23/2018. sz. vélemény a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló bizottsági javaslatokról (70. cikk (1) bekezdés b) pont)

Elfogadás időpontja: 2018. szeptember 26.

Tartalom

Az Európai Adatvédelmi Testület

Tekintettel 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 70. cikke (1) bekezdésének b) pontjára,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

Bevezetés

2018 áprilisában a Bizottság a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló rendeletre irányuló javaslatot, valamint a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályok meghatározásáról szóló irányelvre irányuló javaslatot terjesztett be. A két javaslat – COM(2018) 225 final és COM(2018) 226 final – kiegészíti egymást. A Bizottság általános célja az, hogy javítsa a tagállami hatóságok és szolgáltatók közötti együttműködést, a nem uniós országokban székhellyel rendelkező szolgáltatókat is beleértve, és hogy megoldásokat javasoljon a joghatóságnak a kibertérben történő meghatározásával és érvényesítésével kapcsolatos problémára.

Míg a rendelettervezet a megőrzésre és közlésre kötelező határozatoknak az elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók részére történő kibocsátására, kézbesítésére és végrehajtására vonatkozó szabályokat és eljárásokat határozza meg, az irányelvtervezet az EU-ban nem letelepedett szolgáltatók jogi képviselőjének kijelölésére vonatkozó minimumszabályokat tartalmazza.

2017 novemberében[1], még mielőtt a Bizottság bármilyen javaslattervezetet benyújtott volna, a 29. cikk szerinti munkacsoport emlékeztetett annak szükségességére, hogy minden jogalkotási javaslat teljes mértékben feleljen meg elsősorban a meglévő uniós adatvédelmi vívmányoknak, valamint általánosságban az uniós jognak és ítélkezési gyakorlatnak.

A 29. cikk szerinti munkacsoport különösen a személyes adatok védelméhez és a magánélet tiszteletben tartásához való jognak a távközlési és az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatók által feldolgozott adatok tekintetében és különösen ezen adatok bűnüldöző hatóságok általi további feldolgozása esetén felmerülő korlátozására hívta fel a figyelmet, emlékeztetett annak fontosságára, hogy bármely uniós jogi eszköznek összhangban kell állnia az Európa Tanács kiberbűnözésről szóló Budapesti Egyezményével, valamint az európai nyomozási határozatról (ENYH) szóló uniós irányelvvel, és azt javasolta, hogy pontosítsák az elektronikus bizonyítékokhoz való hozzáférést szabályozó nemzeti és uniós szintű eljárási szabályokat annak biztosítása érdekében, hogy az új eszköz ne ruházzon olyan új hatásköröket a hatóságokra, amelyekkel saját rendszerükben nem rendelkeznének. Ezen általános megjegyzéseken túl a 29. cikk szerinti munkacsoport a Bizottság által akkor vizsgált, az érintett adatkategóriákkal és az azokhoz való hozzáférést garantáló megfelelő biztosítékokkal kapcsolatos jogalkotási lehetőségeket, a szolgáltatókat az EU-n kívül található adatok megadására kényszerítő, közlésre kötelező

[1] Lásd a 29. cikk szerinti munkacsoport nyilatkozatát (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

határozatok/kérelmek kezelésének lehetővé tételét, valamint az adatokhoz való közvetlen hozzáféréssel kapcsolatos lényegi és eljárási feltételeket és szükséges biztosítékokat is véleményezte.

Mivel most már rendelkezésre állnak az elektronikus bizonyítékokkal kapcsolatos konkrét javaslatok, az Európai Adatvédelmi Testület adatvédelmi szempontból részletesebben kívánja elemezni a javasolt jogi eszközöket.

1. A rendeletre irányuló javaslat jogalapja (az EUMSZ 82. cikke)

Az elektronikus bizonyítékokról szóló rendelettervezet javasolt jogalapja az EUMSZ 82. cikkének (1) bekezdése (büntetőügyekben folytatott igazságügyi együttműködés), amely így rendelkezik:

> „(1) Az Unióban a büntetőügyekben folytatott igazságügyi együttműködés a büntetőügyekben hozott bírósági ítéletek és határozatok kölcsönös elismerésének elvén alapul, és magában foglalja a tagállamok törvényi, rendeleti és közigazgatási rendelkezéseinek közelítését a (2) bekezdésben és a 83. cikkben említett területeken.
>
> Az Európai Parlament és a Tanács rendes jogalkotási eljárás keretében intézkedéseket állapít meg, amelyek célja:
>
> a) a bírósági ítéletek és határozatok minden formájának az Unió egészén belüli kölcsönös elismerését biztosító szabályok és eljárások megállapítása,
>
> b) a tagállamok közötti joghatósági összeütközések megelőzése és rendezése,
>
> c) a bírák, ügyészek és az igazságügyi alkalmazottak képzésének támogatása,
>
> d) a tagállamok igazságügyi vagy annak megfelelő hatóságai közötti együttműködés megkönnyítése a büntetőeljárások keretében és a határozatok végrehajtása terén.”

Ahogyan a Bizottság a javaslatokat kísérő hatásvizsgálatban is hangsúlyozta, „a 82. cikk (1) bekezdése kimondja, hogy a büntetőügyekben folytatott igazságügyi együttműködésnek a kölcsönös elismerés elvén kell alapulnia. Ez a jogalap vonatkozna a szolgáltatókkal való közvetlen együttműködésről szóló esetleges jogszabályra, amely szerint a kibocsátó tagállamban található hatóság közvetlenül fordulhatna a végrehajtó tagállamban található jogalanyhoz (szolgáltatóhoz), sőt még kötelezettségeket is róhatna rá. Ez pedig új dimenzióval gazdagítaná a kölcsönös elismerést, amely túlmutat az Unión belüli hagyományos, eddig két – a kibocsátó államban és a végrehajtó államban található – igazságügyi hatóság részvételével zajló eljárásokon alapuló igazságügyi együttműködésen.” (saját kiemelés)

Mivel újszerű e jogalapnak a hatóságok és magánszervek közötti közvetlen kérések összefüggésében történő alkalmazása, az Európai Adatvédelmi Testület sajnálatát fejezi ki amiatt, hogy a Bizottság sem további elemzést, sem értékelést nem végzett.

Valójában – ahogyan azt a munkacsoport korábbi nyilatkozatában is kiemelte– az Európai Adatvédelmi Testület továbbra is hangsúlyozza e jogalap megfelelőségével kapcsolatos kétségeit, amely kétségeket az Európai Unió Bírósága és főtanácsnoka által beterjesztett 1/15. sz. indítványban található elemzés is alátámaszt. A 82. cikk mint az EU és Kanada közötti PNR-megállapodás tervezetét alátámasztó jogalap érvényességével kapcsolatos fejleményeket illetően a Bíróság hangsúlyozta, hogy a hatáskörrel rendelkező kanadai hatóság „*nem minősül sem igazságügyi, sem pedig annak*

megfelelő hatóságnak"[2]. Az elektronikus bizonyítékról szóló javaslatok összefüggésében az egyik fő cél a Bizottság szerint a „túl nehézkes" igazságügyi együttműködés elkerülése. A javaslat ennek következtében azon az elven alapul, hogy az együttműködésnek egy hatóság és egy szolgáltató, nem pedig két hatóság között kell létrejönnie. A tervezett eljárás elsősorban a magánjogi szervezeteket helyezi a megkeresett fél szerepébe, és nekik kell válaszolniuk az igazságügyi hatóságoktól érkező kérésekre.

Az Európai Adatvédelmi Testület megjegyzi, hogy a közlésre vagy megőrzésre kötelező határozatok végrehajtásának folyamata során megkeresett hatóság bevonására is sor kerülhet, amennyiben a megkeresett szolgáltató nem teljesíti kötelezettségeit, ami a határozat utólagos végrehajtását teheti szükségessé. Mivel azonban a kialakított eljárás fő célja pontosan a megkeresett hatóság bevonásának elkerülése, az Európai Adatvédelmi Testület kétli, hogy ez a kiegészítő eljárás indokolttá tehetné a 82. cikknek az új jogi eszköz kizárólagos jogalapjaként történő alkalmazását.

Ezért az Európai Adatvédelmi Testület úgy véli, hogy a 82. cikk jogalapként történő alkalmazásához az együttműködés fő eljárási lépéseinek két igazságügyi hatóság között kell lezajlaniuk, és hogy az ilyen jellegű együttműködéshez másik jogalap alkalmazása szükséges.

2. Az elektronikus bizonyítékok szükségessége a jogsegélyszerződésekkel és az európai nyomozási határozattal összevetve

Az Európai Adatvédelmi Testület megállapítja, hogy a Bizottság elkötelezett a bűnügyi nyomozás útjában álló akadályok felülvizsgálata mellett, különös tekintettel az elektronikus bizonyítékokhoz való hozzáférés kérdésére. Az indokolásban a Bizottság megadja a javaslat hátterét, és kiemeli az elektronikus bizonyítékok változékony jellegét, azok nemzetközi vetületét, valamint annak szükségességét, hogy az együttműködési mechanizmusok igazodjanak a digitális korhoz. Az elektronikus bizonyítékok továbbításáról és az azokhoz való hozzáférésről szóló rendeletre és irányelvre irányuló javaslatnak nem célja, hogy a büntetőügyekben folytatott együttműködés korábbi eszközeinek, például a Budapesti Egyezménynek, a kölcsönös jogsegélyszerződésnek és az európai nyomozási határozatnak (ENYH-irányelv) a helyébe lépjen. A Bizottság szerint az elektronikus bizonyítékról szóló javaslatok célja a büntetőügyekben folytatott igazságügyi együttműködés javítása a hatóságok és a szolgáltatók között egyrészt az Európai Unión belül, másrészt pedig harmadik országokkal, különös tekintettel az Amerikai Egyesült Államokra.

Mivel ezek az új kiegészítő eszközök kifejezetten az elektronikus bizonyítékokhoz való hozzáférésére és azok továbbítására vonatkoznak, az Európai Adatvédelmi Testület megvizsgálja az eszközöknek az ENYH-irányelvvel és a jogsegélyszerződésekkel összevethető hozzáadott értékét.

a) Az elektronikus bizonyíték szükségessége, összevetve az ENYH és a jogsegélyszerződések által nyújtott biztosítékokkal

A Bizottság által az elektronikus bizonyítékokra vonatkozó javaslatok mellett felhozott fő érv az, hogy mindez felgyorsítja a másik joghatósági területen található szolgáltató által tárolt és/vagy birtokában lévő elektronikus bizonyítékok biztosításának és beszerzésének folyamatát.

[2] Lásd az 1/15. sz. vélemény (103) pontját és a főtanácsnok ebben az ügyben készült beadványának (108) pontját.

Az Európai Adatvédelmi Testület azonban sajnálattal veszi tudomásul, hogy a hatásvizsgálat nem igazolta az elektronikus bizonyítékokhoz való hozzáférés megszervezését szolgáló új jogi eszköz szükségességét. A javaslatokból valójában hiányzik annak igazolása, hogy kisebb beavatkozással járó eszközök révén nem lehetett volna elérni az elektronikus bizonyítékról szóló javaslat célját, vagy hogy alternatív megoldásokat is mérlegeltek volna. Például az ENYH-irányelv módosításának és továbbfejlesztésének lehetőségét is meg lehetett volna vizsgálni, ami megfelel annak az ENYH-irányelvben foglalt követelménynek, amely szerint 2019. május 21-ig értékelni kell a szöveg esetleges módosításának szükségességét[3]. Egy másik lehetőség lett volna a megőrzésre kötelező határozatoknak az adatok befagyasztására történő felhasználása mindaddig, amíg jogsegélyszerződésen alapuló hivatalos kérés benyújtására nem kerül sor. Ezek az opciók lehetővé tették volna az említett jogi eszközökben előírt biztosítékokat, ugyanakkor biztosították volna, hogy a keresett személyes adatokat ne töröljék.

Az Európai Adatvédelmi Testület megjegyzi, hogy az ENYH-irányelvben megállapított határidők hosszabbak az elektronikus bizonyítékra vonatkozó javaslatban foglalt határidőknél. A végrehajtó hatóságnak ténylegesen 30 napja van arra, hogy a kérés elismerésére vonatkozó döntést meghozza[4], majd 90 napon belül végre kell hajtania a határozatot[5]. Az Európai Adatvédelmi Testület úgy véli, hogy a végrehajtó hatóságok részére biztosított 30 napos mérlegelési időtartam olyan kulcsfontosságú biztosíték, amely lehetővé teszi számukra annak vizsgálatát, hogy a végrehajtásra irányuló kérés kellően megalapozott-e, és megfelel-e az ENYH kibocsátására és továbbítására irányuló valamennyi feltételnek[6].

Az Európai Adatvédelmi Testületet aggasztja, hogy az elektronikus bizonyítékokkal kapcsolatos javaslatokban a közlésre kötelező európai határozatra vonatkozó tanúsítvány (KKEHT) végrehajtására megállapított 10 napos, mérlegelésre nem elegendő határidő nem teszi lehetővé annak megfelelő vizsgálatát, hogy a KKEHT megfelel-e az összes kritériumnak, és azt megfelelően állították-e ki.

Ezért az Európai Adatvédelmi Testület azt javasolja, hogy több időt biztosítsanak a KKEHT címzettjének annak megállapításához, hogy a határozat végrehajtása indokolt-e vagy sem.

Az Európai Adatvédelmi Testület megjegyzi, hogy a megőrzésre kötelező európai határozatra vonatkozó tanúsítvány (MKEHT) esetében nincs garancia arra, hogy az adatok megőrzése a közléshez szükséges adatokra korlátozódik. Valójában az adatok megőrzésének időtartama a 60 napot is meghaladhatja, hiszen a kibocsátó hatóságra nem vonatkozik semmilyen határidő, amelyen belül köteles tájékoztatni a címzettet a kibocsátás elvetéséről vagy a közlésre kötelező határozat visszavonásáról. Ezért az Európai Adatvédelmi Testület azt ajánlja, hogy – a GDPR-ben megállapított adattakarékosság elvének[7] való megfelelés érdekében – legalább egy olyan határidőt állapítsanak meg, amelyen belül a kibocsátó hatóság köteles a kibocsátást elvetni vagy a közlésre kötelező határozatot visszavonni.

Az Európai Adatvédelmi Testület végül azt is megjegyzi, hogy az ENYH-irányelv megállapítja a bizonyítékok kibocsátó államtól a végrehajtó hatóságnak történő visszaszolgáltatására[8] irányuló lehetőséget. Az elektronikus bizonyítékokról szóló rendeletre irányuló javaslatban azonban nem esik

[3] Lásd az ENYH-irányelv 37. cikkét.
[4] ENYH-irányelv 12. cikk (3) bekezdés.
[5] ENYH-irányelv 12. cikk (4) bekezdés.
[6] ENYH-irányelv 6. cikk.
[7] A GDPR 5. cikke (1) bekezdésének c) pontja.
[8] Az ENYH-irányelv 13. cikkének (3) és (4) bekezdése.

szó ilyen lehetőségről. Nem tisztázott, hogy mi történik az elektronikus bizonyítékokkal azután, hogy azokat a kibocsátó hatóságnak visszaszolgáltatták.

Ezért az Európai Adatvédelmi Testület azt ajánlja, hogy a rendeletre irányuló javaslat nyújtson több információt arról, hogy hogyan használják az elektronikus bizonyítékokat, miután továbbították azokat a kibocsátó hatóságnak, a GDPR-nek és az átláthatóság elvének[9], valamint a célhoz kötöttség jogsegélyszerződések által megállapított elvének való megfelelés érdekében.

b) A kettős büntethetőség elvének felszámolása

Az Európai Adatvédelmi Testület tudomásul veszi, hogy a kölcsönös elismerés a kettős büntethetőség alkalmazásától függ, amely a szuverenitás megőrzésének lehetőségét nyújtja a tagállamok számára. A kettős büntethetőség azonban egyre inkább tekinthető a zavartalan igazságügyi együttműködést akadályozó tényezőnek. Az uniós tagállamok egyre nagyobb hajlandóságot mutatnak az együttműködésre még akkor is, ha a nyomozási cselekmények olyan cselekményekre vonatkoznak, amelyek a saját nemzeti joguk szerint nem minősülnek bűncselekménynek. Az Európai Adatvédelmi Testület azonban emlékeztet arra, hogy a kettős büntethetőség elvének célja az, hogy kiegészítő biztosítékot nyújtson annak biztosítására, hogy egy állam ne támaszkodhasson egy másik állam segítségére olyan büntetőjogi szankció alkalmazásához, amely a másik állam joga értelmében nem létezik. Ez például megakadályozhatja az egyik államot abban, hogy segítséget kérjen egy másik államtól egy adott személy politikai nézetei miatti bebörtönzéséhez, ha ezek a politikai nézetek a megkeresett államban nem minősülnek bűncselekménynek, vagy hogy abortusz miatt büntetőeljárást indítsanak egy adott személy ellen, ha az a személy olyan államban lakik, ahol az abortusz nem illegális. A kettős büntethetőség elvét gyakran a szankciókkal kapcsolatos további korlátozások vagy biztosítékok kísérik, amennyiben e szankciók a megkereső és a végrehajtó állam között jelentősen eltérnek. A legfontosabb példa a halálbüntetés alkalmazásának mellőzésére irányuló kötelezettségvállalás egyes jogsegélyszerződésekben, amennyiben az egyik aláíró fél jogában nem létezik halálbüntetés.

Az Európai Adatvédelmi Testület megjegyzi, hogy az elektronikus bizonyítékról szóló rendeletjavaslat kizárja a kettős büntethetőség elvét. Ez azonban nem csupán a kölcsönös elismerés szokásos alakiságainak törlését, hanem magához a kettős büntethetőség elvéhez kapcsolódó biztosítékok törlését is eredményezi.

Sőt, az Európai Adatvédelmi Testület azt is megjegyzi, hogy nem történik utalás annak az országnak a jogára, amelyben a megkeresett szolgáltató található, továbbá hogy az adatok megőrzését, valamint az előfizetői vagy hozzáférési adatok közlésére kötelező határozat kibocsátására bármilyen bűncselekmény vonatkozásában sor kerülhet[10], függetlenül attól, hogy a többi tagállamban létezik-e hasonló bűncselekmény.

Ugyanakkor közlésre kötelező határozat csak akkor bocsátható ki és hajtható végre, ha a kibocsátó államban ugyanazon bűncselekmény vonatkozásában hasonló belföldi helyzetben rendelkezésre állna egy hasonló intézkedés[11]. Ezen túlmenően, és amint azt a rendeletre irányuló javaslat indokolásában a Bizottság is kifejti, a tranzakciós adatok és a tartalmi adatok egyedi jellege is megállapításra kerül, mivel ezek szenzitívebb adatoknak minősülnek. Sőt, az arányosság és az érintett személyek jogainak biztosítása érdekében a tranzakciós vagy tartalmi adatokra vonatkozó

[9] A GDPR 5. cikke (1) bekezdésének a) pontja.
[10] Az elektronikus bizonyítékokról szóló rendeletre irányuló javaslat 5. cikkének (3) bekezdése és 6. cikkének (2) bekezdése.
[11] Az elektronikus bizonyítékokról szóló rendeletre irányuló javaslat 5. cikkének (2) bekezdése.

határozatok kibocsátására olyan bűncselekmények esetében kerülhet sor, amelyek büntetési tételének felső határa legalább három év szabadságvesztés[12]. Az Európai Adatvédelmi Testület azonban hangsúlyozza, hogy az EU-ban még nem került sor harmonizációra az olyan bűncselekmények esetében, amelyek büntetési tételének felső határa legalább három év szabadságvesztés.

Az Európai Adatvédelmi Testület ellenzi a kettős büntethetőség elvének felszámolását, amelynek célja annak biztosítása, hogy valamely állam ne számíthasson más államok segítségére saját büntetőjogának az állam területén kívül, egy olyan állam által történő alkalmazása terén, amely nem osztja ugyanazt a megközelítést, különös tekintettel a büntetőjog területén érvényes, egyéb hagyományos jelentős biztosítékok megszűnésére (lásd az alábbi 3. pontot a helyhez kötöttség feltétele, valamint a 7. pont g) alpontját a harmadik országok jogával való esetleges összeférhetetlenségek tekintetében).

c) Milyen következményekkel jár a vállalatok közvetlen megkeresése?

Az Európai Adatvédelmi Testület tudomásul veszi, hogy az elektronikus bizonyítékok egyre inkább a magántulajdonban lévő infrastruktúrákban érhetők el, és az is előfordulhat, hogy e bizonyítékok a nyomozást végző országon kívül találhatók, és a szolgáltatók tulajdonában állnak.

Az Európai Adatvédelmi Testület megjegyzi, hogy a Belgiumban a *Yahoo!*[13] és a *Skype*[14] ügyében hozott határozatokat követően és a terrortámadások összefüggésében zökkenőmentesebb és gyorsabb együttműködésre van szükség a közjogi és a magánjogi szervezetek között. A hatásvizsgálatban a Bizottság háromfajta, a hatóságokra és a szolgáltatókra egyaránt vonatkozó eljárásjogi eszközre hivatkozik. Ezek a következők: az igazságügyi együttműködés, a közvetlen együttműködés és a közvetlen hozzáférés. Ha az első eszköz nem a szolgáltatóra, hanem a végrehajtó hatóságra rója az ENYH végrehajtásának feladatát[15], a második eszköz, azaz a közvetlen együttműködés a szolgáltató részéről mutatott együttműködésen alapul. A szolgáltató szempontjából a legtöbb beavatkozással járó eszköz a közvetlen hozzáférés, mivel általa a hatóságok közvetítő segítsége nélkül férhetnek hozzá az adatokhoz.

Az Európai Adatvédelmi Testület ezért attól tart, hogy a szolgáltatók közvetlen megkeresése esetén e szolgáltatók a személyes adatok védelmét nem biztosítják olyan hatékonyan, mint ahogyan azt a hatóságok képesek és kötelesek is biztosítani, és hangsúlyozza, hogy ez az igazságügyi együttműködés összefüggésében a személyekre, valamint magukra a vállalatokra nézve előírt egyes eljárási garanciák alkalmazhatatlanságát is eredményezi[16]. Valójában például egy megkeresett szolgáltatónak egy másik (tag-)állam bíróságához kellene fordulnia, hogy megtámadja a határozatot, míg az igazságügyi együttműködés keretében saját országának hatóságaival kerülne szembe. Az Európai Adatvédelmi Testület azt ajánlja, hogy a rendeletjavaslatban további tényezőket is határozzanak meg, amelyek igazolják, hogy a szolgáltatók valóban megvédik a személyek olyan alapvető jogait, mint például a személyes adatok védelme, valamint a magánélet és a családi élet

[12] Az elektronikus bizonyítékokról szóló rendeletre irányuló javaslat 5. cikke (4) bekezdésének a) pontja.
[13] Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N, 2015. december 1.
[14] Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12, 2016. október 27. (A Skype fellebbezett a határozat ellen.)
[15] 10–16. cikk.
[16] Nemzetközi adatvédelmi szempontból lásd még: „Munkadokumentum – Adatvédelemre és a személyes adatok védelmére vonatkozó szabályok a határokon átnyúló, bűnüldözési célú adatkérések területén”, a távközlés adatvédelmi kérdéseivel foglalkozó nemzetközi munkacsoport, 63. ülés, 2018. április 9–10., Budapest (Magyarország).

tiszteletben tartása, továbbá az ellenőrzés lehetővé tételének biztosítása céljából az illetékes adatvédelmi hatóság tájékoztatása.

3. Az új joghatósági ok és a helyhez kötöttség feltételének úgynevezett megszűnése

Az Európai Adatvédelmi Testület megjegyzi, hogy a Bizottság is hangsúlyozta, hogy a szóban forgó javaslatok által támasztott egyik fő kihívás a helyhez kötöttség feltételének megszűnése, valamint annak lehetősége, hogy az illetékes hatóságok az adatok tényleges tárolási helyétől függetlenül kérhessék ezen adatok megőrzését és közlését.

Adatvédelmi szempontból nem jelent újdonságot, hogy az uniós adatvédelmi jog attól függetlenül is alkalmazandó, hogy hol tárolják az érintett személyek adatait. A GDPR alkalmazhatósága valójában vagy attól függ, hogy az adatkezelő az Unióban letelepedett-e, vagy attól, hogy uniós érintettek adatait dolgozzák-e fel, még akkor is, ha az adatkezelő nem az Unióban telepedett le[17], amely esetben az EU-ban jogi képviselőt is ki kell jelölnie[18]. Adatvédelmi szempontból fontos megjegyezni, hogy a kibővített területi hatály célja az uniós érintettek teljesebb körű védelme, amely független az adataikat kezelő vállalat letelepedési helyétől.

Ezért bár a helyhez kötöttség feltételének megszűnése a büntetőjog terén újdonságként hathat, adatvédelmi szempontból nem tűnik komoly változásnak. Az Európai Adatvédelmi Testület továbbá azt is megjegyzi, hogy az EU területével való összefüggés továbbra is fennáll, hiszen csak az Unióban szolgáltatásokat nyújtó szolgáltatók tartoznak a javaslatok hatálya alá, és az a tény, hogy a kéréseket kizárólag nyomozás keretében lehet kezelni, az EU-val való összefüggést feltételezi (vagy azért, mert a bűncselekményt valamely tagállam területén követték el, vagy mert a sértett vagy a bűnöző valamely tagállam állampolgára).

Amennyiben a helyhez kötöttség feltételének megszűnését most már a büntetőjog terén is alkalmazni kell, az Európai Adatvédelmi Testület számára az a legfontosabb kérdés, hogy hogyan biztosítható, hogy ez a fejlemény ne hasson károsan az adatvédelemre, valamint az érintettek és a megkeresett szolgáltatók büntetőjogi eljárási jogaira. Ebből a szempontból az Európai Adatvédelmi Testület elismeri, hogy az EU-n belül az eljárási biztosítékokat – legalábbis részben – harmonizálták, és azokat az Emberi Jogok Egyetemes Nyilatkozatának megfelelően kell biztosítani. Kijelenthető tehát, hogy a helyhez kötöttség feltételének megszűnése valószínűleg korlátozottabb következményekkel jár akkor, ha a bizonyítékot az EU-n belül keresik, szemben a fordított helyzettel, amikor harmadik országok hatóságai az elektronikus bizonyítékokról szóló rendelettervezetben megállapított feltételekkel azonos feltételek mellett kérnek adatokat az EU-ban letelepedett vállalatoktól. Az Európai Adatvédelmi Testületet valójában különösen aggasztja, hogy ez még problémásabb helyzeteket eredményezhet. Ebben az összefüggésben egy olyan harmadik ország hatóságai, amelyben a büntetőjog területén eltérő és potenciálisan kevesebb eljárási biztosítékot alkalmaznak, olyan adatokhoz is hozzáférhetnek, amelyeket az EU-n belül kiegészítő biztosítékok védenének. Ebből a szempontból az Európai Adatvédelmi Testület felidézi a kettős mércével és az alapvető jogok gyengülésével kapcsolatos aggályait, amelyek szerint a szolgáltatók és az érintettek egy harmadik ország hatóságától érkező megkeresés esetén nem részesülnek az uniós jog szerinti eljárási biztosítékok nyújtotta előnyökből.

[17] Lásd a 3. cikket, különösen annak (2) bekezdését.
[18] Lásd a 27. cikket.

Sőt, mivel ez az új, „az adatok helyétől független” joghatósági ok egy, elsősorban illetékes hatóságoktól közvetlenül a szolgáltatókhoz érkező kéréseken alapuló eljárással párosul, az Európai Adatvédelmi Testületet aggasztja, hogy az adatvédelmi biztosítékokat a megkeresett magánvállalatok nem alkalmazzák, ráadásul nem vonatkozik rájuk olyan jogi eszköz, mint a jogsegélyszerződés, amely hagyományosan az igazságügyi hatóságok közötti adatcseréket szabályozza, és biztosítékokat is nyújt. Különösen a jogsegélyszerződések összefüggésében a minimális adatvédelmi biztosítékok például titoktartási kötelezettségeket és a célhoz kötöttség elvét vonják maguk után, amely szerint az adatokat nem lehet más célból kezelni.

Az Európai Adatvédelmi Testület ezért arra emlékeztet, hogy legalább az (EU) 2016/680 irányelvben előírt biztosítékokat kötelezően alkalmazandóvá kell tenni – az adattovábbítást is beleértve –, különös tekintettel az irányelv 39. cikkére, amennyiben a szolgáltató az e területre vonatkozó megfelelőségi határozattal nem rendelkező harmadik országban telepedett le. Az Európai Adatvédelmi Testület különösen azt hangsúlyozza, hogy ez a rendelkezés elsősorban a határozato(ka)t és az azok továbbításával kapcsolatos dokumentációt kibocsátó hatóság szerinti tagállamban található illetékes adatvédelmi hatóság – többek között a harmadik ország illetékes hatóságának címzett továbbítás eredménytelenségének vagy alkalmatlanságának indokolásával kapcsolatos – tájékoztatását vonja maga után.

4. A „szolgáltatók” fogalmát korlátozni kell vagy ki kell egészíteni az érintettek jogaira vonatkozó kiegészítő biztosítékokkal

Ami a szolgáltatókat illeti, az Európai Adatvédelmi Testület üdvözli azt a tág fogalommeghatározást, amely a hírközlési szolgáltatásokat és az OTT-szolgáltatásokat is magában foglalja, mivel ezek a szolgáltatások funkcionálisan mind egyenértékűek, ezért a rájuk vonatkozó intézkedések hasonló hatással lehetnek a magánélet tiszteletben tartásához és a kommunikáció titkosságához való jogra, lásd a 29. cikk szerinti munkacsoport nyilatkozatát, valamint az elektronikus hírközlési adatvédelmi rendeletre irányuló javaslatról szóló 01/2017. sz. véleményt. Az elektronikus bizonyítékokról szóló rendeletre irányuló javaslat azokra a szolgáltatókra vonatkozik, amelyek az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló irányelv 2. cikkének (4) bekezdésében meghatározott elektronikus hírközlési szolgáltatásokat, az (EU) 2015/1535 irányelv 1. cikke (1) bekezdésének b) pontjában meghatározott, információs társadalommal összefüggő szolgáltatásokat nyújtanak, „amelyek esetében az adattárolás meghatározó eleme a felhasználó részére nyújtott szolgáltatásoknak, beleértve a közösségi oldalakat is, a felhasználóik közötti ügyleteket megkönnyítő online piacterek, egyéb tárhelyszolgáltatók”, vagy internetes domainnév- és IP-szám szolgáltatatásokat nyújtanak, „mint például az IP-cím szolgáltatók, domain-név nyilvántartások és nyilvántartók, valamint a kapcsolódó titkosítási és proxy szolgáltatók”[19].

A rendelettervezet értelmében azonban a szolgáltató „olyan természetes vagy jogi személy, amely a szolgáltatások egy vagy több alábbi kategóriáját nyújtja”, ezért az Európai Adatvédelmi Testületet aggasztja, hogy ez a jogi eszköz a GDPR értelmében vett adatkezelőkre és adatfeldolgozókra egyaránt vonatkozhat. Mivel a rendelettervezet 2. cikkének (4) bekezdésében meghatározott „szolgáltatások nyújtása” magában foglalja egyrészt egy vagy több tagállamban annak lehetővé tételét jogi vagy természetes személyek számára, hogy igénybe vegyék a felsorolt szolgáltatásokat, másrészt azt, hogy érdemi kapcsolat álljon fenn a hivatkozott tagállammal vagy tagállamokkal, e tevékenységek az

[19] Az elektronikus bizonyítékokról szóló rendeletre irányuló javaslat 2. cikke (3) bekezdésének c) pontja.

adatfeldolgozó által az adatkezelő részére végzett tevékenységeket, például az adatok tárolását is magukban foglalják.

Az Európai Adatvédelmi Testület ezért attól tart, hogy a GDPR értelmében adatkezelőként eljáró szolgáltatókra vonatkozó korlátozások nélkül, továbbá olyan külön kötelezettség nélkül, amely szerint az adatfeldolgozó közlésre vagy megőrzésre kötelező határozat fogadása esetén köteles értesíteni az adatkezelőt, az érintettek jogait ki lehet játszani. Ez különösen aktuális, mivel az egymással esetlegesen ütköző, a címzettet a kapott határozatok kézbesítésében megakadályozó kötelezettségek összefüggésében az igazságügyi hatóságokat maga a rendelettervezet ösztönzi arra, hogy az alkalmazandó adatvédelmi szabályoktól függetlenül a legmegfelelőbb szereplőhöz forduljanak, különös tekintettel arra, hogy bármilyen adatot kérhetnek, nem csupán a GDPR hatálya alá tartozó személyes adatokat[20].

A GDPR szerint az adatfeldolgozó csak az adatkezelő utasításai alapján járhat el. Ezért az adatkezelő feladata annak biztosítása, hogy az érintettek jogait tiszteletben tartsák, és megadják számukra a releváns információkat, beleértve az adataik címzettjeit, például a hozzáférési joguk gyakorlásának összefüggésében. Mivel nem az adatfeldolgozó kap ilyen kéréseket az érintettektől, nincs abban a helyzetben, hogy válaszoljon azokra, kivéve, ha az adatkezelő kifejezetten hozzá intéz kérdést.

Következésképpen az Európai Adatvédelmi Testület hangsúlyozza, hogy amennyiben az érintettek jogait a GDPR alkalmazásában nem korlátozták, előfordulhat, hogy a GDPR alkalmazásának előnyeit élvező érintettek nem tudják hatékonyan érvényesíteni jogaikat, ha az adatkezelő nincs abban a helyzetben, hogy teljes körű tájékoztatást nyújtson. Az Európai Adatvédelmi Testület továbbá azt is megjegyzi, hogy az információk hiányának valószínűsége még ennél is nagyobb lesz, ha az adatfeldolgozóra nem rónak olyan külön kötelezettséget, amely szerint tájékoztatnia kell az adatkezelőt, ha a kért adatok olyan érintettekre vonatkoznak, akik nem részesülnek a GDPR által nyújtott védelemből. Az adatokat kérő igazságügyi hatóságok valójában ebben az esetben nem feltétlenül kötelesek tájékoztatni az érintetteket az általuk végzett további adatkezelésről. Az Európai Adatvédelmi Testület ezért a hatálynak a GDPR értelmében vett adatkezelőkre történő korlátozására vagy egy olyan rendelkezés bevezetésére szólít fel, amely pontosítja, hogy amennyiben a megkeresett szolgáltató nem az adatok kezelője, köteles az adatkezelőt értesíteni.

5. A „letelepedés” és a „jogi képviselő” fogalmát e javaslatok összefüggésében világosan meg kell különböztetni a GDPR összefüggésében értelmezett fogalmuktól

Mivel az adatokra nem alkalmazható a helyhez kötöttség feltétele, a közlésre és a megőrzésre kötelező határozatok címzettjei a rendeletjavaslat értelmében az Unióban szolgáltatásokat nyújtó szolgáltatókra korlátozódnak, függetlenül attól, hogy az EU-ban letelepedett szolgáltatókról van-e szó vagy sem, amelyek az irányelvtervezetben javasolt szabályok szerint kötelesek jogi képviselőt kijelölni. A „letelepedés” és a „jogi képviselő” fogalmát tehát a jogszabálytervezetek is meghatározzák.

Az Európai Adatvédelmi Testület megjegyzi, hogy ezek a fogalmak más uniós jogszabályok, különösen a GDPR összefüggésében is előkerülnek. Következésképpen szükség van e fogalmak

[20] Lásd a 7. cikk (3) és (4) bekezdését.

meghatározásának pontosítására és a GDPR összefüggésében használt értelmezésüktől való elkülönítésére.

a) Letelepedés

Az Európai Adatvédelmi Testület arra is emlékeztet, hogy a „letelepedés” rendelettervezetben használt fogalmát nem szabad összekeverni a GDPR összefüggésében értelmezendő fogalmával. Valójában a rendelettervezet alkalmazásában a letelepedésnek a 2. cikk (5) bekezdésében meghatározott fogalma tágabb, mint a GDPR szerinti, mivel a következőket tartalmazza: „gazdasági tevékenység tényleges folytatása határozatlan időn át olyan állandó infrastruktúra révén, amelyen keresztül szolgáltatásokat nyújtanak vagy olyan állandó infrastruktúra révén, amelyen keresztül a gazdasági tevékenységet irányítják”, függetlenül attól, hogy a személyes adatok kezelése e letelepedéssel kapcsolatos tevékenységek összefüggésében történt-e. Ezért ha a GDPR értelmében vett „letelepedést” minden kétséget kizáróan be kell emelni a letelepedés rendelettervezetben meghatározott fogalmába, előfordulhat, hogy ennek ellenkezője nem igaz.

Az Európai Adatvédelmi Testület ezért arra figyelmeztet, hogy a szolgáltatóknak a rendelettervezet értelmében vett letelepedése nem feltétlenül jelenti azt, hogy a GDPR alkalmazásának a 3. cikk (1) bekezdése szerinti feltételei teljesülnek. Ebben az összefüggésben az adatkezelőnek és az adatfeldolgozónak érdemes ellenőriznie, hogy a GDPR alkalmazhatósága nem a 3. cikk (2) bekezdéséből fakad-e, ami az EU-n belül jogi képviselő kijelölését és az egységességi mechanizmus hiányát eredményezné.

b) Jogi képviselő

Nyilatkozatában a 29. cikk szerinti munkacsoport hangsúlyozta, hogy kerülni kell a jogi képviselőnek a GDPR 27. cikke értelmében történő kijelölése és az elektronikus bizonyítékokról szóló rendelettervezetben előírt jogi képviselő közötti keveredést.

A szóban forgó javaslattervezettel kapcsolatban az Európai Adatvédelmi Testület emlékeztetni kíván ezekre az ajánlásokra, és különösen azt kívánja hangsúlyozni, hogy saját értelmezése szerint a jogi képviselő kijelöléséről szóló irányelvtervezet értelmében és az elektronikus bizonyítékról szóló javaslatok összefüggésében minden esetben ki kell jelölni jogi képviselőt, őt konkrét feladatokkal felruházni, amelyek a szolgáltató által adott megbízatástól függetlenek, a jogi képviselőnek rendelkeznie kell a megfelelő hatáskörrel ahhoz, hogy válaszoljon a megkeresésekre és a szolgáltató nevében eljárjon, továbbá a GDPR szerinti jogi képviselőnél nagyobb felelősség terheli.

Az Európai Adatvédelmi Testület továbbá azt is hangsúlyozza, hogy az elektronikus bizonyítékokról szóló javaslattervezetek szerinti azon kötelezettség, hogy jogi képviselőt mindenképpen ki kell jelölni, függetlenül attól, hogy a szolgáltató az EU-ban letelepedett-e vagy sem, az elektronikus bizonyítékokról szóló irányelvtervezet szerinti azon lehetőség, hogy ugyanazon szolgáltató részére akár több jogi képviselőt is kijelöljenek, valamint az a kötelezettség, amely szerint a jogi képviselő kijelöléséről értesíteni kell a tagállami hatóságokat, eltér a GDPR-től, amely nem rendelkezik a jogi képviselő kijelöléséről történő értesítésére vonatkozó kötelezettségről, a kijelölés alóli mentesség eseteiről, valamint a jogi képviselő korlátozott felelősségi köreiről.

Ezért egyfelől a szerepkör, felelősség és a szolgáltató egyéb telephelyeivel való kapcsolat tekintetében, másfelől az adatkezelő vagy adatfeldolgozó tekintetében fennálló jelentős különbségek miatt az Európai Adatvédelmi Testület azt ajánlja, hogy amennyiben a szolgáltató nem telepedett le az EU-ban, viszont a 3. cikk (2) bekezdése értelmében a GDPR hatálya alá és az elektronikus bizonyítékokról szóló rendelet hatálya alá is tartozik, két külön jogi képviselőt kell kijelölni,

amelyeknek a kijelölés alapjául szolgáló jogi eszköz értelmében egyértelműen elkülönült feladatkörökkel kell rendelkezniük.

6. Új adatkategóriák

A javasolt rendelet 2. cikkében különféle adatkategóriákat határoz meg: előfizetői adatok, hozzáférési adatok, tranzakciós adatok vagy tartalmi adatok. A bizottsági javaslat (20) preambulumbekezdése továbbá azt is meghatározza, hogy *„A rendelet hatálya alá tartozó adatkategóriák közé tartoznak az előfizetői adatok, a hozzáférési adatok, a tranzakciós adatok (e három kategóriát hívják nem tartalmi adatoknak), valamint a tartalmi adatok. E megkülönböztetés, a hozzáférési adatokon kívül megvan számos tagállam jogrendjében, illetve a jelenlegi amerikai jogi keretben is, amely lehetővé teszi a szolgáltatók számára, hogy a nem tartalmi adatokat önkéntes alapon megosszák a külföldi bűnüldöző hatóságokkal."*

Ebben az összefüggésben az Európai Adatvédelmi Testület hangsúlyozza először is azt, hogy az uniós adatvédelmi jogszabályok értelmében mind a négy említett adatkategóriát személyes adatnak kell tekinteni, mivel azonosított vagy azonosítható természetes személyre vonatkozó információkat tartalmaznak, függetlenül attól, hogy az érintettet a rendelettervezetben „előfizetőnek" vagy „felhasználónak" nevezik-e. Ugyanígy azt is meg kell jegyezni, hogy a bizottsági javaslat 2. cikkének (6) bekezdésében meghatározott „elektronikus bizonyíték" mind a négy adatkategóriát magában foglalja, és így személyes adatokhoz kapcsolódik. Ezért ahelyett, hogy a javasolt rendelet megállapítaná a – nemzeti jog és az igazságügyi eljárások alapján meghatározott és minősített – bizonyítékokhoz való hozzáférés szabályait, a személyes adatokhoz való hozzáféréssel kapcsolatban új lényegi és eljárási feltételeket ír elő.

Míg a javasolt rendelet meghatározza a személyes adatok új alkategóriáit, amelyekre különféle hozzáférési eljárási feltételek vonatkoznak, az Európai Adatvédelmi Testület felidézi, hogy az Európai Unió Bíróságának vonatkozó ítélkezési gyakorlatával összhangban a magánélet tiszteletben tartásához való alapvető jogba történő beavatkozás fennállásának megállapításához nem számít, hogy a magánélettel kapcsolatos információ érzékenynek minősül-e, vagy hogy az érintett személyeknek okoztak-e bármilyen kellemetlenséget.

Az Európai Adatvédelmi Testület továbbá arra is emlékeztet, hogy a „nem tartalmi adatokkal" kapcsolatban – amelyek a bizottsági javaslat szerint az előfizeti adatokat, hozzáférési adatokat és a tranzakciós adatokat foglalják magukban – az Európai Unió Bírósága a C-203/15. és a C-698/15. sz., Tele*2 Sverige AB* egyesített ügyekben hozott ítéletében megállapította, hogy az olyan metaadatok, mint a forgalmi és helymeghatározó adatok, eszközül szolgálnak az érintett személyek profiljának megalkotásához, amely információ a magánélet tiszteletben tartásához való jog tekintetében ugyanolyan érzékeny, mint a közléseknek maga a tartalma[21].

Ahogyan az a 29. cikk szerinti munkacsoport „Az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférés adatvédelmi és személyesadat-védelmi szempontjai" című, 2017. november 29-i nyilatkozatában már olvasható volt, az Európai Adatvédelmi Testület megismétli a „nem tartalmi" és tartalmi adatok közötti jelenlegi különbségtétellel, valamint a javasolt rendeletben meghatározott négy személyesadat-kategóriával kapcsolatos kétségeit és aggályait. Valóban úgy tűnik, hogy a javasolt négy kategóriát nem határolták körül egyértelműen, és a „hozzáférési adatok"

[21] Az Európai Unió Bíróságának 2016. december 21-i ítélete, 99. pont.

fogalommeghatározása a többi kategóriával összevetve továbbra is homályos. Az Európai Adatvédelmi Testület ezért sajnálatát fejezi ki amiatt, hogy a Bizottság hatásvizsgálata és javaslata nem indokolta meg kellően a személyes adatok új alkategóriának létrehozását, továbbá aggodalmát fejezi ki a személyes adatok különféle kategóriáihoz való hozzáférés lényegi és eljárási feltételeire vonatkozó, eltérő szintű garanciákkal kapcsolatban, különösen tekintettel az annak ellenőrzésével kapcsolatos gyakorlati nehézségekre, hogy egyes esetekben mely adatkategóriák tartoznak a kért adatok közé. Az IP-címek például tranzakciós adatnak és előfizetői adatnak is minősülhetnek.

Ebben az összefüggésben az Európai Adatvédelmi Testület arra is emlékeztet, hogy a Bizottság az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről szóló rendeletre (elektronikus hírközlési adatvédelmi rendelet) irányuló javaslatának (14) preambulumbekezdésében úgy véli, hogy „az elektronikus hírközlési adatok fogalmát kellően átfogóan, technológiasemleges módon kell meghatározni, és bele kell foglalni minden olyan, a továbbított vagy cserélt tartalommal (az elektronikus hírközlés tartalmával) kapcsolatos információt, valamint az elektronikus hírközlési szolgáltatásokat igénybe vevő végfelhasználóval kapcsolatos információt, amelyet elektronikus hírközlési tartalom továbbítása, terjesztése vagy cseréje céljából kezelnek; idetartoznak a kommunikáció feladójának és címzettjének, valamint a kommunikáció földrajzi helyének, dátumának, időpontjának, időtartamának és típusának nyomon követésére vagy azonosítására szolgáló adatok”. Mivel az elektronikus hírközlési adatvédelem jelenlegi és jövőbeli keretrendszere, valamint a magánélet tiszteletben tartásához való jog kapcsolódó korlátozásai az elektronikus bizonyítékokhoz való, bűnüldözési célú hozzáférésre is vonatkozni fognak, az Európai Adatvédelmi Testület azt ajánlja, hogy a javasolt rendelet az elektronikus hírközlési adatoknak egy tágabb fogalommeghatározását tartalmazza, mert így biztosítható a hozzáférésre vonatkozó megfelelő biztosítékok és feltételek megállapítása, amelyek következetesen vonatkoznak a „nem tartalmi” és a „tartalmi adatokra” egyaránt.

7. A megőrzésre és közlésre kötelező európai határozatokra vonatkozó eljárások elemzése

Tágabb értelemben a közlésre vagy megőrzésre kötelező határozattal kapcsolatos eljárás a következőkből áll:

- Az illetékes igazságügyi hatóság – a kibocsátó hatóság – a kért adatok és a határozat típusától függően az 5. és 6. cikkben felsorolt (hiányos) feltételek alapján kibocsátja a határozatot, harmonizált tanúsítvány formájában megküldi a szolgáltató jogi képviselőjének vagy a szolgáltató EU-ban található bármely telephelyére, azaz a címzettnek.
- A tanúsítvány kézhezvételét követően a címzettnek végre kell hajtania a határozatot – azaz 10 napon belül vagy sürgős esetekben 6 órán belül meg kell küldenie az adatokat, vagy 60 napig meg kell őriznie azokat –, kivéve, ha ez a címzett számára lehetetlen, mert a tanúsítvány hiányos, illetve vis maior vagy de facto lehetetlenség miatt, vagy mert a címzett egymással ütköző kötelezettségek fennállása miatt elutasítja a végrehajtást, akár alapvető jogokra vagy egy harmadik ország alapvető érdekeire való tekintettel, vagy egyéb indokok alapján.
- Amennyiben a címzett nem tesz eleget a határozatnak, anélkül, hogy arra a kibocsátó hatóság által elfogadott indokot szolgáltatna, a határozatoknak a szolgáltató képviselete vagy letelepedési helye szerinti tagállam illetékes végrehajtó hatósága általi végrehajtására

irányuló eljárásokat kell alkalmazni, kivéve korlátozott körű elutasítási okok fennállása esetén, és ha a végrehajtó hatóság elutasítja a határozat elismerését vagy végrehajtását.

- Amennyiben a címzett ütköző kötelezettségek miatt indokolással ellátott kifogást emel a határozat ellen, a kibocsátó hatóságnak az ügyet az illetékes tagállami bírósághoz kell utalnia, amely felel az esetleges konfliktus mérlegelésért, és konfliktus esetén visszavonja a határozatot. Konfliktus esetén az illetékes bíróság vagy saját nemzeti hatóságán keresztül 15 napos válaszadási határidő kitűzése mellett – amely határidő indokolással ellátott kérelem esetén 30 nappal meghosszabbítható – az érintett harmadik országban található központi hatóságokhoz fordul, alapvető jogok vagy harmadik ország alapvető érdekei tekintetében egymással ütköző kötelezettségek esetén, vagy maga dönti el, hogy a címzett által hivatkozott egyéb okok miatt fenntartja vagy visszavonja a határozatot.
- A GDPR és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv (LED) értelmében rendelkezésre álló jogorvoslati lehetőségek sérelme nélkül azoknak a személyeknek, akiknek adatait közlésre kötelező határozattal szerezték meg, szintén biztosítani kell a határozattal szembeni hatékony jogorvoslathoz való jogot.

Az Európai Adatvédelmi Testület megvizsgálta a rendelettervezetben előírt eljárásokat és biztosítékokat, hogy pontosan körülhatárolja az egyes lépéseket, és az alábbiakban ismertetett minden egyes szempont tekintetében a következő biztosítékokat és módosításokat javasolja.

a) Emelni kell a határozatok kibocsátására vonatkozó küszöbértékeket, a határozatokat csak bíróságok bocsáthatják ki vagy engedélyezhetik

A határozatok kibocsátásának feltételeit illetően az Európai Adatvédelmi Testület üdvözli a tranzakciós vagy tartalmi adatokhoz való hozzáféréssel kapcsolatos szigorúbb biztosítékokat. Megjegyzi azonban, hogy a büntetőjogi szankciók tagállamok közötti teljes körű harmonizálásának hiányában a „csak olyan bűncselekmények esetében bocsátható ki, amelyek büntetési tételének felső határa a kibocsátó államban legalább három év szabadságvesztés”[22] hivatkozás az EU-n belül még így is eltérő küszöbértékeket és az érintettek adatainak védelme terén tapasztalható eltéréseket jelent.

Az Európai Adatvédelmi Testület továbbá azt is hangsúlyozza, hogy – különös tekintettel az előfizetői adatok tág fogalommeghatározására – a megadott küszöbérték az előfizetői vagy hozzáférési adatok tekintetében a megőrzésre kötelező határozatok és a közlésre kötelező határozatok esetében igen alacsonynak tűnik, mivel elvben az ilyen határozatok kibocsátása bármely bűncselekménnyel indokolható. Hasonlóképpen az ilyen határozatok kibocsátására jogosult hatóságok köre a tranzakciós vagy tartalmi adatokra vonatkozó közlésre kötelező határozatok összefüggésében korlátozottabb, mint az előfizetői vagy hozzáférési adatok megőrzésére vagy közlésére kötelező határozatok kibocsátása esetében, mivel az ügyészek csak az utóbbi határozatokat bocsáthatják ki, míg a bírók, bíróságok vagy nyomozási bírók bármilyen határozatot kibocsáthatnak vagy engedélyezhetnek.

Az Európai Adatvédelmi Testület különösen azt fogadja sajnálattal, hogy a legalacsonyabb küszöbérték, amely lehetővé teszi a bűnüldöző hatóságok számára, hogy bármely bűncselekmény esetében hozzáférést kérjenek az előfizetői és a hozzáférési adatokhoz, az Európai Unió Bírósága (az egyéb adatokra összpontosító) ítélkezési gyakorlatának „*a contrario*” értelmezésre alapoz, hogy

[22] Lásd az 5. cikk (3) bekezdésének a) pontját.

különbséget tegyen az engedélyezhető biztosítékok tekintetében. Az Európai Unió Bírósága valóban külön hangsúlyozta, hogy a forgalmi és helymeghatározó adatok esetében az illetékes hatóságok hozzáférését szigorúan a súlyos bűncselekmények elleni küzdelemre kell korlátozni[23]. Az Európai Adatvédelmi Testület el tudná fogadni, ha a javaslat biztosítaná a kifejezetten alapvető információkhoz való hozzáférés kérésének lehetőségét, amelyek csupán az adott személy azonosítására alkalmasak, azonban előzetes bírósági engedély nélkül nem közölnek kommunikációs adatokat. Sajnálatát fejezi ki azonban amiatt, hogy a Bizottság ezt az ítéletet tág, „*a contrario*" módon értelmezi, és szigorúbb biztosítékok bevezetését sürgeti, amelyek célja az egyéb előfizetői adatokhoz és hozzáférési adatokhoz való hozzáférés indokainak korlátozása. Az Európai Adatvédelmi Testület azt javasolja, hogy az ilyen adatokhoz való hozzáférést korlátozzák vagy a rendelettervezetben felsorolt bűncselekmények jegyzékére vagy legalább a „súlyos bűncselekményekre", különös tekintettel az ilyen adatokra vonatkozó alacsony előzetes engedélyezési küszöbértékre.

Az Európai Adatvédelmi Testület azt is hangsúlyozza, hogy ez az „*a contrario*" értelmezés ahhoz is vezet, hogy a javaslat megnyitja az ügyészek előtt a határozatok kibocsátásának vagy kibocsátásuk engedélyezésének lehetőségét. Az Európai Adatvédelmi Testület azon a véleményen van, hogy a csupán az adott személy azonosítását lehetővé tevő, azonban kommunikációs adatokat nem közlő alapvető információkhoz való hozzáférésre irányuló kérések kivételével ez az Európai Unió Bíróságának a kommunikációs adatokhoz való hozzáféréssel kapcsolatos ítélkezési gyakorlatával összevetve visszalépést jelent. A kommunikációs adatokhoz való bűnüldözési célú hozzáféréssel kapcsolatos ítélkezési gyakorlatában az Európai Unió Bírósága korlátozta az ilyen hozzáférés engedélyezését – egyéb feltételek mellett – és „*a kellően indokolt sürgős esetek kivételével*"[24] „*olyan előzetes felülvizsgálatra, amelyet olyan bíróság vagy független közigazgatási szerv végez*", „*a megelőzési, felderítési vagy bűnüldözési eljárások keretében az illetékes nemzeti hatóságok által előterjesztett indokolt kérelem alapján*".[25]

Az Európai Adatvédelmi Testület emlékeztet arra, hogy a „bíróság" kifejezés az uniós jogban független fogalom, és hogy az Európai Unió Bírósága folyamatosan rámutat és emlékeztet azokra a kritériumokra, amelyeket ahhoz kell teljesíteni, hogy egy hatóság bíróságnak minősüljön, beleértve a függetlenség kritériumát[26] is, ami az ügyészek esetében nem állja meg a helyét, ahogyan arra az Emberi Jogok Európai Bírósága is emlékeztet ítélkezési gyakorlatában[27].

Következésképpen a 4. cikk (1) bekezdésének a) és b) pontja, valamint a 3. cikk a) és b) pontja olyan eljárásokat eredményez, amelyek keretében jóval kevesebb biztosíték vonatkozik az előfizetői és a hozzáférési adatokra, mivel az ügyész önmaga kérhet adatokat anélkül, hogy a kért adatok helye szerinti állam hatósága vagy a megkeresett vállalkozás jogi képviselőjének helye szerinti állam hatósága további ellenőrzést végezhetne, vagy független közigazgatási szerv végezhetne bármilyen ellenőrzést.

Az Európai Adatvédelmi Testület továbbá azt is megjegyzi, hogy az 5. cikk (2) bekezdése egy úgynevezett kiegészítő biztosítékot is tartalmaz, amely a közlésre kötelező európai határozat kibocsátásának lehetőségét azokra az esetekre korlátozza, amikor ugyanazon bűncselekmény vonatkozásában hasonló belföldi helyzetben rendelkezésre állna egy hasonló intézkedés. A Testület azonban figyelmeztet az ilyen rendelkezés kontraproduktív hatására: kiegészítő biztosítékok nyújtása

[23] Lásd a 203/15. sz. ügyben hozott ítélet (125) pontját.
[24] Lásd a 203/15. sz. ügyben hozott ítélet (120) pontját.
[25] Lásd a C293/12. és a C594/12. sz. egyesített ügyekben hozott ítélet (62) pontját.
[26] Lásd például a C 203/14. sz. ügyet.
[27] Lásd például a Moulin kontra Franciaország ügyben hozott 2010.11.23-i ítéletet.

helyett úgy tűnik, hogy arra ösztönzi a tagállamokat, hogy a közlésre kötelező határozatoknak a jelen rendelet szerinti kibocsátásának biztosítása érdekében kibővítsék az előfizetői vagy hozzáférési adatok közlésének kérésére irányuló nemzeti lehetőségeiket.

b) Az adatszolgáltatásra vonatkozó határidőket meg kell indokolni

Az Európai Adatvédelmi Testület megjegyzi, hogy a 9. cikk (1) és (2) bekezdésében előírtaknak megfelelően a közlésre kötelező európai határozatra legkésőbb a tanúsítvány kézhezvételétől számított 10 napon belül válaszolni kell, kivéve, ha a kibocsátó hatóság feltüntette a korábbi közlés indokait, sürgős esetekben pedig legkésőbb 6 órán belül kell válaszolni.

Az Európai Adatvédelmi Testület azonban semmi olyan kritériumot nem talált a szövegben, amely körülhatárolná a hatóságok azon kötelezettségét, amely szerint igazolniuk kell az adatközlés sürgős jellegét – akár utólag –, hogy ezáltal biztosítsák e jelentősen felgyorsított eljárás alkalmazásának lehetséges ellenőrzését, ugyanakkor a hat órás határidő valószínűleg igen gyenge ellenőrzést tesz csak lehetővé az adatok közlése előtt, vagy akár a szolgáltató részéről az ellenőrzés teljes hiányával is járhat. A hatásvizsgálat valóban hangsúlyozza annak szükségességét, hogy az illetékes hatóságok időben hozzáférjenek az adatokhoz. A hatásvizsgálatban megadott példák azonban mind súlyos bűncselekmények elkövetése (túszejtéssel járó terrorcselekmények, gyermekek folyamatban lévő szexuális bántalmazása) esetén igényelt bizonyítékokra vonatkoznak, de a bizonyítékok változékonyságára alapozott indokolás nem tűnik jónak akkor, amikor az adatok lehetséges változékony jellegén túl nem áll fenn egyéb sürgető jelleg. Az adatok változékony jellege ráadásul nem jelent kiegészítő indokolást annak arányosságával kapcsolatban, hogy az ilyen helyzetekben az adatokhoz való hozzáférésre kevesebb biztosítékkal kerüljön sor, amennyiben az adatok változékony jellegén túl nincs egyéb sürgető jelleg.

Az Európai Adatvédelmi Testület azt is kétli, hogy valóban szükséges a hat órás határidő biztosítása, miközben a szöveg úgy is rendelkezik, hogy ez a határidő nem lép érvénybe addig, amíg a kibocsátó hatóság „legkésőbb 5 napon belül” nem nyújt kiegészítő felvilágosítást, amennyiben a szolgáltató a kötelezettségének nem tud eleget tenni.

Az Európai Adatvédelmi Testület ezért arra szólít fel, hogy a hatásvizsgálatban kiegészítő elemekkel indokolják meg a határidők szükségességét azokban az esetekben, amelyekben az elkövetett vagy az eljárás tárgyát képező bűncselekmény nem súlyos, és ilyen részletes elemek hiányában adjanak meg egyértelmű kritériumokat, amelyekkel a KKEHT kibocsátása esetében a sürgősség indokolható. Lehetne például ugyanazt a modellt alkalmazni, amelyet az ENYH-irányelvben. Az ENYH-irányelv abban az esetben biztosít rövidebb határidőt, ha azt „az eljárási határidők, a bűncselekmény súlyossága vagy egyéb, különösen sürgető körülmények” indokolják (lásd a 12. cikk (2) bekezdését vagy az ideiglenes intézkedésekről való döntéshez szükséges 24 órás határidőről lásd a 32. cikk (2) bekezdését). A rendelettervezet hatásvizsgálata valóban nem tartalmaz részletes elemeket annak indokolására, hogy ezek a határidők miért nem működnek. Csak azokat az elemeket hangsúlyozza, amelyek szerint a nagy számban kiküldött kérések túlterhelik a megkeresett igazságügyi hatóságokat, amelyek így nem tudják tartani a határidőket.

c) A közlésre és megőrzésre kötelező európai határozatokat nem lehet egy másik tagállamban tartózkodó érintett adatainak kérésére felhasználni anélkül, hogy legalább a szóban forgó tagállam illetékes hatóságait értesítették volna, különösen tartalmi adatok esetében

Az Európai Adatvédelmi Testület emlékeztet arra, hogy a meglévő jogi eszközök rendelkeznek az igazságügyi együttműködésről és így a kiegészítő biztosítékokról is, különösen a kérések

szükségességének és arányosságának ellenőrzése érdekében, továbbá hangsúlyozza, hogy ezek a biztosítékok még inkább indokoltak azokban az esetekben, amikor a kért adatok olyan tartalmi adatok, amelyek még inkább korlátozzák az érintetteknek a személyes adatok és a magánélet védelmére irányuló jogait. Ebben a tekintetben az Európai Adatvédelmi Testület arra emlékeztet, hogy az ENYH-irányelv szintén rendelkezik a más tagállam által nyújtott technikai segítséggel végzett titkos távközlési információgyűjtés lehetőségéről (lásd a 30. cikket), valamint arról a kötelezettségről, amely szerint ha nincs szükség technikai segítségre, a titkos információgyűjtésről értesíteni kell a másik tagállam illetékes hatóságát minden olyan esetben, amikor az érintett személy a szóban forgó tagállam területén tartózkodik vagy fog tartózkodni (lásd a 31. cikket).

Az Európai Adatvédelmi Testület semmilyen indokot nem lát arra, hogy az elektronikus bizonyítékokról szóló rendelettervezetben előirányzott eljárás lehetővé tegye a tartalmi adatok oly módon történő közlését, hogy abban legalább az érintett tartózkodási helye szerinti tagállam illetékes hatóságai ne vegyenek részt.

d) A megőrzésre kötelező európai határozatot nem lehet a szolgáltatók adatmegőrzési kötelezettségeinek megkerülésére felhasználni

Az Európai Adatvédelmi Testület megjegyzi, hogy a megőrzésre kötelező európai határozatok fő célja az adatok törlésének megakadályozása.

Bár az Európai Adatvédelmi Testület elismeri, hogy az ilyen határozatok kibocsátása egyes esetekben lehet szükséges és arányos, sajnálatát fejezi az azzal kapcsolatos biztosítékok hiánya miatt. Az Európai Adatvédelmi Testület különösen azt ajánlja, hogy ha a megőrzésre kötelező határozatok csak bizonyos adatokra vonatkoznak, ahol a rendelettervezet látszólag szélesebb körű kérésekre is lehetőséget ad, és hogy ha az ilyen határozatokat az adatmegőrzési elvnek való megfelelés érdekében törlendő adatokra vonatkozóan bocsátják ki, a határozat soha nem adhat alapot a szolgáltatónak arra, hogy az adatokat az adattörlés kezdőnapja után dolgozza fel. Más szóval az adatokat „be kell fagyasztani”.

Ezenkívül a megőrzésre kötelező európai határozat és az azt követő, adatközlésre irányuló kérés közötti kapcsolatot – történjen az közlésre kötelező európai határozat, ENYH-kérés vagy kölcsönös jogsegély iránti kérelem révén – meg kell erősíteni annak érdekében, hogy a megőrzésre kötelező európai határozatokat csak olyankor bocsássák ki, amikor a másik kérés biztos (és nem csupán lehetőségként merül fel), és hogy ha a másik kérést elutasítják, a megőrzésre kötelező határozat szintén veszítse hatályát anélkül, hogy 60 napot[28] kellene várni akkor, ha az azt követő kérést utasítják el hamarabb.

e) Titoktartás és a felhasználók tájékoztatása

Az Európai Adatvédelmi Testület megjegyzi, hogy a rendelettervezet egy, kifejezetten a határozatok titkosságával foglalkozó cikket[29] is tartalmaz. Az adatvédelemhez való joggal való összekeverést és a félreértéseket elkerülendő az Európai Adatvédelmi Testület emlékeztet rá, hogy bár a GDPR úgy rendelkezik, hogy az érintettek adatainak a bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása céljából történő korlátozásáról jogszabályban kell rendelkezni, és ezért annak nyilvánosan hozzáférhetőnek kell lennie[30], valamint hogy e jogalkotási intézkedések tartalmazhatnak az érintettek arra vonatkozó

[28] Lásd a 10. cikk (1) bekezdését.
[29] Lásd a 11. cikket.
[30] Lásd a 23. cikk (1) bekezdésének d) pontját.

jogával kapcsolatos külön intézkedéseket, hogy tájékoztatást kapjanak a korlátozásról, kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját[31], nem rendelkezik arról a kötelezettségről, hogy az érintetteket a bűnüldöző hatóságok által benyújtott minden egyes adatkérésről külön-külön kell tájékoztatni.

Az Európai Adatvédelmi Testület ugyanakkor emlékeztet arra, hogy az adatvédelmi irányelv rendelkezik az érintettek azon jogáról, hogy maguktól az illetékes hatóságoktól kapjanak tájékoztatást, kivéve, ha ezt a jogot valamely érintettre korlátozták anélkül, hogy ez a jog kizárólag az EU területén lakóhellyel rendelkező érintettekre vonatkozna.

f) A határozat végrehajtására irányuló eljárás, amikor a szolgáltató megtagadja annak végrehajtását

Az Európai Adatvédelmi Testület megjegyzi, hogy a rendelettervezet 14. cikke rendelkezik egy olyan eljárásról, amely biztosítja a címzett által be nem tartott határozat végrehajtását, és a kibocsátó hatóság és a végrehajtó államban található illetékes hatóság közötti igazságügyi együttműködésen alapul.

Úgy tűnik azonban, hogy ez az eljárás nem teszi lehetővé a végrehajtó hatóság számára, hogy a pusztán eljárási indokokon túl más indokkal is elutasíthassa a megküldött határozat végrehajtását (akárcsak a címzett, elsősorban a nyújtott információ hiányát vagy az adatszolgáltatás tényleges lehetetlenségét illetően), mivel az adott állam nemzeti joga értelmében az érintett adatokat mentességgel vagy kiváltsággal védik, vagy mert az adatok közlése olyan alapvető érdekeket érintheti, mint a nemzetbiztonság és a védelem[32].

Az Európai Adatvédelmi Testület ezért megismétli a kiküldött határozatot fogadó illetékes hatóság általi kettős ellenőrzés megszüntetésével kapcsolatos aggályait, az egyéb jogi eszközökkel összevetve. Még a határozat végrehajtásának elutasítása esetén az az indok, hogy az sértené a Chartát, is fontosabbnak tűnik, mint az érintett személy alapvető jogainak megsértésével kapcsolatos klasszikus küszöbérték. Következésképpen az európai elfogatóparancs példáiból kiindulva, amely az elutasítás kötelező és szabadon választható indokairól egyaránt rendelkezik, vagy legalábbis az ENYH-irányelv példáiból kiindulva, amely általában úgy rendelkezik, hogy megdönthető a feltevés, amely szerint „ szabadságon, a biztonságon és a jog érvényesülésén alapuló térségnek az Unión belüli létrehozása a kölcsönös bizalmon és annak vélelmezésén alapul, hogy más tagállamok is tiszteletben tartják az uniós jogot, és azon belül is különösen az alapvető jogokat”[33], a rendeletnek legalább azt a minimális klasszikus eltérést tartalmaznia kell, hogy ha alapos okkal feltételezhető, hogy a határozat végrehajtása valamely alapvető jog sérelmét eredményezné, és hogy a végrehajtó állam elmulasztaná a Chartában elismert alapvető jogok védelme tekintetében fennálló kötelezettségei teljesítését, a határozat végrehajtását meg kell tagadni.

g) Határozatok végrehajtása és a harmadik ország jogából származó, egymással ütköző kötelezettségek (15–16. cikk)

Az Európai Adatvédelmi Testület üdvözli a rendelettervezetben foglalt lehetőséget, amely szerint a címzett azzal indokkal utasíthatja el a határozatot, hogy az ütközne az alapvető jogokkal, mivel ennek célja, hogy biztosítékokat nyújtson az egymással ütköző jogi kötelezettségek esetén. Az Európai

[31] Lásd a 23. cikk (2) bekezdésének h) pontját.
[32] Lásd a 14. cikk (2) bekezdését.
[33] Lásd a ENYH-irányelv (19) preambulumbekezdését.

Adatvédelmi Testület azt is fontosnak találja, hogy a javaslat a harmadik országok hatóságaival való egyeztetésről rendelkezik – legalábbis kollízió esetén –, valamint azt a kötelezettséget, amely szerint vissza kell vonni a határozatot akkor, ha a harmadik ország hatósága kifogást emel.

Ezért jelentősen tovább kell fejleszteni azt az eljárást, amelyet valamely határozat végrehajtásának egy harmadik ország joga értelmében egymással ütköző kötelezettségek fennállása miatti elutasítása esetén kell alkalmazni.

Először is az Európai Adatvédelmi Testület megjegyzi, hogy a rendelettervezet a közlésre kötelező határozat címzettjeként eljáró magánvállalkozásokra bízza annak értékelését, hogy a határozat ütközik-e a harmadik országnak a kért adatok közlését tiltó, alkalmazandó jogszabályaival. A vállalkozásnak indokolással ellátott kifogást kell emelnie, amely tartalmazza a harmadik ország jogszabályainak valamennyi releváns részletét, annak a szóban forgó ügyre történő alkalmazhatóságával és az ütköző kötelezettség jellegével együtt.

Ami ennél is fontosabb: az Európai Adatvédelmi Testületet aggasztja, hogy ilyen kifogás emelése esetén a kibocsátó hatóság szerinti tagállami illetékes bírósága egyedül értékeli, hogy fennáll-e ilyen kollízió, mivel a bíróság csak akkor lép kapcsolatba a harmadik ország hatóságaival, ha megállapította a kollízió fennállását. Az illetékes uniós bíróság ezért azt a hatáskört kapja, hogy ebben az összefüggésben következetesen értelmezze a harmadik ország jogát anélkül, hogy az ügy tartalmát illetően megfelelő szakértelemmel rendelkezne. Az Európai Adatvédelmi Testület ezért úgy véli, hogy a harmadik ország illetékes hatóságaival való egyeztetésre irányuló kötelezettség a jelenlegi javaslatban túlontúl korlátozott. Az adatvédelmet illetően az Európai Adatvédelmi Testület felhívja a jogalkotó figyelmét arra a tényre, hogy amennyiben egy harmadik ország illetékes bírósága a GDPR-t annak értékelése érdekében értelmezné, hogy az ütközik-e saját követelményeivel, akkor is az uniós adatvédelmi hatóságok és az illetékes bíróságok rendelkeznek illetékességgel az olyan adattovábbítás jogszerűségének értékelése terén, amely valamely harmadik ország bíróságának bármely olyan ítéletén, illetve közigazgatási hatóságának bármely olyan döntésén alapul, amely személyes adatok továbbítását vagy közlését írja elő[34].

Az Európai Adatvédelmi Testület azt is hangsúlyozza, hogy a harmadik ország jogának az uniós megkereső állam illetékes bírósága általi értékelésének objektív elemeken kell alapulnia, és aggodalommal veszi tudomásul azokat a feltételeket, amelyeket a rendelettervezet 15. cikkének (4) bekezdése és 16. cikke (5) bekezdésének a) pontja értelmében az illetékes bíróságnak a harmadik ország jogával kapcsolatban végzett értékelése során figyelembe kell vennie. A bíróságnak valójában azt kell értékelnie, hogy „ahelyett, hogy az alapvető jogok vagy a harmadik ország nemzetbiztonsággal vagy védelemmel kapcsolatos alapvető érdekeinek védelmére törekedne", a harmadik ország joga „nyilvánvalóan más érdekeket próbál-e meg védeni, illetve az arra irányul-e, hogy jogellenes tevékenységeket védelmezzen a nyomozásokkal összefüggő bűnüldözési célú megkeresésekkel szemben" vagy „a harmadik ország releváns joga által védett érdeket, beleértve a harmadik ország érdekét az adatokat közlésének megakadályozásához". Például bár elvben ehhez az értékeléshez az összes rendelkezésre álló információ figyelembevételével végzett, bizonyítékokon alapuló értékelés szükséges, tekintettel legalábbis az ilyen jellegű döntés lehetséges hatásaira, a megfogalmazás („is being aimed to", azaz „arra irányul") nem elég egyértelmű, ezért azt módosítani kell („has the aim/objective to", azaz „az a célja, hogy").

Az Európai Adatvédelmi Testület sajnálattal veszi tudomásul, hogy az egyetlen olyan eset, amikor a harmadik ország hatóságaival egyeztetnek, és amikor e hatóságok a közlésre kötelező határozat

[34] Lásd a GDPR 48. cikkét.

végrehajtása ellen kifogást emelhetnek, az, amikor az említett illetékes uniós bíróság releváns konfliktus fennállását állapítja meg, minden információt megküld az érintett harmadik országban található központi hatóságok részére, és a szóban forgó harmadik ország központi hatósága legfeljebb 50 napos (15 nap, amely 30 napra, majd egy utolsó lehetséges emlékeztető után további 5 nappal meghosszabbítható) szoros határidőn belül kifogást emelhet. Minden más esetben az illetékes bíróság abban a helyzetben van, hogy fenntarthatja a határozatot, és pénzbeli szankciót alkalmazhat a határozat végrehajtását elutasító szolgáltatóval szemben. Ennek következtében az Európai Adatvédelmi Testület aggódik amiatt, hogy az illetékes uniós bíróságokra nem vonatkozik egy olyan tágabb kötelezettség, amely szerint az érintett harmadik országok illetékes hatóságaival egyeztetniük kell annak biztosítása érdekében, hogy az eljárás szisztematikusabban biztosítsa, hogy mindkét fél érveit figyelembe vegyék, és még nagyobb tiszteletet kell tanúsítaniuk a harmadik országok joga iránt.

Amint az a 29. cikk szerinti munkacsoport nyilatkozatában és a fentiekben is szerepelt, az Európai Adatvédelmi Testület emlékeztet rá, hogy külön figyelmet kell fordítani a harmadik országok által elfogadott hasonló eszközökre, amelyek érinthetik az EU területén belül található érintettek jogait és a magánélet tiszteletben tartásához való jogukat, különös tekintettel az olyan hasonló eszközök jelentette kockázatra, amelyek közvetlenül ütközhetnek az uniós adatvédelmi joggal.

Az Európai Adatvédelmi Testület hangsúlyozza továbbá, hogy az is előfordulhat, hogy a kibocsátó hatóság szerinti tagállam illetékes bírósága nem a rendelettervezet 14. cikkében ismertetett határozat végrehajtásában illetékes bíróság, ami tovább növeli az egymással ütköző eljárásoknak, valamint normakollízió esetén a kölcsönös ellenőrzések hiányának kockázatát. Ez abból következik, hogy bizonyos esetekben akár három állam is lehet érintett: a határozatot kibocsátó hatóság szerinti tagállam, a szolgáltató szerinti harmadik ország, valamint az a tagállam, amelyben a szolgáltató EU-n belüli jogi képviselője található, és ahol a határozatot végre kell hajtani. Következésképpen a jelenleg előírt eljárást követve az A. tagállamban található megkereső hatóság bírósága a szolgáltató szerinti B. harmadik ország jogát saját maga értelmezheti anélkül, hogy e harmadik ország hatóságainak véleményét kikérné (miközben e hatóságok kifogást emeltek volna a határozat ellen), és felkérheti egy másik, C. uniós tagállam bíróságát, hogy döntését ellenvetés lehetősége nélkül hajtsa végre.

Emellett az Európai Adatvédelmi Testület üdvözli a közlésre kötelező határozatok elleni különleges jogorvoslatok bevezetését, a GDPR-ben és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvben biztosított jogorvoslatok mellett. Korábbi nyilatkozatában a 29. cikk szerinti munkacsoport már felhívta a figyelmet az ilyen biztosítékok fontosságára. Az Európai Adatvédelmi Testület azonban sajnálatát fejezi ki amiatt, hogy ezeket a jogorvoslatokat a megőrzésre kötelező határozatokkal szemben nem biztosítják, mivel e határozatok szintén eredményezhetik azon személyek alapvető jogainak korlátozását, akiknek a jogait megőrzik. A megőrzésre kötelező határozatok valóban eredményezhetik az adatoknak az adatvédelmi szabályok szerinti időtartamnál hosszabb ideig történő megőrzését. Ezért a megőrzésre kötelező határozat önmagában az érintett alapvető jogainak korlátozását eredményezi, amelynek indokolása felülvizsgálat és különleges jogorvoslatok tárgyát kell képezze, különösen azokban az esetekben, amikor az adatok megszerzéséhez a megőrzésre kötelező határozatot a közlésre kötelező határozattal együtt bocsátják ki. A 29. cikk szerinti munkacsoport nyilatkozatában is azt ajánlotta, hogy legalább a belföldi esetekben elérhető jogorvoslatokkal egyenértékű jogorvoslatot kell biztosítani.

h) Az adattovábbítás biztonsága egy határozatra történő válaszadáskor

Az Európai Adatvédelmi Testület megjegyzi, hogy a rendelettervezet csak arról rendelkezik, hogy a határozatok az Európai Unió területén található címzetteknek szólhatnak, és így nem rendelkezik a

címzettek és az Európai Unión kívül található szolgáltatók közötti adattovábbításhoz használandó csatornáról.

Bár az Európai Adatvédelmi Testület üdvözli az uniós adatvédelem általános keretrendszerétől való további eltérések hiányát, emlékeztet arra, hogy a címzetthez küldött bármely olyan határozatnak, amely az EU-n kívülre történő adattovábbítással járhat, meg kell felelnie a GDPR által szolgáltatott jogi keretnek. Az igazságügyi együttműködésnek az adatvédelmi biztosítékok tiszteletben tartásáról rendelkező jogi keretének megkerülése valójában nem eredményezheti az adattovábbítási követelményeknek a közlésre vagy megőrzésre kötelező határozatok címzettjei általi, a szóban forgó határozatoknak való megfelelés érdekében történő megkerülését.

Ezenkívül bár az Európai Adatvédelmi Testület üdvözli a titkosított adatok dekódolására irányuló kötelezettséget tartalmazó rendelkezés hiányát[35], aggasztja, hogy a javaslattervezetek nem írnak elő olyan külön követelményt a címzettek számára, amely szerint értékelniük kell a közölt adatok hitelességét, és hangsúlyozza, hogy az ilyen értékelés az igazságügyi együttműködésen alapuló hagyományos eszközök nyújtotta hozzáadott érték, továbbá arra is figyelmeztet, hogy az érintettekre nézve az ilyen értékelés hiánya megnövekedett kockázatot jelent.

Következtetések

Ezen értékelés alapján az Európai Adatvédelmi Testület a következő ajánlásokat fogalmazza meg a társjogalkotók felé:

1) Az EUMSZ 82. cikkének (1) bekezdése nem lehet a rendelet jogalapja.
2) Megfelelőbb igazolást kell nyújtani arról, hogy a meglévő ENYH-irányelvvel vagy a jogsegélyszerződésekkel összevetve valóban szükség van-e egy új eszközre. Részletes elemzést kell végezni az alapvető jogok szempontjából kisebb beavatkozással járó eszközökről, mint amilyen például az említett meglévő eszközök módosítása vagy a szóban forgó eszköz hatályának a megőrzésre kötelező határozatokra történő korlátozása, az adatokhoz való hozzáférés igénylésére irányuló egyéb meglévő eljárásokkal együttesen alkalmazva.
3) A rendeletnek hosszabb határidőt kell biztosítania, amely lehetővé teszi a végrehajtó szolgáltató számára, hogy az alapvető jogok védelmének tiszteletben tartására irányuló biztosítékokat nyújtson.
4) A kettős büntethetőség elvét fenn kell tartani, különösen akkor, ha a mindkét érintett tagállamban (a megkereső hatóság szerinti tagállamban és a szolgáltató helye szerinti tagállamban) nyújtott biztosítékok figyelembevételére irányuló kötelezettség fenntartása érdekében az adatok helyére vonatkozó feltétel megszűnik.
5) A rendelet hatályát a GDPR értelmében vett adatkezelőkre kell korlátozni, vagy tartalmaznia kell egy olyan rendelkezést, amely pontosítja, hogy amennyiben a megkeresett szolgáltató nem az adatok kezelője, hanem azok feldolgozója, köteles az adatkezelőt értesíteni.
6) A rendeletnek az adatok továbbítására vonatkozó biztosítékokat is tartalmaznia kell olyan esetekre, amikor a szolgáltató az e területtel kapcsolatos megfelelőségi határozattal nem rendelkező harmadik országban telepedett le, vagy az abban foglalt biztosítékok alkalmazhatósága érdekében hivatkoznia kell az (EU) 2016/680 irányelvre.

[35] Lásd a hatásvizsgálat (19) preambulumbekezdését és 240. oldalát.

7) Mivel a jogi képviselő kötelező kijelölése eltér a GDPR-től, a rendeletnek pontosítania kell, hogy az elektronikus bizonyítékokról szóló rendelet értelmében kijelölt jogi képviselő eltér a GDPR 3. cikke (2) bekezdésének értelmében kijelölt jogi képviselőtől.
8) A rendeletnek tágabban kell meghatároznia az elektronikus hírközlési adatok fogalmát annak biztosítása érdekében, hogy a nem tartalmi és a tartalmi adatokra egyaránt megfelelő biztosítékokat és hozzáférési feltételeket állapítson meg.
9) A rendeletnek emelnie kell a határozatok kibocsátására vonatkozó küszöbértékeket. A határozatokat csak bíróságok bocsáthatják ki vagy engedélyezhetik, kivéve az előfizetői adatokat, amennyiben ezen adatkategória fogalommeghatározását drasztikusan leszűkítik a csupán az adott személy azonosításához szükséges alapvető információkra, ami nem teszi lehetővé a kommunikációs adatokhoz való hozzáférést.
10) A rendeletnek egy szigorúan meghatározott bűncselekménylistára vagy legalábbis „súlyos bűncselekményekre" kell korlátoznia az előfizetői és a hozzáférési adatokhoz való hozzáférést.
11) Az adatszolgáltatásra, különösen a sürgős esetekre vonatkozó határidőt a rendeletnek jobban meg kell indokolnia, a 6 órás gyorsított eljárásnak pedig azt a kötelezettséget is tartalmaznia kell, amely szerint a megkereső hatóságoknak – akár utólag – igazolniuk kell az ilyen eljárást elindító sürgős esetet, ami lehetővé teszi az ilyen kivételes hatáskörök alkalmazásának ellenőrzését.
12) A tartalmi adatoknak az érintett tartózkodási helye szerinti tagállam illetékes hatóságának mindenfajta bevonása nélküli közlését lehetővé tevő eljárást el kell hagyni.
13) A rendeletben további javítást igényelnek a megőrzésre kötelező európai határozat kibocsátásával kapcsolatos biztosítékok.
14) A rendeletnek legalább azt a minimális klasszikus derogációt tartalmaznia kell, hogy ha alapos okkal feltételezhető, hogy a határozat végrehajtása valamely alapvető jog sérelmét eredményezné, és ennek eredményeként a végrehajtó állam elmulasztaná a Chartában elismert alapvető jogok védelme tekintetében fennálló kötelezettségei teljesítését, a határozat végrehajtását meg kell tagadni.
15) A rendeletnek tartalmaznia kell egy szélesebb körű kötelezettséget, amely szerint normakollízió esetén egyeztetni kell azon harmadik ország illetékes hatóságaival, ahol az adatszolgáltatásra felkért szolgáltató található, hogy ezáltal elkerüljék az egyetlen bíróság által adott szubjektív értelmezéseket.
16) A megőrzésre kötelező határozatok érvényességének és időtartamának szorosabban össze kell függnie az azokat kísérő, közlésre kötelező határozatokkal.
17) Az adattovábbítások biztonságosságát jobban kell biztosítani.
18) Rendelkezni kell az adatok hitelességének ellenőrzéséről, különösen akkor, ha titkosított adatok megadására is lehetőség van.

Az Európai Adatvédelmi Testület részéről

az elnök

(Andrea Jelinek)