A BÍRÓSÁG ÍTÉLETE (nagytanács)

2020. július 16.*

„Előzetes döntéshozatal – A természetes személyek védelme a személyes adatok kezelése vonatkozásában – Az Európai Unió Alapjogi Chartája – 7., 8. és 47. cikk – (EU) 2016/679 rendelet – A 2. cikk (2) bekezdése – Hatály – Személyes adatok kereskedelmi célú továbbítása harmadik országokba – 45. cikk – A Bizottság megfelelőségi határozata – 46. cikk – Megfelelő garanciák alapján történő adattovábbítások – 58. cikk – A felügyeleti hatóságok jogkörei – A továbbított adatoknak valamely harmadik ország hatóságai által nemzetbiztonsági célból történő kezelése – A harmadik országban biztosított védelmi szint megfelelőségének értékelése – 2010/87/EU határozat – Személyes adatok harmadik országokba történő továbbítására vonatkozó általános adatvédelmi kikötések – Az adatkezelő által nyújtott megfelelő garanciák – Érvényesség – (EU) 2016/1250 végrehajtási határozat – Az Európai Unió–Egyesült Államok adatvédelmi pajzs által biztosított védelem megfelelősége – Érvényesség – Olyan természetes személy panasza, akinek az adatait az Európai Unióból az Egyesült Államokba továbbították”

A C-311/18. sz. ügyben,

az EUMSZ 267. cikk alapján benyújtott előzetes döntéshozatal iránti kérelem tárgyában, amelyet a High Court (felsőbíróság, Írország) a Bírósághoz 2018. május 9-én érkezett, 2018. május 4-i határozatával terjesztett elő

a **Data Protection Commissioner**

és

a **Facebook Ireland Ltd**,

Maximillian Schrems

között,

The United States of America,

az **Electronic Privacy Information Centre**,

a **BSA Business Software Alliance Inc.**,

a **Digitaleurope**

részvételével folyamatban lévő eljárásban,

* Az eljárás nyelve: angol.

A BÍRÓSÁG (nagytanács),

tagjai: K. Lenaerts elnök, R. Silva de Lapuerta elnökhelyettes, A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P. G. Xuereb, L. S. Rossi és I. Jarukaitis, tanácselnökök, M. Ilešič, T. von Danwitz (előadó) és D. Šváby bírák,

főtanácsnok: H. Saugmandsgaard Øe,

hivatalvezető: C. Strömholm tanácsos,

tekintettel az írásbeli szakaszra és a 2019. július 9-i tárgyalásra,

figyelembe véve a következők által előterjesztett észrevételeket:

– a Data Protection Commissioner képviseletében D. Young solicitor, B. Murray és M. Collins SC, valamint C. Donnelly BL,

– a Facebook Ireland Ltd képviseletében P. Gallagher és N. Hyland SC, A. Mulligan és F. Kieran BL, valamint P. Nolan, C. Monaghan, C. O'Neill és R. Woulfe solicitors,

– M. Schrems képviseletében H. Hofmann Rechtsanwalt, E. McCullough, J. Doherty és S. O'Sullivan SC, valamint G. Rudden solicitor,

– The United States of America képviseletében E. Barrington SC, S. Kingston BL, S. Barton és B. Walsh solicitors,

– az Electronic Privacy Information Centre képviseletében S. Lucey solicitor, G. Gilmore és A. Butler BL, valamint C. O'Dwyer SC,

– a BSA Business Software Alliance Inc. képviseletében B. Van Vooren és K. Van Quathem advocaten,

– a Digitaleurope képviseletében N. Cahill barrister, J. Cahir solicitor és M. Cush SC,

– Írország képviseletében A. Joyce és M. Browne, meghatalmazotti minőségben, segítőjük: D. Fennelly BL,

– a belga kormány képviseletében J.-C. Halleux és P. Cottin, meghatalmazotti minőségben,

– a cseh kormány képviseletében M. Smolek, J. Vláčil, O. Serdula és A. Kasalická, meghatalmazotti minőségben,

– a német kormány képviseletében J. Möller, D. Klebs és T. Henze, meghatalmazotti minőségben,

– a francia kormány képviseletében A.-L. Desjonquères, meghatalmazotti minőségben,

– a holland kormány képviseletében C. S. Schillemans, M. K. Bulterman és M. Noort, meghatalmazotti minőségben,

– az osztrák kormány képviseletében J. Schmoll és G. Kunnert, meghatalmazotti minőségben,

– a lengyel kormány képviseletében B. Majczyna, meghatalmazotti minőségben,

– a portugál kormány képviseletében L. Inez Fernandes, A. Pimenta és C. Vieira Guerra, meghatalmazotti minőségben,

– az Egyesült Királyság kormánya képviseletében S. Brandon, meghatalmazotti minőségben, segítői: J. Holmes QC és M. C. Knight barrister,

– az Európai Parlament képviseletében M. J. Martínez Iglesias és A. Caiola, meghatalmazotti minőségben,

– az Európai Bizottság képviseletében D. Nardi, H. Krämer és H. Kranenborg, meghatalmazotti minőségben,

– az Európai Adatvédelmi Testület (EDPB) képviseletében A. Jelinek és K. Behn, meghatalmazotti minőségben,

a főtanácsnok indítványának a 2019. december 19-i tárgyaláson történt meghallgatását követően,

meghozta a következő

Ítéletet

1 Az előzetes döntéshozatal iránti kérelem lényegében

– a személyes adatok feldolgozása [helyesen: kezelése] vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv (HL 1995. L 281., 31. o.; magyar nyelvű különkiadás 13. fejezet, 15. kötet, 355. o.) 3. cikke (2) bekezdése első francia bekezdésének, 25. és 26. cikkének, valamint 28. cikke (3) bekezdésének az EUSZ 4. cikk (2) bekezdésével és az Európai Unió Alapjogi Chartája (a továbbiakban: Charta) 7., 8. és 47. cikkével összefüggésben történő értelmezésére,

– a 2016. december 16-i (EU) 2016/2297 bizottsági végrehajtási határozattal (HL 2016. L 344., 100. o.) módosított, a 95/46 irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2010. február 5-i 2010/87/EU bizottsági határozat (HL 2010. L 39., 5. o.; a továbbiakban: ÁSZF-határozat) értelmezésére és érvényességére, valamint

– a 95/46 irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló, 2016. július 12-i (EU) 2016/1250 bizottsági végrehajtási határozat (HL 2016. L 207., 1. o.; a továbbiakban: AVP-határozat) értelmezésére és érvényességére vonatkozik.

2 E kérelmet a Data Protection Commissioner (adatvédelmi biztos, Írország) (a továbbiakban: biztos), valamint a Facebook Ireland Ltd és Maximillian Schrems között folyamatban lévő jogvita keretében terjesztették elő, amelynek tárgya az ez utóbbi által a személyes adatainak a Facebook Ireland által a Facebook Inc. részére az Egyesült Államokba történő továbbítása vonatkozásában benyújtott panasz.

Jogi háttér

A 95/46 irányelv

3 A 95/46 irányelvnek „Az irányelv hatálya” címet viselő 3. cikke a (2) bekezdésében a következőket mondta ki:

„Az irányelv nem alkalmazandó [helyesen: nem alkalmazható] az alábbi személyesadat-feldolgozásokra [helyesen: személyesadat-kezelésekre]:

– a közösségi jog hatályán kívül eső tevékenységek, mint például az Európai Unióról szóló szerződés V. és VI. címeiben megállapítottak, valamint a közbiztonsággal, a védelemmel, a nemzetbiztonsággal (beleértve az ország gazdasági jólétét is, ha a feldolgozási [helyesen: az adatkezelési] művelet nemzetbiztonsági ügyre vonatkozik [helyesen: nemzetbiztonsági üggyel kapcsolatos]), továbbá a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási [helyesen: adatkezelési] műveletek,

[…]”

4 Ezen irányelv 25. cikke a következőképpen rendelkezett:

„(1) A tagállamoknak rendelkezniük kell arról, hogy a […] személyes adatok csak akkor továbbíthatók harmadik országba, ha – az ezen irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseknek való megfelelés sérelme nélkül – az adott harmadik ország megfelelő védelmi szintet tud biztosítani [helyesen: biztosít].

(2) A harmadik ország által nyújtott védelem szintjének megfelelő mivoltát az adattovábbítási művelet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni; […]

[…]

(6) A Bizottság a 31. cikk (2) bekezdésében említett eljárásnak megfelelően megállapíthatja, hogy a harmadik ország megfelelő védelmi szintet biztosít e cikk (2) bekezdése értelmében, az egyének magánéletének, jogainak és szabadságainak védelmére vonatkozó belföldi jog, vagy a vállalt nemzetközi kötelezettségek, különösen az (5) bekezdésben említett tárgyalások végeredménye alapján [helyesen: belföldi joga vagy az egyének magánéletének, alapvető jogainak és szabadságainak védelme érdekében, különösen az (5) bekezdésben említett tárgyalások végeredménye alapján vállalt nemzetközi kötelezettségei alapján].

A tagállamok megteszik azokat az intézkedéseket, amelyek szükségesek ahhoz, hogy megfeleljenek a Bizottság határozatának.”

5 Az említett irányelv 26. cikkének (2) és (4) bekezdése előírta:

„(2) Az (1) bekezdés sérelme nélkül a tagállamok engedélyezhetik a személyes adatok olyan harmadik országba irányuló továbbítását vagy továbbítássorozatát, amely a 25. cikk (2) bekezdése értelmében nem biztosít megfelelő szintű védelmet, amennyiben az adatkezelő megfelelő garanciákat teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében; ilyen garanciát jelenthetnek elsősorban a megfelelő szerződési feltételek.

[…]

(4) Amennyiben a Bizottság a 31. cikk (2) bekezdésében említett eljárásnak megfelelően úgy dönt, hogy egyes általános szerződési feltételek megfelelő biztosítékot nyújtanak a (2) bekezdés értelmében, a tagállamok megteszik a szükséges intézkedéseket a Bizottság határozatának teljesítésére."

6 Ugyanezen irányelv 28. cikkének (3) bekezdése értelmében:

„A hatóságok különösen a következő jogosultságokkal rendelkeznek:

– vizsgálati jogkör, mint például az adatfeldolgozási [helyesen: adatkezelési] műveletek tárgyát képező adatokhoz való hozzáférés joga, továbbá a felügyeleti feladatok ellátásához szükséges adatok gyűjtésének joga,

– tényleges beavatkozási jogosultságok, mint például a 20. cikknek megfelelően végzett adatfeldolgozási [helyesen: adatkezelési] műveletek megkezdése előtti véleményezés joga, e vélemények megfelelő közzétételének biztosítása, az adatok zárolásának, törlésének vagy megsemmisítésének elrendelése, az adatfeldolgozás [helyesen: adatkezelés] átmeneti vagy végleges tilalmának megállapítása, az adatkezelő figyelmeztetése vagy megrovása, illetve az ügy nemzeti parlament vagy más politikai intézmény elé terjesztése,

– bírósági eljárásban való részvétel joga az irányelv értelmében elfogadott nemzeti rendelkezések megsértése esetén, továbbá e jogsértések igazságszolgáltatási hatóságok elé terjesztésének joga.

[…]"

A GDPR

7 Ezt az irányelvet hatályon kívül helyezte és felváltotta a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet) (HL 2016. L 119., 1. o.; helyesbítések: HL 2016. L 314., 72. o.; HL 2018. L 127., 2. o.; a továbbiakban: GDPR).

8 A GDPR (6), (10), (101), (103), (104), (107)–(109), (114), (116) és (141) preambulumbekezdése kimondja:

„(6) A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi. Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia egyaránt átalakította a gazdasági és a társadalmi életet, és egyre inkább elősegíti a személyes adatok Unión belüli szabad áramlását és a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítását, biztosítva egyúttal a személyes adatok magas szintű védelmét.

[…]

(10) A természetes személyek következetes és magas szintű védelmének biztosítása és a személyes adatok Unión belüli áramlása előtti akadályok elhárítása érdekében a természetes személyeknek az ilyen adatok kezelésével összefüggésben fennálló jogait és szabadságait minden tagállamban azonos szintű védelemben kell részesíteni. A természetes személyeknek a személyes adataik feldolgozásához kapcsolódó alapvető jogai és szabadságai védelmére vonatkozó szabályok következetes és egységes alkalmazását az Unió egész területén biztosítani kell. A tagállamok

számára lehetővé kell tenni, hogy az e rendeletben foglalt szabályok alkalmazását pontosító nemzeti rendelkezéseket tartsanak fenn vagy vezessenek be, ha a személyes adatok kezelésére jogi kötelezettség teljesítéséhez, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához szükséges. A 95/46/EK irányelvet végrehajtó általános és horizontális adatvédelmi jogszabályokhoz kapcsolódóan a tagállamok számos ágazatspecifikus jogszabályt hoztak azokon a területeken, ahol konkrétabb rendelkezésekre van szükség. Ez a rendelet a tagállamok számára mozgásteret biztosít ahhoz, hogy pontosítsák a benne meghatározott szabályokat, ideértve a személyes adatok különleges kategóriáira („különleges adatok”) vonatkozókat is. Ennyiben tehát ez a rendelet nem zárja ki olyan tagállami jog elfogadását, amely meghatározza a különleges adatkezelési helyzetek körülményeit, ezen belül pontosabban megállapítja, hogy milyen feltételek mellett jogszerű a személyes adatok kezelése.

[…]

(101) A nemzetközi kereskedelem és a nemzetközi együttműködés bővítéséhez szükség van a személyes adatoknak az Unión kívüli országok és a nemzetközi szervezetek viszonylatában megvalósuló forgalmára. Ezen áramlások növekedése új kihívásokat és aggodalmakat támasztott a személyes adatok védelme tekintetében. Mindazonáltal a személyes adatoknak az Unióból harmadik országbeli adatkezelőknek, adatfeldolgozóknak, egyéb címzetteknek vagy nemzetközi szervezetek részére történő továbbítása esetén nem sérülhet a természetes személyeknek az Unióban e rendelettel biztosított védelem szintje, és annak fenn kell maradnia az ilyen személyes adatoknak az adott harmadik országból vagy nemzetközi szervezettől ezt követően ugyanazon vagy másik harmadik országbeli adatkezelőnek, adatfeldolgozónak vagy nemzetközi szervezetnek történő újbóli továbbítása esetén is. A harmadik országokba és a nemzetközi szervezetekhez való továbbítás csak e rendelet teljes betartása mellett hajtható végre. A továbbításra akkor kerülhet csak sor, ha az adatkezelő vagy az adatfeldolgozó – e rendelet egyéb rendelkezéseire is figyelemmel – teljesíti az harmadik országok vagy nemzetközi szervezeteknek történő adattovábbításra vonatkozó, e rendeletben meghatározott feltételeket.

[…]

(103) Az Unió egészére kiterjedő hatállyal a Bizottság dönthet úgy, hogy harmadik ország, egy harmadik ország valamely területe vagy meghatározott ágazata, illetve valamely nemzetközi szervezet megfelelő adatvédelmi szintet nyújt, így biztosítva az Unió egész területén a jogbiztonságot és az egységességet az ilyen védelmi szintet biztosító harmadik országok vagy nemzetközi szervezetek tekintetében. Ilyen esetekben a személyes adatok az említett országokba vagy nemzetközi szervezetek részére történő továbbítása további engedély beszerzése nélkül lehetséges. A Bizottság a harmadik országnak vagy nemzetközi szervezetnek küldött, teljes körű indokolással ellátott értesítést követően határozhat úgy is, hogy visszavonja ezt a döntést.

(104) A Bizottság – az Unió alapjául szolgáló alapvető értékekkel, így különösen az emberi jogok védelmével összhangban – a harmadik országra vagy egy harmadik ország valamely területére vagy meghatározott ágazatára vonatkozó értékelés elkészítésekor figyelembe veszi azt, hogy az adott harmadik országban mennyire tartják tiszteletben a jogállamiságot, az igazságszolgáltatáshoz való jogot, valamint a nemzetközi emberi jogi normákat és előírásokat, valamint megvizsgálja az adott ország általános és ágazati jogszabályait, ideértve a közbiztonságra, a védelemre és a nemzetbiztonságra vonatkozó jogszabályait, valamint közrendjét és büntetőjogát is. Az adott ország valamely területére vagy meghatározott ágazatára vonatkozó megfelelőségi határozat elfogadásakor olyan egyértelmű és objektív szempontokat szükséges figyelembe venni, mint például a konkrét adatkezelési tevékenységek, továbbá a harmadik országban alkalmazandó jogi normák és jogszabályok hatálya. A harmadik országnak olyan kötelezettséget kell vállalnia, amelyek megfelelő – az Unión belül biztosítottal lényegében megegyező – védelmi szintet biztosítanak, különösen amikor a személyes adatokat egy vagy több

konkrét ágazatban kezelik. A harmadik országnak különösen gondoskodnia kell a tényleges, független adatvédelmi felügyeletről és tagállami adatvédelmi hatóságokkal való együttműködési mechanizmusairól, továbbá biztosítania kell, hogy az érintettek tényleges és érvényesíthető jogokkal, valamint hatékony közigazgatási és bírósági jogorvoslati lehetőségekkel rendelkezzenek.

[…]

(107) A Bizottság azt is megállapíthatja, hogy az adott harmadik ország, a harmadik ország valamely területe vagy meghatározott ágazata, illetve valamely nemzetközi szervezet már nem biztosít megfelelő szintű adatvédelmet. Következésképpen a személyes adatok ilyen harmadik országba vagy nemzetközi szervezet részére történő továbbítását meg kell tiltani, kivéve, ha e rendeletbe foglalt, a személyes adatok továbbítása megfelelő garanciák alapján történik, ideértve a kötelező erejű vállalati szabályokat, és a meghatározott helyzetekben biztosított eltérésekre vonatkozó követelményeket. Erre az esetre a Bizottság és az ilyen harmadik országok vagy nemzetközi szervezetek közötti konzultációkra vonatkozó eljárásokról rendelkezni kell. A Bizottság megfelelő időben tájékoztatja az érintett harmadik országot vagy nemzetközi szervezetet az indokokról, és vele a helyzet orvoslása érdekében konzultációkat folytat.

(108) Megfelelőségi határozat hiányában az adatkezelő vagy az adatfeldolgozó a megfelelő garanciák érintett számára való biztosítása útján gondoskodik az adatvédelem harmadik országbeli hiányosságainak ellensúlyozásáról. Ezek a megfelelő garanciák magukban foglalhatják a kötelező erejű vállalati szabályok, a Bizottság által elfogadott általános adatvédelmi kikötések, a felügyeleti hatóság által elfogadott általános adatvédelmi kikötések vagy a felügyeleti hatóság által engedélyezett általános szerződési feltételek alkalmazását. A garanciák biztosítják az adatvédelmi követelményeknek való megfelelést, és az Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat biztosítanak az érintettek számára, beleértve az érintettek jogainak érvényesíthetőségét és a hatékony jogorvoslat lehetőségét, ezen belül ideértve azt, hogy az érintettek hatékony közigazgatási vagy bírósági jogorvoslatot vehessenek igénybe és kártérítést igényelhessenek az Unióban vagy egy harmadik országban. A garanciák különösen a személyes adatok kezelésre vonatkozó általános elveknek, valamint a beépített és alapértelmezett adatvédelem elveinek való megfelelésre vonatkoznak. […]

(109) Az a lehetőség, mely szerint az adatkezelő vagy az adatfeldolgozó alkalmazhatja a Bizottság vagy a felügyeleti hatóság által elfogadott általános adatvédelmi kikötéseket, egyik sem zárja ki, hogy az adatkezelő vagy az adatfeldolgozó szélesebb körű szerződésben – ideértve az adatfeldolgozó és valamely egyéb adatfeldolgozó közötti szerződéseket is – alkalmazza ezen általános adatvédelmi kikötéseket, sem azt, hogy további rendelkezéseket vagy garanciákat adjon hozzá, feltéve hogy azok sem közvetlen, sem közvetett módon nem ellentétesek a Bizottság vagy a felügyeleti hatóság által elfogadott általános szerződési feltételekkel, és nem sértik az érintettek alapvető jogait és szabadságait. Az adatkezelőket és az adatfeldolgozókat arra kell ösztönözni, hogy az általános adatvédelmi kikötéseket kiegészítő további szerződéses kötelezettségvállalások útján még erőteljesebb garanciákat nyújtsanak.

[…]

(114) Ha a Bizottság az adott harmadik ország viszonylatában nem hozott határozatot a harmadik ország megfelelő adatvédelemi szintjéről, az adatkezelő vagy az adatfeldolgozó olyan megoldásokhoz folyamodhat, amelyek az érintettek számára olyan tényleges és érvényesíthető jogokat biztosítanak, hogy az érintettek az adattovábbítást követően is élvezhetik az őket megillető alapvető jogokat és garanciákat.

[…]

(116) A személyes adatok uniós külső határokat átlépő továbbításakor megnövekedhet annak a kockázata, hogy a természetes személyek adatvédelmi jogaikat nem képesek gyakorolni, különösen, ami az adatok jogellenes felhasználása vagy közlése elleni védelmet illeti. Ezzel egyidejűleg a felügyelő hatóságok megállapíthatják, hogy képtelenek a panaszok érvényesítésére vagy vizsgálat lefolytatására a határaikon kívül folyó tevékenységek tekintetében. A határokon átnyúló összefüggésben tett erőfeszítéseiket az elégtelen megelőzési vagy jogorvoslati hatáskör, az egymásnak ellentmondó jogrendszerek, valamint olyan gyakorlati akadályok is hátráltathatják, mint a források korlátozott volta. […]

[…]

(141) Minden érintett jogosult arra, hogy panaszt tegyen egy – különösen a szokásos tartózkodási helye szerinti tagállambeli – felügyeleti hatóságnál, és a Charta 47. cikkével összhangban hatékony bírósági jogorvoslattal éljen, ha az úgy ítéli meg, hogy az e rendelet alapján elfogadott rendelkezések értelmében őt megillető jogokat megsértették, vagy ha a felügyeleti hatóság nem jár el valamely panasza alapján, illetve részben vagy egészben elutasítja vagy megalapozatlannak tekinti a panaszát, vagy nem jár el olyan esetben, amikor fellépése az érintett jogainak védelmében szükséges lenne. […]”

9 E rendelet 2. cikkének (1) és (2) bekezdése előírja:

„(1) E rendeletet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon való kezelésére, amelyek valamely nyilvántartó rendszer részét képezik, vagy amelyeket egy nyilvántartó rendszer részévé kívánnak tenni.

(2) E rendelet nem alkalmazandó a személyes adatok kezelésére, ha azt:

a) az uniós jog hatályán kívül eső tevékenységek során végzik;

b) a tagállamok az EUSZ V. címe 2. fejezetének hatálya alá tartozó tevékenységek során végzik;

c) természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik;

d) az illetékes hatóságok bűncselekmények megelőzése, nyomozása, felderítése, vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzik, ideértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését.”

10 Az említett rendelet 4. cikke a következőképpen rendelkezik:

„E rendelet alkalmazásában:

[…]

2. »adatkezelés«: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közléstovábbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

[…]

7. »adatkezelő«: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

8. »adatfeldolgozó«: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

9. »címzett«: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Nem tekintendők azonban címzetteknek azok a közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban kaphatnak személyes adatot, és az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

[…]”

11 Ugyanezen rendelet 23. cikke kimondja:

„(1) Az adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja a 12–22. cikkben és a 34. cikkben foglalt, valamint a 12–22. cikkben meghatározott jogokkal és kötelezettségekkel összhangban lévő rendelkezései tekintetében az 5. cikkben foglalt jogok és kötelezettségek hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban:

a) nemzetbiztonság;

b) honvédelem;

c) közbiztonság;

d) bűncselekmények megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését;

[…]

(2) Az (1) bekezdésben említett jogalkotási intézkedések adott esetben részletes rendelkezéseket tartalmaznak legalább:

a) az adatkezelés céljaira vagy az adatkezelés kategóriáira,

b) a személyes adatok kategóriáira,

c) a bevezetett korlátozások hatályára,

d) a visszaélésre, illetve a jogosulatlan hozzáférésre vagy továbbítás megakadályozását célzó garanciákra,

e) az adatkezelő meghatározására vagy az adatkezelők kategóriáinak meghatározására,

f) az adattárolás időtartamára, valamint az alkalmazandó garanciákra, figyelembe véve az adatkezelés vagy az adatkezelési kategóriák jellegét, hatályát és céljait,

g) az érintettek jogait és szabadságait érintő kockázatokra, és

h) az érintettek arra vonatkozó jogára, hogy tájékoztatást kapjanak a korlátozásról, kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját."

12 A GDPR-nek „A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása" címet viselő V. fejezete tartalmazza e rendelet 44–50. cikkét. E rendeletnek „Az adattovábbításra vonatkozó általános elv" című 44. cikke a következőket mondja ki:

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

13 E rendeletnek az „Adattovábbítás megfelelőségi határozat alapján" címet viselő 45. cikkének (1)–(3) bekezdése a következőket írja elő:

„(1) Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha a Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély.

(2) A védelmi szint megfelelőségének mérlegelése során a Bizottság különösen a következő tényezőket veszi figyelembe:

a) a jogállamiság, az emberi jogok és alapvető szabadságok tiszteletben tartása, a vonatkozó általános és ágazati jogszabályok, köztük a közbiztonságra, a védelemre, valamint a nemzetbiztonságra vonatkozó és a büntetőjogi rendelkezések, a közhatalmi szerveknek a személyes adatokhoz való hozzáférését szabályozó rendelkezések, valamint e jogszabályok végrehajtása, adatvédelmi szabályok, szakmai szabályok és biztonsági intézkedések, ideértve a személyes adatok másik harmadik ország vagy nemzetközi szervezet részére történő újbóli továbbítására vonatkozó azon szabályokat, amelyeknek az adott országban vagy nemzetközi szervezeten belül meg kell felelni; ítélkezési gyakorlat, továbbá az, hogy az érintettek, akiknek a személyes adatait továbbítják, rendelkeznek-e hatékonyan érvényesíthető – a hatékony közigazgatási és bírósági jogorvoslatot is magukban foglaló – jogokkal;

b) a szóban forgó harmadik országban létezik-e egy vagy több olyan független és hatékonyan működő felügyeleti hatóság – a szóban forgó nemzetközi szervezet pedig ilyen hatóság ellenőrzése alatt áll-e –, amely felelős az adatvédelmi szabályok betartásának biztosításáért és végrehajtásáért, rendelkezik többek között megfelelő kikényszerítési hatáskörrel, és felelős az érintettek részére történő, a jogaik gyakorlásával kapcsolatos segítségnyújtásért és tanácsadásért, valamint a tagállami felügyeleti hatóságokkal való együttműködésért; továbbá

c) a szóban forgó harmadik ország vagy nemzetközi szervezet nemzetközi kötelezettségei vagy egyéb, jogilag kötelező erejű egyezményekből vagy jogi eszközökből, valamint többoldalú vagy regionális rendszerekben való részvételéből eredő – különösen a személyes adatok védelmével kapcsolatos – kötelezettségei.

(3) A védelmi szint megfelelőségének értékelését követően a Bizottság végrehajtási jogi aktusok útján határozhat arról, hogy a harmadik ország, a harmadik ország valamely területe, illetve egy vagy több meghatározott ágazata, illetve valamely nemzetközi szervezet a (2) bekezdés értelmében biztosítja a megfelelő védelmi szintet. A végrehajtási jogi aktusban rendelkezni kell egy rendszeres, legalább négyévente elvégzendő felülvizsgálatra irányuló mechanizmusról, amely az adott harmadik országban vagy nemzetközi szervezetnél végbement valamennyi releváns fejleményt figyelembe vesz. A végrehajtási jogi aktusban pontosan rögzíteni kell annak területi és ágazati alkalmazási körét, és – adott esetben – meg kell határozni a (2) bekezdés b) pontjában említett felügyeleti hatóságot, illetve hatóságokat. A végrehajtási jogi aktust a 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárásnak megfelelően kell elfogadni.”

14 Az említett rendelet „Megfelelő garanciák alapján történő adattovábbítások” című 46. cikkének (1)–(3) bekezdése a következőképpen rendelkezik:

„(1) A 45. cikk (3) bekezdése szerinti határozat hiányában az adatkezelő vagy adatfeldolgozó csak abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

(2) A felügyeleti hatóság külön engedélye nélkül az (1) bekezdés szerinti megfelelő garanciákat az alábbiak jelenthetik:

a) közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz;

b) a 47. cikk szerinti kötelező erejű vállalati szabályok;

c) a Bizottság által a 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban elfogadott általános adatvédelmi kikötések;

d) a felügyeleti hatóság által elfogadott és a Bizottság által a 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárásnak megfelelően jóváhagyott általános adatvédelmi kikötések;

e) a 40. cikk szerinti, jóváhagyott magatartási kódex a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő – ideértve az érintettek jogaira vonatkozó – garanciákat; vagy

f) a 42. cikk szerinti, jóváhagyott tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is.

(3) Az illetékes felügyeleti hatóság engedélyével az (1) bekezdésben említett megfelelő garanciákként különösen az alábbiak is szolgálhatnak:

a) az adatkezelő vagy adatfeldolgozó és a harmadik országbeli vagy a nemzetközi szervezeten belüli adatkezelő, adatfeldolgozó vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések; vagy

b) közhatalmi vagy egyéb, közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezések, köztük az érintettek érvényesíthető és tényleges jogaira vonatkozó rendelkezések.”

15 Ugyanezen rendelet „Különös helyzetekben biztosított eltérések” című 49. cikke kimondja:

„(1) A 45. cikk (3) bekezdése szerinti megfelelőségi határozat, illetve a 46. cikk szerinti megfelelő garanciák hiányában – beleértve a kötelező erejű vállalati szabályokat is –, a személyes adatok harmadik ország vagy nemzetközi szervezet részére történő továbbítására vagy többszöri továbbítására csak az alábbi feltételek legalább egyikének teljesülése esetén kerülhet sor:

a) az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – lehetséges kockázatokról;

b) az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;

c) az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;

d) az adattovábbítás fontos közérdekből szükséges;

e) az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;

f) az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;

g) a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

Ha az adattovábbítás nem alapulhat a 45. vagy a 46. cikk rendelkezésein, beleértve a kötelező erejű vállalati szabályok rendelkezéseit is, és az első albekezdésben említett egyedi helyzetekre vonatkozó eltérések egyike sem alkalmazandó, harmadik országok és nemzetközi szervezetek részére történő adattovábbítás csak akkor történhet, ha az adattovábbítás nem ismétlődő, csak korlátozott számú érintettre vonatkozik, az adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, és az adatkezelő az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében. Az adatkezelőnek tájékoztatnia kell a felügyeleti hatóságot az adattovábbításról. Az adatkezelő a 13. és a 14. cikkben említett információk nyújtásán kívül az érintettet tájékoztatja az adattovábbításról, valamint az adatkezelő kényszerítő erejű jogos érdekéről.

(2) Az (1) bekezdés első albekezdésének g) pontja szerinti adattovábbítás nem érintheti a nyilvántartásban szereplő személyes adatok vagy személyes adatok kategóriáinak összességét. Ha a nyilvántartásba csak olyan személyek tekinthetnek be, akiknek ehhez jogos érdeke fűződik, az adattovábbításra csak e személyek kérelmére kerülhet sor, illetve abban az esetben, ha ők a címzettek.

(3) Az (1) bekezdés első albekezdésének a), b) és c) pontja, valamint második albekezdése nem alkalmazandó a közhatalmi szervek által közhatalmi jogosítványaik gyakorlása során végzett tevékenységekre.

(4) Az (1) bekezdés első albekezdésének d) pontjában említett közérdeket akkor kell figyelembe venni, ha azt az uniós jog vagy az adatkezelőre vonatkozó tagállami jog elismeri.

(5) Megfelelőségi határozat hiányában az uniós jog vagy a tagállami jog fontos közérdekből kifejezetten korlátozhatja bizonyos kategóriákba tartozó személyes adatok valamely harmadik országba vagy nemzetközi szervezethez történő továbbítását. A tagállamok az ilyen rendelkezéseket bejelentik a Bizottságnak.

(6) Az adatkezelő vagy az adatfeldolgozó az e cikk (1) bekezdésének második albekezdésében említett vizsgálatot és megfelelő garanciákat a 30. cikkben említett nyilvántartásban dokumentálja."

16 A GDPR 51. cikkének (1) bekezdése kimondja:

„A természetes személyek alapvető jogainak és szabadságainak a személyes adataik kezelése tekintetében történő védelme, valamint a személyes adatok Unión belüli szabad áramlásának megkönnyítése érdekében minden tagállam előírja, hogy e rendelet alkalmazásának ellenőrzéséért egy vagy több független közhatalmi szerv (felügyeleti hatóság) felel."

17 E rendelet 55. cikkének (1) bekezdése szerint „[a] felügyeleti hatóság a saját tagállamának területén illetékes az e rendelet alapján ráruházott feladatok végzésére és hatáskörök gyakorlására".

18 Az említett rendelet 57. cikkének (1) bekezdése előírja:

„Az e rendeletben meghatározott egyéb feladatok sérelme nélkül, a felügyeleti hatóság a saját területén ellátja a következő feladatokat:

a) nyomon követi és kikényszeríti e rendelet alkalmazását;

[…]

f) kezeli az érintett vagy valamely szerv, szervezet vagy egyesület által a 80. cikkel összhangban benyújtott panaszokat, a panasz tárgyát a szükséges mértékben kivizsgálja, továbbá észszerű határidőn belül tájékoztatja a panaszost a vizsgálattal kapcsolatos fejleményekről és eredményekről, különösen, ha további vizsgálat vagy egy másik felügyeleti hatósággal való együttműködés válik szükségessé;

[…]"

19 Ugyanezen rendelet 58. cikkének (2) és (4) bekezdése értelmében:

„(2) A felügyeleti hatóság korrekciós hatáskörében eljárva:

[…]

f) átmenetileg vagy véglegesen korlátozza az adatkezelést, ideértve az adatkezelés megtiltását is;

[…]

j) elrendeli a harmadik országbeli címzett vagy nemzetközi szervezet felé irányuló adatáramlás felfüggesztését.

[…]

(4) Az e cikk alapján a felügyeleti hatóságra ruházott hatáskörök gyakorlására megfelelő garanciák mellett kerülhet sor, ideértve az uniós és a tagállami jogban a Chartával összhangban meghatározott hatékony bírósági jogorvoslatot és tisztességes eljárást is."

20 A GDPR 64. cikkének (2) bekezdése kimondja:

„Bármely felügyeleti hatóság, a Testület elnöke vagy a Bizottság kérheti, hogy a Testület vizsgáljon meg egy általános érvényű vagy egynél több tagállamban hatással bíró ügyet, és bocsásson ki róla véleményt, különösen, ha valamely illetékes felügyeleti hatóság nem teljesíti a 61. cikk szerinti kölcsönös segítségnyújtás vagy a 62. cikk szerinti közös műveletek tekintetében fennálló kötelezettségeit.”

21 E rendelet 65. cikkének (1) bekezdése szerint:

„Annak érdekében, hogy az egyes esetekben biztosított legyen e rendelet helyes és egységes alkalmazása, a Testület kötelező erejű döntést fogad el az alábbi esetekben:

[…]

c) ha valamely illetékes felügyeleti hatóság nem kéri ki a Testület véleményét a 64. cikk (1) bekezdésében említett esetekben, vagy nem a Testület által a 64. cikk alapján kibocsátott vélemény alapján jár el. Ebben az esetben bármely érintett felügyeleti hatóság vagy a Bizottság a Testület tudomására hozhatja az ügyet.”

22 Az említett rendeletnek „A felügyeleti hatóságnál történő panasztételhez való jog” című 77. cikke kimondja:

„(1) Az egyéb közigazgatási vagy bírósági jogorvoslatok sérelme nélkül, minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti e rendeletet.

(2) Az a felügyeleti hatóság, amelyhez a panaszt benyújtották, köteles tájékoztatni az ügyfelet a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről, ideértve azt is, hogy a 78. cikk alapján az ügyfél jogosult bírósági jogorvoslattal élni.”

23 Ugyanezen rendeletnek „A felügyelő hatósággal szembeni hatékony bírósági jogorvoslathoz való jog” című 78. cikkének (1) és (2) bekezdése a következőket írja elő:

„(1) Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.

(2) Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden érintett jogosult a hatékony bírósági jogorvoslatra, ha az 55. vagy 56. cikk alapján illetékes felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a 77. cikk alapján benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.”

24 A GDPR 94. cikke a következőképpen rendelkezik:

„(1) A [95/46] irányelv 2018. május 25-i hatállyal hatályát veszti.

(2) A hatályon kívül helyezett irányelvre történő hivatkozásokat az e rendeletre történő hivatkozásnak kell tekinteni. A [95/46] irányelv 29. cikke által létrehozott, a természetes személyeknek a személyes adatok feldolgozása tekintetében való védelmével foglalkozó munkacsoportra történő hivatkozást az e rendelet által létrehozott Európai Adatvédelmi Testületre történő hivatkozásnak kell tekinteni.”

25 E rendelet 99. cikke szerint:

„(1) Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

(2) Ezt a rendeletet 2018. május 25-től kell alkalmazni.”

Az ÁSZF-határozat

26 A megtámadott ÁSZF-határozat (11) preambulumbekezdésének szövege a következő:

„A tagállamok felügyeleti hatóságai kulcsfontosságú szerepet játszanak e szerződéses mechanizmusban, mivel ők biztosítják, hogy a személyes adatok továbbításukat követően megfelelő védelemben részesüljenek. Kivételes esetekben, amikor az adatátadók nem hajlandók vagy nem képesek megfelelő módon tájékoztatni az adatátvevőket – ami az érintettek számára súlyos károkat okozhat –, az általános szerződési feltételeknek lehetővé kell tenniük, hogy a felügyeleti hatóságok ellenőrizhessék az adatátvevőket és további feldolgozókat, és – adott esetben – rájuk nézve kötelező határozatokat hozzanak. A felügyeleti hatóságoknak megfelelő hatáskörrel kell rendelkezniük ahhoz, hogy az általános szerződési feltételek alapján megtiltsanak vagy felfüggesszenek adattovábbítást vagy adattovábbításokat azokban a kivételes esetekben, amikor megállapítást nyer, hogy egy szerződés alapján teljesített adattovábbításnak vélhetően súlyosan hátrányos hatása lesz az érintettek számára megfelelő védelmet biztosító garanciákra és kötelezettségekre.”

27 E határozat 1. cikke a következőképpen rendelkezik:

„A mellékletben meghatározott általános szerződési feltételek megfelelő biztosítékokat kínálnak a magánélet tiszteletben tartásához való jog, az egyének alapvető jogainak és szabadságjogainak védelme tekintetében, valamint a [95/46] irányelv 26. cikke (2) bekezdése értelmében meghatározott, ezekhez kapcsolódó jogok érvényesítése tekintetében.”

28 Az említett határozat 2. cikkének második bekezdése értelmében e határozat „a személyes adatok továbbításának azon eseteire vonatkozik, amikor az Európai Unióban letelepedett adatkezelők a személyes adatokat olyan, az Európai Unión kívül letelepedett adatátvevőknek továbbítják, akik csak adatfeldolgozói feladatokat látnak el”.

29 Ugyanezen határozat 3. cikke ekként rendelkezik:

„E határozat alkalmazásában:

[…]

c) »adatátadó«: a személyes adatokat továbbító adatkezelő;

d) »adatátvevő«: egy harmadik országban letelepedett olyan feldolgozó, aki vállalja, hogy az adatátadó utasításaival és e határozat feltételeivel összhangban történt adattovábbítást követően átveszi az adatátadótól a személyes adatokat – annak nevében történő – adatfeldolgozás céljából, és aki nem tartozik egy harmadik ország – [95/46] irányelv 25. cikkének (1) bekezdése szerinti – megfelelő védelmet biztosító rendszerének hatálya alá;

[…]

f) »alkalmazandó adatvédelmi jog«: az egyének alapvető jogaik és szabadságjogaik, különösen – a személyes adatok feldolgozásával kapcsolatban – a magánélet tiszteletben tartásához való jogaik védelméről szóló, az adatátadó letelepedési helye szerinti tagállamban tevékenykedő adatkezelőre vonatkozó jogszabály;

[…]”

30 A 2016/2297 végrehajtási határozat hatálybalépését megelőző eredeti változatában a 2010/87 határozat 4. cikke előírta:

„(1) A [95/46] irányelv II., III., V. és VI. fejezete alapján elfogadott nemzeti rendelkezéseknek való megfelelés céljából tett intézkedésekre vonatkozó hatásköröket nem érintve, a tagállamok illetékes hatóságai a magánszemélyek – személyes adatainak feldolgozására tekintettel történő – védelme érdekében élhetnek azzal a jogukkal, hogy megtilthatják vagy felfüggeszthetik a harmadik országokba történő adattovábbítást olyan esetekben, ha:

a) megállapítják, hogy az adatátvevőre vagy a további feldolgozóra irányadó jog olyan követelményeket támaszt vele szemben, amelyek értelmében el kell térnie az alkalmazandó adatvédelmi jogtól, valamint amelyek – a [95/46] irányelv 13. cikkében foglalt, a demokratikus társadalomban szükséges korlátozásokat – túllépik; és amennyiben ezek a követelmények vélhetően jelentős hátrányos hatással lesznek az alkalmazandó adatvédelmi jog és az általános szerződési feltételek által nyújtott garanciákra;

b) az illetékes hatóság megállapította, hogy az adatátvevő vagy a további feldolgozó nem tartotta be a mellékletben szereplő általános szerződési feltételeket; vagy

c) nagy a valószínűsége, hogy a mellékletben szereplő általános szerződési feltételeknek nem tesznek eleget vagy nem fognak eleget tenni, és az adattovábbítás folytatása súlyosan veszélyeztetné az érintetteket.

(2) Az (1) bekezdésben említett tilalmat vagy felfüggesztést azonnal megszüntetik, amint a felfüggesztés vagy tilalom okai megszűnnek.

(3) A tagállamok késedelem nélkül tájékoztatják a Bizottságot az (1) és (2) bekezdés értelmében elfogadott intézkedésekről, amely továbbítja ezt az információt a többi tagállamnak.”

31 A 2015. október 6-i Schrems ítélet (C-362/14, EU:C:2015:650) kihirdetését követően elfogadott 2016/2297 végrehajtási határozat (5) preambulumbekezdésének szövege a következő:

„A [95/46] irányelv 26. cikkének (4) bekezdése szerint elfogadott bizottsági határozat értelemszerűen kötelező erejű a tagállamok címzett szerveire, köztük a független felügyeleti hatóságokra nézve, amennyiben ennek következményeként elismerik, hogy az abban foglalt általános szerződési feltételek alapján végzett adattovábbítások – az említett irányelv 26. cikke (2) bekezdésében előírtak szerint – elegendő biztosítékot nyújtanak. Ez nem akadályozza meg, hogy a nemzeti felügyeleti hatóság gyakorolja az adatáramlások ellenőrzéséra vonatkozó jogkörét, beleértve a személyes adatok továbbításának felfüggesztését vagy tilalmát, ha a hatóság megállapítja, hogy az uniós vagy a nemzeti adatvédelmi jog megsértésével végzik az adattovábbítást, így például az adatátvevő nem tartja tiszteletben az általános szerződési feltételeket.”

32 Az ÁSZF-határozat 2016/2297 végrehajtási határozattal módosított 4. cikke kimondja:

„Ha a tagállamok hatáskörrel rendelkező hatóságai oly módon gyakorolják a [95/46] irányelv 28. cikkének (3) bekezdése alapján őket megillető jogköreiket, hogy ez – az egyéneknek a személyes adataik kezelése tekintetében történő védelme érdekében – harmadik országokba irányuló adatáramlás felfüggesztéséhez vagy végleges tilalmához vezet, az érintett tagállam haladéktalanul tájékoztatja erről a Bizottságot, amely továbbítja ezt a tájékoztatást a többi tagállamnak.”

33 Az ÁSZF-határozat „Általános szerződési feltételek (adatfeldolgozók)” című melléklete tizenkét általános feltételt tartalmaz. E melléklet 3. általános feltétele, amelynek címe „A kedvezményezett harmadik személyről szóló rendelkezés”, a következőket írja elő:

„(1) Az érintett az adatátadóval szemben – kedvezményezett harmadik személyként – érvényesítheti ezt az általános szerződési feltételt, a 4. általános szerződési feltétel b)–i) pontját, az 5. általános szerződési feltétel a)–e), valamint g)–j) pontját, a 6. általános szerződési feltétel (1) és (2) bekezdését, a 7. általános szerződési feltételt, a 8. általános szerződési feltétel (2) bekezdését, valamint a 9–12. általános szerződési feltételt.

(2) Az érintett az adatátvevővel szemben érvényesítheti ezt az általános szerződés feltételt, az 5. általános szerződési feltétel a)–e) és g) pontját, a 6. és 7. általános szerződési feltételt, a 8. általános szerződési feltétel (2) bekezdését, valamint a 9–12. általános szerződési feltételt azokban az esetekben, amikor az adatátadó vállalkozása ténylegesen vagy jogilag megszűnik létezni, feltéve hogy nincs olyan jogutód, amely az adatátadó valamennyi jogi kötelezettségét szerződéses vagy jogszabályi úton átvállalta, aminek eredményeként gyakorolja az adatátadó jogait és kötelezettségeit, amely esetben az érintett ezeket érvényesítheti e jogutóddal szemben.

[…]”

34 E melléklet 4. általános feltétele szerint, amelynek címe „Az adatátadó kötelezettségei”:

„Az adatátvevő elfogadja és garantálja, hogy:

a) a személyes adatok feldolgozása, ideértve magát az adattovábbítást is, megfelelt és továbbra is megfelel az alkalmazandó adatvédelmi jog vonatkozó hatályos rendelkezéseinek (és adott esetben erről értesítették az adatátadó letelepedési helye szerinti tagállam hatóságait), valamint nem sérti az adott állam vonatkozó rendelkezéseit;

b) ellátta és a személyes adatok feldolgozása során folyamatosan ellátja az adatátvevőt arra vonatkozó utasításokkal, hogy a továbbított személyes adatokat csak az adatátadó megbízásából és az alkalmazandó adatvédelmi joggal, továbbá az általános szerződési feltételekkel összhangban lehet feldolgozni;

[…]

f) amennyiben az adattovábbítás különleges adatkategóriákat érint, az érintettet az adattovábbítást megelőzően vagy – a lehető legrövidebb időn belül – az adattovábbítást követően tájékoztatják arról, hogy az adatokat egy olyan harmadik országba továbbítják, amely nem biztosítja a [95/46 irányelv] szerinti megfelelő mértékű védelmet;

g) továbbítja az adatvédelmi felügyeleti hatóság felé az adatátvevőtől és bármely további feldolgozótól az 5. általános szerződési feltétel b) pontja és a 8. általános szerződési feltétel (3) bekezdése értelmében átvett értesítést, amennyiben az adatátadó úgy dönt, hogy folytatja az adattovábbítást vagy megszünteti a felfüggesztést;

[…]”

35 Az említett mellékletnek „Az adatátadó kötelezettségei […]” című 5. általános feltétele a következőképpen rendelkezik:

„Az adatátvevő elfogadja és garantálja, hogy:

a) csak az átadó nevében, utasításaival és az általános szerződési feltételekkel összhangban dolgozza fel a személyes adatokat; amennyiben bármely oknál fogva nem képes megfelelni ezeknek a követelményeknek, haladéktalanul tájékoztatja erről az adatátadót, aki ez esetben jogosult felfüggeszteni az adattovábbítást és/vagy a szerződéstől elállni;

b) nincs tudomása arról, hogy a rá vonatkozó jogszabályok akadályoznák az adatátadótól kapott utasítások és a szerződésben vállalt kötelezettségek teljesítését – abban az esetben, ha a jogszabályok módosítása előreláthatóan jelentősen hátrányos hatással lenne az általános szerződési feltételekben rá vonatkozóan megállapított garanciákra és kötelezettségekre, mihelyt azonban tudomást szerez erről, azonnal értesíti a módosításról az adatátadót –, ebben az esetben az adatátadó jogosult felfüggeszteni az adattovábbítást és/vagy a szerződéstől elállni;

[…]

d) azonnal értesíti majd az adatátadót a következőkről:
   i. ellenkező értelmű tilalom – például egy bűnügyi nyomozás titkosságának megőrzése érdekében fennálló büntetőjogi tilalom – hiányában a bűnüldöző szervek jogilag kötelező erejű felhívása a személyes adatok közlésére;
   ii. bármilyen véletlen vagy jogosulatlan hozzáférés; és
   iii. közvetlen az érintettek részéről érkező kérelem, erre adott válasz nélkül, kivéve, ha erre felhatalmazást kapott.

[…]”

36 Az ezen 5. feltétel címében hivatkozott lábjegyzet kimondja:

„Az adatátvevőre vonatkozó nemzeti jogszabályok kötelező követelményei, amelyek nem lépnek túl azon, amire a 95/46/EK irányelv 13. cikkének (1) bekezdésében felsorolt érdekek valamelyike alapján egy demokratikus társadalomban szükség van; vagyis amennyiben ezek az érdekek olyan intézkedések alkalmazását írják elő, amelyek a nemzetbiztonsági, honvédelmi, közbiztonsági érdekek érvényesítését, a bűncselekmények megelőzését, a nyomozást, felderítését vagy üldözését, vagy – szabályozott szakmákban – etikai szabályok megsértését, az állam fontos gazdasági vagy pénzügyi érdekének védelmét, az érintett védelmét vagy mások jogainak vagy szabadságainak védelmét érintik, és nem ellentétesek az általános szerződési feltételekkel. […]”

37 Az ÁSZF-határozat mellékletének „Felelősség” című 6. feltétele a következőket írja elő:

„(1) A felek megállapodnak abban, hogy az érintett, aki a 3. vagy a 11. általános szerződési feltételben említett kötelezettségek egyik fél vagy a további felhasználó általi megsértésének következményeként kárt szenved, kártérítésre jogosult az adatátadótól.

(2) Amennyiben az érintett – az adatátvevőnek vagy az általa megbízott további feldolgozónak a 3. vagy a 11. általános szerződési feltételben meghatározott kötelezettsége valamelyikének megszegéséből eredően – nem tudja érvényesíteni az (1) bekezdés szerinti kártérítési igényt az adatátadóval szemben azért, mert az adatátadó ténylegesen megszűnt, jogilag megszűnt létezni vagy fizetésképtelenné vált, az adatátvevő hozzájárul ahhoz, hogy az érintett vele szemben érvényesíthesse az adatátadóval szembeni kártérítési igényét […].

[…]”

38 Az e melléklet „Együttműködés a felügyeleti hatóságokkal” című 8. feltételének (2) bekezdése a következőképpen rendelkezik:

„A felek megállapodnak abban, hogy a felügyeleti hatóságnak jogában áll az adatátvevő és valamennyi további feldolgozó ellenőrzése; az ellenőrzés hatálya és feltételei megegyeznek az alkalmazandó adatvédelmi jog értelmében az adatátadónál elvégzendő ellenőrzés hatályával és feltételeivel.”

39 Az említett melléklet „Irányadó jog” című 9. feltétele kifejti, hogy a feltételekre az adatátadó letelepedési helye szerinti tagállam joga az irányadó.

40 Az ugyanezen melléklet „További feldolgozás” című 11. feltétele értelmében:

„(1) Az adatátvevő az adatátadó előzetes írásos beleegyezése nélkül nem adhatja ki alvállalkozásba az általános szerződési feltételek alapján az adatátadó nevében végzett adatfeldolgozási tevékenységeit. Amennyiben az adatátvevő alvállalkozásba adja az általános szerződési feltételekből fakadó kötelezettségeit az adatátadó beleegyezésével, ezt kizárólag a további feldolgozóval kötött olyan írásos megállapodás útján teszi meg, amely az általános szerződési feltételek értelmében az adatátvevőre vonatkozóakkal azonos kötelezettségeket határoz meg. […]

(2) Az adatátvevő és a további feldolgozó közötti előzetes írásos megállapodás tartalmazza a kedvezményezett harmadik személyről szóló rendelkezést is – a 3. általános szerződési feltételben megállapítottak szerint – azon esetekre vonatkozóan, amikor az érintett nem tudja érvényesíteni a 6. általános szerződési feltétel (1) bekezdésében említett kártérítési igényt az adatátadóval vagy az adatátvevővel szemben azért, mert ténylegesen megszűntek, jogilag megszűntek létezni vagy fizetésképtelenné váltak, és nincs olyan jogutód, amely az adatátadó vagy az adatátvevő valamennyi jogi kötelezettségét szerződéses vagy jogszabályi úton átvállalta. A további feldolgozó harmadik féllel szembeni polgári jogi felelőssége az általános szerződési feltételek alapján végzett saját adatfeldolgozási műveleteire korlátozódik.

[…]”

41 Az ÁSZF határozat mellékletének „A személyes adatok feldolgozásának megszüntetése után fennálló kötelezettség” című 12. feltétele az (1) bekezdésében kimondja:

„A felek megállapodnak abban, hogy – amennyiben az adatátvevőre vonatkozó jogszabályok a részére továbbított személyes adatok egy részének vagy egészének visszaszolgáltatását vagy megsemmisítését nem tiltják – az adatfeldolgozás megszüntetését követően az adatátvevő és a további feldolgozó az adatátadó döntése alapján visszaszolgáltatja a számára megküldött valamennyi személyes adatot és azok másolatait az adatátadó részére, vagy megsemmisíti az összes személyes adatot, és ennek megtörténtét igazolja az adatátadó felé. […]”

Az AVP-határozat

42 A 2015. október 6-i Schrems ítéletével (C-362/14, EU:C:2015:650) a Bíróság érvénytelenítette a 95/46 irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő” adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló, 2000. július 26-i 2000/520/EK bizottsági határozatot (HL 2000. L 215., 7. o.; magyar nyelvű különkiadás 16. fejezet, 1. kötet, 119. o.), amelyben a Bizottság megállapította, hogy e harmadik ország megfelelő szintű védelmet biztosít.

43 Ezen ítélet kihirdetését követően a Bizottság elfogadta az AVP-határozatot, miután annak elfogadása céljából értékelte az Egyesült Államok szabályozását, amint azt az említett határozat (65) preambulumbekezdése kifejti:

„A Bizottság megvizsgálta az Egyesült Államok jogában rendelkezésre álló korlátozásokat és biztosítékokat az Egyesült Államok hatóságainak az [Európai Unió–Egyesült Államok] adatvédelmi pajzs alapján továbbított személyes adatokhoz való nemzetbiztonsági, bűnüldözési és egyéb közérdekű célokból történő hozzáférése, és azok ilyen célokból történő felhasználása tekintetében. Ezenfelül az Egyesült Államok kormánya a nemzeti hírszerzés igazgatójának hivatala (ODNI) […] útján részletes nyilatkozatokat és kötelezettségvállalásokat szolgáltatott a Bizottságnak, amelyeket e határozat VI. melléklete tartalmaz. A külügyminiszter által aláírt és e határozat III. mellékletében csatolt levélben az Egyesült Államok kormánya kötelezettséget vállalt arra is, hogy létrehoz egy új, a nemzetbiztonsági beavatkozással foglalkozó felügyeleti mechanizmust, az adatvédelmi ombudsmant, aki független a hírszerzéstől. Végezetül az Egyesült Államok Igazságügyi Minisztériumának e határozat VII. mellékletébe foglalt nyilatkozata ismerteti a hatóságok bűnüldözési és egyéb közérdekű célokból történő adathozzáférésére és -használatára vonatkozó korlátozásokat és biztosítékokat. Az említett kötelezettségvállalások átláthatóságának fokozása és jogi jellegének kidomborítása érdekében az e határozatban felsorolt és ahhoz mellékelt minden egyes dokumentumot közzé fognak tenni az Egyesült Államok Szövetségi Közlönyében *[U. S. Federal Register]*."

44 A Bizottságnak az e korlátozásokra és garanciákra vonatkozó elemzését az AVP-határozat (67)–(135) preambulumbekezdése foglalja össze, míg ezen intézménynek az Európai Unió–Egyesült Államok adatvédelmi pajzs keretében biztosított védelem megfelelő szintjére vonatkozó következtetései a határozat (136)–(141) preambulumbekezdésében szerepelnek.

45 E határozat (68), (69), (76), (77), (109), (112)–(116), (120), (136) és (140) preambulumbekezdése kimondja:

„(68) Az Egyesült Államok Alkotmánya értelmében a nemzetbiztonság biztosítása az elnök hatásköre főparancsnoki és államfői minőségében, a külföldi hírszerzés vonatkozásában pedig az Egyesült Államok külpolitikájának irányítójaként […]. Bár a Kongresszus hatásköre, hogy korlátozásokat állapítson meg, és ezt sokféle tekintetben meg is tette, e határok között az elnök irányíthatja az Egyesült Államok hírszerzésének tevékenységét elsősorban elnöki rendeletek és irányelvek révén. […] Jelenleg a két központi jogi eszköz e tekintetben az 12333. sz. elnöki rendelet [*Executive Order* 12333; a továbbiakban: EO 12333] […] és a 28. sz. elnöki politikai irányelv [*Presidential Policy directive* 28; a továbbiakban: PPD-28].

(69) A 2014. január 17-én kiadott [PPD-28] több korlátozást határoz meg a jelfelderítési műveletekre […]. Ez az elnöki irányelv jogilag kötelező erővel rendelkezik az Egyesült Államok hírszerzési hatóságaira nézve […], és az Egyesült Államok kormányának megváltozásáig marad hatályban [helyesen: és az Egyesült Államok kormányának megváltozását követően is hatályban marad] […]. A PPD-28 különösen fontos a nem amerikai személyek, így az uniós érintettek számára. […]

[…]

(76) Jóllehet nem ezzel a jogi kifejezéssel éltek, a [PPD-28 említett elvei] megragadják a szükségesség és arányosság elvének lényegét. […]

(77) Az elnök államfői minőségben kiadott irányelvébe foglalt, szóban forgó követelmények az összes hírszerzési szervezet számára kötelezőek, és további végrehajtásuk az ügynökségek azon szabályai és eljárásai szerint történik, amelyek az általános elveket átültetik a napi működés konkrét irányításába. […]

[…]

(109) Ezzel ellentétben a [Foreign Intelligence Surveillance Act (FISA)] 702. szakasza alapján a [United States Foreign Intelligence Surveillance Court (FISC) (az Egyesült Államok hírszerzési felügyeleti bírósága)] nem egyéni megfigyelési intézkedéseket, hanem megfigyelési programokat (mint a PRISM, UPSTREAM), engedélyez a [United States Attorney General (legfőbb ügyész)] és a [Director of National Intelligence (DNI) (nemzeti hírszerzési igazgató)] által készített éves igazolások alapján. […] Amint jeleztük, a FISC által jóváhagyott tanúsítványok nem tartalmaznak információkat a célba vett egyes egyének tekintetében, hanem a külföldi hírszerzési információk kategóriáit határozzák meg […]. Bár a FISC nem értékeli – a valószínű ok vagy bármely más standard alapján –, hogy az egyéneket megfelelően veszik-e célba a külföldi hírszerzési információk megszerzéséhez, […] a bíróság felügyelete kiterjed annak a feltételnek az ellenőrzésére, hogy »az adatszerzés jelentős célja külföldi hírszerzési információk megszerzése« […]

[…]

(112) Először is a [FISA] több olyan jogorvoslatot biztosít a jogellenes elektronikus megfigyelés megtámadására, amelyek a nem amerikai személyek számára is rendelkezésre állnak […]. Ez kiterjed az egyének azon lehetőségére, hogy pénzbeli kártérítés iránti polgári jogi keresetet indítsanak az Egyesült Államok ellen, amennyiben jogellenesen és szándékosan használták vagy hozták nyilvánosságra a velük kapcsolatos információkat […]; hogy magánszemélyi minőségükben pénzbeli kártérítés iránti keresetet indítsanak az Egyesült Államok kormányzati tisztviselőivel szemben (hivatali visszaélés) […]; továbbá hogy vitassák a megfigyelés jogszerűségét (és az információk törlését követeljék) abban az esetben, ha az Egyesült Államok kormánya az elektronikus megfigyelés során megszerzett vagy abból származó bármely információt szándékozik felhasználni vagy nyilvánosságra hozni az adott személlyel szemben, az Egyesült Államokban zajló bírósági vagy közigazgatási eljárások során […].

(113) Másrészt az Egyesült Államok kormánya a Bizottság számára hivatkozott számos további jogorvoslati lehetőségre, amelyeket az uniós érintettek felhasználhatnak ahhoz, hogy jogorvoslatot igényeljenek a kormányzati tisztviselőkkel szemben a személyes adatokhoz való jogellenes kormányzati hozzáférés vagy azok jogellenes felhasználása miatt, ideértve az elérni kívánt nemzetbiztonsági célokat […].

(114) Az Egyesült Államok kormánya végezetül rámutatott, hogy a [Freedom of information Act (FOIA), az információhoz való szabad hozzáférésről szóló törvény] olyan eszköz, amely alapján nem amerikai személyek hozzáférést igényelhetnek a meglévő szövetségi hivatali nyilvántartásokhoz, többek között azokhoz, amelyek egyének személyes adatait tartalmazzák […]. Hangsúlyának köszönhetően a FOIA nem nyújt lehetőséget egyéni jogorvoslatra önmagában véve a személyes adatokba való beavatkozással szemben, bár elvben lehetőséget biztosíthat az egyének számára, hogy hozzáférést kapjanak a nemzeti hírszerző ügynökségek birtokában lévő, releváns adatokhoz. […]

(115) Jóllehet az egyéneknek – köztük az uniós érintetteknek – tehát számos jogorvoslati lehetőség áll a rendelkezésére, ha nemzetbiztonsági célú, jogellenes (elektronikus) megfigyelést folytatnak velük szemben, az is egyértelmű, hogy e jogorvoslati lehetőségek nem terjednek ki legalább néhány olyan jogalapra (pl. az [EO 12333-ra]), amelyet az Egyesült Államok hírszerzési hatóságai igénybe vehetnek. Ezenfelül, még ha elvben léteznek is bírósági jogorvoslati lehetőségek a nem amerikai személyek számára, például a FISA alapján végzett megfigyelés esetében, a rendelkezésre álló kereseti jogcímek korlátozottak […], és az egyének (köztük az amerikai személyek) által indított kereseteket elfogadhatatlannak nyilvánítják, amennyiben nem tudnak olyan »perképességet« […] igazolni, amely korlátozza a rendes bíróságokhoz fordulást […].

(116) Annak érdekében, hogy további jogorvoslati lehetőséget biztosítson valamennyi uniós érintett számára, az Egyesült Államok kormánya úgy döntött, hogy új ombudsmani mechanizmust hoz létre, az Egyesült Államok külügyminiszterének a Bizottsághoz címzett, e határozat III. mellékletében foglalt levélben kifejtettek szerint. Ez a mechanizmus lényegesen túllép az eredeti koncepción, amely arra épül, hogy a PPD-28 alapján magas szintű koordinátort (miniszterhelyettesi szinten) neveznek ki a Külügyminisztériumban a külföldi kormányok kapcsolattartó pontjaként, akinél azok felvethetik az Egyesült Államok jelfelderítési tevékenységeivel kapcsolatos aggályaikat.

[…]

(120) Másrészt az Egyesült Államok kormánya annak biztosítására kötelezi magát, hogy az adatvédelmi pajzs ombudsmanja feladatainak ellátása során számíthat az Egyesült Államok jogában meglévő más felügyeleti és megfelelőség-felülvizsgálati mechanizmusok együttműködésére. […] Ha az említett felügyeleti szervek egyike megállapította megfelelés hiányát, a hírszerzés érintett szervezetének (pl. hírszerző ügynökségnek) orvosolnia kell a megfelelés hiányát, mivel csak ez teszi lehetővé, hogy az ombudsman »pozitív« választ adjon (vagyis hogy minden megfelelési problémát orvosoltak) annak a személynek, akivel szemben az Egyesült Államok kormánya kötelezettséget vállalt. […]

[…]

(136) A fenti megállapítások alapján a Bizottság úgy ítéli meg, hogy az Egyesült Államok megfelelő szintű védelmet biztosít az [Európai Unió–Egyesült Államok] adatvédelmi pajzs keretében az Unióból az öntanúsított egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében.

[…]

(140) Végezetül az Egyesült Államok jogrendszerével kapcsolatban rendelkezésre álló információk – többek között az Egyesült Államok kormányának nyilatkozatai és kötelezettségvállalásai – alapján a Bizottság úgy ítéli meg, hogy az Egyesült Államok hatóságainak nemzetbiztonsági, bűnüldözési vagy egyéb közérdekű célokból azon személyek alapvető jogaiba történő beavatkozása, akiknek az adatait az adatvédelmi pajzs keretében az Unióból az Egyesült Államokba továbbították, valamint ebből következően az öntanúsított vállalatokra az elvek elfogadása tekintetében meghatározott korlátozások a szóban forgó törvényes cél eléréséhez feltétlenül szükséges mértékűre fognak korlátozódni, továbbá hogy hatékony jogvédelem létezik az ilyen beavatkozással szemben.”

46 Az AVP-határozat 1. cikkének szövege szerint:

„(1) A [95/46 irányelv] 25. cikke (2) bekezdésének alkalmazásában az Egyesült Államok megfelelő szintű védelmet biztosít az [Európai Unió–Egyesült Államok] adatvédelmi pajzs keretében az Unióból az egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében.

(2) Az [Európai Unió–Egyesült Államok] adatvédelmi pajzsot az Egyesült Államok Kereskedelmi minisztériuma által 2016. július 7-én kibocsátott, a II. mellékletben ismertetett elvek, valamint az I. és a III–VII. mellékletben felsorolt dokumentumokban foglalt hivatalos nyilatkozatok és kötelezettségvállalások alkotják.

(3) Az (1) bekezdés alkalmazásában a személyes adatok az [Európai Unió–Egyesült Államok] adatvédelmi pajzs keretében kerülnek továbbításra, amennyiben az Unióból egy olyan egyesült államokbeli szervezethez továbbítják azokat, amelyet – a II. mellékletben ismertetett elvek I. és

III. szakaszának megfelelően – felvettek az »adatvédelmi pajzsban részt vevő szervezetek listájára«, amelyet az Egyesült Államok Kereskedelmi Minisztériuma vezet és a nyilvánosság számára hozzáférhetővé tesz."

47 Az AVP-határozatnak „Az [Európai Unió–Egyesült Államok] adatvédelmi pajzs keretrendszer elvei[,] kiadta az Egyesült Államok Kereskedelmi Minisztériuma" című II. melléklete I.5. pontjában előírja, hogy az elvek betartása »a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek« révén korlátozhatók.

48 E határozat III. melléklete tartalmazza az akkori Secretary of State (külügyminiszter, Egyesült Államok), John Kerry 2016. július 7-i levelét, amelyet a jogérvényesülésért, a fogyasztópolitikáért és a nemek közötti esélyegyenlőségért felelős biztoshoz írt, és amelyhez az A. mellékletben csatolták az „[Európai Unió–Egyesült Államok] adatvédelmi pajzs ombudsmani mechanizmus [a jelfelderítés tekintetében]" című feljegyzést, amely a következő szövegrészt tartalmazza:

„Jelfelderítés tekintetében az [Európai Unió–Egyesült Államok] adatvédelmi pajzs fontosságának elismeréseként ez a feljegyzés meghatározza az új mechanizmus megvalósításának a folyamatát, összhangban a jelfelderítésre vonatkozó 28. sz. elnöki rendelettel [PPD-28].

[…] Obama elnök bejelentette egy új elnöki rendelet, a PPD-28 kibocsátását, amelynek célja »világosan leírni, hogy a tengerentúli felderítési tevékenységünk keretében mit teszünk és mit nem«.

A PPD-28 4(d) pontja arra utasítja a külügyminisztert, hogy nevezzen ki egy »nemzetközi informatikai diplomáciai főkoordinátort« (főkoordinátor), »aki a kapcsolattartó lesz azon külföldi kormányok felé, amelyek aggodalmukat akarják kifejezni az Egyesült Államok jelfelderítési tevékenysége kapcsán«.

[…]

1. [A főkoordinátor] adatvédelmi pajzs ombudsmanként fog tevékenykedni és […] szorosan együttműködik más minisztériumok és hivatalok megfelelő tisztségviselőivel, akiknek feladata a kérelmek kezelése az Egyesült Államok vonatkozó jogszabályaival és politikájával összhangban. Az ombudsman független a hírszerzési közösségtől. Az ombudsman közvetlenül a külügyminiszternek tesz jelentést, aki biztosítja, hogy az ombudsman tárgyilagosan az adandó válasz megváltoztatására alkalmas, helytelen befolyásolásától mentesen láthassa el a feladatát.

[…]"

49 Az AVP-határozat VI. melléklete tartalmazza a nemzeti hírszerzés igazgatója irodájának (Office of the Director of National Intelligence) az amerikai kereskedelmi minisztérium és a nemzetközi kereskedelmi igazgatóság részére címzett 2016. június 21-i levelét, amelyben az szerepel, hogy a PPD-28 lehetővé teszi „a »nagy mennyiségű« gyűjtés[ét] viszonylag nagy mennyiségű jelfelderítési információ[nak] vagy adat[nak] olyan körülmények között, amikor a hírszerzés nem tud a konkrét célszemélyhez társítható azonosítót […] alkalmazni az adatgyűjtés fókuszálása céljából."

Az alapeljárás és az előzetes döntéshozatalra előterjesztett kérdések

50 M. Schrems, Ausztriában lakóhellyel rendelkező osztrák állampolgár 2008 óta felhasználója a Facebook közösségi hálónak (a továbbiakban: Facebook).

51 Az Unió területén lakó és a Facebookot használni kívánó valamennyi személynek a regisztráció során alá kell írnia egy szerződést az Egyesült Államokban letelepedett Facebook Inc. leányvállalatával, a Facebook Irelanddel. Az Unió területén lakóhellyel rendelkező Facebook-felhasználókra vonatkozó személyes adatokat részben vagy egészben a Facebook Inc. Egyesült Államokban található szervereire továbbítják, és azokat ott kezelik.

52 2013. június 25-én M. Schrems panaszt nyújtott be a biztoshoz, amelyben lényegében azt kérte, hogy tiltsa meg a Facebook Ireland számára a személyes adatainak az Egyesült Államokba történő továbbítását, arra hivatkozva, hogy az ebben az országban hatályban lévő jog és gyakorlat nem biztosít a területén tárolt személyes adatok számára elégséges védelmet a hatóságok által folytatott megfigyelési tevékenységekkel szemben. E panaszt többek között azzal az indokkal utasították el, hogy a Bizottság a 2000/520 határozatában megállapította, hogy az Egyesült Államok megfelelő védelmi szintet biztosít.

53 A High Court (felsőbíróság, Írország), amely előtt M. Schrems keresetet nyújtott be panaszának elutasításával szemben, előzetes döntéshozatal iránti kérelmet terjesztett a Bíróság elé a 2000/520 határozat értelmezésére és érvényességére vonatkozóan. A Bíróság a 2015. október 6-i Schrems ítéletben (C-362/14, EU:C:2015:650) e határozatot érvénytelennek nyilvánította.

54 Ezen ítéletet követően a kérdést előterjesztő bíróság megsemmisítette M. Schrems panaszának elutasítását, és e panaszt visszautalta a biztos elé. Az utóbbi által megindított vizsgálat keretében a Facebook Ireland kifejtette, hogy a személyes adatok nagy részét az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötések alapján továbbították a Facebook Inc. részére. E tényezőkre tekintettel a biztos felhívta M. Schremset panaszának újrafogalmazására.

55 Az így újrafogalmazott és 2015. december 1-jén benyújtott panaszában M. Schrems többek között arra hivatkozott, hogy az amerikai jog arra kötelezi a Facebook Inc.-t, hogy a neki továbbított személyes adatokat az amerikai hatóságok, így a National Security Agency (NSA) és a Federal Bureau of Investigation (FBI) rendelkezésére bocsássa. Azt állította, hogy mivel ezeket az adatokat különböző megfigyelési programok keretében a Charta 7., 8. és 47. cikkével összeegyeztethetetlen módon használták fel, az ÁSZF-határozat nem igazolhatja az említett adatoknak az Egyesült Államokba történő továbbítását. E körülmények között M. Schrems azt kérte a biztostól, hogy tiltsa meg vagy függessze fel személyes adatainak a Facebook Inc. részére történő továbbítását.

56 2016. május 24-én a biztos a vizsgálatának ideiglenes következtetéseit összefoglaló „határozattervezetet” tett közzé. Ebben a tervezetben ideiglenesen úgy ítélte meg, hogy fennáll a veszélye annak, hogy az uniós polgároknak az Egyesült Államokba továbbított személyes adataihoz az amerikai hatóságok olyan módon férnek hozzá, és azokat olyan módon kezelik, amely összeegyeztethetetlen a Charta 7. és 8. cikkével, valamint hogy az Egyesült Államok joga nem biztosít e polgárok számára a Charta 47. cikkével összeegyeztethető jogorvoslati lehetőségeket. A biztos úgy ítélte meg, hogy az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötések nem orvosolják ezt a hiányosságot, mivel az érintett személyek számára kizárólag szerződéses jogokat biztosítanak az adatok átadójával és átvevőjével szemben, anélkül azonban, hogy kötnék az amerikai hatóságokat.

57 Mivel a biztos úgy vélte, hogy e körülmények között M. Schrems újrafogalmazott panasza felvetette az ÁSZF-határozat érvényességének kérdését, 2016. május 31-én a High Courthoz (felsőbíróság) fordult a 2015. október 6-i Schrems ítéletből (C-362/14, EU:C:2015:650, 65. pont) eredő ítélkezési gyakorlatra támaszkodva, annak érdekében, hogy ez utóbbi ezzel kapcsolatban kérdést intézzen a Bírósághoz. 2018. május 4-i határozatával a High Court (felsőbíróság) a jelen előzetes döntéshozatal iránti kérelemmel fordult a Bírósághoz.

58 A High Court (felsőbíróság) ezen előzetes döntéshozatal iránti kérelemhez mellékelt egy 2017. október 3-án kihirdetett ítéletet, amelyben rögzítette a nemzeti eljárás keretében elé terjesztett bizonyítékok vizsgálatának eredményét, amely eljárásban az amerikai kormány is részt vett.

59 Ebben az ítéletben, amelyre az előzetes döntéshozatal iránti kérelem több alkalommal hivatkozik, a kérdést előterjesztő bíróság rámutatott, hogy főszabály szerint nemcsak jogosult, hanem köteles is megvizsgálni az elé terjesztett valamennyi tényt és érvet annak érdekében, hogy azok alapján eldöntse, hogy szükséges-e az előzetes döntéshozatal iránti kérelem, vagy sem. Mindenesetre köteles figyelembe venni a jog azon esetleges módosításait, amelyek a kereset benyújtása és az előtte tartott tárgyalás között következtek be. E bíróság pontosította, hogy az alapeljárás keretében a saját értékelése nem korlátozódik a biztos által felhozott érvénytelenségi jogalapokra, így hivatalból más érvénytelenségi jogalapokra is hivatkozhat, és ezek alapján előzetes döntéshozatal iránti kérelmet terjeszthet elő.

60 Az említett ítéletben szereplő megállapítások szerint az amerikai hatóságoknak az Egyesült Államokba továbbított személyes adatokra vonatkozó hírszerző tevékenységei többek között a FISA 702. cikkén és az EO 12333-on alapulnak.

61 A FISA 702. cikkét illetően a kérdést előterjesztő bíróság ugyanebben az ítéletben pontosítja, hogy e cikk lehetővé teszi a legfőbb ügyész és a nemzeti hírszerzési igazgató számára, hogy a FISC jóváhagyását követően a „külföldi hírszerzési információk” megszerzése céljából közösen engedélyezzék az Egyesült Államok területén kívül tartózkodó nem amerikai állampolgárok megfigyelését, és az többek között a PRISM és az UPSTREAM megfigyelési programok alapjául szolgál. A PRISM program keretében az internetszolgáltatók e bíróság megállapításai szerint kötelesek az NSA-nak minden, „kiválasztási tényező” [selector] révén küldött és kapott közlést továbbítani, amelyek egy részét megküldik az FBI és a Central Intelligence Agency (CIA) (Központi Hírszerző Ügynökség) részére is.

62 Az UPSTREAM programot illetően az említett bíróság megállapította, hogy e program keretében az internetes „gerinchálózatot”– vagyis a kábelek, kapcsolók és routerek hálózatát – üzemeltető távközlési vállalkozások kötelesek lehetővé tenni az NSA számára az internetes forgalom másolását és szűrését annak érdekében, hogy összegyűjtse a „kiválasztási tényező” révén megcélzott nem amerikai állampolgár által vagy vele kapcsolatban továbbított, illetve őt érintő közlést. Az említett program keretében az NSA – ugyanezen bíróság megállapításai szerint – hozzáfér mind az érintett közlések metaadataihoz, mind azok tartalmához.

63 Ami az EO 12333-at illeti, a kérdést előterjesztő bíróság megállapítja, hogy az lehetővé teszi az NSA számára, hogy az Egyesült Államokba irányuló „átmenő” adatokhoz hozzáférjen az Atlanti-óceán fenekén elhelyezett tenger alatti kábelekhez való hozzáférés révén, valamint hogy ezeket az adatokat összegyűjtse és megőrizze azt megelőzően, hogy azok megérkeznek az Egyesült Államokba és ott a FISA rendelkezéseinek hatálya alá kerülnek. Kifejti, hogy az EO 12333 alapján végzett tevékenységeket nem szabályozza törvény.

64 A hírszerző tevékenység korlátait illetően a kérdést előterjesztő bíróság arra a tényre helyezi a hangsúlyt, hogy a nem amerikai személyek kizárólag a PPD-28 hatálya alá tartoznak, és hogy ez utóbbi csupán azt állapítja meg, hogy a hírszerző tevékenységeknek „a lehető legcélzottabbnak” *(as tailored as feasible)* kell lenniük. A megállapításai alapján az említett bíróság úgy véli, hogy az Egyesült Államok tömeges adatkezelést végez, anélkül hogy a Charta 7. és 8. cikkében biztosított védelemmel lényegében azonos védelmet biztosítana.

65 A bírói jogvédelmet illetően ugyanezen bíróság kifejti, hogy az uniós polgárok nem férhetnek hozzá ugyanazon jogorvoslatokhoz, mint amelyekkel az amerikai állampolgárok rendelkeznek az amerikai hatóságok által végzett személyesadat-kezeléssel szemben, mivel a Constitution of the United States (az Egyesült Államok alkotmánya) negyedik kiegészítése, amely a legfontosabb védelmet jelenti a jogellenes megfigyeléssel szemben, nem alkalmazható az uniós polgárokra. E tekintetben a kérdést előterjesztő bíróság pontosítja, hogy az ez utóbbiak rendelkezésére álló egyéb jogorvoslatok jelentős akadályokba, különösen a kereshetőségi joguk – szerinte túlzottan nehezen teljesíthető – igazolására vonatkozó kötelezettségbe ütköznek. Egyébiránt e bíróság megállapításai szerint az NSA EO 12333-on alapuló tevékenységei nem tartoznak bírósági felügyelet alá, és nem lehet velük kapcsolatban bírósági jogorvoslattal élni. Végül az említett bíróság úgy véli, hogy mivel álláspontja szerint az adatvédelmi

pajzs ombudsmanja nem minősül a Charta 47. cikke értelmében vett bíróságnak, az amerikai jog nem biztosít az uniós polgárok számára az e cikkben szentesített alapvető jog által biztosított védelmi szinttel lényegében azonos védelmi szintet.

66 Előzetes döntéshozatal iránti kérelmében a kérdést előterjesztő bíróság pontosítja továbbá, hogy az alapeljárásban részt vevő felek nem értenek egyet többek között abban a kérdésben, hogy alkalmazható-e az uniós jog az olyan személyes adatok harmadik országba történő továbbítására, amelyeket ezen ország hatóságai többek között nemzetbiztonsági célból kezelhetnek, valamint hogy mely tényezőket kell figyelembe venni az említett ország által biztosított megfelelő védelmi szint értékelése céljából. E bíróság különösen azt állapítja meg, hogy a Facebook Ireland szerint a Bizottságnak a harmadik ország által biztosított védelmi szint megfelelőségére vonatkozó megállapításai, mint amelyek az AVP-határozatban szerepelnek, kötik a felügyeleti hatóságokat az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötéseken alapuló személyesadat-továbbítással összefüggésben is.

67 Ami ezen általános adatvédelmi kikötéseket illeti, az említett bíróság azt kérdezi, hogy az ÁSZF-határozat érvényesnek tekinthető-e, noha ugyanezen bíróság szerint az említett kikötések nem kötelezőek az érintett harmadik ország állami hatóságaira nézve, és ennélfogva nem alkalmasak arra, hogy orvosolják a megfelelő védelmi szint ezen országban esetlegesen fennálló hiányát. E tekintetben e bíróság úgy véli, hogy a 2010/87 határozat 4. cikke (1) bekezdése a) pontjának a 2016/2297 végrehajtási határozat hatálybalépését megelőző változata által a tagállamok illetékes hatóságai számára elismert azon lehetőség, hogy megtiltsák a személyes adatoknak az adatátvevő számára az ugyanezen kikötésekben foglalt biztosítékokkal összeegyeztethetetlen kötelezettségeket előíró harmadik országba történő továbbítását, azt bizonyítja, hogy a harmadik ország jogának állapota az – akár az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötések alapján megvalósított – adattovábbítás nyilvánvaló tilalmát igazolhatja, és így alátámasztja, hogy azok elégtelenek lehetnek a megfelelő védelem biztosításához. Mindemellett a kérdést előterjesztő bíróság arra keresi a választ, hogy milyen terjedelmű a biztosnak az e kikötéseken alapuló adattovábbításra vonatkozó jogköre, úgy ítélve meg, hogy a diszkrecionális jogkör nem lehet elegendő a megfelelő védelem biztosításához.

68 E körülmények között a High Court (felsőbíróság) úgy határozott, hogy az eljárást felfüggeszti, és előzetes döntéshozatal céljából a következő kérdéseket terjeszti a Bíróság elé:

„(1) Olyan körülmények között, amikor valamely magánvállalkozás az [Unió] tagállamából harmadik országbeli magánvállalkozás részére kereskedelmi célból személyes adatot továbbít [az ÁSZF-határozat] alapján, és a szóban forgó harmadik országban annak hatóságai nemzetbiztonsági célból, ezen felül azonban bűnüldözési célból, valamint e harmadik ország külügyi tevékenysége céljából is e személyes adatok további kezelését végezhetik, az EUSZ 4. cikk (2) bekezdésének nemzeti biztonsággal kapcsolatos rendelkezései és a [95/46 irányelv] 3. cikke (2) bekezdésének első francia bekezdésében foglalt, a közbiztonsággal, a védelemmel és a nemzetbiztonsággal kapcsolatos rendelkezései ellenére alkalmazható-e az uniós jog (ideértve [a Chartát]) az adattovábbításra?

2) a) Annak meghatározása során, hogy sérti-e valamely magánszemély jogát az [Unióból] [az ÁSZF-határozat] alapján harmadik országba irányuló adattovábbítás, ahol ezeket az adatokat nemzetbiztonsági okból további kezelés alá vonhatják, vajon a vonatkozó összehasonlítási alap [a 95/46 irányelv] értelmében:
   i. a Charta, az EU-Szerződés, az EUM-Szerződés, [a 95/46 irányelv], [a Rómában 1950. november 4-én aláírt, az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény; kihirdette: 1993. évi XXXI. törvény; a továbbiakban: EJEE] (vagy az uniós jog valamely más rendelkezése); vagy
   ii. egy vagy több tagállam nemzeti jogszabályai?
   b) Amennyiben a [ii. alpont] a vonatkozó összehasonlítási alap, be kell-e vonni az összehasonlítási alapba egy vagy több tagállam nemzetbiztonsággal kapcsolatos gyakorlatát?

3) Annak értékelése során, hogy valamely harmadik ország [a 95/46 irányelv] 26. cikke értelmében biztosítja-e az uniós jog által a szóban forgó országba továbbított személyes adatokkal összefüggésben megkövetelt szintű védelmet, a védelem e harmadik országban biztosított szintjét az alábbiak közül melyekre való hivatkozással kell vizsgálni:
   a) a harmadik országban a saját nemzeti jogszabályaiból vagy nemzetközi kötelezettségvállalásaiból eredően alkalmazandó szabályokra, és az e szabályokkal való összhang biztosítását szolgáló gyakorlatra, beleértve a harmadik országban érvényesülő szakmai szabályokat és biztonsági intézkedéseket;

      vagy
   b) az a) pontban hivatkozott szabályokra az adott harmadik országban fennálló közigazgatási, szabályozási és megfelelőségi gyakorlattal és szakpolitikai biztosítékokkal, eljárásokkal, protokollokkal, felügyeleti mechanizmusokkal és bíróságon kívüli jogorvoslatokkal együtt?

4) Tekintettel a High Court (felsőbíróság) által az Egyesült Államok jogával kapcsolatban tett ténymegállapításokra, sérti-e a magánszemélyeknek a Charta 7. és/vagy 8. cikkében foglalt jogait, ha a személyes adatokat [az Unióból] az Egyesült Államokba [az ÁSZF-határozat] alapján továbbítják?

5) Tekintettel a High Court (felsőbíróság, Írország) által az Egyesült Államok jogával kapcsolatban tett ténymegállapításokra, ha a személyes adatokat az EU-ból az Egyesült Államokba az [ÁSZF-határozat] alapján továbbítják:
   a) Az Egyesült Államok által biztosított védelem szintje tiszteletben tartja-e a Charta 47. cikke által a magánszemélyeknek az adatvédelmi jogai megsértése miatti bírósági jogorvoslathoz való joga lényegét?

      Az 5) a) kérdésre adandó igenlő válasz esetén:
   b) Az Egyesült Államok jogában előírt, valamely magánszemély bírósági jogorvoslathoz való jogának az Egyesült Államok nemzetbiztonságával összefüggésben való korlátozása arányos-e a Charta 52. cikkének értelmében, és nem haladja-e meg azt, ami egy demokratikus társadalomban nemzetbiztonsági szempontból szükséges?

6) a) Milyen szintű védelmet kell biztosítani a harmadik országokba [a 95/46 irányelv 26. cikkének (4) bekezdése] szerint hozott bizottsági határozatnak megfelelően elfogadott általános szerződési feltételek alapján továbbított személyes adatok tekintetében, figyelemmel [ezen] irányelv rendelkezéseire, és különösen a Chartával összhangban értelmezett 25. és 26. cikkére?
   b) Milyen szempontokat szükséges figyelembe venni annak értékelése során, hogy valamely harmadik országba [az ÁSZF-határozat] alapján továbbított adatok tekintetében biztosított védelem szintje megfelel-e [a 95/46 irányelvben] és a Chartában foglalt követelményeknek?

7) Az a körülmény, hogy az általános szerződési feltételek az adatátadó és az adatátvevő között érvényesülnek, és valamely harmadik ország nemzeti hatóságaira nézve nem kötelezőek, amely ország előírhatja az adatátadó részére, hogy a biztonsági szolgálatai számára további adatkezelés céljából tegye hozzáférhetővé [az ÁSZF-határozatban] megállapított feltételek alapján továbbított személyes adatokat, megakadályozza-e, hogy e feltételek megfelelő garanciákat teremtsenek, amint azt [a 95/46 irányelv] 26. cikkének (2) bekezdése előírja?

8) Amennyiben valamely harmadik országbeli adatátvevő felügyeleti jogszabályok hatálya alá tartozik, ami az adatvédelmi hatóság álláspontja szerint az [ÁSZF-határozat] mellékletében foglalt feltételekbe vagy az irányelv 25. és 26. cikkébe és/vagy a Charta rendelkezéseibe ütközik, az adatvédelmi hatóság köteles-e gyakorolni az irányelv 28. cikkének (3) bekezdése szerinti végrehajtási jogkörét az adatáramlás felfüggesztése iránt vagy az ilyen jogosultságok gyakorlása, figyelemmel az irányelv (11) preambulumbekezdésében [az ÁSZF-határozat

(11) preambulumbekezdésében] foglaltakra, kizárólag kivételes esetekre korlátozódik, vagy pedig az adatvédelmi hatóság saját mérlegelési jogkörében eljárva dönthet úgy, hogy nem függeszti fel az adatáramlást?

9) a) [A 95/46 irányelv] 25. cikkének (6) bekezdése értelmében [az AVP-határozat] olyan általános hatályú, a tagállamok [felügyeleti hatóságaira] és bíróságaira nézve kötelező megállapításnak minősül, amely alapján az [Egyesült Államok] [a 95/46 irányelv] 25. cikkének (2) bekezdése értelmében a nemzeti joga, illetve az általa vállalt nemzetközi kötelezettségek révén megfelelő szintű védelmet biztosít?
   b) Amennyiben nem biztosít megfelelő szintű védelmet, adott esetben milyen jelentősége van az [AVP-határozatnak] az Egyesült Államokba az [ÁSZF-határozat] alapján továbbított adatok tekintetében nyújtott biztosítékok megfelelőségének vizsgálata során?

10) Tekintettel a High Court (felsőbíróság) által az Egyesült Államok jogával kapcsolatban tett ténymegállapításokra, az [AVP-határozat] III. mellékletének A. mellékletében foglalt, adatvédelmi ombudsmanra vonatkozó rendelkezés, amennyiben azt az Egyesült Államok fennálló rendszerével összefüggésben értelmezzük, gondoskodik-e arról, hogy az USA a Charta 47. cikkével összeegyeztethető jogorvoslatot biztosít azon érintettek számára, akiknek a személyes adatait az [ÁSZF-határozat] alapján az Egyesült Államokba továbbítják?

11) Sérti-e az [ÁSZF-határozat] a Charta 7., 8. és/vagy 47. cikkében foglaltakat?”

Az előzetes döntéshozatal iránti kérelem elfogadhatóságáról

69 A Facebook Ireland, valamint a német kormány és az Egyesült Királyság kormánya arra hivatkozik, hogy az előzetes döntéshozatal iránti kérelem elfogadhatatlan.

70 A Facebook Ireland által felhozott kifogást illetően e társaság megjegyzi, hogy a 95/46 irányelv azon rendelkezéseit, amelyeken az előzetes döntéshozatalra előterjesztett kérdések alapulnak, a GDPR hatályon kívül helyezte.

71 E tekintetben igaz ugyan, hogy a 95/46 irányelvet a GDPR 94. cikkének (1) bekezdése értelmében 2018. május 25-i hatállyal hatályon kívül helyezték, ezen irányelv még hatályban volt a Bírósághoz 2018. május 9-én érkezett jelen előzetes döntéshozatal iránti kérelem 2018. május 4-i megfogalmazásakor. Ezenkívül a 95/46 irányelv 3. cikke (2) bekezdésének első francia bekezdését, 25. és 26. cikkét, valamint 28. cikkének (3) bekezdését, amelyekre az előzetes döntéshozatalra előterjesztett kérdések hivatkoznak, lényegében átvette a GDPR 2. cikkének (2) bekezdése, illetve 45., 46. és 58. cikke. Egyébiránt emlékeztetni kell arra, hogy a Bíróság feladata az uniós jog minden olyan rendelkezésének értelmezése, amelyre a nemzeti bíróságoknak az eléjük terjesztett jogviták eldöntése érdekében szükségük van, még akkor is, ha e bíróságok az általuk feltett kérdésekben nem jelölik meg kifejezetten ezeket a rendelkezéseket (2020. április 2-i Ruska Federacija ítélet, C-897/19 PPU, EU:C:2020:262, 43. pont, valamint az ott hivatkozott ítélkezési gyakorlat). E különböző okok miatt az a körülmény, hogy az előterjesztő bíróság az előzetes döntéshozatalra előterjesztett kérdéseket kizárólag a 95/46 irányelv rendelkezéseire hivatkozva fogalmazta meg, nem vonja maga után a jelen előzetes döntéshozatal iránti kérelem elfogadhatatlanságát.

72 A maga részéről a német kormány az elfogadhatatlansági kifogását arra a körülményre alapítja, hogy egyrészt a biztos az ÁSZF-határozat érvényességével kapcsolatban csak kétségeket, nem pedig végleges véleményt fejtett ki, másrészt pedig arra, hogy a kérdést előterjesztő bíróság tartózkodott annak vizsgálatától, hogy M. Schrems vitathatatlanul hozzájárult-e az alapügyben szóban forgó adattovábbításhoz, ami – ha ez lett volna a helyzet – azzal a hatással járna, hogy szükségtelenné tenné

az e kérdésre adandó választ. Végül az Egyesült Királyság kormánya szerint az előzetes döntéshozatalra előterjesztett kérdések hipotetikus jellegűek, mivel e bíróság nem állapította meg, hogy ezeket az adatokat ténylegesen az említett határozat alapján továbbították.

73 A Bíróság állandó ítélkezési gyakorlatából következik, hogy kizárólag az alapeljárásban eljáró és a meghozandó bírósági döntésért felelős nemzeti bíróság jogosult mérlegelni – az ügy sajátosságaira figyelemmel – egyrészt az előzetes döntéshozatal szükségességét annak érdekében, hogy döntését meghozhassa, másrészt azt, hogy a Bíróság számára feltett kérdések relevánsak-e. Következésképpen, amennyiben a feltett kérdések valamely uniós jogi rendelkezés értelmezésére vagy érvényességére vonatkoznak, a Bíróság – főszabály szerint – köteles határozatot hozni. Ebből következik, hogy a nemzeti bíróságok által előterjesztett kérdések releváns voltát vélelmezni kell. A nemzeti bíróságok által előterjesztett előzetes döntéshozatal iránti kérelem Bíróság általi elutasítása csak abban az esetben lehetséges, ha nyilvánvaló, hogy a kért értelmezés nem függ össze az alapeljárás tényállásával vagy tárgyával, illetve ha a szóban forgó probléma hipotetikus jellegű, vagy a Bíróság nem rendelkezik azon ténybeli és jogi elemek ismeretével, amelyek szükségesek ahhoz, hogy az említett kérdésekre hasznos választ adjon (2015. június 16-i Gauweiler és társai ítélet, C-62/14, EU:C:2015:400, 24. és 25. pont; 2018. október 2-i Ministerio Fiscal ítélet, C-207/16, EU:C:2018:788, 45. pont; 2019. december 19-i Dobersberger ítélet, C-16/18, EU:C:2019:1110, 18. és 19. pont).

74 A jelen ügyben az előzetes döntéshozatal iránti kérelem elegendő ténybeli és jogi elemet tartalmaz az előzetes döntéshozatalra előterjesztett kérdések terjedelmének megértéséhez. Ezenkívül és legfőképpen, a Bíróság rendelkezésére álló iratok egyike sem teszi lehetővé annak megállapítását, hogy az uniós jog kért értelmezése ne függene össze az alapeljárás tényállásával vagy tárgyával, illetve hogy hipotetikus jellegű lenne többek között amiatt, hogy az alapügyben szóban forgó személyes adatok továbbítása az érintettnek az e továbbításhoz való kifejezett hozzájárulásán, nem pedig az ÁSZF-határozaton alapul. Az e kérelemben szereplő információk szerint ugyanis a Facebook Ireland elismerte, hogy a Facebook Inc.-nek továbbítja az Unióban lakóhellyel rendelkező felhasználóinak személyes adatait, és hogy ezen adattovábbítások nagy része, amelynek jogszerűségét M. Schrems vitatja, az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötések alapján történik.

75 Egyébiránt a jelen előzetes döntéshozatal iránti kérelem elfogadhatósága szempontjából nincs jelentősége annak, hogy a biztos nem fejtette ki végleges álláspontját e határozat érvényességét illetően, mivel a kérdést előterjesztő bíróság úgy véli, hogy az uniós jog szabályainak értelmezése és érvényessége vonatkozásában előzetes döntéshozatalra előterjesztett kérdések megválaszolása szükséges az alapjogvita elbírálásához.

76 Ebből az következik, hogy az előzetes döntéshozatal iránti kérelem elfogadható.

Az előzetes döntéshozatalra előterjesztett kérdésekről

77 Előzetesen emlékeztetni kell arra, hogy a jelen előzetes döntéshozatal iránti kérelem M. Schrems panaszából ered, amely arra irányul, hogy a biztos rendelje el a jövőre nézve a személyes adatainak a Facebook Ireland által a Facebook Inc. részére történő továbbításának felfüggesztését vagy megtiltását. Márpedig, jóllehet az előzetes döntéshozatalra előterjesztett kérdések a 95/46 irányelv rendelkezéseire hivatkoznak, nem vitatott, hogy a biztos még nem hozott végleges határozatot e panaszról, amikor ezt az irányelvet 2018. május 25-i hatállyal hatályon kívül helyezte és felváltotta a GDPR.

78 A nemzeti határozat e hiánya megkülönbözteti az alapügyben szóban forgó helyzetet a 2019. szeptember 24-i Google (Linkek közüli törlés területi hatálya) ítélet (C-507/17, EU:C:2019:772) és a 2019. október 1-jei Planet49 ítélet (C-673/17, EU:C:2019:801) alapjául szolgáló helyzetektől, amelyekben az említett irányelv hatályon kívül helyezését megelőzően elfogadott határozatokról volt szó.

79 Ennélfogva az előzetes döntéshozatalra előterjesztett kérdésekre a GDPR rendelkezéseire, nem pedig a 95/46 irányelv rendelkezéseire tekintettel kell választ adni.

Az első kérdésről

80 Az első kérdésével az előterjesztő bíróság lényegében arra vár választ, hogy a GDPR 2. cikkének (1) bekezdését és 2. cikke (2) bekezdésének a), b) és d) pontját az EUSZ 4. cikk (2) bekezdésével összefüggésben úgy kell-e értelmezni, hogy e rendelet hatálya alá tartozik a személyes adatoknak a valamely tagállamban letelepedett gazdasági szereplő által harmadik országban letelepedett másik gazdasági szereplő részére végzett továbbítása, amennyiben ezeket az adatokat e továbbítás során vagy azt követően ezen ország hatóságai közbiztonsági, honvédelmi és nemzetbiztonsági célból kezelhetik.

81 E tekintetben először is meg kell állapítani, hogy az EUSZ 4. cikk (2) bekezdésében foglalt rendelkezés, amely szerint az Unión belül a nemzeti biztonság az egyes tagállamok kizárólagos feladata marad, kizárólag az Unió tagállamait érinti. Következésképpen e rendelkezés a jelen ügyben nem releváns a GDPR 2. cikke (1) bekezdésének és 2. cikke (2) bekezdése a), b) és d) pontjának értelmezése szempontjából.

82 A GDPR 2. cikkének (1) bekezdése értelmében e törvényt kell alkalmazni a személyes adatok részben vagy egészben automatizált feldolgozására, valamint azoknak a személyes adatoknak a nem automatizált módon való feldolgozására, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni. E rendelet 4. cikkének 2. pontja úgy határozza meg a „kezelés” fogalmát, mint „a személyes adatokon automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége”, és példaként a „közléstovábbítás[t], terjesztés[t] vagy egyéb módon történő hozzáférhetővé tétel[t]” hozza fel, anélkül hogy különbséget tenne aszerint, hogy e műveletekre az Unión belül került-e sor, vagy azok harmadik országhoz kapcsolódnak. Ezenkívül az említett rendelet a személyes adatok harmadik országokba irányuló továbbítását „A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása” című V. fejezetében szereplő különös szabályoknak veti alá, és egyébiránt az ugyanezen rendelet 58. cikke (2) bekezdésének j) pontjában szereplő, erre vonatkozó különös jogkörökkel ruházza fel a felügyeleti hatóságokat.

83 Ebből következik, hogy a személyes adatok valamely tagállamból egy harmadik országba való továbbítására irányuló művelet önmagában a GDPR 4. cikkének 2. pontja értelmében vett, valamely tagállam területén végzett személyesadat-kezelésnek minősül, amelyre e rendelet a 2. cikkének (1) bekezdése értelmében alkalmazandó (lásd analógia útján a 95/46 irányelv 2. cikkének b) pontját és 3. cikkének (1) bekezdését illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 45. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

84 Ami azt a kérdést illeti, hogy az ilyen művelet tekinthető-e úgy, mint amely a GDPR 2. cikkének (2) bekezdése értelmében ki van zárva annak hatálya alól, emlékeztetni kell arra, hogy e rendelkezés kivételeket ír elő e rendeletnek a 2. cikkének (1) bekezdésében meghatározott hatálya alól, és hogy ezeket a kivételeket szigorúan kell értelmezni (lásd analógia útján a 95/46 irányelv 3. cikke (2) bekezdését illetően: 2018. július 10-i Jehovan Todistajat ítélet, C-25/17, EU:C:2018:551, 37. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

85 A jelen ügyben, mivel a személyes adatoknak a Facebook Ireland által a Facebook Inc. részére, azaz két jogi személy között történő továbbítását a Facebook Ireland végzi, e továbbítás nem tartozik a GDPR 2. cikke (2) bekezdése c) pontjának hatálya alá, amely a természetes személyek által kizárólag személyes vagy otthoni tevékenységük keretében végzett adatkezelésre vonatkozik. Az említett adattovábbítás nem tartozik az e rendelet 2. cikke (2) bekezdésének a), b) és d) pontjában szereplő kivételek közé sem, mivel az ott példaként említett tevékenységek minden esetben az állam vagy az

állami hatóságok sajátos tevékenységei, és nem tartoznak a magánszemélyek tevékenységei közé (lásd analógia útján a 95/46 irányelv 3. cikke (2) bekezdését illetően: 2018. július 10-i Jehovan Todistajat ítélet, C-25/17, EU:C:2018:551, 38. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

86 Márpedig az a lehetőség, hogy a két gazdasági szereplő között kereskedelmi célból továbbított személyes adatokat a továbbítás során vagy azt követően az érintett harmadik ország hatóságai által közbiztonsági, honvédelmi és nemzetbiztonsági célból adatkezelés alá vonhatják, nem zárhatja ki az említett továbbítást a GDPR hatálya alól.

87 Egyébiránt még az említett rendelet 45. cikke (2) bekezdése a) pontjának szövege is azáltal, hogy kifejezetten arra kötelezi a Bizottságot, hogy a harmadik ország által biztosított védelmi szint megfelelőségének értékelése során vegye figyelembe többek között „a vonatkozó általános és ágazati jogszabályok[at], köztük a közbiztonságra, a védelemre, valamint a nemzetbiztonságra vonatkozó és a büntetőjogi rendelkezések[et], a közhatalmi szerveknek a személyes adatokhoz való hozzáférését szabályozó rendelkezések[et], valamint e jogszabályok végrehajtás[át]”, arra helyezi a hangsúlyt, hogy a valamely harmadik ország által közbiztonsági, honvédelmi és nemzetbiztonsági célból történő adatkezelés nem kérdőjelezi meg, hogy az említett rendelet alkalmazható a szóban forgó adattovábbításra.

88 Ebből következik, hogy az ilyen továbbítás nem kerülhet ki a GDPR hatálya alól azzal az indokkal, hogy a szóban forgó adatokat az érintett harmadik ország hatóságai e továbbítás során vagy azt követően közbiztonsági, honvédelmi és nemzetbiztonsági célból kezelhetik.

89 Következésképpen az első kérdésre azt a választ kell adni, hogy a GDPR 2. cikkének (1) és (2) bekezdését úgy kell értelmezni, hogy e rendelet hatálya alá tartozik a személyes adatoknak a valamely tagállamban letelepedett gazdasági szereplő által valamely harmadik országban letelepedett másik gazdasági szereplő részére kereskedelmi célból végzett továbbítása, függetlenül attól, hogy ezeket az adatokat e továbbítás során vagy azt követően az érintett harmadik ország hatóságai közbiztonsági, honvédelmi és nemzetbiztonsági célból kezelhetik.

A második, harmadik és hatodik kérdésről

90 A második, harmadik és hatodik kérdésével az előterjesztő bíróság lényegében a személyes adatok harmadik országba történő, általános adatvédelmi kikötéseken alapuló továbbítása keretében a GDPR 46. cikkének (1) bekezdésében és 46. cikke (2) bekezdésének c) pontjában megkövetelt védelmi szintről kérdezi a Bíróságot. E bíróság különösen azt kéri a Bíróságtól, hogy pontosítsa azokat az elemeket, amelyeket figyelembe kell venni annak meghatározása érdekében, hogy e védelmi szint biztosított-e az ilyen adattovábbítással összefüggésben.

91 Ami a védelem megkövetelt szintjét illeti, e rendelkezések együttes olvasatából az következik, hogy az e rendelet 45. cikkének (3) bekezdése alapján elfogadott megfelelőségi határozat hiányában az adatkezelő vagy az adatfeldolgozó csak akkor továbbíthat személyes adatokat harmadik országba, ha az „megfelelő garanciákat” írt elő, és feltéve, hogy az érintett személyek számára „érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre”, és e megfelelő garanciákként különösen a Bizottság által elfogadott általános adatvédelmi kikötések szolgálhatnak.

92 Bár a GDPR 46. cikke nem határozza meg a „megfelelő garanciákra”, az „érvényesíthető jogokra” és a „hatékony jogorvoslati lehetőségekre” való utalásból eredő követelmények jellegét, meg kell állapítani, hogy e cikk e rendelet V. fejezetében szerepel. Következésképpen az említett cikket az említett rendeletnek „Az adattovábbításra vonatkozó általános elv” című 44. cikkére tekintettel kell értelmezni, és az úgy rendelkezik, hogy „[a]z [e fejezet] valamennyi rendelkezését alkalmazni kell annak biztosítása

érdekében, hogy a természetes személyek számára [az ugyanezen] rendeletben biztosított védelem szintje ne sérüljön”. E védelmi szintet következésképpen az említett fejezet azon rendelkezésétől függetlenül kell biztosítani, amely alapján a személyes adatokat harmadik országba továbbítják.

93 Ugyanis, amint arra a főtanácsnok az indítványának 117. pontjában rámutatott, a GDPR V. fejezete rendelkezéseinek célja e védelem magas szintjének folyamatos fenntartása a személyes adatok harmadik országba irányuló továbbítása esetén, az e rendelet (6) preambulumbekezdésében kifejtett célnak megfelelően.

94 A GDPR 45. cikke (1) bekezdésének első mondata előírja, hogy a személyes adatok harmadik országba irányuló továbbítása a Bizottság által hozott olyan határozattal engedélyezhető, amely szerint ez a harmadik ország, ennek valamely területe, vagy egy vagy több meghatározott ágazata megfelelő védelmi szintet biztosít. E tekintetben, anélkül hogy megkövetelné, hogy az érintett harmadik ország az uniós jogrendben biztosítottal megegyező védelmi szintet biztosítson, a „megfelelő védelmi szint” kifejezést – amint azt e rendelet (104) preambulumbekezdése megerősíti – úgy kell érteni, mint amely megköveteli, hogy e harmadik ország – belföldi joga, vagy vállalt nemzetközi kötelezettségei alapján – az említett – Chartával összefüggésben értelmezett – rendelet által az Unióban biztosított védelmi szinttel lényegében azonos védelmi szintet biztosítson ténylegesen az alapvető jogok és szabadságok számára. E követelmény hiányában ugyanis figyelmen kívül maradna az előző pontban említett célkitűzés (lásd analógia útján a 95/46 irányelv 25. cikkének (6) bekezdését illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 73. pont).

95 Ebben az összefüggésben a GDPR (107) preambulumbekezdése kimondja, hogy amennyiben valamely „harmadik ország valamely területe vagy meghatározott ágazata […] már nem biztosít megfelelő szintű adatvédelmet[,] a személyes adatok ilyen harmadik országba vagy nemzetközi szervezet részére történő továbbítását meg kell tiltani, kivéve, ha e rendeletbe foglalt, a személyes adatok [továbbítása] megfelelő garanciák alapján történik […]”. E tekintetben az említett rendelet (108) preambulumbekezdése pontosítja, hogy megfelelőségi határozat hiányában az adatkezelő vagy az adatfeldolgozó által az ugyanezen rendelet 46. cikke (1) bekezdése alapján biztosítandó megfelelő garanciáknak „[kell ellensúlyozniuk] az adatvédelem harmadik országbeli hiányosságai[t]” annak érdekében, hogy „biztosít[s]ák az adatvédelmi követelményeknek való megfelelést, és az Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat biztosít[s]anak az érintettek számára”.

96 Ebből következik, amint arra a főtanácsnok az indítványának 115. pontjában rámutatott, hogy e megfelelő garanciáknak olyannak kell lenniük, hogy biztosítsák, hogy azon személyeket, akiknek az adatait az általános adatvédelmi kikötések alapján továbbítják, – mint a megfelelőségi határozaton alapuló adattovábbítás esetében is – az Unióban biztosított védelmi szinttel lényegében azonos védelmi szint illesse meg.

97 A kérdést előterjesztő bíróság arra is keresi a választ, hogy az Unióban biztosított védelmi szinttel lényegében azonos védelmi szintet az uniós jog, különösen a Chartában biztosított jogok és/vagy az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményben (a továbbiakban: EJEE) biztosított alapvető jogok vagy még a tagállamok nemzeti joga alapján kell-e meghatározni.

98 E tekintetben emlékeztetni kell, hogy jóllehet – amint azt az EUSZ 6. cikk (3) bekezdése megerősíti – az EJEE által biztosított alapvető jogok az uniós jogrend részét képezik mint annak általános elvei, és ugyan a Charta 52. cikkének (3) bekezdése úgy rendelkezik, hogy a Chartában foglalt, az EJEE által biztosított jogoknak megfelelő jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az említett egyezményben szerepelnek, ez az egyezmény nem minősül az uniós jogrendbe szervesen beépülő jogforrásnak addig, amíg az Unió nem csatlakozott hozzá (2013. február 26-i Åkerberg Fransson ítélet, C-617/10, EU:C:2013:105, 44. pont, valamint az ott hivatkozott ítélkezési gyakorlat; 2018. március 20-i Menci ítélet, C-524/15, EU:C:2018:197, 22. pont).

99 E körülmények között a Bíróság kimondta, hogy az uniós jog értelmezését és az uniós jogi aktusok érvényességének vizsgálatát a Charta által biztosított alapvető jogokra tekintettel kell elvégezni (lásd analógia útján: 2018. március 20-i Menci ítélet, C-524/15, EU:C:2018:197, 24. pont).

100 Egyébiránt az állandó ítélkezési gyakorlat szerint az uniós jogi rendelkezések érvényessége, és a tagállamok nemzeti jogára való kifejezett utalás hiányában azok értelmezése nem értékelhető e nemzeti jog alapján, még az alkotmányos szintű nemzeti jog, különösen a nemzeti alkotmányukban megfogalmazott alapvető jogok alapján sem (lásd ebben az értelemben: 1970. december 17-i Internationale Handelsgesellschaft ítélet, 11/70, EU:C:1970:114, 3. pont; 1979. december 13-i Hauer ítélet, 44/79, EU:C:1979:290, 14. pont; 2016. október 18-i Nikiforidis ítélet, C-135/15, EU:C:2016:774, 28. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

101 Ebből következik, hogy mivel egyrészt az olyan személyes adatoknak, mint amelyek az alapeljárásban szerepelnek, a valamely tagállamban letelepedett gazdasági szereplő által valamely harmadik országban letelepedett másik gazdasági szereplő részére kereskedelmi célból történő továbbítása – amint az az első kérdésre adott válaszból kitűnik – a GDPR hatálya alá tartozik, másrészt pedig e rendelet – amint az a (10) preambulumbekezdéséből kitűnik – többek között arra irányul, hogy biztosítsa a természetes személyek következetes és magas szintű védelmét az Unión belül, és e célból biztosítsa e személyeknek a személyes adataik kezeléséhez kapcsolódó alapvető jogai és szabadságai védelmére vonatkozó szabályok következetes és egységes alkalmazását az Unió egész területén, az alapvető jogok védelmének az említett rendelet 46. cikkének (1) bekezdésében megkövetelt szintjét ugyanezen rendeletnek – a Charta által biztosított alapvető jogok fényében értelmezett – rendelkezései alapján kell meghatározni.

102 A kérdést előterjesztő bíróság továbbá azt kívánja megtudni, hogy milyen tényezőket kell figyelembe venni annak meghatározásához, hogy a személyes adatok harmadik országba irányuló továbbításával összefüggésben a GDPR 46. cikke (2) bekezdésének c) pontja alapján elfogadott általános adatvédelmi kikötések alapján megfelelő-e a védelem szintje.

103 E tekintetben, bár e rendelkezés nem sorolja fel azokat a különböző tényezőket, amelyeket az ilyen továbbítás során tiszteletben tartandó védelmi szint megfelelőségének értékelése során figyelembe kell venni, e rendelet 46. cikkének (1) bekezdése pontosítja, hogy az érintett személyeknek megfelelő garanciákkal, valamint érvényesíthető jogokkal és hatékony jogorvoslati lehetőségekkel kell rendelkezniük.

104 Az ilyen továbbítással összefüggésben ehhez megkövetelt értékelésnek figyelembe kell vennie többek között mind az Unióban letelepedett adatkezelő vagy az ott letelepedett adatfeldolgozója és a továbbításnak az érintett harmadik országban letelepedett címzettje között létrejött szerződéses kikötéseket, mind pedig – e harmadik ország hatóságainak a továbbított személyes adatokhoz való esetleges hozzáférését illetően – az ezen ország jogrendszerének releváns elemeit. Ez utóbbi tekintetben az említett rendelet 46. cikke összefüggésében figyelembe veendő tényezők megfelelnek az e rendelet 45. cikkének (2) bekezdésében nem kimerítő jelleggel felsorolt elemeknek.

105 Következésképpen a második, harmadik és hatodik kérdésre azt a választ kell adni, hogy a GDPR 46. cikkének (1) bekezdését és 46. cikke (2) bekezdésének c) pontját úgy kell értelmezni, hogy az e rendelkezések által megkövetelt megfelelő garanciáknak, érvényesíthető jogoknak és hatékony jogorvoslati lehetőségeknek biztosítaniuk kell, hogy azon személyek jogai, akiknek a személyes adatait az általános adatvédelmi kikötések alapján továbbítják harmadik országba, olyan védelmi szinttel rendelkezzenek, amely lényegében azonos az ezen – Charta fényében értelmezett – rendelet által az Unióban biztosított védelmi szinttel. E célból az ilyen továbbítással összefüggésben biztosított védelmi szint értékelésének figyelembe kell vennie többek között mind az Unióban letelepedett adatkezelő vagy az ott letelepedett adatfeldolgozója és a továbbításnak az érintett harmadik országban letelepedett

címzettje között létrejött szerződéses kikötéseket, mind pedig – e harmadik ország hatóságainak az így továbbított személyes adatokhoz való esetleges hozzáférését illetően – az ezen ország jogrendszerének releváns elemeit, különösen az említett rendelet 45. cikkének (2) bekezdésében felsorolt elemeket.

A nyolcadik kérdésről

106 A nyolcadik kérdésével az előterjesztő bíróság lényegében arra keresi a választ, hogy a GDPR 58. cikke (2) bekezdésének f) és j) pontját úgy kell-e értelmezni, hogy az illetékes felügyeleti hatóság köteles felfüggeszteni vagy megtiltani a személyes adatoknak a Bizottság által elfogadott általános adatvédelmi kikötéseken alapuló, harmadik országba irányuló továbbítását, amennyiben e felügyeleti hatóság úgy ítéli meg, hogy e kikötéseket e harmadik országban nem tartják be, vagy azokat ott nem lehet tiszteletben tartani, és hogy a továbbított adatok védelme, amelyet az uniós jog, különösen a GDPR 45. és 46. cikke, valamint a Charta megkövetel, nem biztosítható, vagy abban az értelemben, hogy e hatáskörök gyakorlása csak kivételes esetekre korlátozódik.

107 A Charta 8. cikke (3) bekezdésének, valamint a GDPR 51. cikke (1) bekezdésének és 57. cikke (1) bekezdése a) pontjának megfelelően a nemzeti felügyeleti hatóságok feladata a személyes adatok kezelése vonatkozásában a természetes személyek védelmére vonatkozó uniós szabályok tiszteletben tartásának ellenőrzése. Ezért mindegyik hatóság hatáskörrel rendelkezik annak ellenőrzésére, hogy a személyes adatoknak azon tagállamból valamely harmadik országba való továbbítása, amelyre a hatóság joghatósága kiterjed, tiszteletben tartja-e az e rendeletben támasztott követelményeket (lásd analógia útján a 95/46 irányelv 28. cikkét illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 47. pont).

108 E rendelkezésekből következik, hogy a felügyeleti hatóságok elsődleges feladata, hogy ellenőrizzék a GDPR alkalmazását, és gondoskodjanak annak tiszteletben tartásáról. E feladat ellátása különös jelentőséggel bír a személyes adatok harmadik országba irányuló továbbításával összefüggésben, mivel – amint az e rendelet (116) preambulumbekezdésének szövegéből kitűnik – „[a] személyes adatok uniós külső határokat átlépő továbbításakor megnövekedhet annak a kockázata, hogy a természetes személyek adatvédelmi jogaikat nem képesek gyakorolni, különösen ami az adatok jogellenes felhasználása vagy közlése elleni védelmet illeti”. Ebben az esetben, amint azt ugyanezen preambulumbekezdés kimondja, „a felügyeleti hatóságok nem tudnak az országuk határaikon kívül folyó tevékenységek tekintetében a panaszok kapcsán eljárni vagy vizsgálatot lefolytatni”.

109 Ezenkívül a GDPR 57. cikke (1) bekezdésének f) pontja értelmében minden felügyeleti hatóság a saját területén köteles kezelni azokat a panaszokat, amelyeket bármely személy e rendelet 77. cikke (1) bekezdésének megfelelően jogosult benyújtani, amennyiben úgy ítéli meg, hogy a rá vonatkozó személyes adatok kezelése sérti az említett rendeletet, továbbá a szükséges mértékben köteles kivizsgálni e panaszok tárgyát. A felügyeleti hatóságnak az ilyen panaszt a kellő gondossággal kell kezelnie (lásd analógia útján a 95/46 irányelv 25. cikkének (6) bekezdését illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 63. pont).

110 A GDPR 78. cikkének (1) és (2) bekezdése elismeri, hogy mindenkinek joga van a hatékony bírósági jogorvoslathoz, különösen akkor, ha a felügyeleti hatóság elmulasztja a panaszának kezelését. E rendelet (141) preambulumbekezdése „a Charta 47. cikkével összhangban hatékony bírósági jogorvoslat[ra]” is hivatkozik olyan esetekben, amikor e felügyeleti hatóság „nem jár el olyan esetben, amikor fellépése az érintett jogainak védelmében szükséges lenne”.

111 A benyújtott panaszok elbírálása érdekében a GDPR 58. cikkének (1) bekezdése az egyes felügyeleti hatóságokat jelentős vizsgálati hatáskörökkel ruházza fel. Amennyiben egy ilyen hatóság a vizsgálata végén úgy ítéli meg, hogy az érintett személy, akinek a személyes adatait valamely harmadik országba továbbították, ott nem részesül megfelelő szintű védelemben, az uniós jog alapján köteles megfelelően

reagálni a megállapított hiányosság orvoslása érdekében, mégpedig függetlenül e hiányosság eredetétől vagy jellegétől. E célból e rendelet 58. cikkének (2) bekezdése felsorolja azokat a különböző korrekciós intézkedéseket, amelyeket a felügyeleti hatóság elfogadhat.

112 Noha a megfelelő és szükséges eszköz megválasztása a felügyeleti hatóság feladata, és e hatóságnak e választást a személyes adatok szóban forgó továbbítása valamennyi körülményének figyelembevételével kell meghoznia, e hatóságnak a GDPR teljes körű tiszteletben tartásának biztosításában álló feladatát is kellő gondossággal kell ellátnia.

113 E tekintetben, és amint arra a főtanácsnok az indítványának 148. pontjában szintén rámutatott, az említett hatóság e rendelet 58. cikke (2) bekezdésének f) és j) pontja értelmében köteles felfüggeszteni vagy megtiltani a személyes adatok harmadik országba irányuló továbbítását, ha az e továbbítás sajátos körülményeinek összességére tekintettel úgy ítéli meg, hogy az általános adatvédelmi kikötéseket e harmadik országban nem tartják be, vagy azokat ott nem lehet tiszteletben tartani, és hogy a továbbított adatok uniós jog által megkövetelt védelme más eszközzel nem biztosítható, amennyiben az Unióban letelepedett adatkezelő vagy az ott letelepedett adatfeldolgozója maga nem függesztette fel vagy fejezte be az adattovábbítást.

114 Az előző pontban szereplő értelmezést nem kérdőjelezi meg a biztos azon érvelése, amely szerint a 2010/87 határozat 4. cikkének a 2016/2297 végrehajtási határozat hatálybalépését megelőző szövegváltozata – e határozat (11) preambulumbekezdésével összefüggésben értelmezve – bizonyos kivételes esetekre korlátozta a felügyeleti hatóságok arra vonatkozó hatáskörét, hogy felfüggesszék vagy megtiltsák a személyes adatok harmadik országba irányuló továbbítását. Az ÁSZT-határozat 4. cikkének a 2016/2297 végrehajtási határozatból eredő szövegváltozata ugyanis anélkül hivatkozik arra, hogy e hatóságok – immár a GDPR 58. cikke (2) bekezdésének f) és j) pontja alapján – jogosultak az ilyen adattovábbítás felfüggesztésére vagy megtiltására, hogy e jogkör gyakorlását rendkívüli körülményekre korlátoznák.

115 Mindenesetre a GDPR 46. cikke (2) bekezdésének c) pontja által a Bizottság számára az általános adatvédelmi kikötések elfogadása céljából elismert végrehajtási jogkör nem ruházza fel a Bizottságot azzal a hatáskörrel, hogy korlátozza azon jogköröket, amelyekkel a felügyeleti hatóságok e rendelet 58. cikkének (2) bekezdése alapján rendelkeznek (lásd analógia útján a 95/46 irányelv 25. cikkének (6) bekezdését és 28. cikkét illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 102. és 103. pont). Emellett a 2016/2297 végrehajtási határozat (5) preambulumbekezdése megerősíti, hogy az ÁSZF-határozat „nem akadályozza meg, hogy a [felügyeleti hatóság] gyakorolja az adatáramlások ellenőrzésére vonatkozó jogkörét, beleértve a személyes adatok továbbításának felfüggesztését vagy tilalmát, ha a hatóság megállapítja, hogy az uniós vagy a nemzeti adatvédelmi jog megsértésével végzik az adattovábbítást”.

116 Pontosítani kell azonban, hogy az illetékes felügyeleti hatóság hatásköreit azon határozatot teljes mértékben tiszteletben tartva kell gyakorolni, amelyben a Bizottság adott esetben a GDPR 45. cikke (1) bekezdésének első mondata alapján megállapítja, hogy egy adott harmadik ország megfelelő védelmi szintet biztosít. Ilyen esetben ugyanis e rendelet (103) preambulumbekezdésével összefüggésben értelmezett 45. cikke (1) bekezdésének második mondatából kitűnik, hogy a személyes adatoknak az érintett harmadik országba irányuló továbbítására külön engedély nélkül kerülhet sor.

117 Az EUMSZ 288. cikk negyedik bekezdése értelmében a Bizottság megfelelőségi határozata minden elemében kötelező valamennyi címzett tagállamra nézve, és így valamennyi szervükre is kötelező, amennyiben megállapítja, hogy az érintett harmadik ország megfelelő védelmi szintet biztosít, és az a következménye, hogy engedélyezi ezeket az adattovábbításokat (lásd analógia útján a 95/46 irányelv 25. cikkének (6) bekezdését illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 51. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

118 Így, amíg a Bíróság nem állapítja meg a megfelelőségi határozat érvénytelenségét, a tagállamok és a szerveik, köztük a független felügyeleti hatóságaik, nem fogadhatnak el e határozattal ellentétes olyan intézkedéseket, mint az annak kötelező erejű megállapítására irányuló jogi aktusok, hogy az a harmadik ország, amelyre az említett határozat vonatkozik, nem biztosít megfelelő védelmi szintet (2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 52. pont, valamint az ott hivatkozott ítélkezési gyakorlat), és amelyek célja következésképpen a személyes adatok harmadik országba irányuló továbbításának felfüggesztése vagy megtiltása.

119 Mindazonáltal a Bizottság által a GDPR 45. cikkének (3) bekezdése alapján elfogadott megfelelőségi határozat nem akadályozhatja meg azokat a személyeket, akiknek a személyes adatait valamely harmadik országba továbbították vagy továbbíthatják, hogy a GDPR 77. cikkének (1) bekezdése alapján panaszt nyújtsanak be az illetékes nemzeti felügyeleti hatósághoz ezen adatok kezelése vonatkozásában a jogaik vagy szabadságaik védelmével kapcsolatban. Ehhez hasonlóan az ilyen jellegű határozat nem teheti semmissé, vagy nem csökkentheti a nemzeti felügyeleti hatóságok számára a Charta 8. cikkének (3) bekezdésében, valamint az említett rendelet 51. cikkének (1) bekezdésében és 57. cikke (1) bekezdésének a) pontjában kifejezetten elismert jogköröket (lásd analógia útján a 95/46 irányelv 25. cikkének (6) bekezdését és 28. cikkét illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 53. pont).

120 Így még a Bizottság megfelelőségi határozata esetében is a valamely személy által a rá vonatkozó személyes adatok kezelése vonatkozásában a jogainak vagy szabadságainak védelmével kapcsolatban benyújtott panaszt elbíráló nemzeti felügyeleti hatóságnak jogosultnak kell lennie arra, hogy teljes függetlenséggel megvizsgálja, hogy ezen adattovábbítás tiszteletben tartja-e a GDPR-ben támasztott követelményeket, és adott esetben a nemzeti bíróságok előtt keresetet indítson annak érdekében, hogy amennyiben az utóbbiak osztják e hatóságnak a megfelelőségi határozat érvényessége tekintetében fennálló kétségeit, előzetes döntéshozatali eljárást kezdeményezhessenek ezen érvényesség vizsgálata céljából (lásd analógia útján a 95/46 irányelv 25. cikkének (6) bekezdését és 28. cikkét illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 57. és 65. pont).

121 A fenti megfontolásokra tekintettel a nyolcadik kérdésre azt a választ kell adni, hogy a GDPR 58. cikke (2) bekezdésének f) és j) pontját úgy kell értelmezni, hogy az illetékes felügyeleti hatóság – feltéve, hogy nem létezik a Bizottság által érvényesen elfogadott megfelelőségi határozat – köteles felfüggeszteni vagy megtiltani a személyes adatoknak a Bizottság által elfogadott általános adatvédelmi kikötéseken alapuló, harmadik országba irányuló továbbítását, ha e felügyeleti hatóság az e továbbítás sajátos körülményeinek összességére tekintettel úgy ítéli meg, hogy e kikötéseket e harmadik országban nem tartják be, vagy azokat ott nem lehet tiszteletben tartani, és hogy a továbbított adatok védelme, amelyet az uniós jog, különösen a GDPR 45. és 46. cikke, valamint a Charta megkövetel, más eszközzel nem biztosítható, amennyiben az Unióban letelepedett adatkezelő vagy az ott letelepedett adatfeldolgozója maga nem függesztette fel vagy fejezte be az adattovábbítást.

A hetedik és tizenegyedik kérdésről

122 A hetedik és tizenegyedik kérdésével, amelyeket célszerű együtt vizsgálni, az előterjesztő bíróság lényegében az ÁSZF-határozatnak a Charta 7., 8. és 47. cikkére tekintettel fennálló érvényességéről kérdezi a Bíróságot.

123 Különösen, amint az magából a hetedik kérdés szövegéből és az előzetes döntéshozatal iránti kérelemben szereplő magyarázatokból kitűnik, a kérdést előterjesztő bíróságban felmerül a kérdés, hogy az ÁSZF-határozat alkalmas-e arra, hogy megfelelő védelmi szintet biztosítson a harmadik országokba továbbított személyes adatok számára, amennyiben az abban előírt általános adatvédelmi kikötések nem kötik e harmadik országok hatóságait.

124 Az ÁSZF-határozat 1. cikke úgy rendelkezik, hogy az e rendelet mellékletében szereplő általános szerződési feltételek megfelelő biztosítékot nyújtónak minősülnek, tekintettel az egyének magánélethez való jogának, alapvető jogainak és szabadságjogainak védelmére, valamint a [95/46] irányelv 26. cikkének (2) bekezdése által előírt megfelelő jogok gyakorlására. Ez utóbbi rendelkezést lényegében átvette a GDPR 46. cikkének (1) bekezdése és 46. cikke (2) bekezdésének c) pontja.

125 Ugyanakkor, noha e kikötések kötelezőek az Unióban letelepedett adatkezelőre és a személyes adatok továbbításának harmadik országban letelepedett címzettjére nézve abban az esetben, ha e kikötésekre hivatkozva kötöttek szerződést, nem vitatott, hogy az említett kikötések nem kötelezhetik e harmadik ország hatóságait, mivel ez utóbbiak nem szerződő felek.

126 Amennyiben tehát léteznek olyan helyzetek, amelyekben az ilyen továbbítás címzettje az érintett harmadik országban fennálló jogi helyzettől és gyakorlattól függően képes biztosítani a szükséges adatok védelmét kizárólag az általános adatvédelmi kikötések alapján, léteznek más olyan helyzetek, amelyekben az e kikötésekben szereplő rendelkezések esetleg nem jelenthetnek elegendő eszközt az érintett harmadik országba továbbított személyes adatok hatékony védelmének a gyakorlatban történő biztosítására. Ez az eset áll fenn különösen akkor, ha e harmadik ország joga lehetővé teszi ezen ország hatóságai számára az érintett személyek ezen adatokkal kapcsolatos jogaiba való beavatkozást.

127 Így felmerül a kérdés, hogy az általános adatvédelmi kikötések vonatkozásában a GDPR 46. cikke (2) bekezdésének c) pontja alapján elfogadott bizottsági határozat érvénytelen-e abban az esetben, ha e határozatban nincsenek azon harmadik országok hatóságaival szemben érvényesíthető garanciák, amelyekhez e kikötések alapján a személyes adatokat továbbítják vagy továbbíthatják.

128 A GDPR 46. cikkének (1) bekezdése előírja, hogy megfelelőségi határozat hiányában az adatkezelő vagy az adatfeldolgozó csak akkor továbbíthat személyes adatokat egy harmadik országba, ha megfelelő garanciákat nyújtott, és feltéve, hogy az érintett személyek érvényesíthető jogokkal és hatékony jogorvoslati lehetőségekkel rendelkeznek. E rendelet 46. cikke (2) bekezdésének c) pontja szerint és e garanciákként különösen a Bizottság által elfogadott általános adatvédelmi kikötések szolgálhatnak. Márpedig e rendelkezések nem írják elő, hogy az említett garanciák összességét szükségszerűen tartalmaznia kell egy olyan bizottsági határozatnak, mint amilyen az ÁSZF-határozat.

129 E tekintetben meg kell állapítani, hogy az ilyen határozat különbözik a GDPR 45. cikkének (3) bekezdése alapján elfogadott megfelelőségi határozattól, amely az érintett harmadik ország szabályozásának vizsgálatát követően – figyelembe véve többek között a nemzetbiztonságra és a hatóságok személyes adatokhoz való hozzáférésére vonatkozó releváns jogszabályokat – arra irányul, hogy kötelező erővel állapítsa meg, hogy valamely harmadik ország, ennek valamely területe, vagy egy vagy több meghatározott ágazata megfelelő védelmi szintet biztosít, és hogy ezért az említett harmadik ország hatóságainak ezen adatokhoz való hozzáférése nem képezi akadályát annak, hogy azokat ugyanezen harmadik országba továbbítsák. Ilyen megfelelőségi határozatot a Bizottság tehát csak akkor fogadhat el, ha megállapította, hogy e harmadik ország vonatkozó jogszabályai ténylegesen tartalmazzák az összes olyan szükséges garanciát, amely lehetővé teszi annak megállapítását, hogy megfelelő védelmi szintet biztosít.

130 Ezzel szemben, ami az általános adatvédelmi kikötéseket elfogadó, ÁSZF-határozathoz hasonló bizottsági határozatot illeti, amennyiben az ilyen határozat nem valamely harmadik országra, ennek valamely területére, vagy egy vagy több meghatározott ágazatára vonatkozik, a GDPR 46. cikkének (1) bekezdéséből és 46. cikke (2) bekezdésének c) pontjából nem vonható le az a következtetés, hogy a Bizottság az ilyen határozat elfogadása előtt köteles lenne értékelni azon harmadik ország által biztosított védelem szintjének megfelelő jellegét, amelybe a személyes adatokat ilyen kikötések alapján továbbíthatják.

131 E tekintetben emlékeztetni kell arra, hogy e rendelet 46. cikkének (1) bekezdése értelmében a Bizottság megfelelőségi határozatának hiányában az Unióban letelepedett adatkezelőnek vagy adatfeldolgozónak kell többek között megfelelő garanciákat nyújtania. Az említett rendelet (108) és (114) preambulumbekezdése megerősíti, hogy amennyiben a Bizottság valamely harmadik országot illetően nem nyilatkozott az adatvédelem megfelelő szintjéről, az adatkezelőnek vagy adott esetben az adatfeldolgozójának „a megfelelő garanciák érintett számára való biztosítása útján gondoskodik az adatvédelem harmadik országbeli hiányosságainak ellensúlyozásáról”, és hogy „[e] garanciák biztosítják az adatvédelmi követelményeknek való megfelelést, és az Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat biztosítanak az érintettek számára, beleértve az érintettek jogainak érvényesíthetőségét és a hatékony jogorvoslat lehetőségét […] az Unióban vagy egy harmadik országban”.

132 Mivel – amint az a jelen ítélet 125. pontjából kitűnik – az általános adatvédelmi kikötések szerződéses jellegéhez szorosan kapcsolódik, hogy azok nem köthetik harmadik országok hatóságait, hanem a GDPR 44. cikke, 46. cikkének (1) bekezdése és 46. cikke (2) bekezdésének c) pontja – a Charta 7., 8. és 47. cikkével összefüggésben értelmezve – megköveteli, hogy a természetes személyek számára az e rendelet által biztosított védelem szintje ne sérüljön, szükségesnek bizonyulhat azon garanciák kiegészítése, amelyeket ezen általános adatvédelmi kikötések tartalmaznak. E tekintetben az említett rendelet (109) preambulumbekezdése kimondja, hogy „[a]z a lehetőség, mely szerint az adatkezelő […] alkalmazhatja a Bizottság […] által elfogadott általános adatvédelmi kikötéseket [nem] zárja ki, hogy […] további rendelkezéseket vagy garanciákat adjon hozzá”, és pontosítja különösen, hogy ezeket „arra kell ösztönözni, hogy az általános adatvédelmi kikötéseket kiegészítő […] még erőteljesebb garanciákat nyújtsanak”.

133 Úgy tűnik tehát, hogy a Bizottság által az ugyanezen rendelet 46. cikke (2) bekezdésének c) pontja alapján elfogadott általános adatvédelmi kikötések kizárólag arra irányulnak, hogy az Unióban letelepedett adatkezelőknek vagy az ott letelepedett adatfeldolgozóiknak minden harmadik országban egységesen alkalmazandó szerződéses garanciákat biztosítsanak, és ennélfogva függetlenül az egyes országokban biztosított védelem szintjétől. Mivel ezen általános adatvédelmi kikötések – jellegükre tekintettel – nem nyújthatnak az uniós jog által megkövetelt védelmi szint tiszteletben tartásának biztosítására irányuló szerződéses kötelezettségen túlmenő garanciákat, az egyes harmadik országokban fennálló helyzettől függően szükségessé tehetik, hogy az adatkezelő további intézkedéseket hozzon e védelmi szint tiszteletben tartásának biztosítása érdekében.

134 E tekintetben, amint arra a főtanácsnok az indítványának 126. pontjában rámutatott, a GDPR 46. cikke (2) bekezdésének c) pontjában előírt szerződéses mechanizmus az Unióban letelepedett adatkezelő vagy az ott letelepedett adatfeldolgozója, valamint másodlagosan az illetékes felügyeleti hatóság felelősségvállalásán alapul. Ennélfogva mindenekelőtt ezen adatkezelőnek vagy adatfeldolgozójának feladata, hogy esetről esetre és adott esetben a továbbítás címzettjével együttműködve ellenőrizze, hogy a célországnak számító harmadik ország joga megfelelő védelmet biztosít-e az uniós jog tekintetében az általános adatvédelmi kikötések alapján továbbított személyes adatoknak, szükség esetén az e kikötések által biztosított garanciákon felül további garanciákat nyújtva.

135 Ha az Unióban letelepedett adatkezelő vagy adatfeldolgozója nem hozhat az ilyen védelem biztosításához szükséges további intézkedéseket, az adatkezelő, vagy másodlagosan az illetékes felügyeleti hatóság köteles felfüggeszteni vagy megszüntetni a személyes adatoknak az érintett harmadik országba irányuló továbbítását. Ez az eset áll fenn különösen akkor, ha e harmadik ország joga az Unióból származó személyes adatok továbbításának címzettjével szemben olyan kötelezettségeket ír elő, amelyek ellentétesek az említett kikötésekkel, és amelyek ennélfogva megkérdőjelezhetik az említett harmadik ország hatóságainak ezen adatokhoz való hozzáférésével szembeni megfelelő szintű védelem szerződéses garanciáját.

136 Következésképpen önmagában az a tény, hogy a Bizottság által a GDPR 46. cikke (2) bekezdésének c) pontja alapján elfogadott határozatban szereplő olyan általános adatvédelmi kikötések, mint amelyek az ÁSZF-határozat mellékletében szerepelnek, nem kötik azon harmadik országok hatóságait, amelyekbe a személyes adatok továbbíthatók, nem érintheti e határozat érvényességét.

137 Ez az érvényesség viszont attól függ, hogy a Charta 7., 8. és 47. cikkével összefüggésben értelmezett, a GDPR 46. cikkének (1) bekezdéséből és 46. cikke (2) bekezdésének c) pontjából eredő követelménynek megfelelően az ilyen határozat tartalmaz-e olyan hatékony mechanizmusokat, amelyek a gyakorlatban lehetővé teszik annak biztosítását, hogy az uniós jog által megkövetelt védelmi szintet tiszteletben tartsák, és hogy a személyes adatok ilyen kikötéseken alapuló továbbítását az e kikötések megsértése, illetve tiszteletben tartásuk lehetetlensége esetén felfüggesszék vagy megtiltsák.

138 Ami az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötésekben foglalt garanciákat illeti, e melléklet 4. általános szerződési feltételének a) és b) pontjából, 5. általános szerződési feltételének a) pontjából, 9. általános szerződési feltételéből, valamint 11. általános szerződési feltételének (1) bekezdéséből kitűnik, hogy az Unióban letelepedett adatkezelő, a személyes adatok továbbításának címzettje, valamint ennek esetleges adatfeldolgozója kölcsönösen kötelezettséget vállal arra, hogy ezen adatok kezelése megfelelt és továbbra is megfelel az „alkalmazandó adatvédelmi jog[nak]”, mégpedig az említett határozat 3. cikkének f) pontjában szereplő fogalommeghatározás szerint „az egyének alapvető jogaik és szabadságjogaik, különösen – a személyes adatok feldolgozásával kapcsolatban – a magánélet tiszteletben tartásához való jogaik védelméről szóló, az adatátadó letelepedési helye szerinti tagállamban tevékenykedő adatkezelőre vonatkozó jogszabály[oknak]”. Márpedig a GDPR-nek a Chartával összefüggésben értelmezett rendelkezései e jogszabályok részét képezik.

139 Ezenkívül a személyes adatok továbbításának harmadik országban letelepedett címzettje ezen 5. általános szerződési feltétel a) pontja értelmében kötelezettséget vállal arra, hogy haladéktalanul tájékoztatja az Unióban letelepedett adatkezelőt arról, hogy esetlegesen nem tudja teljesíteni a megkötött szerződésből eredő kötelezettségeit. Különösen az említett 5. általános szerződési feltétel b) pontja szerint e címzett igazolja, hogy nincs tudomása arról, hogy a rá vonatkozó jogszabályok akadályoznák a szerződésben vállalt kötelezettségek teljesítését, és kötelezettséget vállal, hogy mihelyt tudomást szerez erről, azonnal értesíti az adatátadót a nemzeti jogszabályok minden olyan módosításról, amely előreláthatóan jelentősen hátrányos hatással lenne az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötésekben megállapított garanciákra és kötelezettségekre. Egyébiránt, bár ugyanezen 5. általános szerződési feltétel d) pontjának i. alpontja lehetővé teszi a személyes adatok továbbításának címzettje számára, hogy az őt védő olyan jogszabály esetén, mint például egy bűnügyi nyomozás titkosságának megőrzése érdekében fennálló büntetőjogi tilalom, ne közölje az Unióban letelepedett adatkezelővel a személyes adatok közlésére irányuló, a bűnüldöző szervek jogilag kötelező erejű felhívását, az ÁSZF-határozat melléklete 5. általános szerződési feltétele a) pontjának megfelelően azonban köteles tájékoztatni az adatkezelőt arról, hogy nem képes eleget tenni az általános szerződési feltételeknek.

140 Ezen 5. általános szerződési feltétel a) és b) pontja az általa érintett két esetben feljogosítja az Unióban letelepedett adatkezelőt az adattovábbítás felfüggesztésére és/vagy a szerződéstől való elállásra. A Charta 7. és 8. cikkével összefüggésben értelmezett GDPR 46. cikkének (1) bekezdéséből és 46. cikke (2) bekezdésének c) pontjából eredő követelményekre tekintettel az adattovábbítás felfüggesztése és/vagy a szerződéstől való elállás kötelező az adatkezelőre nézve, ha a továbbítás címzettje nem, vagy már nem képes tiszteletben tartani az általános adatvédelmi kikötéseket. Ennek hiányában az adatkezelő nem teljesíti a GDPR és a Charta rendelkezéseinek fényében értelmezett, az ÁSZF határozat melléklete 4. általános szerződési feltételének a) pontjából eredő követelményeket.

141 Úgy tűnik tehát, hogy e melléklet 4. általános szerződési feltételének a) pontja, valamint 5. általános szerződési feltételének a) és b) pontja arra kötelezi az Unióban letelepedett adatkezelőt és a személyes adatok továbbításának címzettjét, hogy győződjön meg arról, hogy a célországnak számító harmadik

ország joga lehetővé teszi az említett címzett számára, hogy a személyes adatok e harmadik országba történő továbbítását megelőzően megfeleljen az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötéseknek. Ezen ellenőrzést illetően az említett 5. általános szerződési feltételre vonatkozó lábjegyzet pontosítja, hogy e jogszabályok kötelező követelményei, amelyek nem lépnek túl azon, amire egy demokratikus társadalomban szükség van többek között a nemzetbiztonság, honvédelem, közbiztonság biztosításához, nem ellentétesek az általános szerződési feltételekkel. Ezzel szemben, amint azt a főtanácsnok az indítványának 131. pontjában hangsúlyozta, a célországnak számító harmadik ország joga által előírt, az e célok eléréséhez szükséges mértéket meghaladó kötelezettségnek való megfelelést az említett kikötések megsértésének kell tekinteni. E gazdasági szereplők részéről az ilyen kötelezettség szükséges jellegének értékelésekor adott esetben figyelembe kell venni az érintett harmadik ország által biztosított védelmi szint megfelelőségének megállapítását, amely a Bizottság által a GDPR 45. cikkének (3) bekezdése alapján elfogadott megfelelőségi határozatban szerepel.

142 Ebből következik, hogy az Unióban letelepedett adatkezelő és a személyes adatok továbbításának címzettje köteles előzetesen ellenőrizni, hogy az érintett harmadik országban tiszteletben tartják-e az uniós jog által megkövetelt védelmi szintet. Az e továbbítás címzettjének az ugyanezen 5. általános szerződési feltétel b) pontja értelmében adott esetben tájékoztatnia kell az adatkezelőt arról, hogy esetleg nem képes eleget tenni e feltételeknek, ez utóbbi pedig köteles felfüggeszteni az adattovábbítást, és/vagy a szerződéstől elállni.

143 Ha a személyes adatok harmadik országba való továbbításának címzettje az ÁSZF-határozat melléklete 5. általános szerződési feltételének b) pontja alapján tudatta az adatkezelővel, hogy az érintett harmadik ország jogszabályai nem teszik lehetővé számára az e mellékletben szereplő általános adatvédelmi kikötéseknek való megfelelést, az említett melléklet 12. általános szerződési feltételéből az következik, hogy az e harmadik országba már továbbított adatokat és a másolatokat teljes egészükben vissza kell szolgáltatni vagy meg kell semmisíteni. Mindenesetre az ugyanezen melléklet 6. általános szerződési feltétele szankcionálja ezen általános feltételek megsértését, és biztosítja az érintett személy számára az elszenvedett kár megtérítéséhez való jogot.

144 Hozzá kell tenni, hogy az ÁSZF határozat melléklete 4. általános szerződési feltételének f) pontja szerint az Unióban letelepedett adatkezelő kötelezettséget vállal arra, hogy amennyiben különleges adatkategóriákat továbbíthatnának olyan harmadik országnak, amely nem biztosít megfelelő védelmi szintet, erről az érintett személyt a továbbítás előtt vagy azt követően a lehető leghamarabb tájékoztatni köteles. Ez az információ alkalmas arra, hogy lehetővé tegye e személy számára az e melléklet 3. általános szerződési feltételének (1) bekezdésében az adatkezelővel szemben biztosított jogorvoslati jog gyakorlását annak érdekében, hogy az függessze fel a tervezett továbbítást, álljon el a személyes adatok továbbításának címzettjével kötött szerződéstől, vagy adott esetben ez utóbbitól a továbbított adatok visszaszolgáltatását vagy megsemmisítését kérje.

145 Végül az említett melléklet 4. általános szerződési feltételének g) pontja értelmében az Unióban letelepedett adatkezelő, ha a személyes adatok továbbításának címzettje e melléklet 5. általános szerződési feltételének b) pontja alapján közli vele, hogy a rá vonatkozó jogszabályok olyan módosítás tárgyát képezik, amely jelentősen hátrányos hatással járhat az általános adatvédelmi kikötések által nyújtott biztosítékokra és előírt kötelezettségekre nézve, köteles ezt az értesítést továbbítani az illetékes felügyeleti hatóságnak, ha az említett értesítés ellenére úgy dönt, hogy folytatja az adattovábbítást vagy megszünteti a felfüggesztést. Az ilyen értesítésnek e felügyeleti hatóság részére történő továbbítása, valamint e hatóságnak a személyes adatok továbbításának címzettjével szembeni, ugyanezen melléklet 8. általános szerződési feltételének (2) bekezdése szerinti ellenőrzési joga lehetővé teszi az említett felügyeleti hatóság számára annak ellenőrzését, hogy a megfelelő védelmi szint biztosítása érdekében fel kell-e függeszteni, vagy meg kell-e tiltani a tervezett továbbítást.

146 Ebben az összefüggésben az ÁSZF-határozatnak a 2016/2297 végrehajtási határozat (5) preambulumbekezdésével összefüggésben értelmezett 4. cikke megerősíti, hogy az ÁSZF-határozat egyáltalán nem akadályozza meg az illetékes felügyeleti hatóságot abban, hogy adott esetben felfüggessze vagy megtiltsa a személyes adatoknak az e határozat mellékletében szereplő általános adatvédelmi kikötéseken alapuló, harmadik országba irányuló továbbítását. E tekintetben, amint az a nyolcadik kérdésre adott válaszból következik, az illetékes felügyeleti hatóság – feltéve, hogy nem létezik a Bizottság által érvényesen elfogadott megfelelőségi határozat – a GDPR 58. cikke (2) bekezdésének f) és j) pontja értelmében köteles felfüggeszteni vagy megtiltani az ilyen továbbítást, amennyiben az e továbbítás sajátos körülményeinek összességére tekintettel úgy ítéli meg, hogy e kikötéseket e harmadik országban nem tartják be, vagy azokat ott nem lehet tiszteletben tartani, és hogy a továbbított adatok védelme, amelyet az uniós jog megkövetel, más eszközzel nem biztosítható, amennyiben az Unióban letelepedett adatkezelő vagy az ott letelepedett adatfeldolgozója maga nem függesztette fel vagy fejezte be az adattovábbítást.

147 Ami a biztos által hivatkozott azon körülményt illeti, amely szerint a személyes adatok ilyen harmadik országba történő továbbítása a különböző tagállamokban esetlegesen a felügyeleti hatóságok eltérő határozatainak tárgyát képezheti, hozzá kell tenni, hogy a GDPR 55. cikkének (1) bekezdéséből és 57. cikke (1) bekezdésének a) pontjából az következik, hogy az e rendelet tiszteletben tartásának felügyeletére vonatkozó feladat főszabály szerint minden egyes felügyeleti hatóságra hárul a saját tagállamának területén. Ezenkívül az eltérő határozatok elkerülése érdekében az említett rendelet 64. cikkének (2) bekezdése előírja annak lehetőségét, hogy az a felügyeleti hatóság, amely úgy ítéli meg, hogy a harmadik országba irányuló adattovábbításokat általános jelleggel meg kell tiltani, vélemény kibocsátása céljából az Európai Adatvédelmi Testülethez forduljon, amely az ugyanezen rendelet 65. cikke (1) bekezdésének c) pontja alapján kötelező erejű döntést fogadhat el, különösen, ha valamely felügyeleti hatóság nem a kibocsátott vélemény alapján jár el.

148 Ebből következik, hogy az ÁSZF-határozat olyan hatékony mechanizmusokat ír elő, amelyek a gyakorlatban lehetővé teszik annak biztosítását, hogy a személyes adatoknak az e határozat mellékletében szereplő általános adatvédelmi kikötések alapján valamely harmadik országba történő továbbítását felfüggesszék vagy megtiltsák, ha az adattovábbítás címzettje nem tartja tiszteletben vagy nem tudja betartani az említett kikötéseket.

149 A fenti megfontolások összességére tekintettel a hetedik és a tizenegyedik kérdésre azt a választ kell adni, hogy az ÁSZF-határozatnak a Charta 7., 8. és 47. cikkére tekintettel történő vizsgálata nem tárt fel olyan tényezőt, amely e határozat érvényességét érintené.

A negyedik, ötödik, kilencedik és tizedik kérdésről

150 A kilencedik kérdésével az előterjesztő bíróság lényegében arra vár választ, hogy kötik-e, és ha igen, milyen mértékben valamely tagállam felügyeleti hatóságát az AVP-határozatban szereplő azon megállapítások, amelyek szerint az Egyesült Államok megfelelő védelmi szintet biztosít. A negyedik, ötödik és tizedik kérdésével e bíróság lényegében arra vár választ, hogy – figyelembe véve az Egyesült Államok jogára vonatkozó saját megállapításait – a személyes adatoknak az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötések alapján történő továbbítása e harmadik országba sérti-e a Charta 7., 8. és 47. cikkében biztosított jogokat, és különösen azt kérdezi a Bíróságtól, hogy az AVP-határozat III. mellékletében említett ombudsman létrehozása összeegyeztethető-e ezen 47. cikkel.

151 Elöljáróban meg kell állapítani, hogy bár a biztos által benyújtott kereset kizárólag az ÁSZF-határozat érvényességét vonja kétségbe, e keresetet az AVP-határozat elfogadását megelőzően nyújtották be a kérdést előterjesztő bírósághoz. Mivel e bíróság a negyedik és ötödik kérdésével általános jelleggel azt kérdezi a Bíróságtól, hogy milyen védelmet kell biztosítani a Charta 7., 8. és 47. cikke alapján az ilyen adattovábbítással összefüggésben, a Bíróság vizsgálatának figyelembe kell vennie az AVP-határozat

időközben bekövetkezett elfogadásából eredő következményeket. Ez annál is inkább így van, mivel az említett bíróság a tizedik kérdésével kifejezetten azt kérdezi, hogy az e 47. cikkben előírt védelmet az ezen utóbbi határozatban említett ombudsman révén biztosítják-e.

152 Ezenkívül az előzetes döntéshozatal iránti kérelemben szereplő információkból kitűnik, hogy az alapeljárás keretében a Facebook Ireland arra hivatkozott, hogy az AVP-határozat a biztos számára kötelező erővel bír az Egyesült Államok által biztosított védelmi szint megfelelőségének megállapítását, és következésképpen a személyes adatoknak az e harmadik országba történő, az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötéseken alapuló továbbítása jogszerű jellegét illetően.

153 Márpedig, amint az a jelen ítélet 59. pontjából kitűnik, az előzetes döntéshozatal iránti kérelemhez csatolt 2017. október 3-i ítéletében a kérdést előterjesztő bíróság hangsúlyozta, hogy figyelembe kell vennie a jog azon módosításait, amelyek a kereset benyújtása és az előtte tartott tárgyalás között következtek be. Úgy tűnik tehát, hogy e bíróság az alapjogvita eldöntése érdekében köteles figyelembe venni a körülmények AVP-határozat elfogadásából eredő megváltozását, valamint e határozat esetleges kötelező hatásait.

154 Különösen az ahhoz fűződő kötelező hatások fennállása, hogy az AVP-határozat megállapítja a megfelelő védelmi szintet az Egyesült Államokban, releváns mind a jelen ítélet 141. és 142. pontjában felidézett, az adatkezelőt és a személyes adatoknak az ÁSZF-határozat mellékletében szereplő általános adatvédelmi kikötések alapján harmadik országba történő továbbításának címzettjét terhelő kötelezettségek, mind pedig az adott esetben a hatóságot terhelő azon kötelezettségek értékelése szempontjából, hogy felfüggessze vagy megtiltsa az adattovábbítást.

155 Ami ugyanis az AVP-határozat kötelező hatásait illeti, e határozat 1. cikkének (1) bekezdése úgy rendelkezik, hogy a GDPR 45. cikkének (1) bekezdése alkalmazásában „az Egyesült Államok megfelelő szintű védelmet biztosít az [Európai Unió–Egyesült Államok] adatvédelmi pajzs keretében az Unióból az egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében”. Az említett határozat 1. cikkének (3) bekezdése értelmében úgy kell tekinteni, hogy a személyes adatok e pajzs keretében kerülnek továbbításra, amennyiben az Unióból olyan egyesült államokbeli szervezetekhez továbbítják azokat, amelyeket – az ugyanezen határozat II. mellékletében ismertetett elvek I. és III. szakaszának megfelelően – felvettek az e pajzsban részt vevő szervezetek listájára, amelyet az Egyesült Államok Kereskedelmi Minisztériuma vezet és a nyilvánosság számára hozzáférhetővé tesz.

156 Amint az a jelen ítélet 117. és 118. pontjában felidézett ítélkezési gyakorlatból következik, az AVP-határozat a felügyeleti hatóságokra nézve kötelező erejű, amennyiben azt állapítja meg, hogy az Egyesült Államok megfelelő védelmi szintet biztosít, és következésképpen azzal a hatással jár, hogy engedélyezi a személyes adatoknak az Európai Unió–Egyesült Államok adatvédelmi pajzs keretében történő továbbítását. Következésképpen mindaddig, amíg e határozatot a Bíróság nem nyilvánítja érvénytelennek, az illetékes felügyeleti hatóság nem függesztheti fel vagy tilthatja meg a személyes adatoknak az e pajzshoz tartozó szervezet részére történő továbbítását azzal az indokkal, hogy a Bizottság által az említett határozatban elfogadott értékeléssel ellentétben úgy ítéli meg, hogy az Egyesült Államok azon jogszabályai, amelyek e harmadik ország hatóságainak az említett pajzs keretében továbbított személyes adatokhoz nemzetbiztonsági, bűnüldözési és egyéb közérdekű célokból történő való hozzáférésére és ezen adatok ilyen célokból történő felhasználására vonatkoznak, nem biztosítanak megfelelő védelmet.

157 Mindazonáltal a jelen ítélet 119. és 120. pontjában felidézett ítélkezési gyakorlatnak megfelelően, ha valamely személy panasszal fordul hozzá, az illetékes felügyeleti hatóságnak teljes függetlenséggel kell megvizsgálnia, hogy a személyes adatok szóban forgó továbbítása tiszteletben tartja-e a GDPR által támasztott követelményeket, és amennyiben megalapozottnak ítéli az e személy által a megfelelőségi határozat érvényességének vitatása érdekében előterjesztett kifogásokat, a nemzeti bíróságok előtt keresetet kell indítania annak érdekében, hogy utóbbiak e határozat érvényességének elbírálása érdekében előzetes döntéshozatal iránti kérelemmel forduljanak a Bírósághoz.

158 Ugyanis a GDPR 77. cikkének (1) bekezdése címén benyújtott kérelmet, amelyben valamely személy, akinek a személyes adatait valamely harmadik országba továbbították vagy továbbíthatják, arra hivatkozik, hogy ezen ország joga és gyakorlatai – a Bizottság által az e rendelet 45. cikkének (3) bekezdése alapján elfogadott határozatban tett megállapítás ellenére – nem biztosítanak megfelelő védelmi szintet, úgy kell érteni, hogy az lényegében e határozatnak a személyek magánélete, valamint alapvető jogai és szabadságai védelmével való összeegyeztethetőségére vonatkozik (lásd analógia útján a 95/46 irányelv 25. cikkének (6) bekezdését és 28. cikkének (4) bekezdését illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 59. pont).

159 A jelen ügyben M. Schrems lényegében azt kérte a biztostól, hogy tiltsa meg vagy függessze fel személyes adatainak a Facebook Ireland által az Egyesült Államokban letelepedett Facebook Inc. részére történő továbbítását, azzal az indokkal, hogy e harmadik ország nem biztosít megfelelő védelmi szintet. Mivel a biztos az M. Schrems állításaira vonatkozó vizsgálatot követően a kérdést előterjesztő bírósághoz fordult, úgy tűnik, hogy ez utóbbi a benyújtott bizonyítékokra és az előtte folyó kontradiktórius vitára tekintettel vizsgálat alá vonja az M. Schrems arra vonatkozó kételyeinek megalapozottságát, hogy megfelelő-e az említett harmadik országban biztosított védelmi szint, annak ellenére, hogy a Bizottság ezt az AVP-határozatban időközben megállapította, ami e bíróságot arra indította, hogy előzetes döntéshozatal céljából előterjessze a negyedik, ötödik és tizedik kérdést.

160 Amint arra a főtanácsnok az indítványának 175. pontjában rámutatott, ezeket az előzetes döntéshozatalra előterjesztett kérdéseket úgy kell értelmezni, hogy azok lényegében a Bizottságnak az AVP-határozatban szereplő azon megállapítását kérdőjelezik meg, amely szerint az Egyesült Államok megfelelő szintű védelmet biztosít az Unióból e harmadik országba továbbított személyes adatok tekintetében, és ennélfogva e határozat érvényességét vonják kétségbe.

161 A jelen ítélet 121. és 157–160. pontjában említett megfontolásokra tekintettel, és annak érdekében, hogy a kérdést előterjesztő bíróság számára teljes körű választ lehessen adni, meg kell tehát vizsgálni, hogy az AVP-határozat megfelel-e a Chartával összefüggésben értelmezett GDPR-ből eredő követelményeknek (lásd analógia útján: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 67. pont).

162 Valamely határozatnak a Bizottság által a GDPR 45. cikkének (3) bekezdése alapján történő elfogadása megköveteli, hogy ezen intézmény kellően megindokolja azon megállapítását, hogy az érintett harmadik ország – belföldi joga, vagy vállalt nemzetközi kötelezettségei alapján – ténylegesen az Unió jogrendjében biztosított védelmi szinttel lényegében megegyező védelmi szintet biztosít az alapvető jogok számára (lásd analógia útján a 95/46 irányelv 25. cikkének (6) bekezdését illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 96. pont).

Az AVP-határozat tartalmáról

163 A Bizottság az AVP-határozat 1. cikkének (1) bekezdésében megállapította, hogy az Egyesült Államok megfelelő szintű védelmet biztosít az Európai Unió–Egyesült Államok adatvédelmi pajzs keretében az Európai Unióból az egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében, amely pajzsot az Egyesült Államok Kereskedelmi Minisztériuma által 2016. július 7-én kibocsátott, az e határozat II. mellékletében ismertetett elvek, valamint az ugyanezen határozat I. és a III–VII. mellékletében felsorolt dokumentumokban foglalt hivatalos nyilatkozatok és kötelezettségvállalások alkotják.

164 Ugyanakkor az AVP-határozat szintén pontosítja az „[Európai Unió–Egyesült Államok] adatvédelmi pajzs keretrendszer elvei” című II. mellékletének I.5. pontjában, hogy ezen elvek betartása többek között „a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítéséhez szükséges mértékben” korlátozható. Így e határozat a 2000/520 határozathoz hasonlóan e követelmények elsőbbségét fejezi ki az említett elvekkel szemben, amely elsőbbség értelmében azok az amerikai

szervezetek, amelyek öntanúsítással rendelkeznek, és személyes adatokat fogadnak az Unióból, korlátozások nélkül kötelesek eltérni ezen elvektől, amennyiben ez utóbbiak összeütközésbe kerülnek e követelményekkel, és azokkal összeegyeztethetetlennek bizonyulnak (lásd analógia útján a 2000/520 határozatot illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 86. pont).

165 Az AVP-határozat II. mellékletének I.5. pontjában szereplő eltérés általános jellegére tekintettel, az a nemzetbiztonságra, a közérdekre vagy az Egyesült Államok belső jogára vonatkozó követelmények alapján így lehetővé teszi a beavatkozást azon személyek alapvető jogaiba, akiknek a személyes adatait az Unióból az Egyesült Államokba továbbítják vagy továbbíthatják (lásd analógia útján a 2000/520 határozatot illetően: 2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 87. pont). Konkrétabban, és amint azt az AVP-határozat megállapítja, az ilyen beavatkozások származhatnak az Unióból az Egyesült Államokba továbbított személyes adatokhoz való hozzáférésből és ezen adatoknak az amerikai hatóságok által a PRISM és az UPSTREAM megfigyelési programok keretében a FISA 702. cikkén, valamint az EO 12333 alapján történő felhasználásából.

166 Ebben az összefüggésben a Bizottság az AVP-határozat (67)–(135) preambulumbekezdésében megvizsgálta az Egyesült Államok szabályozásában, különösen a FISA 702. cikkében, az EO 12333-ban és a PPD-28-ban előírt korlátozásokat és garanciákat az amerikai hatóságoknak az Európai Unió–Egyesült Államok adatvédelmi pajzs alapján továbbított személyes adatokhoz való nemzetbiztonsági, bűnüldözési és egyéb közérdekű célokból történő hozzáférése, és azok ilyen célokból történő felhasználása tekintetében.

167 Ezen értékelés végén a Bizottság e határozat (136) preambulumbekezdésében megállapította, hogy „az Egyesült Államok megfelelő szintű védelmet biztosít […] az Unióból az öntanúsított egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében”, valamint az említett határozat (140) preambulumbekezdésében úgy vélte, hogy „az Egyesült Államok jogrendszerével kapcsolatban rendelkezésre álló információk […] alapján […] az Egyesült Államok hatóságainak nemzetbiztonsági, bűnüldözési vagy egyéb közérdekű célokból azon személyek alapvető jogaiba történő beavatkozása, akiknek az adatait az adatvédelmi pajzs keretében az Unióból az Egyesült Államokba továbbították, valamint ebből következően az öntanúsított vállalatokra az elvek elfogadása tekintetében meghatározott korlátozások a szóban forgó törvényes cél eléréséhez feltétlenül szükséges mértékűre fognak korlátozódni, továbbá hogy hatékony jogvédelem létezik az ilyen beavatkozással szemben”.

A megfelelő védelmi szintre vonatkozó megállapításról

168 A Bizottság által az AVP-határozatban említett elemekre, valamint a kérdést előterjesztő bíróság által az alapeljárásban megállapított körülményekre tekintettel e bíróságnak kétségei vannak azzal kapcsolatban, hogy az Egyesült Államok joga ténylegesen biztosítja-e a Charta 7., 8. és 47. cikkében biztosított alapvető jogok fényében értelmezett GDPR 45. cikkében előírt megfelelő védelmi szintet. Az említett bíróság különösen úgy véli, hogy e harmadik ország joga nem írja elő a nemzeti szabályozása által engedélyezett beavatkozások tekintetében szükséges korlátozásokat és garanciákat, valamint az ilyen beavatkozásokkal szembeni hatékony bírói jogvédelmet sem biztosítja. Ez utóbbi tekintetben hozzáteszi, hogy az adatvédelmi pajzs ombudsmanja intézményének létrehozása szerinte nem orvosolhatja e hiányosságokat, mivel ez az ombudsman nem tekinthető a Charta 47. cikke értelmében vett bíróságnak.

169 Ami először is a Charta 7. és 8. cikkét illeti, amelyek az Unión belül megkövetelt védelmi szinthez tartoznak, amelynek tiszteletben tartását a Bizottságnak meg kell állapítania, mielőtt a GDPR 45. cikkének (1) bekezdése alapján megfelelőségi határozatot fogadna el, emlékeztetni kell arra, hogy a Charta 7. cikke mindenki számára biztosítja a jogot a magán- és családi életének, otthonának és kapcsolattartásának tiszteletben tartásához. Ami a Charta 8. cikkének (1) bekezdését illeti, ez kifejezetten elismeri, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

170 Így valamely természetes személy személyes adataihoz a megőrzésük vagy felhasználásuk érdekében való hozzáférés sérti e személynek a Charta 7. cikkében biztosított, a magánélet tiszteletben tartásához való alapvető jogát, mivel e jog az azonosított vagy azonosítható természetes személyre vonatkozó valamennyi információra vonatkozik. Az említett adatkezelések a Charta 8. cikkéhez is kapcsolódnak, mert az e cikk értelmében vett személyesadat-kezelésnek minősülnek, és következésképpen szükségszerűen meg kell felelniük az említett cikkben előírt adatvédelmi követelményeknek (lásd ebben az értelemben: 2010. november 9-i Volker und Markus Schecke és Eifert ítélet, C-92/09 és C-93/09, EU:C:2010:662, 49. és 52. pont; 2014. április 8-i Digital Rights Ireland és társai ítélet, C-293/12 és C-594/12, EU:C:2014:238, 29. pont; 2017. július 26-i 1/15 [EU-Kanada PNR-megállapodás] vélemény, EU:C:2017:592, 122. és 123. pont).

171 A Bíróság már megállapította, hogy a személyes adatok harmadik személlyel – így például valamely állami hatósággal – való közlése a Charta 7. és 8. cikkében biztosított alapvető jogokba történő beavatkozásnak minősül, függetlenül attól, hogy a közölt információkat utóbb mire használják. Ugyanez vonatkozik a személyes adatok megőrzésére, valamint az említett adatokhoz a hatóságok általi felhasználásuk érdekében való hozzáférésre, függetlenül attól, hogy az érintett, magánéletre vonatkozó információk érzékeny jellegűek-e, vagy hogy az érintetteknek ez a beavatkozás okozott-e esetleges kellemetlenséget, vagy sem (lásd ebben az értelemben: 2003. május 20-i Österreichischer Rundfunk és társai ítélet, C-465/00, C-138/01 és C-139/01, EU:C:2003:294, 74. és 75. pont; 2014. április 8-i Digital Rights Ireland és társai ítélet, C-293/12 és C-594/12, EU:C:2014:238, 33–36. pont; 2017. július 26-i 1/15 [EU-Kanada PNR-megállapodás] vélemény, EU:C:2017:592, 124. és 126. pont).

172 Azonban a Charta 7. és 8. cikkében biztosított jogok nem korlátlan jogosultságokat jelentenek, hanem azokat a társadalomban betöltött szerepük alapján kell megítélni (lásd ebben az értelemben: 2010. november 9-i Volker und Markus Schecke és Eifert ítélet, C-92/09 és C-93/09, EU:C:2010:662, 48. pont, valamint az ott hivatkozott ítélkezési gyakorlat; 2013. október 17-i Schwarz ítélet, C-291/12, EU:C:2013:670, 33. pont, valamint az ott hivatkozott ítélkezési gyakorlat; 2017. július 26-i 1/15 [EU-Kanada PNR-megállapodás] vélemény, EU:C:2017:592, 136. pont).

173 E tekintetben meg kell állapítani azt is, hogy a Charta 8. cikkének (2) bekezdése szerint a személyes adatokat többek között csak „meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni”.

174 Továbbá a Charta 52. cikke (1) bekezdésének első mondata szerint a Chartában elismert jogok és szabadságok gyakorlása csak a törvény által, és e jogok és szabadságok lényeges tartalmának tiszteletben tartásával korlátozható. A Charta 52. cikke (1) bekezdésének második mondata szerint az arányosság elvére figyelemmel, e jogok és szabadságok korlátozására csak akkor és annyiban kerülhet sor, ha és amennyiben az elengedhetetlen és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.

175 Ez utóbbi tekintetben hozzá kell tenni, hogy az a követelmény, miszerint e jog gyakorlása csak a törvény által korlátozható, magában foglalja, hogy a beavatkozást lehetővé tevő jogalapnak magának kell meghatároznia az érintett jog gyakorlásával kapcsolatos korlátozás terjedelmét (2017. július 26-i 1/15 [EU-Kanada PNR-megállapodás] vélemény, EU:C:2017:592, 139. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

176 Végül az arányosság követelményének való megfelelés érdekében, amely szerint a személyes adatok védelme alóli eltéréseknek és e védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk, mivel a szóban forgó, beavatkozást tartalmazó szabályozásnak egyértelmű és pontos szabályokat kell tartalmaznia a szóban forgó intézkedés hatálya és alkalmazása tekintetében, és minimumkövetelményeket kell előírnia, oly módon, hogy azok a személyek, akiknek az adatait továbbították, elegendő garanciákkal rendelkezzenek, amelyek lehetővé teszik a személyes adataiknak a visszaélések veszélyeivel szembeni hatékony védelmét. Meg kell jelölnie különösen, hogy milyen körülmények között és milyen feltételek mellett lehet az ilyen adatok kezelését előíró intézkedést

megtenni, biztosítva ezáltal, hogy a beavatkozás a szigorúan szükséges mértékre korlátozódjék. Az ilyen biztosítékokkal való rendelkezés szükségessége még fontosabb abban az esetben, ha a személyes adatokat automatikusan kezelik (lásd ebben az értelemben: 2017. július 26-i 1/15 [EU-Kanada PNR-megállapodás] vélemény, EU:C:2017:592, 140. és 141. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

177 E tekintetben a GDPR 45. cikke (2) bekezdésének a) pontja pontosítja, hogy annak mérlegelése során, hogy a harmadik ország által biztosított védelmi szint megfelelő-e, a Bizottság figyelembe veszi többek között „[azon érintettek] hatékonyan érvényesíthető [jogait]”, akiknek a személyes adatait továbbítják.

178 A jelen ügyben megkérdőjelezték a Bizottság által az AVP-határozatban tett azon megállapítást, amely szerint az Egyesült Államok a Charta 7. és 8. cikkével összefüggésben értelmezett GDPR által az Unióban biztosított védelmi szinttel lényegében azonos védelmi szintet biztosít, többek között azzal az indokkal, hogy a FISA 702. cikkén és az EO 12333-on alapuló megfigyelési programokból eredő beavatkozásokra nem vonatkoznak olyan követelmények, amelyek az arányosság elvének tiszteletben tartása mellett lényegében a Charta 52. cikke (1) bekezdésének második mondata által biztosított védelmi szinttel lényegében azonos védelmi szintet biztosítanak. Meg kell tehát vizsgálni, hogy e megfigyelési programokat e követelmények betartásával hajtják-e végre, anélkül hogy előzetesen vizsgálni kellene, hogy e harmadik ország tiszteletben tartja-e a Charta 52. cikke (1) bekezdésének első mondatában előírtakkal lényegében azonos feltételeket.

179 E tekintetben a FISA 702. cikkén alapuló megfigyelési programokat illetően a Bizottság az AVP-határozat (109) preambulumbekezdésében megállapította, hogy az említett cikk szerint „a FISC nem egyéni megfigyelési intézkedéseket, hanem megfigyelési programokat (mint a PRISM, UPSTREAM) engedélyez a legfőbb ügyész és a nemzeti hírszerzési igazgató által készített éves tanúsítványok alapján”. Amint az ugyanezen preambulumbekezdésből kitűnik, a FISC által végzett ellenőrzés így annak vizsgálatára irányul, hogy e megfigyelési programok megfelelnek-e a külföldi hírszerzési információk megszerzésére irányuló célnak, de nem terjed ki arra a kérdésre, hogy „az egyéneket megfelelően veszik-e célba a külföldi hírszerzési információk megszerzéséhez”.

180 Úgy tűnik tehát, hogy a FISA 702. cikkéből semmilyen módon nem következik az abban foglalt, a megfigyelési programok külföldi hírszerzés céljából történő végrehajtására vonatkozó felhatalmazás korlátozásának létezése, sem pedig az e programok által esetlegesen érintett, nem amerikai személyek számára szóló garanciák fennállása. E körülmények között, és amint arra a főtanácsnok az indítványának 291., 292. és 297. pontjában lényegében rámutatott, e cikk nem alkalmas arra, hogy a Charta által biztosított, a jelen ítélet 175. és 176. pontjában felidézett ítélkezési gyakorlat által értelmezett védelmi szinttel lényegében azonos védelmi szintet biztosítson, amely szerint az alapvető jogokba való beavatkozást lehetővé tevő jogalapnak az arányosság elvének való megfelelés érdekében magának kell meghatároznia az érintett jog gyakorlása korlátozásának terjedelmét, és egyértelmű és pontos szabályokat kell tartalmaznia a szóban forgó intézkedés hatálya és alkalmazása tekintetében, valamint minimumkövetelményeket kell előírnia.

181 Az AVP-határozatban szereplő megállapítások szerint a FISA 702. cikkén alapuló megfigyelési programokat kétségtelenül a PPD-28-ból eredő követelmények tiszteletben tartásával kell végrehajtani. Ugyanakkor, bár a Bizottság az AVP-határozat (69) és (77) preambulumbekezdésében hangsúlyozta, hogy az ilyen követelmények kötelező jellegűek az amerikai hírszerzési szervezetekre nézve, az amerikai kormány a Bíróság kérdésére adott válaszában elismerte, hogy a PPD-28 nem biztosít az érintett személyek számára az amerikai hatóságokkal szemben a bíróságok előtt érvényesíthető jogokat. Ennélfogva nem alkalmas arra, hogy a Chartából eredő védelmi szinttel lényegében azonos védelmi szintet biztosítson, ellentétben azzal, amit a GDPR 45. cikke (2) bekezdésének a) pontja megkövetel, amely szerint e szint megállapítása többek között azon tényleges és érvényesíthető jogok fennállásától függ, amelyek azokat a személyeket illetik, akiknek az adatait a szóban forgó harmadik országba továbbították.

182 Az EO 12333-on alapuló megfigyelési programokat illetően a Bíróság rendelkezésére álló iratanyagból kitűnik, hogy e rendelet sem biztosít az amerikai hatóságokkal szemben a bíróságok előtt érvényesíthető jogokat.

183 Hozzá kell tenni, hogy a PPD-28, amelyet tiszteletben kell tartani az előző két pontban említett programok alkalmazása során, lehetővé teszi „a „nagy mennyiségű” gyűjtés[ét] viszonylag nagy mennyiségű jelfelderítési információ[nak] vagy adat[nak] olyan körülmények között, amikor a hírszerzés nem tud a konkrét célszemélyhez társítható azonosítót […] alkalmazni az adatgyűjtés fókuszálása céljából”, amint azt az AVP-határozat VI. mellékletében szereplő, a nemzeti hírszerzés igazgatója irodájának (Office of the Director of National Intelligence) az amerikai kereskedelmi minisztérium és a nemzetközi kereskedelmi igazgatóság részére címzett 2016. június 21-i levelében kifejtették. Márpedig ez a lehetőség, amely az EO 12333-on alapuló megfigyelési programok keretében megengedi az Egyesült Államokba továbbított adatokhoz való hozzáférést anélkül, hogy e hozzáférés bármiféle bírósági felügyelet alá tartozna, semmi esetre sem szabályozza kellőképpen egyértelműen és pontosan a személyes adatok ilyen tömeges gyűjtésének terjedelmét.

184 Ennélfogva úgy tűnik, hogy sem a FISA 702. cikke, sem az EO 12333 – a PPD-28-cal összefüggésben értelmezve – nem felel meg az uniós jogban az arányosság elvéhez társított minimális követelményeknek, így nem lehet úgy tekinteni, hogy az e rendelkezéseken alapuló megfigyelési programok a feltétlenül szükséges mértékre korlátozódnak.

185 E körülmények között a személyes adatok védelmének korlátozásai, amelyek az Egyesült Államok azon belső szabályozásából erednek, amelyek az amerikai hatóságok által az Unióból az Egyesült Államokba továbbított ilyen adatokhoz való hozzáférésre és azok felhasználására vonatkoznak, és amely korlátozásokat a Bizottság az AVP-határozatban értékelt, nem úgy lettek szabályozva, hogy megfeleljenek a Charta 52. cikke (1) bekezdésének második mondata által az uniós jogban megkövetelt követelményekkel lényegében azonos követelményeknek.

186 Másodszor, ami a Charta 47. cikkét illeti, amely szintén része az Unión belül megkövetelt védelmi szintnek, és amelynek tiszteletben tartását a Bizottságnak meg kell állapítania, mielőtt a GDPR 45. cikkének (1) bekezdése alapján megfelelőségi határozatot fogadna el, emlékeztetni kell arra, hogy e 47. cikk első bekezdése megköveteli, hogy mindenkinek, akinek az Unió joga által biztosított jogait és szabadságait megsértették, a hivatkozott cikkben megállapított feltételek mellett joga van a bíróság előtti hatékony jogorvoslathoz. E cikk második bekezdése szerint mindenkinek joga van arra, hogy ügyét független és pártatlan bíróság tárgyalja.

187 Az állandó ítélkezési gyakorlat szerint az uniós jogi rendelkezések tiszteletben tartásának biztosítására irányuló hatékony bírói felülvizsgálat fennállása a jogállamiság létének velejárója. Így az olyan szabályozás, amely nem biztosít a jogalany számára semmilyen jogorvoslati lehetőséget abból a célból, hogy a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltesse, nem tartja tiszteletben a hatékony bírói jogvédelemhez való jog lényegét, amelyet a Charta 47. cikke mond ki (2015. október 6-i Schrems ítélet, C-362/14, EU:C:2015:650, 95. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

188 E célból a GDPR 45. cikke (2) bekezdésének a) pontja megköveteli, hogy a Bizottság a harmadik ország által biztosított védelmi szint megfelelőségének értékelésekor figyelembe vegye többek között azt, hogy „az érintettek, akiknek a személyes adatait továbbítják, rendelkeznek-e […] hatékony közigazgatási és bírósági jogorvoslat[tal]”. A GDPR (104) preambulumbekezdése e tekintetben hangsúlyozza, hogy a harmadik országnak „gondoskodnia kell a tényleges, független adatvédelmi felügyeletről és tagállami adatvédelmi hatóságokkal való együttműködési mechanizmusairól, továbbá biztosítania kell, hogy az érintettek tényleges és érvényesíthető jogokkal, valamint hatékony közigazgatási és bírósági jogorvoslati lehetőségekkel rendelkezzenek”.

189 Az ilyen hatékony jogorvoslati lehetőségeknek az érintett harmadik országban való fennállása különös jelentőséggel bír a személyes adatoknak az e harmadik országba irányuló továbbításával összefüggésben, mivel – amint az a GDPR (116) preambulumbekezdéséből kitűnik – az érintett személyek szembesülhetnek a tagállamok közigazgatási és igazságügyi hatóságainak arra vonatkozó hatásköreinek és eszközeinek elégtelenségével, hogy kielégítő választ adjanak az így továbbított adatok e harmadik országban történő állítólagosan jogellenes kezelésén alapuló panaszaikra, amely arra kényszeríti őket, hogy ugyanezen harmadik ország nemzeti hatóságaihoz és bíróságaihoz forduljanak.

190 A jelen ügyben megkérdőjelezték a Bizottság által az AVP-határozatban tett azon megállapítást, amely szerint az Egyesült Államok a Charta 47. cikkében biztosított védelmi szinttel lényegében azonos védelmi szintet biztosít, többek között azzal az indokkal, hogy az adatvédelmi pajzs ombudsmanja intézményének létrehozása nem küszöbölheti ki a Bizottság által azon személyek bírói jogvédelmét illetően megállapított hiányosságokat, akiknek a személyes adatait e harmadik országba továbbítják.

191 E tekintetben a Bizottság az AVP-határozat (115) preambulumbekezdésében rámutatott, hogy jóllehet „az egyéneknek – köztük az uniós érintetteknek – tehát számos jogorvoslati lehetőség áll a rendelkezésére, ha nemzetbiztonsági célú, jogellenes (elektronikus) megfigyelést folytatnak velük szemben, az is egyértelmű, hogy e jogorvoslati lehetőségek nem terjednek ki legalább néhány olyan jogalapra (pl. az [EO 12333]), amelyet az Egyesült Államok hírszerzési hatóságai igénybe vehetnek”. Így az EO 12333 kapcsán az említett (115) preambulumbekezdésben a jogorvoslati lehetőségek hiányára helyezi a hangsúlyt. Márpedig a jelen ítélet 187. pontjában felidézett ítélkezési gyakorlat szerint az ezen elnöki rendeleten alapuló megfigyelési programokhoz kapcsolódó beavatkozásokkal kapcsolatos bírói jogvédelemben mutatkozó ilyen hiányosság megakadályozza annak megállapítását, hogy – amint azt a Bizottság az AVP-határozatban tette – az Egyesült Államok joga a Charta 47. cikkében biztosított védelmi szinttel lényegében azonos védelmi szintet biztosít.

192 Egyébiránt, ami mind a FISA 702. cikkén alapuló megfigyelési programokat, mind pedig az EO 12333-on alapuló megfigyelési programokat illeti, a jelen ítélet 181. és 182. pontjában megállapításra került, hogy sem a PPD-28, sem az EO 12333 nem biztosít az érintett személyeknek olyan jogokat, amelyek az amerikai hatóságokkal szemben érvényesíthetők a bíróságok előtt, így e személyek nem rendelkeznek hatékony jogorvoslathoz való joggal.

193 A Bizottság azonban az AVP-határozat (115) és (116) preambulumbekezdésében megállapította, hogy az amerikai hatóságok által bevezetett ombudsmani mechanizmus fennállása miatt, amint azt az amerikai külügyminiszter által a jogérvényesülésért, a fogyasztópolitikáért és a nemek közötti esélyegyenlőségért felelős európai biztoshoz intézett, e határozat III. mellékletében szereplő 2016. július 7-i levél kifejti, valamint az ombudsmanra háruló feladatkör jellege okán, amely a jelen esetben „nemzetközi informatikai diplomáciai főkoordinátor”, az Egyesült Államok úgy tekinthető, mint amely a Charta 47. cikkében biztosított védelmi szinttel lényegében azonos védelmi szintet biztosít.

194 Azon kérdés vizsgálatának, hogy az AVP-határozatban említett ombudsmani mechanizmus valóban alkalmas-e arra, hogy kiküszöbölje a bírói jogvédelemhez való jog Bizottság által megállapított korlátozásait, a Charta 47. cikkéből és a jelen ítélet 187. pontjában felidézett ítélkezési gyakorlatból eredő követelményeknek megfelelően abból az elvből kell kiindulnia, hogy a jogalanyoknak rendelkezniük kell azzal a lehetőséggel, hogy független és pártatlan bíróság előtt éljenek jogorvoslati lehetőségekkel abból a célból, hogy a rájuk vonatkozó személyes adatokhoz hozzáférést kapjanak, vagy az ilyen adatokat helyesbíttetni vagy töröltetni tudják.

195 Márpedig a jelen ítélet 193. pontjában hivatkozott levélben az adatvédelmi pajzs ombudsmanját, jóllehet úgy jellemzik, hogy a „[hírszerző szervezetektől] független”, úgy mutatták be, hogy „közvetlenül a külügyminiszternek tesz jelentést, aki biztosítja, hogy az ombudsman tárgyilagosan az adandó válasz megváltoztatására alkalmas, helytelen befolyásolásától mentesen láthassa el a feladatát”. Egyébiránt, azon a tényen kívül, hogy – amint azt a Bizottság e határozat (116) preambulumbekezdésében megállapította – az ombudsmant a külügyminiszter nevezi ki, és az

Egyesült Államok külügyminisztériumának szerves részét képezi, az említett határozatban – amint azt a főtanácsnok az indítványának 337. pontjában megállapította – nincs arra vonatkozó utalás, hogy az ombudsman visszahívásához vagy kinevezésének megszüntetéséhez bármilyen különös garancia kapcsolódna, ami olyan jellegű, hogy megkérdőjelezi az ombudsmannak a végrehajtó hatalomtól való függetlenségét (lásd ebben az értelemben: 2020. január 21-i Banco de Santander ítélet, C-274/14, EU:C:2020:17, 60. és 63. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

196 Ugyanígy, amint azt a főtanácsnok az indítványának 338. pontjában hangsúlyozta, bár az AVP-határozat (120) preambulumbekezdése említést tesz az amerikai kormány azon kötelezettségvállalásáról, hogy a hírszerzési szervezetek érintett egységének orvosolnia kell az alkalmazandó szabályoknak az adatvédelmi pajzs ombudsmanja által észlelt bármely megsértését, az említett határozat *semmilyen utalást nem tartalmaz arra vonatkozóan, hogy ezen ombudsmannak felhatalmazása lenne* arra, hogy e szervezetekkel szemben kötelező erejű határozatokat *hozzon*, és nem tartalmaz olyan jogszabályi garanciákat sem, amelyek e kötelezettségvállaláshoz társulnának, és amelyekre az érintett személyek hivatkozhatnának.

197 Ennélfogva az AVP-határozatban említett ombudsmani mechanizmus nem biztosít jogorvoslati lehetőséget olyan szerv előtt, amely a Charta 47. cikkében előírt garanciákkal lényegében azonos garanciákat nyújtana azon személyek számára, akiknek az adatait az Egyesült Államokba továbbították.

198 Következésképpen a Bizottság azzal, hogy az AVP-határozat 1. cikkének (1) bekezdésében megállapította, hogy az Egyesült Államok megfelelő szintű védelmet biztosít az Unióból az Európai Unió–Egyesült Államok adatvédelmi pajzs keretében az e harmadik országban letelepedett szervezetek részére továbbított személyes adatok tekintetében, megsértette a Charta 7., 8. és 47. cikkével összefüggésben értelmezett GDPR 45. cikkének (1) bekezdéséből eredő követelményeket.

199 Ebből következik, hogy az AVP-határozat 1. cikke összeegyeztethetetlen a Charta 7., 8. és 47. cikkével összefüggésben értelmezett GDPR 45. cikkének (1) bekezdésével, és ezért érvénytelen.

200 Mivel az AVP-határozat 1. cikke elválaszthatatlan annak 2–6. cikkétől, valamint a mellékleteitől, annak érvénytelensége e határozat egészének érvényességét érinti.

201 A fenti megfontolások összességére tekintettel meg kell állapítani, hogy az AVP-határozat érvénytelen.

202 Azon kérdés kapcsán, hogy fenn kell-e tartani e határozat joghatásait a joghézag kialakulásának elkerülése érdekében (lásd ebben az értelemben: 2016. április 28-i Borealis Polyolefine és társai ítélet, C-191/14, C-192/14, C-295/14, C-389/14 és C-391/14–C-393/14, EU:C:2016:311, 106. pont), mindenesetre meg kell jegyezni, hogy tekintettel a GDPR 49. cikkére, az AVP-határozathoz hasonló megfelelőségi határozat megsemmisítése nem keletkeztethet ilyen joghézagot. E cikk ugyanis pontosan meghatározza azokat a feltételeket, amelyek mellett a személyes adatok harmadik országba történő továbbítására az említett rendelet 45. cikkének (3) bekezdése szerinti megfelelőségi határozat vagy az ugyanezen rendelet 46. cikke szerinti megfelelő garanciák hiányában sor kerülhet.

A költségekről

203 Mivel ez az eljárás az alapeljárásban részt vevő felek számára a kérdést előterjesztő bíróság előtt folyamatban lévő eljárás egy szakaszát képezi, ez a bíróság dönt a költségekről. Az észrevételeknek a Bíróság elé terjesztésével kapcsolatban felmerült költségek, az említett felek költségeinek kivételével, nem téríthetők meg.

A fenti indokok alapján a Bíróság (nagytanács) a következőképpen határozott:

1) 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 szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet) 2. cikkének (1) és (2) bekezdését úgy kell értelmezni, hogy e rendelet hatálya alá tartozik a személyes adatoknak a valamely tagállamban letelepedett gazdasági szereplő által valamely harmadik országban letelepedett másik gazdasági szereplő részére kereskedelmi célból végzett továbbítása, függetlenül attól, hogy ezeket az adatokat e továbbítás során vagy azt követően az érintett harmadik ország hatóságai közbiztonsági, honvédelmi és nemzetbiztonsági célból kezelhetik.

2) A 2016/679 rendelet 46. cikkének (1) bekezdését és 46. cikke (2) bekezdésének c) pontját úgy kell értelmezni, hogy az e rendelkezések által megkövetelt megfelelő garanciáknak, érvényesíthető jogoknak és hatékony jogorvoslati lehetőségeknek biztosítaniuk kell, hogy azon személyek jogai, akiknek a személyes adatait az általános adatvédelmi kikötések alapján továbbítják harmadik országba, olyan védelmi szinttel rendelkezzenek, amely lényegében azonos az Európai Unió Alapjogi Chartája fényében értelmezett e rendelet által az Európai Unióban biztosított védelmi szinttel. E célból az ilyen továbbítással összefüggésben biztosított védelmi szint értékelésének figyelembe kell vennie többek között mind az Európai Unióban letelepedett adatkezelő vagy az ott letelepedett adatfeldolgozója és a továbbításnak az érintett harmadik országban letelepedett címzettje között létrejött szerződéses kikötéseket, mind pedig – e harmadik ország hatóságainak az így továbbított személyes adatokhoz való esetleges hozzáférését illetően – az ezen ország jogrendszerének releváns elemeit, különösen az említett rendelet 45. cikkének (2) bekezdésében felsorolt elemeket.

3) A 2016/679 rendelet 58. cikke (2) bekezdésének f) és j) pontját úgy kell értelmezni, hogy az illetékes felügyeleti hatóság – feltéve, hogy nem létezik az Európai Bizottság által érvényesen elfogadott megfelelőségi határozat – köteles felfüggeszteni vagy megtiltani a személyes adatoknak a Bizottság által elfogadott általános adatvédelmi kikötéseken alapuló, harmadik országba irányuló továbbítását, ha e felügyeleti hatóság az e továbbítás sajátos körülményeinek összességére tekintettel úgy ítéli meg, hogy e kikötéseket e harmadik országban nem tartják be, vagy azokat ott nem lehet tiszteletben tartani, és hogy a továbbított adatok védelme, amelyet az uniós jog, különösen az e rendelet 45. és 46. cikke, valamint az Alapjogi Charta megkövetel, más eszközzel nem biztosítható, amennyiben az Unióban letelepedett adatkezelő vagy az ott letelepedett adatfeldolgozója maga nem függesztette fel vagy fejezte be az adattovábbítást.

4) A 2016. december 16-i (EU) 2016/2297 bizottsági végrehajtási határozattal módosított, a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2010. február 5-i 2010/87/EU bizottsági határozatnak az Alapjogi Charta 7., 8. és 47. cikkére tekintettel történő vizsgálata nem tárt fel olyan tényezőt, amely e határozat érvényességét érintené.

5) A 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló, 2016. július 12-i (EU) 2016/1250 bizottsági végrehajtási határozat érvénytelen.

Aláírások