvégzése érdekében, szorosan együttműködve az egyes érintett országokkal és területekkel.

A Bizottság nyomonkövetési kötelezettségeinek támogatása érdekében a tizenegy ország vagy terület mindegyike átfogó tájékoztatást nyújtott a Bizottságnak az adatvédelmi rendszerében a megfelelőségi határozat elfogadása óta bekövetkezett fejleményekről. Emellett a Bizottság mind a tizenegy országtól vagy területtől részletes tájékoztatást kért a személyes adatokhoz – különösen bűnüldözési és nemzetbiztonsági célokból – való kormányzati hozzáférésre vonatkozó szabályokról, amelyek az adott országban vagy területen alkalmazandók. A Bizottság emellett információkat kért nyilvános forrásokból, felügyeleti és végrehajtó hatóságoktól, valamint helyi szakértőktől a határozatok végrehajtásáról, valamint az egyes érintett országok és területek jogszabályaiban és gyakorlatában bekövetkezett releváns fejleményekről, mind a magánszereplőkre alkalmazandó adatvédelmi szabályok, mind a kormányzati hozzáférés tekintetében. Végezetül adott esetben kellően figyelembe vette az ezen országok/területek által a regionális vagy egyetemes eszközök keretében vállalt nemzetközi kötelezettségvállalásokat.

Ennek alapján a Bizottság intenzív párbeszédet folytatott az érintett országokkal és területekkel. E párbeszéd keretében számos említett ország és terület korszerűsítette és megerősítette adatvédelmi jogszabályait átfogó vagy részleges reformok révén (például Andorra, Kanada, Feröer szigetek, Svájc, Új-Zéland), amit többek között a megfelelőségi határozatok folytonosságának biztosítása is szükségessé tesz. Egyes ilyen országok a végrehajtási gyakorlat vagy az ítélkezési gyakorlat alapján új adatvédelmi követelmények bevezetésére (például Izrael és Uruguay) vagy bizonyos adatvédelmi szabályok pontosítására (például Argentína, Kanada, Guernsey, Jersey, Man-sziget, Izrael, Új-Zéland) vonatkozó rendeleteket és/vagy az adatvédelmi hatóságuk által kiadott iránymutatásokat fogadtak el. Ezen túlmenően a védelem szintje közötti lényeges különbségek kezelése érdekében néhány érintett országgal és területtel az Európából továbbított személyes adatokra vonatkozóan további biztosítékokról tárgyaltak és állapodtak meg, amennyiben ez szükséges volt a megfelelőségi határozat folytonosságának biztosításához. Például a kanadai kormány a közszféra által kezelt személyes adatokhoz való hozzáférés és helyesbítés jogát állampolgárságuktól vagy lakóhelyüktől függetlenül valamennyi egyénre kiterjesztette (mivel ezek a jogok korábban csak kanadai állampolgárokra, állandó lakosokra vagy Kanadában tartózkodó személyekre vonatkoztak)[31]. Az izraeli kormány például olyan konkrét biztosítékokat vezetett be az Európai Gazdasági Térségből továbbított személyes adatok védelmének megerősítése érdekében, amelyek új kötelezettségeket teremtenek az adatok pontossága és az adatmegőrzés terén, megerősítik a tájékoztatáshoz és a törléshez való jogot, illetve a különleges adatok további kategóriáit vezetik be[32].

Ezzel párhuzamosan a Bizottság szolgálatai összegyűjtötték az Európai Parlament (az Állampolgári Jogi, Bel- és Igazságügyi Bizottság)[33], a Tanács (az adatvédelmi munkacsoporton

[31] Az adatvédelmi törvény 12. szakasza, az adatvédelmi törvény hatályának kiterjesztéséről szóló 1. és 2. rendelet.
[32] A magánélet védelméről szóló rendeletek (az Európai Gazdasági Térségből Izraelnek továbbított adatokra vonatkozó utasítások), 5783-2023, közzétéve az izraeli Hivatalos Közlönyben (*Reshumut*), 2023. május 7-én.
[33] Lásd például az Európai Parlament 2021. március 25-i állásfoglalását: Az általános adatvédelmi rendelet végrehajtásáról szóló bizottsági értékelő jelentés – a rendelet alkalmazásának két éve, (2020/2717(RSP), amely a következő linken érhető el: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_HU.html

keresztül)[34], az Európai Adatvédelmi Testület[35] és az általános adatvédelmi rendelettel foglalkozó, több érdekelt felet tömörítő (a civil társadalom, az ipar, a tudományos élet és a jogi szakemberek képviselőiből álló) szakértői csoport[36] véleményét, és rendszeresen tájékoztatták őket az értékelés előrehaladásáról.

Ez a jelentés és a kísérő bizottsági szolgálati munkadokumentum ezért az egyes érintett országokkal és területekkel folytatott szoros együttműködés, valamint az érintett uniós intézményekkel és szervekkel folytatott konzultáció és az ezektől kapott visszajelzések eredménye. Számos forrásra támaszkodik, ideértve a jogszabályokat, a rendeleti jellegű jogi aktusokat, az ítélkezési gyakorlatot, az adatvédelmi hatóságok határozatait és iránymutatásait, a (független) felügyeleti szervek jelentéseit és az érdekelt felek észrevételeit. E jelentés elfogadását megelőzően valamennyi fent említett ország és terület lehetőséget kapott arra, hogy ellenőrizze a bizottsági szolgálati munkadokumentumban a rendszerére vonatkozóan megadott információk tényszerű pontosságát.

4. FŐ MEGÁLLAPÍTÁSOK ÉS KÖVETKEZTETÉSEK

Az első felülvizsgálat kimutatta, hogy a megfelelőségi határozatok elfogadása óta az érintett tizenegy országban vagy területen érvényben lévő adatvédelmi keretek tovább közeledtek az uniós kerethez. Ezen túlmenően a személyes adatokhoz való kormányzati hozzáféréssel kapcsolatban az első felülvizsgálat rámutatott arra, hogy ezen országok vagy területek joga megfelelő biztosítékokat és korlátozásokat ír elő, valamint felügyeleti és jogorvoslati mechanizmusokat biztosít ezen a téren.

A tizenegy országra és területre vonatkozó részletes megállapításokat az e jelentést kísérő bizottsági szolgálati munkadokumentum ismerteti. E megállapítások alapján a Bizottság arra a következtetésre jutott, hogy a tizenegy ország és terület mindegyike továbbra is megfelelő szintű védelmet biztosít az Európai Unióból továbbított személyes adatok tekintetében az általános adatvédelmi rendelet értelmében, a Bíróság értelmezésének megfelelően. Az egyes megfelelőnek minősített országokra és területekre vonatkozó megállapításokat az alábbiakban foglaljuk össze.

4.1. Andorra

A Bizottság üdvözli az andorrai jogi keretben a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve a jogszabályi módosításokat és a felügyeleti szervek tevékenységét. Mindenekelőtt a 2022 májusában hatályba lépett, a személyes adatok védelméről szóló, 29/2021. számú minősített törvény elfogadása hozzájárult az adatvédelem

[34] Lásd például az általános adatvédelmi rendelet (GDPR) alkalmazásával kapcsolatos, 2019. december 19-én elfogadott tanácsi álláspontot és megállapításokat, amelyek a következő linken érhetők el: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/hu/pdf

[35] Lásd például az Európai Adatvédelmi Testület hozzájárulását az általános adatvédelmi rendelet 97. cikk szerinti értékeléséhez, amelyet 2020. február 18-án fogadtak el, és a következő linken érhető el: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf

[36] Lásd például a több érdekelt felet tömörítő szakértői csoportnak az általános adatvédelmi rendelet értékeléséről szóló jelentését, amely a következő linken érhető el: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=hu&do=groupDetail.groupMeeting&meetingId=21356

magasabb szintjéhez, mivel a törvény a szerkezetét és főbb elemeit tekintve szorosan összhangban van az általános adatvédelmi rendelettel.

A személyes adatokhoz való kormányzati hozzáférés tekintetében Andorra közigazgatási szerveire egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó jogi keretből és a nemzetközi kötelezettségvállalásokból, nevezetesen az andorrai alkotmányból, az emberi jogok európai egyezményéből (EJEE) és az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményéből (108. sz. egyezmény és az azt módosító, a korszerűsített 108+ egyezményt létrehozó jegyzőkönyv), valamint a személyes adatoknak a bűnüldözéssel összefüggésben történő kezelésére vonatkozó egyedi adatvédelmi szabályokból következnek, amelyek lényegében az (EU) 2016/680 irányelv[37] alapvető elemeit tükrözik. Az andorrai jog emellett számos konkrét feltételt és korlátozást ír elő a személyes adatokhoz való, a közigazgatási szervek által hozzáférésre és az ilyen adatok felhasználására vonatkozóan, illetve felügyeleti és jogorvoslati mechanizmusokat biztosít e téren.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Andorra továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében.

A bűnüldöző hatóságok általi adatkezelésre jelenleg alkalmazandó konkrét adatvédelmi szabályok tekintetében a Bizottság üdvözli az andorrai jogalkotó azon szándékát, hogy ezeket a szabályokat olyan átfogóbb rendszerrel váltsa fel, amely még inkább igazodni fog az EU-ban alkalmazandó szabályokhoz. A Bizottság szoros figyelemmel fogja kísérni a jövőbeli fejleményeket ezen a területen.

4.2. Argentína

A Bizottság üdvözli az argentin jogi keretben a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve a jogszabályi módosításokat, az ítélkezési gyakorlatot és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. Mindenekelőtt, a 746/17. sz. rendelet jelentősen megerősítette az argentin adatvédelmi felügyeleti hatóság függetlenségét, és az adatvédelmi jogszabályoknak való megfelelőség felügyeletével az *Agencia de Acceso a la Información Públicát* (AAIP) bízta meg. Az AAIP ezenkívül számos kötelező erejű rendeletet és véleményt adott ki, amelyben pontosítja, hogyan kell értelmezni és a gyakorlatban alkalmazni az adatvédelmi keretet, ezáltal segítve az adatvédelmi jog naprakészen tartását. Argentína megerősítette továbbá az adatvédelem terén tett nemzetközi kötelezettségvállalásait azáltal, hogy 2019-ben csatlakozott az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményéhez és annak kiegészítő jegyzőkönyvéhez, valamint 2023-ban megerősítette a

[37] 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.

személyes adatok gépi feldolgozása során az egyének védelméről szóló korszerűsített egyezményt létrehozó módosító jegyzőkönyvet.

A személyes adatokhoz való kormányzati hozzáférés terén Argentína közigazgatási szerveire egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó jogi keretből és a nemzetközi kötelezettségvállalásokból, nevezetesen az argentin alkotmányból, az Emberi Jogok Amerikai Egyezményéből, a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményből és a személyes adatok gépi feldolgozása során az egyének védelméről szóló korszerűsített egyezményből, valamint az argentin adatvédelmi szabályokból (a személyes adatok védelméről szóló, 2000. október 4-i 25.326. sz. törvény) következnek, amelyek a személyes adatoknak az argentin közigazgatási szervek általi, többek között bűnüldözési és nemzetbiztonsági célú kezelésére is alkalmazandók. Az argentin jog emellett számos konkrét feltételt és korlátozást ír elő a személyes adatokhoz való bűnüldözési és nemzetbiztonsági célú hozzáférésre és az ilyen adatok felhasználására vonatkozóan, illetve felügyeleti és jogorvoslati mechanizmusokat biztosít e téren.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Argentína továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében.

A Bizottság ugyanakkor azt ajánlja, hogy a jogbiztonság növelése és e követelmények megszilárdítása érdekében foglalják bele a jogszabályokba a nem jogalkotási szinten kidolgozott védelmeket. Az argentin kongresszusban nemrégiben előterjesztett adatvédelmi törvénytervezet lehetőséget kínálhat az ilyen fejlemények kodifikálására, és ezáltal az argentin adatvédelmi keret további megerősítésére. A Bizottság szoros figyelemmel fogja kísérni a jövőbeli fejleményeket ezen a területen.

4.3. Kanada

A Bizottság üdvözli a kanadai jogi keretben a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve számos jogszabály módosítását, az ítélkezési gyakorlatot és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. A személyes információk védelméről és az elektronikus dokumentumokról szóló törvényt (PIPEDA) tovább erősítették különböző módosítások révén (például az érvényes hozzájárulás feltételei és az adatvédelmi incidensekről szóló értesítések tekintetében), míg a legfontosabb adatvédelmi követelményeket (például az érzékeny adatok kezelésére vonatkozóan) tovább pontosította az ítélkezési gyakorlat, valamint a kanadai szövetségi adatvédelmi hatóság, az adatvédelmi biztos hivatala által kiadott iránymutatás. A Bizottság ugyanakkor azt ajánlja, hogy a jogbiztonság növelése és e követelmények megszilárdítása érdekében foglalják bele a jogszabályokba a nem jogalkotási szinten kidolgozott védelmek egy részét. A PIPEDA folyamatban lévő jogalkotási reformja lehetőséget kínálhat az ilyen fejlemények kodifikálására, és ezáltal a kanadai adatvédelmi keret további

megerősítésére. A Bizottság szoros figyelemmel fogja kísérni a jövőbeli fejleményeket ezen a területen.

A személyes adatokhoz való kormányzati hozzáférés terén a kanadai közigazgatási szervekre egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó alkotmányos keretből (a Jogok és Szabadságok Kanadai Chartája), az ítélkezési gyakorlatból, az adatokhoz való hozzáférést szabályozó különös jogszabályokból, valamint az adatvédelmi szabályokból (azaz az adatvédelmi törvényből és a hasonló, tartományi szintű jogszabályokból) következnek, amelyek a személyes adatoknak a kanadai közigazgatási szervek általi kezelésére is vonatkoznak, többek között bűnüldözési és nemzetbiztonsági célokból. A kanadai jogrendszer emellett hatékony felügyeleti és jogorvoslati mechanizmusokat biztosít e téren, többek között azáltal, hogy a közelmúltban kiterjesztette az érintettek jogait és jogorvoslati lehetőségeit a nem kanadai állampolgárokra vagy lakosokra.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Kanada továbbra is megfelelő szintű védelmet biztosít az EU-ból a PIPEDA hatálya alá tartozó adatátvevőknek továbbított személyes adatok tekintetében. A fentieknek megfelelően a PIPEDA jelenleg olyan jogalkotási reform tárgyát képezi, amely tovább erősítheti a magánélet védelmét, többek között a megfelelőség megállapítása szempontjából releváns területeken.

4.4. Feröer szigetek

A Bizottság üdvözli a Feröer szigetek jogi keretében a megfelelőségi határozat elfogadása óta bekövetkezett változásokat, beleértve a jogszabályi módosításokat, az ítélkezési gyakorlatot és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. A Feröer szigetek jelentősen korszerűsítette adatvédelmi keretét, amikor elfogadta a 2021-ben hatályba lépett adatvédelmi törvényt, és szorosan összehangolta a Feröer szigeteki rendszert az általános adatvédelmi rendelettel.

A személyes adatokhoz való kormányzati hozzáférés terén a Feröer szigeteki közigazgatási szervekre egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó jogi keretből és a nemzetközi kötelezettségvállalásokból, nevezetesen az alkotmányos keretből és az EJEE-ből, valamint az adatokhoz való kormányzati hozzáférést szabályozó különös jogszabályokból és a személyes adatoknak a bűnüldözéssel összefüggésben történő kezelésére vonatkozó adatvédelmi szabályokból (a személyes adatoknak a bűnüldöző hatóságok általi kezeléséről szóló törvényből, amely 2022-ben lépett hatályba a Feröer szigeteken, és a Dánia által az (EU) 2016/680 irányelvnek a Feröer-szigeteken történő végrehajtása céljából elfogadott jogszabályokat ülteti át), valamint a (Biztonsági és Hírszerző Szolgálatról szóló törvényben szereplő) nemzetbiztonsági célokból következnek. Ezen túlmenően hatékony felügyeleti és jogorvoslati mechanizmusok állnak rendelkezésre e téren.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Feröer szigetek továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében.

4.5. Guernsey

A Bizottság üdvözli a Guernsey jogi keretében a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve a jogszabályi módosításokat és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. Guernsey jelentősen korszerűsítette adatvédelmi keretét, amikor elfogadta a 2019 óta alkalmazandó és a guernsey-i rendszert az általános adatvédelmi rendelettel szorosan összehangoló 2017. évi adatvédelmi törvényt (Guernsey Bailiffség).

A személyes adatokhoz való kormányzati hozzáférés terén a guernsey-i közigazgatási szervekre egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó jogi keretből és a nemzetközi kötelezettségvállalásokból, nevezetesen az EJEE-ből és a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményből, valamint a guernsey-i adatvédelmi szabályokból következnek, beleértve a személyes adatoknak a bűnüldözés összefüggésében történő kezelésére vonatkozó különös rendelkezéseket, amelyeket a 2018. évi adatvédelmi (bűnüldözési és kapcsolódó ügyek) (Guernsey Bailiffség) rendelet határoz meg. Guernsey joga emellett számos konkrét feltételt és korlátozást ír elő a személyes adatokhoz való bűnüldözési és nemzetbiztonsági célú hozzáférésre és az ilyen adatok felhasználására vonatkozóan, illetve felügyeleti és jogorvoslati mechanizmusokat biztosít e téren.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Guernsey továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében.

4.6. Man-sziget

A Bizottság üdvözli a Man-sziget jogi keretében a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve a jogszabályi módosításokat és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. A Man-sziget 2018-ban új jogszabályt fogadott el (a 2018. évi adatvédelmi törvényt, amelyet az adatvédelemről [az általános adatvédelmi rendelet alkalmazásáról] szóló, 2018. évi rendelet egészít ki), amely az uniós adatvédelmi keret legtöbb rendelkezését beépíti a Man-sziget jogrendjébe, miközben csak kisebb kiigazításokat hajtott végre bizonyos szempontok tekintetében, különösen a keret helyi viszonyokhoz igazítása érdekében.

A személyes adatokhoz való kormányzati hozzáférés terén a Man-szigeti közigazgatási szervekre egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a

korlátozások és biztosítékok az átfogó jogi keretből és a nemzetközi kötelezettségvállalásokból, nevezetesen az EJEE-ből és a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményből, valamint a Man-sziget adatvédelmi szabályaiból következnek, beleértve a személyes adatoknak a bűnüldözés összefüggésében történő kezelésére vonatkozó, az adatvédelemről (a bűnüldözési irányelv alkalmazásáról) szóló 2018. évi rendeletben és a bűnüldözési irányelvet végrehajtó, 2018. évi végrehajtási rendeletekben meghatározott különös rendelkezéseket. A Man-sziget joga emellett számos konkrét korlátozást ír elő a személyes adatokhoz való bűnüldözési és nemzetbiztonsági célú hozzáférésre és az ilyen adatok felhasználására vonatkozóan, illetve felügyeleti és jogorvoslati mechanizmusokat biztosít e téren.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Man-sziget továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében.

4.7. Izrael

A Bizottság üdvözli az izraeli jogi keretben a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve a jogszabályi módosításokat, az ítélkezési gyakorlatot és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. Izrael konkrét biztosítékokat vezetett be az Európai Gazdasági Térségből továbbított személyes adatok védelmének megerősítése érdekében az 5783-2023. számú, a magánélet védelméről szóló rendelet (Az Európai Gazdasági Térségből Izraelnek továbbított adatokra vonatkozó utasítások) elfogadásával. Izrael megerősítette továbbá az adatbiztonsági követelményeket, amikor elfogadta az 5777-2017. számú, a magánélet védelméről szóló (adatbiztonsági) rendeletet, és kötelező erejű kormányhatározatban megerősítette adatvédelmi felügyeleti hatósága függetlenségét.

A személyes adatokhoz való kormányzati hozzáférés terén az izraeli közigazgatási szervekre egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó jogi keretből, nevezetesen az izraeli alaptörvényből, valamint a magánélet védelméről szóló, 5741-1981. számú törvényből és az annak alapján elfogadott rendeletekből következnek, amelyek a személyes adatok izraeli közigazgatási szervek általi, többek között bűnüldözési és nemzetbiztonsági célú kezelésére vonatkoznak. Az izraeli jog emellett számos konkrét korlátozást ír elő a személyes adatokhoz való bűnüldözési és nemzetbiztonsági célú hozzáférésre és az ilyen adatok felhasználására vonatkozóan, illetve felügyeleti és jogorvoslati mechanizmusokat biztosít e téren.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Izrael továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében.

A Bizottság ugyanakkor azt ajánlja, hogy a jogbiztonság fokozása és e követelmények megszilárdítása érdekében foglalják bele a jogszabályokba a nem jogalkotási szinten és az

ítélkezési gyakorlat révén kidolgozott védelmet. A nemrégiben az izraeli parlament elé terjesztett, a magánélet védelméről szóló, 5722-2022. számú törvényjavaslat (14. módosítás) fontos lehetőséget kínál az ilyen fejlemények megszilárdítására és kodifikálására, és ezáltal a magánélet védelmére vonatkozó izraeli keret további megerősítésére. A Bizottság szoros figyelemmel fogja kísérni a jövőbeli fejleményeket ezen a területen.

4.8. Jersey

A Bizottság üdvözli a Jersey jogi keretében a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve a jogszabályi módosításokat, az ítélkezési gyakorlatot és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. Jersey jelentősen korszerűsítette adatvédelmi keretét, amikor elfogadta a 2018. évi adatvédelmi (Jersey) törvényt és az adatvédelmi hatóságról (Jersey) szóló 2018. évi törvényt, amely 2018-ban lépett hatályba, és szorosan hozzáigazítja a jersey-i rendszert az általános adatvédelmi rendelethez.

A személyes adatokhoz való kormányzati hozzáférés terén a jersey-i közigazgatási szervekre egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó jogi keretből és a nemzetközi kötelezettségvállalásokból, nevezetesen az EJEE-ből és a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményből, valamint a jersey-i adatvédelmi szabályokból következnek, beleértve a személyes adatoknak a bűnüldözés összefüggésében történő kezelésére vonatkozó, a 2018. évi adatvédelmi törvényben (Jersey) meghatározott, az említett törvény 1. függelékével módosított különös rendelkezéseket. A jersey-i jog emellett számos konkrét korlátozást ír elő a személyes adatokhoz való bűnüldözési és nemzetbiztonsági célú hozzáférésre és az ilyen adatok felhasználására vonatkozóan, illetve felügyeleti és jogorvoslati mechanizmusokat biztosít e téren.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Jersey továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében.

4.9. Új-Zéland

A Bizottság üdvözli az új-zélandi jogi keretben a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve a jogszabályi módosításokat, az ítélkezési gyakorlatot és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. Az adatvédelmi rendszer átfogó reformon ment keresztül a magánélet védelméről szóló, 2020. évi törvény elfogadásával, amely tovább fokozta az uniós adatvédelmi kerettel való konvergenciát, különös tekintettel a személyes adatok nemzetközi továbbítására vonatkozó szabályokra és az adatvédelmi hatóság (az adatvédelmi biztos hivatala) hatásköreire.

A személyes adatokhoz való kormányzati hozzáférés terén az új-zélandi közigazgatási szervekre egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen

szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó alkotmányos keretből (például az alapvető polgári jogokról szóló törvényből [Bill of Rights Act]) és az ítélkezési gyakorlatból, továbbá az adatokhoz való kormányzati hozzáférést szabályozó konkrét jogszabályokból, valamint a magánélet védelméről szóló törvény azon rendelkezéseiből következnek, amelyek a személyes adatoknak a bűnüldöző hatóságok és a nemzetbiztonsági hatóságok általi kezelésére is vonatkoznak. Az új-zélandi jogrendszer emellett különböző felügyeleti és jogorvoslati mechanizmusokat ír elő e téren.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Új-Zéland továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében. A Bizottság üdvözli továbbá az új-zélandi kormány által nemrégiben a parlament elé terjesztett, a magánélet védelméről szóló, 2020. évi törvénynek a meglévő átláthatósági követelmények további megerősítése érdekében történő módosításáról szóló törvényjavaslatot. A Bizottság szoros figyelemmel fogja kísérni a jövőbeli fejleményeket ezen a területen.

4.10. Svájc

A Bizottság üdvözli a svájci jogi keretben a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve a jogszabályi módosításokat, az ítélkezési gyakorlatot és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. Idetartozik különösen a korszerűsített szövetségi adatvédelmi törvény, amely tovább fokozta az uniós adatvédelmi kerettel való konvergenciát, különösen az érzékeny adatok védelme és a nemzetközi adattovábbításra vonatkozó szabályok tekintetében. Svájc emellett megerősítette az adatvédelem terén tett nemzetközi kötelezettségvállalásait, amikor 2023 szeptemberében megerősítette a személyes adatok gépi feldolgozása során az egyének védelméről szóló korszerűsített egyezményt.

A személyes adatokhoz való kormányzati hozzáférés terén a svájci közigazgatási szervekre egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó jogi keretből és a nemzetközi kötelezettségvállalásokból, nevezetesen a svájci szövetségi alkotmányból, az EJEE-ből és a személyes adatok gépi feldolgozása során az egyének védelméről szóló korszerűsített egyezményből, valamint a svájci adatvédelmi szabályokból, többek között az adatvédelemről szóló szövetségi törvényből, valamint a bűnüldöző, illetve a nemzetbiztonsági hatóságokra vonatkozó konkrét adatvédelmi szabályokból (például a büntetőeljárási törvényből, illetve a hírszerző szolgálatokról szóló törvényből) következnek. A svájci jog emellett számos konkrét korlátozást ír elő a személyes adatokhoz való bűnüldözési és nemzetbiztonsági célú hozzáférésre és az ilyen adatok felhasználására vonatkozóan, illetve felügyeleti és jogorvoslati mechanizmusokat biztosít e téren.

A bizottsági szolgálati munkadokumentumban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Svájc továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében.

4.11. Uruguay

A Bizottság üdvözli az uruguayi jogi keretben a megfelelőségi határozat elfogadása óta bekövetkezett fejleményeket, beleértve számos jogszabályi módosítást, az ítélkezési gyakorlatot és a felügyeleti szervek tevékenységeit, amelyek hozzájárultak az adatvédelem magasabb szintjéhez. Uruguay 2018-ban és 2020-ban jogszabályi módosítás révén korszerűsítette és megerősítette a személyes adatok védelméről szóló, 18.331. sz. törvényt és a 2008. évi „Habeas Data" intézkedést, és ezzel kibővítette az adatvédelmi jogszabályok területi hatályát, új elszámoltathatósági követelményeket vezetett be (például hatásvizsgálatok, beépített és alapértelmezett adatvédelem, adatvédelmi incidensek bejelentése és adatvédelmi tisztviselők kinevezése), valamint további védelmet vezetett be a biometrikus adatok tekintetében. Uruguay emellett megerősítette az adatvédelem terén tett nemzetközi kötelezettségvállalásait azáltal, hogy 2019-ben csatlakozott a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményhez, 2021-ben pedig megerősítette a személyes adatok gépi feldolgozása során az egyének védelméről szóló korszerűsített egyezményt.

A személyes adatokhoz való kormányzati hozzáférés terén az uruguayi közigazgatási szervekre egyértelmű, pontos és hozzáférhető szabályok vonatkoznak, amelyek alapján az ilyen szervek közérdekű célokból, különösen bűnüldözési és nemzetbiztonsági célokból hozzáférhetnek az EU-ból továbbított adatokhoz, és ezt követően felhasználhatják őket. Ezek a korlátozások és biztosítékok az átfogó jogi keretből és a nemzetközi kötelezettségvállalásokból, nevezetesen az uruguayi alkotmányból, az Emberi Jogok Amerikai Egyezményéből, a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményből és a személyes adatok gépi feldolgozása során az egyének védelméről szóló korszerűsített egyezményből, valamint a személyes adatok védelméről szóló, 18.331. sz. törvényben foglalt adatvédelmi szabályokból és a „Habeas Data" intézkedésből következnek, amelyek a személyes adatoknak az uruguayi közigazgatási szervek általi, bűnüldözési és nemzetbiztonsági célú kezelésére alkalmazandók. Az uruguayi jog emellett számos konkrét feltételt és korlátozást ír elő a közigazgatási szervek által a személyes adatokhoz való hozzáférésre és azok felhasználására vonatkozóan, illetve felügyeleti és jogorvoslati mechanizmusokat biztosít e téren.

Az ebben az első felülvizsgálatban foglalt általános megállapítások alapján a Bizottság arra a következtetésre jutott, hogy Uruguay továbbra is megfelelő szintű védelmet biztosít az EU-ból továbbított személyes adatok tekintetében.

5. JÖVŐBELI NYOMON KÖVETÉS ÉS EGYÜTTMŰKÖDÉS

A Bizottság elismeri és nagyra értékeli az egyes érintett országok és területek illetékes hatóságaival e felülvizsgálat során folytatott kiváló együttműködést. A Bizottság továbbra is szoros figyelemmel fogja kísérni az érintett országok és területek védelmi keretének és tényleges gyakorlatának alakulását. Abban az esetben, ha egy megfelelőnek minősített

országban vagy területen olyan fejlemények következnek be, amelyek hátrányosan befolyásolnák a megfelelőnek ítélt adatvédelmi szintet, a Bizottság szükség esetén élni fog az általános adatvédelmi rendelet 45. cikkének (5) bekezdése szerinti hatáskörével a megfelelőségi határozat felfüggesztése, módosítása vagy visszavonása tekintetében.

Ez a felülvizsgálat megerősíti, hogy a megfelelőségi határozat elfogadása nem „végpont”, hanem lehetőséget kínál a hasonlóan gondolkodó nemzetközi partnerekkel az adatáramlásról és általában a digitális kérdésekről folytatott párbeszéd és együttműködés további fokozására. E tekintetben a Bizottság várakozással tekint az illetékes hatóságokkal folytatandó jövőbeli eszmecserék elé a biztonságos és szabad adatáramlás előmozdítása terén folytatott nemzetközi szintű együttműködés további fokozása érdekében, többek között megerősített végrehajtási együttműködés révén. E párbeszéd fokozása, valamint az információ- és tapasztalatcsere előmozdítása érdekében a Bizottság 2024-ben magas szintű találkozót kíván szervezni, amelyen az EU és a megfelelőségi határozat által érintett országok képviselői vesznek részt.