



ELFOGADOTT SZÖVEGEK

P8_TA(2018)0529

A személyes adatok Japán által biztosított védelmének megfelelősége

Az Európai Parlament 2018. december 13-i állásfoglalása a személyes adatok Japán által biztosított védelmének megfelelőségéről (2018/2979(RSP))

Az Európai Parlament,

- tekintettel az Európai Unióról szóló szerződésre, az Európai Unió működéséről szóló szerződésre és az Európai Unió Alapjogi Chartájának 6., 7., 8., 11., 16., 47. és 52. cikkére,
- tekintettel 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 rendeletre (általános adatvédelmi rendelet)¹, és egyéb vonatkozó uniós adatvédelmi vívmányokra,
- tekintettel a Bíróság által a C-362/14. sz. Maximillian Schrems kontra adatvédelmi biztos ügyben hozott, 2015. október 6-i ítéletre²,
- tekintettel a Bíróság által a C-203/15. sz. Tele2 Sverige AB kontra Post- och telestyrelsen és a C-698/15. sz. Secretary of State for the Home Department kontra Tom Watson és társai egyesített ügyekben hozott, 2016. december 21-i ítéletre³,
- tekintettel „A digitális kereskedelmi stratégia felé” című, 2017. december 12-i állásfoglalására⁴
- tekintettel a 29. cikk szerinti munkacsoport „Megfelelőségi referencia” című, 2018. február 6-i dokumentumára⁵, amely iránymutatást nyújt a Bizottság és az Európai Adatvédelmi Testület számára az általános adatvédelmi rendelet keretében a harmadik

¹ HL L 119., 2016.5.4., 1. o.

² ECLI:EU:C:2015:650.

³ ECLI:EU:C:2016:970.

⁴ HL C 369., 2018.10.11., 22. o.

⁵ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108; amelyet az Európai Adatvédelmi Testület első plenáris ülésén hagyott jóvá.

országokban és nemzetközi szervezetekben biztosított adatvédelem szintjének értékeléséhez,

- tekintettel az Európai Adatvédelmi Testület az EU–Japán közötti megfeleléségi határozat tervezetéről szóló, 2018. december 5-i véleményére,
 - tekintettel a személyes adatok Japán által biztosított megfelelő védelméről szóló (EU) 2016/679 európai parlamenti és tanácsi rendelet szerinti bizottsági végrehajtási határozatra irányuló tervezetre (COM(2018)XXXX),
 - tekintettel a 2017. októberben az Állampolgári Jogi, Bel- és Igazságügyi Bizottság eseti küldöttsége által Japánban tett látogatás megállapításaira, amelyet a megfeleléségi tárgyalások keretében az érintett japán hatóságokkal és az érdekelt felekkel való találkozás céljából szerveztek azokkal az alapvető elemekkel kapcsolatban, amelyeket a Bizottságnak a megfeleléségi határozat elfogadásakor figyelembe kell vennie,
 - tekintettel eljárási szabályzata 123. cikkének (2) bekezdésére,
- A. mivel az általános adatvédelmi rendeletet 2018. május 25. óta kell alkalmazni; mivel az általános adatvédelmi rendelet 45. cikkének (2) bekezdése meghatározza azokat az elemeket, amelyeket a Bizottságnak figyelembe kell vennie a harmadik ország vagy nemzetközi szervezet által nyújtott védelem szintje megfeleléségének értékelése során;
- B. mivel a Bizottságnak különösen figyelembe kell vennie a jogállamiságot, az emberi jogok és alapvető szabadságok tiszteletben tartását, a vonatkozó – mind általános, mind ágazati – jogszabályokat, beleértve a közbiztonságra, a védelemre, a nemzetbiztonságra, a büntetőjogra és a közigazgatási szervek személyes adatokhoz való hozzáférésére vonatkozó jogszabályokat, az egy vagy több független felügyeleti hatóság meglétét és hatékony működését, valamint a harmadik ország vagy nemzetközi szervezet által vállalt nemzetközi kötelezettségeket;
- C. mivel a Bíróság által a C-362/14. sz. Maximillian Schrems kontra adatvédelmi biztos ügyben hozott, 2015. október 6-i ítéletében világossá tette, hogy a valamely harmadik országban biztosított, megfelelő szintű védelmet úgy kell értelmezni, hogy az „lényegében egyenértékű” az Európai Unióban a Chartával összefüggésben értelmezett 95/46/EK irányelv értelmében biztosított védelemmel;
- D. mivel Japán az EU egyik fő kereskedelmi partnere, amellyel a közelmúltban gazdasági partnerségi megállapodást (GPM) kötött, amely rögzíti a közös értékeket és elveket, miközben mindkét védelmet biztosít az érzékeny területek számára mindkét partner vonatkozásában; mivel az alapvető jogok – többek között a magánélet védelme és az adatvédelem – közös elismerése fontos a megfeleléségi határozat megalapozásához, amely jogi alapot biztosít majd az EU-ból Japánba továbbított személyes adatok esetében;
- E. mivel az Állampolgári Jogi, Bel- és Igazságügyi Bizottság Japánba indított eseti küldöttsége figyelmét felhívták arra, hogy a japán hatóságok és az érdekelt felek nem csupán az általános adatvédelmi rendelet új előírásainak alkalmazása iránt érdeklődnek, hanem az EU és Japán közötti olyan biztos és magas szintű személyesadat-továbbítási mechanizmus iránt is, amely a védelmi szint vonatkozásában megfelelne az uniós jogi

keret által meghatározott feltételeknek, amelyet lényegében egyenértékűnek tekintenek az uniós adatvédelmi jogszabályok által biztosított védelmi szinttel;

- F. mivel a személyes adatok EU és Japán közötti, kereskedelmi célú átadása az EU–Japán kapcsolatok fontos eleme a globális gazdaság egyre növekvő digitalizációja fényében; mivel az ilyen adattovábbításnak a személyes adatok védelméhez való jog és a magánélethez való jog maradéktalan tiszteletben tartása mellett kell történnie; mivel az EU egyik alapvető célkitűzése az alapvető jogok védelme az Európai Unió Alapjogi Chartájában foglaltaknak megfelelően;
- G. mivel az EU és Japán 2017 januárjában kezdett tárgyalásokat annak érdekében, hogy világszerte páratlan módon „kölsönös megfeleléségi megállapítás” révén előmozdítsa a személyes adatok kereskedelmi célú továbbítását; mivel a Parlament „A digitális kereskedelmi stratégia felé” című 2017. december 12-i állásfoglalásában kifejezetten „elismeri, hogy a megfeleléségi határozatok [...] alapvető mechanizmusát képezik a személyes adatok Unióból harmadik országba történő átadásának”;
- H. mivel a személyes adatok Japánba történő továbbítására vonatkozó megfeleléségi határozat az első ilyen határozat lenne, amelyet az általános adatvédelmi rendelet új és szigorúbb szabályai alapján fogadtak el;
- I. mivel Japán a közelmúltban korszerűsítette és megerősítette az adatvédelmi jogszabályait annak érdekében, hogy összhangba hozza azokat a nemzetközi normákkal, különösen az új európai adatvédelmi jogszabályi keretben foglalt biztosítékokkal és személyhez fűződő jogokkal; mivel a japán adatvédelmi jogi keret különböző pillérekből áll, ahol a személyes információk védelméről szóló jogi aktus (APPI) a jogszabályok központi elemét képezi;
- J. mivel a japán kabinet 2018. június 12-én kabineti rendeletet fogadott el, amelynek értelmében a személyes információk védelmével foglalkozó bizottságot (PPC), mint az APPI igazgatásáért és végrehajtásáért felelős hatóságot azzal a jogkörrel ruházza fel, hogy a jogi aktus 6. cikke alapján megtegye a szükséges lépéseket a Japán és az érintett külföldi ország rendszerei és műveletei közötti különbségek áthidalására, az ezen országtól kapott személyes információk megfelelő kezelésének biztosítása céljából”; mivel ez a rendelet megállapítja, hogy mindez magában foglalja azt a jogkört, hogy a személyes információk védelméről szóló jogi aktusban és a kabineti rendeletben meghatározottakat kiegészítő és meghaladó, szigorúbb szabályok elfogadásával a személyes információk védelmével foglalkozó bizottság fokozott védelmet hozzon létre; mivel e rendelet értelmében ezek a szigorúbb szabályok a japán üzleti szereplők tekintetében kötelező érvényűvé és végrehajthatóvá válnak;
- K. mivel a személyes adatok Japán által biztosított megfelelő védelméről szóló bizottsági végrehajtási határozatra irányuló tervezethez az I. mellékletében csatolták a PPC által 2018. június 15-én elfogadott kiegészítő szabályokat, amelyek az APPI 6. cikkén alapulnak, amely kifejezetten lehetővé teszi a PPC számára, hogy szigorúbb szabályokat fogadjon el, többek között a nemzetközi adattovábbítások előmozdítása céljából; mivel a kiegészítő szabályok nyilvánosan még nem elérhetők;
- L. mivel e kiegészítő szabályok célja a japán és az uniós adatvédelmi jog közötti releváns különbségek kezelése annak érdekében, hogy biztosítsák az EU-tól kapott személyes adatok megfelelő kezelését a megfeleléségi határozat alapján, különös tekintettel a

különleges gondosságot igénylő személyes adatokra (érzékeny adatok), a megőrzött személyes adatokra, meghatározva a felhasználás célját, továbbá a felhasználási célból fakadó korlátozásra, a harmadik fél számára más országban történő rendelkezésre bocsátás korlátozására, valamint a névtelenül feldolgozott információkra;

- M. mivel a kiegészítő szabályok jogilag kötelező érvényűek lennének a személyes információkat kezelő minden olyan üzleti szereplőre nézve, amely az EU-ból megfelelőségi határozat alapján továbbított személyes adatokat kap, és ezért meg kell felelnie az említett szabályoknak és tiszteletben kell tartania minden kapcsolódó jogot és kötelezettséget, valamint hogy e szabályok mind a PPC, mind pedig a japán bíróságok által érvényesíthetők lennének;
- N. mivel annak érdekében, hogy az EU-ból Japánba továbbított személyes adatok lényegében azonos szintű védelme biztosított legyen, a kiegészítő szabályok szigorúbb feltételek vagy korlátozások alapján további védelmet teremtenek az EU-ból továbbított személyes adatok feldolgozása tekintetében, így például a különleges gondosságot igénylő személyes információk, az adattovábbítás, az anonim adatok és a célhoz kötöttség esetében;
- O. mivel a japán adatvédelmi jogi keret különbséget tesz a „személyes információ” és a „személyes adat” között, és bizonyos esetekben a személyes adatok egy speciális kategóriájára, nevezetesen a „megőrzött személyes adatokra” utal;
- P. mivel az APPI 2. cikkének (1) bekezdése szerint a „személyes információ” fogalma magában foglal minden olyan, élő személyre vonatkozó információt, amely lehetővé teszi az adott személy azonosítását; mivel a meghatározás különbséget tesz a személyes adatok két kategóriája, nevezetesen i) az egyedi azonosító kódok és ii) az egyéb személyes adatok között, amelyek alapján egy adott személyt azonosítani lehet; mivel ez utóbbi kategória olyan információkat tartalmaz, amelyek önmagukban nem teszik lehetővé az azonosítást, de más információkkal összeillesztve lehetővé teszik egy adott személy azonosítását;
- Q. mivel az APPI 2. cikkének (4) bekezdése szerint a „személyes adatok” alatt többek között a személyes információk adatbázist alkotó személyes információkat kell érteni; mivel az APPI 2. cikkének (1) bekezdése kimondja, hogy az ilyen adatbázisokban szereplő információk rendszerezettek, ami hasonlatos az általános adatvédelmi rendelet 2. cikkének (1) bekezdése szerinti nyilvántartási rendszer koncepciójához; mivel az általános adatvédelmi rendelet 4. cikke (1) bekezdésének megfelelően a „személyes adat” alatt azonosított vagy azonosítható természetes személyre vonatkozó bármely információ értendő; mivel az a természetes személy minősül azonosíthatónak, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat vagy online azonosító, valamint a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára jellemző egy vagy több tényező alapján azonosítható; mivel egy természetes személy azonosíthatóságának meghatározásakor minden olyan módszert figyelembe kell venni – ideértve például a megjelölést –, amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja;
- R. mivel az APPI 2. cikkének (7) bekezdése szerint a „megőrzött személyes adat” olyan személyes adat, amelyet egy személyes információkat kezelő üzleti szereplőnek jogában

áll közzétenni, helyesbíteni, kiegészíteni vagy tartalmát eltávolítani, felhasználását megszüntetni, törölni, harmadik fél rendelkezésére bocsátását megszüntetni, és nem lehet olyan adat, amely kabineti rendelet szerint sértheti a köz- vagy egyéb érdekeket, amennyiben létezésére vagy hiányára fény derül, sem olyan, amelyet kabineti rendelet értelmében legfeljebb egy éven belül törölni kell; mivel a kiegészítő szabályok a „megőrzött személyes adatok” fogalmát hozzáigazítják a „személyes adatok” fogalmához annak biztosítása érdekében, hogy az előbbihez kapcsolódó, személyhez fűződő jogok bizonyos korlátozásai ne vonatkozzanak az EU-ból továbbított adatokra;

- S. mivel a japán adatvédelmi jogszabály, amely a végrehajtási határozatra irányuló tervezet tárgya, több ágazatot kizár a hatálya alól abban az esetben, ha a személyes adatokat meghatározott célból dolgozzák fel; mivel a végrehajtási határozat tervezete nem vonatkozik a személyes adatoknak az Unióból egy olyan címzett részére történő továbbítására, amely a japán adatvédelmi jog által előírt, fent említett kivételek közé tartozik;
- T. mivel az uniós személyes adatok Japánból harmadik országok részére történő továbbítása tekintetében a végrehajtási határozat tervezete kizárja a japán adatátadó és a harmadik országbeli adatátvevő közötti jogilag kötelező érvényű kapcsolat kialakítását nem biztosító, és a megkövetelt védelmi szintet nem garantáló átviteli eszközök ilyen típusú adattovábbításkor történő alkalmazását; mivel ez a helyzet állna fenn például az Ázsiai és Csendes-óceáni Gazdasági Együttműködés határokön átnyúló adatvédelmi szabályrendszere (APEC CBPR) tekintetében, amelyben Japán gazdasága is részt vesz, mivel ebben a rendszerben a védelem nem az adatátadó és az adatátvevő között kétoldalú kapcsolat keretében létrejött jogilag kötelező erejű rendelkezésekből fakad, és egyértelműen alacsonyabb szintű mint az APPI és a kiegészítő szabályok együttes alkalmazásával biztosított védelem;
- U. mivel 2018. december 5-i véleményében az Európai Adatvédelmi Testület az Európai Bizottság által rendelkezésére bocsátott dokumentumok alapján értékeli, hogy a japán adatvédelmi jogi keretben rendelkezésre állnak-e kielégítő biztosítékok az egyének megfelelő adatvédelmi szintjének biztosításához; mivel az Európai Adatvédelmi Testület üdvözli az Európai Bizottság és a japán PPC által tett, a személyes adatok továbbításának elősegítése céljából a japán és az uniós jogi keret közötti konvergencia fokozására irányuló erőfeszítéseket; mivel az Európai Adatvédelmi Testület elismeri, hogy a kiegészítő szabályokban foglalt, a két jogi keret közötti különbségek áthidalását célzó kiigazítások kiemelkedő jelentőségűek és megfelelő fogadtatásban részesültek; mivel megjegyzi, hogy számos aggodalomra adó részlet maradt, többek között az EU-ból Japánba továbbított személyes adatok teljes életciklusuk során való védelme tekintetében, és ajánlja az Európai Bizottságnak, hogy nyújtson be további bizonyítékokat és magyarázatot a felvetett kérdések kapcsán, és szorosan kövesse figyelemmel a gyakorlati alkalmazást.
- V. mivel a végrehajtási határozat tervezetét a tervezet II. mellékletében csatolt, az igazságügyi miniszter 2018. szeptember 14-i levele is kíséri, amelyben említést tesznek egy, – a japán közigazgatási szervek által bűnüldözési és nemzetbiztonsági célból gyűjtött és felhasznált személyes adatokról szóló – az Igazságügyi Minisztérium, valamint több minisztérium és ügynökség által készített dokumentumról, amelyben áttekintést adnak az alkalmazandó jogi keretről, és a legmagasabb miniszteri és ügynökségi szinten aláírt hivatalos nyilatkozatokat, ígéreteket és kötelezettségvállalásokat tesznek a Bizottság felé;

1. tudomásul veszi a Bizottság által a megfelelőségi végrehajtási határozat tervezetében megadott részletes elemzést a kereskedelmi szereplők által végzett adatfeldolgozásra, valamint a japán állami hatóságok adatokhoz való hozzáférésére vonatkozó biztosítékokkal – köztük a felügyeleti és jogorvoslati mechanizmusokkal – kapcsolatban, különösen a bűnüldözés és a nemzetbiztonság területén;
2. tudomásul veszi, hogy Japán egyidejűleg készíti elő a Japánból az EU-ba továbbított személyes adatok védelmi szintjének elismerését az APPI 23. cikkének megfelelően, amely az első kölcsönös megfelelőségi megállapítást eredményezné világszerte, és a szabad és biztonságos adatáramlás világszerte legnagyobb térségének létrehozásához vezetne;
3. üdvözli ezt a fejleményt, amely a magas adatvédelmi színvonal globális elterjedésének kifejeződése; rámutat azonban arra, hogy ez az EU megfelelőségi határozataiban semmilyen módon nem vezethet arányos viszonyosságon alapuló megközelítés alkalmazásához; emlékeztet arra, hogy az általános adatvédelmi rendelet szerinti megfelelőségi határozat esetében a Bizottságnak objektíven értékelnie kell a harmadik ország, a terület, az ágazat vagy a nemzetközi szervezet jogi és tényleges helyzetét;
4. rámutat arra, hogy az Európai Unió Bírósága ítéletében kimondta, hogy a „megfelelő védelmi szint” fogalma nem követel meg az EU-ban biztosított védelmi szinttel megegyező védelmi szintet, ugyanakkor azt úgy kell érteni, mint amely megköveteli, hogy e harmadik ország – belföldi joga, vagy vállalt nemzetközi kötelezettségei alapján – az Unióban a Chartával összefüggésben értelmezett általános adatvédelmi rendelet által biztosított védelmi szinttel lényegében azonos védelmi szintet biztosítson ténylegesen az alapvető jogok és szabadságok számára;
5. megjegyzi, hogy a magánélet tiszteletben tartásához és a személyes adatok védelméhez való jog mind Japánban, mind pedig az EU-ban alkotmányos szinten garantált, azonban az EU és Japán szabályainak teljes körű összehangolása nem lehetséges az alkotmányos szerkezet és a kultúra közötti különbségek miatt;
6. tudomásul veszi az APPI 2017. május 30-án hatályba lépett módosításait; üdvözli az érdemi javításokat;
7. megjegyzi, hogy az üzleti és feldolgozási tevékenységek azon kategóriáit, amelyek nem tartoznak az APPI tárgyi hatálya alá, kifejezetten kizárták a megfelelőségi megállapítás hatálya alól;
8. úgy véli, hogy a módosított APPI és az általános adatvédelmi rendelet 2016. évi elfogadását követően a japán és az uniós adatvédelmi rendszerek az elvek, a biztosítékok és a személyhez fűződő jogok, valamint a felügyeleti és végrehajtási mechanizmusok tekintetében magas fokú konvergenciát mutatnak; különösen kiemeli, hogy az APPI módosításával létrehoztak egy független felügyeleti hatóságot, a PPC-t;
9. megjegyzi azonban, hogy maga a PPC jut arra következtetésre, hogy „a két rendszer közötti nagyfokú konvergencia ellenére jelentős különbségek mutatkoznak”; megjegyzi továbbá, hogy az EU-ból továbbított személyes adatok magasabb szintű védelme érdekében a PPC 2018. június 15-én kiegészítő szabályokat fogadott el;

10. üdvözlí a kiegészítı szabályok fontos pontosításait, többek között az APPI-ban foglalt „anonimizált személyes információk” fogalmának összhangba hozását az általános adatvédelmi rendeletben szereplı „anonim információ” fogalommeghatározásával;
11. úgy véli, hogy a kiegészítı szabályok kiegészítı védelme csak a megfelelıségi határozatok alapján történı adattovábbításokat fedi le; emlékeztet arra, hogy tekintettel a megfelelıségi határozat hatályára, bizonyos adattovábbításokra a szóban forgó egyéb mechanizmusok keretében fog sor kerülni;
12. elismeri, hogy a kiegészítı szabályokban foglalt kiegészítı védelem az Európából továbbított személyes adatokra korlátozódik, ezért a japán és európai személyes adatokat egyidejőleg feldolgozó üzleti szereplıknek eleget kell tenniük a kiegészítı szabályoknak, többek között technikai („címkézés”) vagy szervezeti módszerek (pl. célzott adatbázisban való tárolás) alkalmazásával annak érdekében, hogy az ilyen személyes adatokat egész „életciklusuk” alatt azonosítani tudják; felhívja a Bizottságot, hogy kísérje figyelemmel a helyzetet az esetleges joghézagok megelőzése érdekében, amelyek révén a piaci szereplık megkerülhetnék a kiegészítı szabályokban megállapított kötelezettségeket azáltal, hogy harmadik országokon keresztül továbbítják az adatokat;
13. megjegyzi, hogy a „személyes adat” APPI-ban foglalt meghatározása nem tartalmazza azokat az adatokat, amelyekrıl kabineti rendelet mondja ki, hogy felhasználási módjuk miatt kevésbé valószínű, hogy sértik az egyén jogait és érdekeit; sürgeti a Bizottságot annak értékelésére, hogy ez a káralapú megközelítés összhangban áll-e az uniós megközelítéssel, amely szerint a személyes adatok bármilyen feldolgozása az adatvédelmi jog hatálya alá tartozik; megjegyzi ugyanakkor azt is, hogy e megközelítést nagyon kevés esetben kellene alkalmazni;
14. megjegyzi továbbá, hogy a „személyes információ” APPI-ban foglalt meghatározása csak az olyan információra korlátozódik, „amely alapján egy adott személy azonosítható”; megjegyzi továbbá, hogy ez a meghatározás nem foglalja magában az általános adatvédelmi rendelet által nyújtott pontosítást, amely szerint a személyes információkat akkor is személyes adatnak kell tekinteni, ha az pusztán egy személy „kiválasztására” használható fel, ahogy azt az Európai Bíróság egyértelmően megállapítja;
15. aggodalmát fejezi ki amiatt, hogy a „személyes adat” APPI-ban foglalt szőkebb (a „személyes információ” meghatározásán alapuló) meghatározása esetleg nem felel meg az általános adatvédelmi rendelet „lényegi egyenértékűségi” előírásának és az Európai Bíróság ítélkezési gyakorlatának; ezért megkérdőjelezi a végrehajtási határozat tervezetében szereplı megállapítást, miszerint az uniós adatok mindig az APPI szerinti „személyes adatok” kategóriájába fognak tartozni; felhívja a Bizottságot, hogy a megfelelıségi határozat alkalmazása és idıszakos felülvizsgálata során szorosan kövesse nyomon a különbözı elképzelések gyakorlati vonatkozásait;
16. felhívja a Bizottságot, hogy nyújtson be további pontosításokat, és szükség esetén kérje fel a japán hatóságokat további kötelezı erejű kiegészítı szabályok létrehozására annak biztosítása érdekében, hogy az általános adatvédelmi rendelet értelmében vett valamennyi személyes adat védelemben részesüljön, amikor azokat Japánba továbbítják;

17. aggodalommal jegyzi meg, hogy az automatizált döntéshozatalt és a profilalkotást illetően az uniós jogtól eltérő módon sem az APPI, sem a PPC iránymutatásai nem tartalmaznak jogi rendelkezéseket, és csak bizonyos ágazati szabályok foglalkoznak ezzel a kérdéssel, anélkül, hogy átfogó, általános jogi keretet és egyben alapvető és erős védelmet biztosítanának az automatizált döntéshozatallal és profilalkotással szemben; felhívja a Bizottságot annak bemutatására, hogy a japán adatvédelmi keretrendszer hogyan kezeli mindezt úgy, hogy egyúttal egyenértékű védelmi szintet biztosít; úgy véli, hogy ez különösen fontos, tekintettel a Facebook/Cambridge Analytica legújabb profilalkotási eseteire;
18. úgy véli, hogy az Európai Adatvédelmi Testület Megfelelőségi referenciájának fényében, mivel az APPI nem tartalmaz konkrét rendelkezéseket, további mélyreható pontosítások szükségesek a direkt marketing kapcsán, annak érdekében, hogy bizonyítani lehessen, hogy Japánban egyenértékű a személyes adatok védelmi szintje;
19. tudomásul veszi az Európai Adatvédelmi Testület véleményét, amelyben számos problémás kérdést határoz meg, többek között az EU-ból Japánba továbbított személyes adatok teljes életciklusuk során való védelme tekintetében; felhívja a Bizottságot, hogy megfelelően orvosolja a kérdést, és a végrehajtási határozatban terjesszen elő további bizonyítékot és magyarázatot a megfelelő biztosítékok meglétének alátámasztására;
20. felhívja a Bizottságot annak tisztázására, hogy a harmadik fél számára történő adattovábbítások tekintetében a kiegészítő szabályokban foglalt megoldásból, amely az uniós érintett előzetes hozzájárulását követeli meg a más országban található harmadik fél részére történő adattovábbítás esetén, hiányoznak olyan lényeges elemek, amelyek lehetővé tennék az érintettek számára hozzájárulásuk megadását, mivel nem határozza meg egyértelműen, hogy az általános adatvédelmi rendelet 13. cikkével összhangban mi tartozik „az érintett hozzájárulására vonatkozó döntéséhez szükséges, az adattovábbítás körülményeire vonatkozó információk” fogalmába, például az adattovábbítás rendeltetési helye szerinti harmadik ország; felhívja a Bizottságot annak további pontosítására, hogy az érintett számára milyen következményekkel jár, ha megtagadja a személyes adatainak továbbításához szükséges hozzájárulás megadását;
21. sajnálja, hogy az APPI eredményes végrehajtása tekintetében a büntetőhatóságok által kiszabott esetleges bírságok szintje nem elegendő a jogszabály betartásának eredményes biztosításához, mivel nem tűnik arányosnak, hatékonynak vagy visszatartó erejűnek a jogsértés súlyához mérten; megjegyzi azonban, hogy az APPI büntetőjogi szankciók, többek között szabadságvesztés kiszabását is előírja; felhívja a Bizottságot, hogy nyújtson tájékoztatást a közigazgatási bírságok és büntetőjogi szankciók múltbeli tényleges alkalmazásáról;
22. megjegyzi, hogy a PPC nem felügyeli a bűnüldözési ágazat adatfeldolgozási tevékenységeit, ugyanakkor léteznek más felügyeleti mechanizmusok, többek között a független, közbiztonsággal foglalkozó prefektusi bizottság által gyakorolt felügyelet; megjegyzi, hogy az információk közzétételével és a személyes információk védelmével foglalkozó felülvizsgálati testület rendelkezik bizonyos hatáskörökkel ezen a téren, ideértve többek között a hozzáférési kérelmek felülvizsgálatát és a vélemények közzétételét, rámutat azonban, hogy ezek a hatáskörök jogilag nem kötelező erejűek; üdvözli, hogy az EU és Japán megállapodtak abban, hogy konkrét jogorvoslati mechanizmust hoznak létre, amelyet a PPC irányít és felügyel, és amely a személyes

adatoknak a bűnüldözés és a nemzetbiztonság területén történő feldolgozására alkalmazandó;

23. megjegyzi, hogy az igazgatási szervek birtokában lévő személyes adatok védelméről szóló japán jogszabály (APPIHAO) értelmében a gazdasági szereplők „önkéntes alapon” is szolgáltathatnak adatokat a bűnüldöző hatóságok számára; rámutat arra, hogy erről nem rendelkezik az általános adatvédelmi rendelet vagy a rendőrségi irányelv, és felhívja a Bizottságot annak értékelésére, hogy ez megfelel-e annak az előírásnak, amely „lényegi egyenértékűséget” ír elő az általános adatvédelmi rendelettel;
24. tisztában van a jelfelderítéssel foglalkozó japán igazgatóságról (DFS) szóló sajtóbeszámolókkal, amely mintegy 1 700 embert foglalkoztat, és legalább hat olyan felderítő létesítménnyel rendelkezik, amelyek a nap 24 órájában a telefonhívások, az e-mailek és más kommunikációs formák lehallgatását végzik¹; aggodalmát fejezi ki amiatt, hogy a válogatás nélküli tömeges megfigyelés ezen elemét még csak meg sem említik a végrehajtási határozat tervezetében; felhívja a Bizottságot, hogy nyújtson be több információt a Japánban folyó tömeges megfigyelésről; súlyos aggodalmának ad hangot amiatt, hogy ez a tömeges megfigyelés nem felel meg az Európai Bíróság Schrems-ügyben hozott ítéletében (C-362/14.) megállapított kritériumoknak;
25. sajnálja, hogy a japán közigazgatási szervek által bűnüldözési és nemzetbiztonsági célból gyűjtött és felhasznált személyes adatokról szóló dokumentum, amely a végrehajtási határozat tervezetének II. mellékletét képezi, nem rendelkezik a kiegészítő szabályokéval megegyező jogilag kötelező erővel;

Következtetések

26. felhívja a Bizottságot, hogy terjesszen elő további bizonyítékokat és magyarázatot a fent említett – többek között az Európai Adatvédelmi Testület 2018. december 5-i véleményében meghatározott – ügyekkel kapcsolatban annak bizonyítására, hogy a japán adatvédelmi jogi keret az európai adatvédelmi jogi keretben biztosítottal lényegében egyenértékű, megfelelő szintű védelmet biztosít;
27. meggyőződése, hogy ez a megfelelőségi határozat erőteljes jelzést küldhet a világ országai számára arról, hogy az EU magas szintű adatvédelmi normáival való konvergencia rendkívül kézzelfogható eredményeket kínál; hangsúlyozza e tekintetben az említett megfelelőségi határozat fontosságát, mivel az precedensként szolgálhat jövőbeli partnerségekhez olyan további országokkal, amelyekben korszerű adatvédelmi jogszabályok vannak érvényben;
28. utasítja az Állampolgári Jogi, Bel- és Igazságügyi Bizottságot, hogy továbbra is kövesse nyomon az e téren történt fejleményeket, köztük a Bíróság elé vitt ügyeket, és kövesse nyomon az ezen állásfoglalásban megfogalmazott ajánlások megvalósítását;

o

o o

¹ Ryan Gallagher, ‘The Untold Story of Japan’s Secret Spy Agency’ [A japán titkos hírszerzés eddig ismeretlen története], The Intercept, 2018. május 19., <https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/>

29. utasítja elnökét, hogy továbbítsa ezt az állásfoglalást a Tanácsnak, a Bizottságnak, a tagállamok kormányainak és parlamentjeinek, az Európai Adatvédelmi Testületnek, az európai adatvédelmi biztosnak, az általános adatvédelmi rendelet 93. cikkének (1) bekezdése alapján létrehozott bizottságnak, az Európa Tanácsnak és Japán kormányának.