EURÓPAI
BIZOTTSÁG

Brüsszel, 2024.10.9.
COM(2024) 451 final

A BIZOTTSÁG JELENTÉSE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

az EU–USA adatvédelmi keretről szóló megfelelőségi határozat működésének első időszakos felülvizsgálatáról

1. AZ ELSŐ IDŐSZAKOS FELÜLVIZSGÁLAT – HÁTTÉR, ELŐKÉSZÍTÉS ÉS FOLYAMAT

2023. július 10-i határozatában (a továbbiakban: megfelelőségi határozat) a Bizottság megállapította, hogy az EU–USA adatvédelmi keret megfelelő szintű védelmet biztosít az Európai Unióból az egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében[1]. A megfelelőségi határozat előírja a Bizottság számára, hogy időszakos felülvizsgálatokat végezzen, amelyek közül az elsőt a megfelelőségi határozatról szóló, a tagállamoknak küldött értesítéstől számított egy év elteltével kell elvégezni. Ez a jelentés lezárja ezt az első felülvizsgálatot.

A megfelelőségi határozat (211) preambulumbekezdésében előírtak szerint ez az első felülvizsgálat, amelyre az új keret működésének első évét követően kerül sor, annak ellenőrzésére összpontosított, hogy a keretben előírt valamennyi elemet végrehajtották-e, és azok hatékonyan működnek-e. A felülvizsgálat a keret működésének valamennyi vonatkozására kiterjedt, többek között a megfelelőségi határozat elfogadása óta bekövetkezett jogi fejlemények fényében.

A felülvizsgálat előkészítése során a Bizottság információkat gyűjtött az érdekelt felektől, különösen a digitális jogok és a magánélet védelme terén szakértelemmel rendelkező nem kormányzati szervezetektől (NGO-k)[2], az adatvédelmi keret alapján tanúsított szervezetektől, azok szakmai szövetségein[3] keresztül, valamint a keret végrehajtásában részt vevő egyesült államokbeli hatóságoktól. A Bizottság az „Ossza meg velünk véleményét!” portálon[4] közzétett külön véleményezési felhívás útján visszajelzéseket gyűjtött a nyilvánosságtól is.

2024. július 18–19-én Washingtonban felülvizsgálati ülésre került sor. Didier Reynders, a jogérvényesülésért és a fogyasztópolitikáért felelős uniós biztos és Gina Raimondo amerikai kereskedelmi miniszter nyitotta meg[5].

---

[1] A Bizottság (EU) 2023/1795 végrehajtási határozata (2023. július 10.) az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint a személyes adatoknak az EU–USA adatvédelmi keret által biztosított megfelelő szintű védelméről.

[2] A Bizottság kilenc nem kormányzati szervezetnek (Human Rights Watch, Amerikai Polgárjogi Unió, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Center for Democracy and Technology) küldött kérdőívet, amely az Egyesült Államok jogi keretének releváns fejleményeire, a felügyeleti és végrehajtási mechanizmusokra, valamint a jogorvoslati mechanizmusok működésére összpontosított. A Bizottság szolgálatai és az Európai Adatvédelmi Testület képviselői 2024. július 9-én online is találkoztak ezekkel a nem kormányzati szervezetekkel.

[3] A Bizottság kilenc szakmai szövetségnek (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, the Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association, Engine) küldött kérdőívet, amely az adatvédelmi keret alapján tanúsított vállalatok tapasztalataira összpontosított, különös tekintettel a tanúsítási eljárásra, az adatvédelmi keret elveinek való megfelelés érdekében tett lépésekre, az egyének kéréseinek és panaszainak kezelésére szolgáló mechanizmusokra stb.

[4] A beérkezett visszajelzések a következő linken érhetők el: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-A-Bizottsag-jelentese-az-EU-USA-adatvedelmi-keret-mukodeserol_hu.

[5] A felülvizsgálati ülés téma szerint szerveződött, és minden egyes külön napirendi pontot az illetékes egyesült államokbeli hatóság, illetve az illetékes uniós képviselő vagy szervezet rövid ismertetése vezetett be, amelyet részletes kérdések és válaszok követtek. A keret „kereskedelmi vonatkozásaival” (azaz az adatvédelmi keret alapján tanúsított vállalatokra vonatkozó követelmények alkalmazásával és érvényesítésével) az első napon

Az EU esetében a felülvizsgálatot az Európai Bizottság Jogérvényesülési és Fogyasztópolitikai Főigazgatóságának képviselői végezték az Európai Adatvédelmi Testület (EDPB) által kijelölt öt, különböző nemzeti adatvédelmi hatóságoktól érkező képviselővel és az európai adatvédelmi biztossal együtt[6]. Az Egyesült Államok részéről a Kereskedelmi Minisztérium, a Külügyminisztérium, a Szövetségi Kereskedelmi Bizottság (FTC), a Közlekedési Minisztérium, a Nemzeti Hírszerzési Igazgatóság (ODNI), az Igazságügyi Minisztérium, a Hírszerzési Közösség főellenőre, valamint az adatvédelmi és polgári szabadságjogi felügyelő tanács (PCLOB) képviselői vettek részt a felülvizsgálatban. Emellett a független vitarendezési szolgáltatásokat nyújtó szervezetek és az Amerikai Választottbírósági Szövetség képviselői is tájékoztatást nyújtottak a vonatkozó felülvizsgálati üléseken. A felülvizsgálathoz hozzájárultak továbbá az adatvédelmi keret alapján tanúsított szervezetek prezentációi arról, hogy a vállalkozások miként felelnek meg a keret követelményeinek.

A Bizottság megállapításaihoz felhasználtak továbbá nyilvánosan hozzáférhető anyagokat is, köztük bírósági ítéleteket, az Egyesült Államok érintett hatóságainak végrehajtási szabályait és eljárásait, nem kormányzati szervezetek által készített jelentéseket és tanulmányokat, az adatvédelmi keret alapján tanúsított vállalkozások által közzétett átláthatósági jelentéseket, független felügyeleti szervek éves jelentéseit, valamint médiatudósításokat.

2. MEGÁLLAPÍTÁSOK

2.1. Kereskedelmi vonatkozások

2.1.1. A tanúsítási eljárás

Az EU-ból az adatvédelmi keret alapján továbbított személyes adatok fogadása érdekében az egyesült államokbeli vállalatoknak tanúsítaniuk, majd évente újból tanúsítaniuk kell a Kereskedelmi Minisztérium számára, hogy betartják az adatvédelmi követelményeket (a továbbiakban: az adatvédelmi keret elvei). A tanúsításhoz az szükséges, hogy a vállalat az FTC vagy a Közlekedési Minisztérium vizsgálati és végrehajtási hatáskörébe tartozzon, nyilvánosan kinyilvánítsa az adatvédelmi keret elveinek való megfelelés iránti elkötelezettségét, nyilvánosan közzétegye adatvédelmi politikáját, valamint maradéktalanul végrehajtsa ezeket a követelményeket[7]. A tanúsítás véglegesítése előtt a Kereskedelmi Minisztérium ellenőrzi, hogy a vállalat megfelel-e az összes tanúsítási követelménynek[8].

A felülvizsgálati ülésen a Kereskedelmi Minisztérium kifejtette, hogy az adatvédelmi keret működésének első évében a tanúsítási folyamat bevezetésén volt a hangsúly, beleértve a célzott informatikai eszközök kifejlesztését, az eljárások frissítését, a vállalatokkal való együttműködést, valamint az egyéb tájékoztatási/tudatosságnövelő tevékenységeket. A felülvizsgálati ülés időpontjáig több mint 2 800 vállalat szerezte meg az adatvédelmi keret szerinti tanúsítást. Ez azt jelenti, hogy működésének első évében több vállalat szerezte meg az adatvédelmi keret szerinti tanúsítást, mint az előző keret, az adatvédelmi pajzs alapján[9]. A

foglalkoztak, a személyes adatokhoz való kormányzati hozzáféréssel kapcsolatos kérdéseket pedig a második napon vitatták meg.

[6] A Bizottság és az Európai Adatvédelmi Testület képviselői 2024. június 12-én és július 10-én találkoztak, hogy előkészítsék a felülvizsgálatot, megvitassák a beérkezett észrevételeket, és meghatározzák, hogy milyen vonatkozásban van szükség további információgyűjtésre és pontosításra.

[7] A megfelelőségi határozat I. mellékletének I.2. szakasza.

[8] A megfelelőségi határozat III. melléklete.

[9] Az egyenértékű időszakban 2 400 vállalat szerezte meg az adatvédelmi pajzs szerinti tanúsítást.

Kereskedelmi Minisztérium által szolgáltatott információk szerint a résztvevők 70 %-a kkv, az adatvédelmi keret szerinti tanúsítással rendelkező vállalatok nagy része (47 %) pedig az információs, kommunikációs és technológiai (IKT) ágazatban tevékenykedik. Emellett a vállalatok 60 %-a kizárólag a nem HR-adatok, 2,5 %-a kizárólag a HR-adatok, 37,5 %-a pedig mind a HR-adatok, mind a nem HR-adatok vonatkozásában egyaránt rendelkezik tanúsítással.

A Kereskedelmi Minisztérium elfogadta a vállalatok kérelmeinek kezeléséhez szükséges eljárásokat. A vállalatoknak a tanúsítás iránti kérelmüket a Kereskedelmi Minisztérium adatvédelmi kerettel foglalkozó weboldalán (https://www.dataprivacyframework.gov/) kell benyújtaniuk. Ez a weboldal információkat tartalmaz az adatvédelmi kerethez való csatlakozás módjáról[10] és a vállalatok keret szerinti kötelezettségeiről[11]. A Kereskedelmi Minisztériumon belül – az adatvédelmi keretért felelős külön igazgató felelőssége mellett – egy külön csoport felel az adatvédelmi keret irányításával és igazgatásával kapcsolatos valamennyi szempontért, beleértve a tanúsítási folyamatot és a megfelelés nyomon követését. Minden kérelmet egy adott munkatárshoz rendelnek, aki a tanúsítási folyamat egésze során felelős az adott vállalatért.

A keret szerinti tanúsításhoz a vállalatok benyújtják a kérelmüket, beleértve az adatvédelmi szabályzat tervezetét. A Kereskedelmi Minisztérium ellenőrzi, hogy az megfelel-e az adatvédelmi keret vonatkozó követelményeinek. Ha a szervezetek egy vállalatcsoporton belül különböző jogalanyokat (pl. különböző leányvállalatokat) kívánnak tanúsítani, a Kereskedelmi Minisztérium vagy egy átfogó adatvédelmi szabályzatot kér és vizsgál felül, amely egyértelműen feltünteti az összes érintett szervezetet, vagy külön szabályzatot kér minden egyes jogalanyra vonatkozóan. A Kereskedelmi Minisztérium a kérelemben megjelölt független jogorvoslati mechanizmusnál[12] is ellenőrzi, hogy a szervezet ténylegesen regisztrált-e nála. Azon vállalatok esetében, amelyek az adatvédelmi hatóság testületét választják (például azért, mert HR-adatokat dolgoznak fel), a Kereskedelmi Minisztérium ellenőrzi, hogy a vállalat befizette-e a testület használatához szükséges díjakat. Szükség esetén a Kereskedelmi Minisztérium azt is ellenőrzi, hogy a kérelmező az FTC vagy a Közlekedési Minisztérium joghatósága alá tartozik-e (és ezért jogosult-e az adatvédelmi kerethez való csatlakozásra).

Ha valamennyi feltétel teljesül, a Kereskedelmi Minisztérium tájékoztatja a szervezetet arról, hogy a honlapján közzéteheti az adatvédelmi keretre utaló adatvédelmi szabályzatát. Amint az adatvédelmi szabályzat nyilvánossá válik, a Kereskedelmi Minisztérium megerősíti a tanúsítást, és felveszi a vállalatot az adatvédelmi keretben részt vevő szervezetek listájára a honlapján. Az adatvédelmi keret attól az időponttól kezdve vonatkozik az EU-ból származó személyes adatok fogadására, amikor a Kereskedelmi Minisztérium felveszi a szervezetet az említett listára[13].

Amint az a felülvizsgálati ülésen elhangzott, a Kereskedelmi Minisztérium által végzett ellenőrzések eddig 33 kérelem elutasításához vezettek, mivel azok nem feleltek meg az adatvédelmi keret követelményeinek. Általánosságban elmondható, hogy a Kereskedelmi Minisztérium együttműködik a vállalatokkal az esetleges hiányosságok orvoslása érdekében. Amennyiben a Kereskedelmi Minisztérium hiányosságokat tár fel, tájékoztatja a vállalatot, hogy ezeket orvosolnia kell, és hogy a megadott határidőn belüli válaszadás elmulasztása vagy

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Magánszektorbeli vitarendezési mechanizmusok, amelyek révén minden magánszemély panaszait és vitáit kivizsgálják és gyorsan, a magánszemély számára költségmentesen rendezik.

[13] A megfelelőségi határozat I. melléklete I. szakaszának (3) bekezdése.

a Kereskedelmi Minisztérium eljárásai szerinti öntanúsítás egyéb elmulasztása esetén a kérelmet visszavontnak kell tekinteni. Ha 12 hónapon belül nem kerül sor az első tanúsítás kiállítására/módosítására, a Kereskedelmi Minisztérium úgy ítéli meg, hogy a kérelmet visszavonták.

Az egyes vállalatokra vonatkozó éves újratanúsítás esedékességi időpontját az adatvédelmi keretben részt vevő szervezetek listája tartalmazza. Annak érdekében, hogy emlékeztesse a vállalatokat az újratanúsítás kérelmezésének szükségességére, a Kereskedelmi Minisztérium létrehozott egy rendszert, amely emlékeztetőt küld arról, hogy a tanúsítás hamarosan lejár. A szervezetek emlékeztetőt kapnak egy hónappal, két héttel, majd egy nappal az esedékesség előtt. Azokat, amelyek hagyták, hogy tanúsításuk lejárjon, törlik az az adatvédelmi keretben részt vevő szervezetek listájáról. A megfelelőségi határozat III. mellékletében leírtak szerint a Kereskedelmi Minisztérium honlapján van egy külön szakasz, amely felsorolja azokat az egyesült államokbeli szervezeteket, amelyek már nem aktív résztvevők, és meghatározza azokat az okokat, amelyek miatt az érintett vállalatokat törölték a listáról (például lejárat vagy visszavonás) (a továbbiakban: az aktív regisztrációval nem rendelkező szervezetek listája). Amikor a szervezeteket azért törlik az adatvédelmi keretben részt vevő szervezek listájáról, mert hagyták lejárni a tanúsításukat, a Kereskedelmi Minisztérium kapcsolatba lép velük annak megerősítése érdekében, hogy ki kívánnak-e lépni, vagy inkább újra kívánják tanúsítani a szervezetet, és ez utóbbi esetben ellenőrzi, hogy abban az időszakban, amikor a lejárat miatt nem volt érvényes tanúsításuk, alkalmazták-e az adatvédelmi keret elveit az adatvédelmi keretnek megfelelően kapott személyes adatokra, és elmagyarázza, hogy milyen lépéseket fog tenni az újbóli tanúsításukat késleltető lezáratlan kérdések kezelésére. Amikor egy vállalat értesíti a Kereskedelmi Minisztériumot, hogy ki kíván lépni az adatvédelmi keretből, a Kereskedelmi Minisztérium előírja számára annak megerősítését, hogy visszaküldi-e vagy törli-e az adatvédelmi keretnek megfelelően kapott adatokat, megőrzi-e az ilyen adatokat és továbbra is alkalmazza rájuk az adatvédelmi keret elveit (amit évente meg kell erősíteni), vagy megőrzi-e őket és egyéb módon biztosítja a védelmüket (például az Európai Bizottság által elfogadott általános szerződési feltételekkel).

A szakmai szövetségektől és a vállalatoktól kapott visszajelzések azt mutatják, hogy az adatvédelmi keret alapján tanúsított vállalatok számos lépést tettek az adatvédelmi keret elveinek való megfelelés biztosítása érdekében. Például *a jogorvoslat, a végrehajtás és a felelősség elvének* való megfelelés érdekében a szervezetek önértékelés vagy külső megfelelőségi felülvizsgálat révén belső ellenőrzéseket végeztek. A felülvizsgálati ülésen részt vevő két magánszektorbeli független jogorvoslati mechanizmus elmondta, hogy az adatvédelmi szabályzatok felülvizsgálata révén külső megfelelőségi felülvizsgálatot is végeznek, az egyik magánszektorbeli független jogorvoslati mechanizmus pedig kifejtette, hogy ellenőrzéseket és szúrópróbaszerű ellenőrzéseket is végez, például a *hozzáférés,* a *választás* és az *újbóli adattovábbítás* elveire összpontosítva. A tanúsított vállalatok továbbá belső megfelelési programokat és felügyeleti mechanizmusokat dolgoztak ki, alkalmazottakat képeztek, olyan mechanizmusokat vezettek be, amelyek lehetővé teszik a magánszemélyek számára a jogaik gyakorlását, adatvédelmi hatásvizsgálatokat végeztek, valamint felülvizsgálták a meglévő szerződéseket.

2.1.2. A megfelelés ellenőrzése, a részvételre vonatkozó hamis állítások és a végrehajtás

Az adatvédelmi keret értelmében a Kereskedelmi Minisztérium feladata az adatvédelmi keret elveinek való megfelelés különböző eszközök – többek között hivatalból történő (saját

kezdeményezésű) ellenőrzések, *ad hoc* helyszíni ellenőrzések és megfelelőségi kérdőívek – alkalmazásával történő nyomon követése. Ez magában foglalja a keretben való részvételre vonatkozó hamis állítások keresését és kezelését, például internetes keresések révén[14].

Annak nyomon követése érdekében, hogy az adatvédelmi keret alapján tanúsított vállalatok megfelelnek-e az elveknek, a Kereskedelmi Minisztérium az elmúlt évben főként ad hoc internetes keresésekre és (közösségi) médiaellenőrzésekre támaszkodott. A Kereskedelmi Minisztérium arról számolt be, hogy ebben az első évben nem tárt fel problémákat az adatvédelmi keret elveinek való megfeleléssel kapcsolatban, és egyetlen vállalat ügyét sem utalta az FTC-hez vagy a Közlekedési Minisztériumhoz esetleges végrehajtási intézkedés céljából. Külön kapcsolattartó pontot is létrehozott az adatvédelmi hatóságokkal való együttműködés megkönnyítése, valamint a magánszemélyektől érkező panaszok és a más hatóságoktól (például adatvédelmi hatóságoktól vagy az FTC-től) érkező megkeresések fogadása érdekében. Az elmúlt évben azonban nem érkezett panasz, és nem utaltak át egyetlen ügyet sem. Míg az adatvédelmi keret működésének első éve a keret és a tanúsítási folyamat kidolgozására összpontosított, a Kereskedelmi Minisztérium a felülvizsgálati ülésen kifejtette, hogy a megfelelőség ellenőrzését automatizált eszközökkel tervezi elvégezni azok szisztematikusabb végrehajtása érdekében, és jelenleg az ehhez szükséges informatikai eszközök kifejlesztésén dolgozik.

A Bizottság elismeri, hogy a Kereskedelmi Minisztériumnak az első évben a keret és a tanúsítási folyamat kidolgozására kellett összpontosítania erőfeszítéseit. A továbbiakban fontos, hogy a Kereskedelmi Minisztérium fokozza az elveknek való megfelelés nyomon követésére és ellenőrzésére irányuló erőfeszítéseit, ami szükséges a keretnek való folyamatos és magas szintű megfelelés biztosításához, valamint a további végrehajtási intézkedéseket igénylő esetek felderítéséhez, beleértve a vállalatok esetleges hamis állításait a részvételükre vonatkozóan. Ebben a tekintetben a Bizottság üdvözli, hogy a Kereskedelmi Minisztérium megerősítette azon szándékát, hogy (automatizált) eszközöket dolgozzon ki és használjon a megfelelési problémák és a hamis állítások hatékonyabb és szisztematikusabb azonosítására, és úgy véli, hogy ennek a rendelkezésére álló különböző eszközök (pl. helyszíni ellenőrzések, megfelelés-felülvizsgálati kérdőívek, információkérések stb.) szélesebb körű használatára irányuló szélesebb körű erőfeszítés részét kell képeznie, beleértve az adatvédelmi keret szerinti konkrét követelményeknek való megfelelés ellenőrzését[15].

Az adatvédelmi keretben részt vevő szervezetek az FTC és a Közlekedési Minisztérium joghatósága alá tartoznak. A felülvizsgálati ülésen a Közlekedési Minisztérium megerősítette, hogy rendelkezik a megfelelő végrehajtási intézkedések meghozatalához szükséges valamennyi eljárással. Azt is kifejtette, hogy a joghatósága alá tartozó vállalatok közül nagyon kevés vállalat csatlakozott az adatvédelmi kerethez (azaz néhány jegyértékesítő, de légitársaságok nem). Az FTC megerősítette, hogy minden egyes adatvédelmi vizsgálata során következetesen ellenőrzi az adatvédelmi keret esetleges megsértését. Az FTC-hez eddig nem érkezett megkeresés más hatóságoktól. Érkezett néhány panasz, amely megemlíti az adatvédelmi keretet, bár ezek közül kettő az aktív regisztrációval nem rendelkező szervezetek

[14] Lásd a megfelelőségi határozat III. mellékletét. Hamis állításokról például akkor lehet szó, ha egy vállalat azt állítja, hogy részt vesz az adatvédelmi keretben, de vagy soha nem kezdte el a tanúsítási eljárást, vagy elkezdte, de nem fejezte be, vagy hagyta lejárni a tanúsítást.

[15] Például az újbóli adattovábbítást illetően az adatvédelmi keret 3. b. elve szerinti azon lehetőség kihasználásával, hogy újbóli adattovábbítás esetében a szerződések megfelelő adatvédelmi rendelkezéseinek összefoglalóját vagy reprezentatív példányát kérjék.

listáján szereplő vállalatokra, kettő pedig a kerethez nem csatlakozott vállalatokra vonatkozott, illetve egy panasz nem érintett az EU-ból továbbított személyes adatokat. E jelentés készítésének időpontjáig az FTC nem hozott határozatokat az adatvédelmi keretnek való megfelelés érvényesítése érdekében, bár megerősítette, hogy jelenleg több, az adatvédelmi keret alapján tanúsított vállalat esetében is vizsgálat folyik.

A Bizottság üdvözli, hogy az FTC valamennyi adatvédelmi vizsgálata során következetesen ellenőrzi az adatvédelmi keret esetleges megsértését. Mivel az adatvédelmi keret folyamatos hatékonysága a szigorú végrehajtástól függ, az FTC várhatóan tovább fogja gyakorolni vizsgálati hatáskörét a keret alapján, többek között azáltal, hogy proaktívan olyan online ellenőrzési akciókat hajt végre, amelyek az adatvédelmi keret egyes követelményeinek való megfelelésre és/vagy bizonyos ágazatokra összpontosítanak.

2.1.3. Panaszkezelés

Az adatvédelmi keret különböző jogorvoslati lehetőségeket biztosít az uniós polgárok számára azokban az esetekben, amikor a tanúsított szervezetek nem feleltek meg az adatvédelmi keret elveinek[16]. Ez magában foglalja a panasz rendezését az adatvédelmi keret alapján tanúsított szervezettel való közvetlen kapcsolatfelvétel révén, és a szervezetnek 45 napon belül választ kell adnia az érintett magánszemélynek. A panaszok kivizsgálása és rendezése érdekében a magánszemélyek panaszt nyújthatnak be a szervezet által kijelölt független jogorvoslati mechanizmushoz is. A körülményektől függően ez lehet alternatív vitarendezési testület vagy adatvédelmi hatóság[17]. Végezetül, amennyiben a többi rendelkezésre álló jogorvoslati lehetőség egyike sem rendezte kielégítően az érintett panaszát, a magánszemélyek „végső lehetőségként” kötelező erejű választottbírósági eljárást kezdeményezhetnek az EU–USA adatvédelmi kerettel foglalkozó testület előtt.

2.1.3.1. A vállalatok általi panaszkezelés

A szakmai szövetségeknek és a vállalatoknak a Bizottság által küldött kérdőívekre adott válaszai azt mutatják, hogy az adatvédelmi keret alapján tanúsított vállalatokhoz nagyon kevés panasz érkezett – ha érkezett egyáltalán – magánszemélyektől az adatvédelmi keret elveinek való meg nem feleléssel kapcsolatban. Ugyanakkor a vállalatok különböző olyan mechanizmusokat és eszközöket vezettek be, amelyek lehetővé teszik, hogy az egyének gyakorolhassák jogaikat és panaszt nyújthassanak be, többek között internetes formanyomtatványokon, e-mailben és telefonon.

2.1.3.2. *Független jogorvoslati mechanizmusok*

A felülvizsgálati ülésen kapott visszajelzések és a szakmai szövetségek által szolgáltatott információk azt mutatják, hogy nagyon kevés panasz érkezett a független jogorvoslati mechanizmusokhoz. A vállalatok által választott független jogorvoslati mechanizmusok közé tartozik a BBB National Programs, a JAMS, a TRUSTe és a VeraSafe. Az adatvédelmi keret előírja, hogy a független jogorvoslati mechanizmusoknak éves jelentést kell közzétenniük, amely összesített statisztikákat tartalmaz a vitarendezési szolgáltatásaik igénybevételéről. E

[16] Lásd a megfelelőségi határozat 2.4. szakaszát.

[17] Az adatvédelmi keret alapján tanúsított szervezetek kötelesek együttműködni az adatvédelmi hatóság által végzett vizsgálat és panaszrendezés során, amennyiben az a munkaviszony keretében gyűjtött HR-adatok feldolgozására vonatkozik, vagy ha az adott szervezet önként vállalta az adatvédelmi hatóságok általi felügyeletet.

jelentés elfogadásakor már valamennyi érintett független jogorvoslati mechanizmus közzétette éves jelentését[18].

Ezenkívül a felülvizsgálati ülésen a BBB és a VeraSafe részletesen beszámolt az elmúlt évi tevékenységéről. Elmondták, hogy a korábbi keretekhez képest nőtt a szolgáltatásaikat választó üzleti résztvevők száma, és megemlítették, hogy néhány panasz érkezett hozzájuk, bár a túlnyomó többségük esetében az üzleti résztvevők nem voltak jogosultak panaszkezelésre. A BBB-hez például 87 panasz érkezett uniós magánszemélyektől, és közülük csak kettő volt jogosult rendezésre. Bár a BBB kifejtette, hogy a panaszokat átlagosan öt munkanapon belül dolgozzák fel, az említett két panaszt végül lezárták a magánszemélyek válaszának hiánya miatt. A VeraSafe-hez 26 panaszt érkezett, amelyek közül hat volt jogosult rendezésre. Ezek közül kettő, hozzáférési és törlési kérelemre vonatkozó panaszt rendeztek, kettő függőben maradt, kettőt pedig visszavontak vagy lezártak a magánszemély válaszának hiánya miatt. Mindkét független jogorvoslati mechanizmus kifejtette, hogy a magánszemélyek nyelvén kívánják megválaszolni a panaszokat.

Az adatvédelmi keret alapján tanúsított, az EU-ból továbbított HR-adatokat feldolgozó vállalatoknak az érintett adatok tekintetében az uniós adatvédelmi hatóságokat kell választaniuk független jogorvoslati mechanizmusként, míg az adatvédelmi keret alapján tanúsított vállalatok önkéntes alapon választhatják független jogorvoslati mechanizmusként az uniós adatvédelmi hatóságokat az adatvédelmi keret alapján továbbított személyes adatok egyéb típusai tekintetében. Üdvözlendő, hogy a felülvizsgálat idején az adatvédelmi keret alapján tanúsított vállalatok több mint fele ezt a megoldást választotta[19]. A megfelelőségi határozat elfogadása óta az Európai Adatvédelmi Testület elfogadta az uniós adatvédelmi hatóságok informális testületének eljárási szabályzatát. A testület hatáskörrel rendelkezik arra, hogy kötelező erejű tanácsot adjon az egyesült államokbeli szervezeteknek az adatvédelmi keret alapján az EU-ból továbbított személyes adatok kezelésével kapcsolatban magánszemélyektől érkező megoldatlan panaszok tekintetében. Eljárási szabályzata alapján a testületet egy vezető adatvédelmi hatóságként eljáró adatvédelmi hatóság és más kijelölt felülvizsgálati társhatóságként eljáró adatvédelmi hatóságok alkotják[20]. A testület az adatvédelmi kerettel kapcsolatos panasz kézhezvételétől számított 60 napon belül kötelező

---

[18] ANA – https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs – https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA – https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Insights association – https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS – https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services – https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution – https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;
Verasafe – https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Röviddel a felülvizsgálati ülés után az adatvédelmi keret weboldala jelezte, hogy a 2 892 résztvevő közül 1 511 választott uniós adatvédelmi hatóságot jogorvoslati mechanizmusként.

[20] 2024. április 17-én az Európai Adatvédelmi Testület az EU–USA adatvédelmi keretnek megfelelően elfogadta az uniós adatvédelmi hatóságok informális testületének eljárási szabályzatát. A dokumentum itt érhető el: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_hu.pdf.

erejű tanácsot ad. Az Európai Adatvédelmi Testület közzétette továbbá az adatvédelmi hatóságokhoz benyújtott panaszok bejelentésére szolgáló formanyomtatvány mintáját[21], valamint az európai magánszemélyek[22] és vállalkozások[23] számára az adatvédelmi kerettel kapcsolatban gyakran ismételt kérdéseket. A felülvizsgálat idején a testülethez még nem érkezett panasz.

2.1.3.3. A kötelező erejű választottbírósági mechanizmus

A Kereskedelmi Minisztérium a kötelező erejű választottbírósági mechanizmus kezelésére a Nemzetközi Vitarendezési Központot (ICDR) választotta, amely az Amerikai Választottbírósági Szövetség nemzetközi részlege. A megfelelőségi határozat elfogadását követően a Kereskedelmi Minisztérium a Bizottsággal együtt 11, a magánélet védelme terén tapasztalattal, illetve különböző háttérrel – beleértve a választottbírósági eljárást, az igazságszolgáltatást, a tudományos köröket és a civil társadalmat –rendelkező választottbírót választott[24]. Ezenkívül elfogadták az adatvédelmi kerettel foglalkozó testület választottbírósági szabályait[25] és a választottbírák magatartási kódexét[26], és mindezek elérhetők az ICDR honlapján. A felülvizsgálat idején uniós magánszemélyek még nem aktiválták a választottbírósági mechanizmust.

2.1.4. Iránymutatás, együttműködés és figyelemfelkeltés

Az adatvédelmi keret hatálybalépése óta a Kereskedelmi Minisztérium különböző figyelemfelkeltő tevékenységeket végzett: roadshow-kat, webináriumokat és konferenciákat szervezett, megkereste a szakmai szövetségeket, és több mint 3 000 vállalattal vette fel közvetlenül a kapcsolatot az adatvédelmi kerettel kapcsolatos tájékoztatás érdekében. Közzétett egy iránymutatást is, többek között a magánszemélyeknek, valamint az uniós és az egyesült államokbeli vállalkozásoknak címzett GYIK formájában[27]. Az Európai Adatvédelmi Testület pedig magánszemélyeknek és vállalkozásoknak szóló panasznyomtatványokat és GYIK-okat dolgozott ki. Hasonlóképpen, a Bizottság a megfelelőségi határozatának elfogadásakor kérdéseket és válaszokat, illetve tájékoztatót tett közzé az adatvédelmi keretről[28].

Ugyanakkor a felülvizsgálati ülés során kiderült, hogy további munkára van szükség a magánszemélyek tudatosságának növeléséhez és a vállalatoknak nyújtott iránymutatáshoz. A vállalatoktól és a független jogorvoslati mechanizmusoktól kapott információk, valamint a panaszok nagyon alacsony száma arra enged következtetni, hogy a magánszemélyek nem feltétlenül ismerik mindig a jogaikat és/vagy az azok gyakorlására vonatkozó mechanizmust. A felülvizsgálati ülésen a Kereskedelmi Minisztérium érdeklődését fejezte ki az uniós adatvédelmi hatóságokkal való, arra irányuló együttműködés iránt, hogy növeljék az uniós

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_hu.

[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_hu.

[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_hu.

[24] https://go.adr.org/DPF_Arbitrator_Bios.html.

[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf. https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.

[27] Lásd például az alábbi internetes oldalt: https://www.dataprivacyframework.gov/US-Businesses.

[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_hu.

polgárok kerettel kapcsolatos tudatosságát. A Bizottság ösztönzi az ilyen kezdeményezéseket, emellett lépéseket tesz a magánszemélyek jobb tájékoztatása érdekében, többek között azáltal, hogy a honlapján további információkat nyújt az adatvédelmi keretről, például az Európai Adatvédelmi Testület, a Kereskedelmi Minisztérium és más egyesült államokbeli hatóságok által elfogadott releváns iránymutatásokra mutató linkekkel és hivatkozásokkal.

Ami az adatvédelmi keret elveivel kapcsolatos iránymutatást illeti, az Európai Adatvédelmi Testület képviselői a felülvizsgálati ülésen megállapodtak abban, hogy az elkövetkező hónapokban együttműködnek, hogy tovább pontosítsák a HR-adatok adatvédelmi keret szerinti fogalmát és az ilyen adatok kezelésére vonatkozó külön kötelezettségeket. Megvizsgálták az iránymutatásba belefoglalandó különböző elemeket. Ez az iránymutatás foglalkozhatna például egyes olyan gyakorlati forgatókönyvekkel, amelyekben a munkavállalók adatait az adatvédelmi keret alapján dolgoznák fel (például egy felhőszolgáltató), és kifejthetné, hogy az ilyen forgatókönyvek esetében az adatvédelmi keret mely kötelezettségei relevánsak. Emellett javasolhatná, hogy azok a vállalatok, amelyek uniós magánszemélyek munkavállalói adatait fogadják (de nem feltétlenül használják fel ezeket az adatokat munkaviszony összefüggésében), az adatvédelmi hatóság testületét válasszák független jogorvoslati mechanizmusként. Ez biztosítaná, hogy ezek a magánszemélyek olyan hatósághoz fordulhassanak, amely közel van a lakóhelyükhöz és szükség esetén jobban ismeri a HR-adatokra alkalmazandó nemzeti jogszabályokat.

Emellett úgy tűnik, hogy hasznos lenne több iránymutatás (a szakmai szövetségektől kapott információk alapján is) az adatvédelmi keret újbóli adattovábbításra vonatkozó követelményeivel kapcsolatban. A Kereskedelmi Minisztérium jelezte továbbá, hogy érdemes lenne megvizsgálni, hogy egyes ágazatok számára előnyös lehet-e további iránymutatás az adatvédelmi keret elveinek a tevékenységeikre való alkalmazása tekintetében, például az egészségügyi kutatás és a pénzügyi szolgáltatások területén.

A Bizottság üdvözli, hogy mindkét fél kész iránymutatást kidolgozni, és arra számít, hogy hamarosan megkezdődik a fent említett témákkal kapcsolatos munka.

Általánosabban fogalmazva, számos mechanizmust hoztak létre az Egyesült Államok hatóságai és az adatvédelmi hatóságok közötti információcsere és együttműködés biztosítása érdekében, többek között az FTC-n és a Kereskedelmi Minisztériumon belüli olyan külön kapcsolattartó pontok kijelölésével, amelyek az adatvédelmi hatóságok megkereséseivel foglalkoznak.

2.1.5. Az Egyesült Államok jogrendszerének releváns fejleményei

A megfelelőségi határozat elfogadása óta számos fejlemény történt az Egyesült Államok jogi keretrendszerében az adatvédelem terén. Ez jogalkotási, szabályozási és az ítélkezési gyakorlattal kapcsolatos fejleményeket is magában foglal. Ezek általában azt jelzik, hogy az EU és az Egyesült Államok egyre inkább közelíti egymáshoz a magánélet védelmével kapcsolatos bizonyos kihívásokra vonatkozó megközelítéseit, többek között hasonló jogi fogalmak használatával. E fejlemények némelyike folyamatban van, és további nyomon követésre lesz szükség.

Szövetségi szinten az elnök számos olyan elnöki rendeletet adott ki, amely releváns a személyes adatok felhasználása szempontjából. Mindenekelőtt a 2024. február 28-i 14117. sz.

elnöki rendelet[29] tiltja vagy korlátozza a különleges adatok (például egészségügyi adatok, biometrikus azonosítók, emberi genomikai adatok) bizonyos kategóriáit érintő tranzakciókat egyes „aggodalomra okot adó országokban[30]” működő szervezetek összefüggésében. Az elfogadott rendelet arra utasítja a főügyészt, hogy javasoljon – e jelentés elfogadásakor még kiadandó – rendeleteket a végrehajtása további pontosítása érdekében. Emellett a mesterséges intelligenciáról szóló, 2023. október 30-i 14110. sz. elnöki rendelet[31] a biztonságos, védett és megbízható mesterséges intelligencia fejlesztésére összpontosít. Több szövetségi hivatal számára is előírja, hogy dolgozzon ki mesterséges intelligenciával kapcsolatos biztonsági szabványokat és iránymutatásokat, többek között a magánéletet érintő konkrét MI-kockázatokra és a magánélet védelmét szolgáló technikákra vonatkozóan.

Ami a jogalkotási munkát illeti, míg az elmúlt években szövetségi adatvédelmi törvényeket terjesztettek elő a Kongresszusban, 2024 júliusáig 20 amerikai szövetségi állam fogadott el átfogó adatvédelmi törvényt, amelyek közül nyolc lépett hatályba az alábbi államokban: Kalifornia, Colorado, Oregon, Virginia, Connecticut, Utah, Texas és Florida. Ezen túlmenően 17 amerikai szövetségi állam fogadott el olyan jogszabályokat, amelyek foglalkoznak az automatizált adatkezeléssel (vagy legalábbis annak bizonyos formáival), és a „profilalkotáson[32]” alapuló döntéshozatal bizonyos típusai esetében általában lehetővé teszik annak megtagadását.

Ami az ítélkezési gyakorlat fejleményeit illeti, a civil társadalom számos képviselője rámutatott a Legfelsőbb Bíróságnak a Loper Bright Enterprises kontra Raimondo ügyben a közelmúltban hozott ítéletére (2024. június 28.). Ez az ítélet hatályon kívül helyezi a *Chevron*-doktrínával kapcsolatos korábbi ítélkezési gyakorlatot, amely szerint a bíróságok az alkalmazkodás elvét alkalmazzák a szabályozó ügynökség észszerű jogértelmezését illetően az adott ügynökség által érvényesített jogszabály kétértelműsége esetén. Mindenekelőtt egyes nem kormányzati szervezetek aggodalmukat fejezték ki a Legfelsőbb Bíróság ezen ítélete által az FTC magánélet védelmével kapcsolatos szabályozási hatáskörére gyakorolt hatással kapcsolatban, ugyanakkor elismerték, hogy a végrehajtási hatáskörére viszont nem vagy csak korlátozottan lehet hatással.

---

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Ezek közé tartozik a javasolt szabályozásról szóló, 2024. május 3-án kiadott előzetes értesítésben a főügyész által javasoltaknak megfelelően Kína, Kuba, Hongkong és Makaó, Irán, Észak-Korea és Venezuela. Lásd: https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[32] Bár az egyes államok eltérően értelmezik a „profilalkotás” fogalmát, a profilalkotás általában a személyes adatok automatizált kezelésének bármely olyan formája, amelyet az azonosított vagy azonosítható személy gazdasági helyzetével, egészségi állapotával, személyes preferenciáival, érdeklődésével, megbízhatóságával, viselkedésével, tartózkodási helyével vagy mozgásával kapcsolatos személyes szempontok értékelése, elemzése vagy előrejelzése céljából végeznek. Jellemzően a fogyasztók dönthetnek úgy, hogy nem vesznek részt a profilalkotásban. A következő államok dolgoztak ki profilalkotásra vonatkozó jogszabályokat: Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518, Delaware (Del. Code Ann. tit. 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Maryland Online Data Privacy Act of 2024, hatálybalépés: 2024. május 9.), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Rhode Island Data Transparency and Privacy Protection Act, hatálybalépés: 2024. június 29.), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051), és Virginia (Va. Code Ann. § 59.1-577).

A felülvizsgálati ülésen az FTC elmondta, hogy még korai lenne tudni ezen ítélet pontos következményeit. Ugyanakkor kifejtette, hogy az FTC általi szabályozás más közigazgatási hivatalokhoz képest eltérő, az FTC-ről szóló törvényben foglalt hatáskörben történik, és annak esetében a *Chevron*-doktrína kevésbé volt releváns. A közelmúltbeli ítéletnek ezért korlátozott hatása lehet ezen a területen.

Az FTC tájékoztatást nyújtott az automatizált adatkezeléssel és a mesterséges intelligenciával kapcsolatos megközelítésének közelmúltbeli fejleményeiről is. Ez magában foglalja az automatizált rendszereken belüli megkülönböztetés és elfogultság elleni közös nyilatkozat más végrehajtó hatóságokkal együtt történő elfogadását[33], valamint számos végrehajtási intézkedés tartozik ide, amelyekben az FTC többek között az átláthatóságra, az automatizált adatkezelés méltányosságára és a magánszemélyek azon képességére összpontosít, hogy megtámadják az eredményeket. E tekintetben a legszembetűnőbb eset az FTC 2024 márciusában a *Rite Aid* ellen hozott határozata, amely ötéves tilalmat vezetett be az arcfelismerő technológia e cég általi biztonsági célú használatára vonatkozóan[34]. Az FTC különösen azt állapította meg, hogy a *Rite Aid* nem hozott észszerű intézkedéseket annak érdekében, hogy megelőzze a hibás eredményeket és tájékoztassa a fogyasztókat az alkalmazott technológiáról. Általánosabban véve, a felülvizsgálati ülésen az FTC kitért a jelenlegi prioritásaira és különösen azokra a területekre, amelyek véleménye szerint proaktívabb jogérvényesítési megközelítést érdemelnek. Ez magában foglalja a különleges adatok (például az egészségügyi adatok, a biometrikus adatok és a földrajzi helymeghatározás)[35] védelmét, a gyermekek[36] és kiskorúak online védelmét, valamint az adatbiztonságot[37].

A Bizottság továbbra is szorosan figyelemmel fogja kísérni ezeket és az Egyesült Államokban bekövetkezett egyéb fejleményeket, különösen az átfogó szövetségi adatvédelmi törvény irányába tett további lépéseket, valamint a Legfelsőbb Bíróság közelmúltbeli ítélkezési gyakorlata által az FTC magánélet védelme terén betöltött szerepére gyakorolt lehetséges hatást.

A Bizottság üdvözli az FTC által nyújtott tájékoztatást a közelmúltban végzett jogérvényesítési tevékenységéről és jelenlegi prioritásairól, amelyek nagyrészt megfelelnek az európai adatvédelmi jogérvényesítés tendenciáinak és prioritásainak. Az FTC aktívan részt vesz az uniós megfelelőségi határozat előnyeit élvező országokat tömörítő hálózatban is, amelyet a

---

33 https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

34 https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

35 Lásd például az FTC közelmúltbeli végzését az X-Mode ellen a hívó helyére vonatkozó érzékeny információk eladása és megosztása ügyében (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) és a Monument ellen az érzékeny egészségügyi adatok harmadik felek részére marketing célokra történő átadása ügyében (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

36 Az FTC például nemrégiben bejelentette, hogy perhez vezető vizsgálatot indított a TikTok és anyavállalata, a Bytedance ellen a gyermekek magánéletére vonatkozó jogszabályok állítólagos megsértése miatt. Állításuk szerint egyik vállalat sem tett eleget annak a követelménynek, hogy a 13 éven aluli gyermekektől származó személyes adatok gyűjtése és felhasználása előtt erről tájékoztatást kell nyújtani és meg kell szerezni a szülői hozzájárulást (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

37 Lásd a közelmúltbeli jogérvényesítési tevékenységek áttekintését az FTC 2023. évi adatvédelmi és adatbiztonsági frissítésében: https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

Bizottság 2024 márciusában indított[38]. Ennek a fokozott konvergenciának ösztönöznie kell és meg kell könnyítenie az Atlanti-óceán mindkét partján működő adatvédelmi jogalkalmazók közötti szorosabb együttműködést, különösen az adatvédelmi keret működésével kapcsolatos kérdésekben.

2.2. Az EU–USA adatvédelmi keret alapján továbbított személyes adatokhoz az Egyesült Államok hatóságai általi hozzáférés és felhasználás szempontjai

A megfelelőségi határozat tartalmazza az EU-ból az adatvédelmi keret alapján tanúsított vállalatok részére továbbított személyes adatoknak az Egyesült Államok hatóságai általi – különösen bűnüldözési és nemzetbiztonsági célokból történő – gyűjtésére és felhasználására vonatkozó szabályok részletes értékelését. A megfelelőségi határozat elfogadása óta – amint azt az Egyesült Államok hatóságai a felülvizsgálati ülésen megerősítették – az adatvédelmi keret működésének első évében nem történt releváns fejlemény az adatokhoz való bűnüldözési vagy szabályozási célú hozzáférésre alkalmazandó jogi kerettel kapcsolatban. Ezért az alábbi megállapítások csak a nemzetbiztonság területén bekövetkezett fejleményekre vonatkoznak.

A hírszerző ügynökségek adatokhoz való hozzáférésével kapcsolatban a megfelelőségi határozatban levont következtetések a több releváns jogkörnek megfelelően végzett jelfelderítési műveletekre vonatkozó – különösen a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény (FISA) 702. szakaszában és a 12333. sz. elnöki rendeletben [39] megfogalmazott, az Egyesült Államok elnöke által 2022. október 7-én elfogadott, az egyesült államokbeli jelfelderítésre vonatkozó biztosítékok megerősítéséről szóló 14086. sz. elnöki rendelettel kiegészített és megerősített – feltételek és korlátozások elemzésén alapulnak. A 14086. sz. elnöki rendeletben meghatározott biztosítékok az Egyesült Államok valamennyi jelfelderítési tevékenységére vonatkoznak, függetlenül attól, hogy e tevékenységek mely hatáskörön alapulnak, illetve hol kerül rájuk sor, és védik a nem egyesült államokbeli személyek (köztük az európaiak) adatait[40]. A 14086. sz. elnöki rendelet új jogorvoslati mechanizmust is létrehozott, amelyen keresztül az uniós magánszemélyek hivatkozhatnak ezekre a kötelező biztosítékokra és érvényesíthetik őket.

A következő szakaszok ismertetik az Egyesült Államok hatóságai által a 14086. sz. elnöki rendeletnek való megfelelés érdekében a megfelelőségi határozat elfogadása óta tett lépéseket, valamint a fent említett jogi kerettel kapcsolatos releváns fejleményeket.

2.2.1. Az Egyesült Államok jogi keretével kapcsolatos releváns fejlemények

2.2.1.1. A 14086. sz. elnöki rendelet hírszerző ügynökségek általi végrehajtása

A 14086. sz. elnöki rendelet által bevezetett korlátozások és biztosítékok kiegészítik a FISA 702. szakaszában és a 12333. sz. elnöki rendeletben foglalt korlátozásokat és biztosítékokat.

---

[38] Lásd: https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. A 2024. márciusi ülés eredményeként úgy határoztak, hogy több tematikus ülést tartanak. Az elsőre 2024 júliusában került sor, és olyan eszközök kidolgozására összpontosított, amelyek támogathatják a kis- és középvállalkozásokat az adatvédelmi jogszabályoknak való megfelelésben.

[39] Az EU-ból továbbított adatok tekintetében a FISA értelmében hozható egyéb intézkedések közé tartozik az egyedi elektronikus megfigyelés (a FISA 105. szakasza), a fizikai keresés (a FISA 302. szakasza), a kimenő és bejövő hívások adatait rögzítő eszközök használata (a FISA 402. szakasza), valamint az üzleti nyilvántartások gyűjtése bizonyos vállalatoktól (közös fuvarozók, nyilvános szálláshelyek, gépjármű-bérbeadó létesítmények vagy raktározási létesítmények, a FISA 501. szakasza). A megfelelőségi határozat részletesen elemzi ezeket a különböző jogalapokat (a (142)–(152) preambulumbekezdés).

[40] További információkért lásd a megfelelőségi határozat 3.2.1.2. szakaszát.

Ezek minden hírszerző ügynökségre nézve kötelezőek, és az egyes ügynökségek által elfogadott politikák és eljárások révén működésük tovább javult.

Az első felülvizsgálat részeként az Egyesült Államok hatóságai megerősítették, hogy a 14086. sz. elnöki rendelet nem módosult az elfogadása óta. Emellett egyértelművé tették, hogy az Egyesült Államok elnöke nem élt a 14086. sz. elnöki rendelet 2. szakasza (b) pontja (i) alpontjának (B) szakaszában és 2. szakasza (b) pontja (ii) alpontjának (C) szakaszában ismertetett hatáskörrel azon jogszerű célok listájának frissítése érdekében, amelyek tekintetében jelfelderítés folytatható, vagy azon célok listájának frissítése érdekében, amelyekre a tömegesen gyűjtött adatok felhasználhatók[41]. A 14086. sz. elnöki rendelet külön eljárást vezetett be, hogy meghatározza azokat a konkrétabb hírszerzési prioritásokat, amelyek tekintetében jelfelderítés folytatható. Mindenekelőtt konzultálni kell az ODNI polgári szabadságjogok védelmével foglalkozó tisztviselőjével (ODNI CLPO), hogy minden prioritás esetében értékelje, hogy 1) az előmozdítja-e az elnöki rendeletben felsorolt egy vagy több jogszerű célkitűzést, 2) azt nem arra tervezték és nem is várták, hogy jelfelderítési adatgyűjtéshez vezessen az elnöki rendeletben felsorolt tiltott célkitűzések érdekében, és 3) azt valamennyi személy magánéletének és polgári szabadságjogainak megfelelő figyelembevételét követően állapították meg[42]. Az ODNI CLPO a felülvizsgálati ülésen megerősítette, hogy miután áttekintette a nemzeti hírszerzési igazgató által a 2023. évi nemzeti hírszerzési prioritásokról szóló keretben javasolt prioritásokat, arra a következtetésre jutott, hogy azok megfelelnek a fenti követelményeknek, és megosztotta következtetését a nemzeti hírszerzési igazgatóval (DNI), aki a prioritásokat jóváhagyásra benyújtotta az elnöknek. Az ODNI CLPO a 14086. sz. elnöki rendelet követelményeiről képzést is nyújtott a Hírszerző Közösség azon munkatársainak, akik részt vesznek a hírszerzési prioritások kidolgozásában.

Emellett az Egyesült Államok hatóságai az elmúlt évben további gyakorlati lépéseket tettek annak érdekében, hogy napi működésük során végrehajtsák a 14086. sz. elnöki rendeletet. A hírszerző ügynökségek mindenekelőtt további belső politikákat és iránymutatásokat vezettek be az elnöki rendelet alkalmazására vonatkozóan, például belső eljárásokat (belső engedélyezési követelmények vagy dokumentált hozzáférés-ellenőrzés révén, hogy csak a megfelelően képzett és a szükséges küldetési követelményekkel rendelkező személyek férjenek hozzá az információkhoz stb.) annak biztosítása érdekében, hogy a rendelet szükségességi és arányossági követelményei mind a célzott, mind a tömeges adatgyűjtéssel összefüggésben teljesüljenek[43]. Emellett képzést biztosítottak a 14086. sz. elnöki rendelettel kapcsolatban a különböző hírszerző ügynökségek (pl. NSA, CIA, FBI) személyzete számára, beleértve az ODNI CLPO által szervezett éves és ad hoc képzéseket, valamint az ODNI-hoz csatlakozó valamennyi új munkatárs számára kötelező képzéseket.

A Bizottság üdvözli a 14086. sz. elnöki rendelet végrehajtása és az annak való megfelelés biztosítása érdekében bevezetett különböző intézkedéseket. Mivel már több tapasztalat áll rendelkezésre az elnöki rendelet biztosítékainak gyakorlati alkalmazásával kapcsolatban, a Bizottság nagyra értékelné, ha a jövőbeli felülvizsgálatok során konkrét példákat vitathatnának

---

41 E jogszerű célkitűzések/célok közé tartozik például a kémkedés, szabotázs, gyilkosság vagy más, külföldi kormány, szervezet vagy személy által, nevében vagy segítségével végzett hírszerzési tevékenység elleni védelem, a terrorizmus, a túszejtés, valamint a valamely külföldi kormány, szervezet vagy személy által vagy nevében történő fogva tartás elleni védelem.

42 A 14086. sz. elnöki rendelet 2. szakasza (b) pontjának (iii) alpontja.

43 Lásd: https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, közzététel dátuma: 2023. július 3.

meg arra vonatkozóan, hogyan alkalmazzák az elnöki rendeletet a gyakorlatban (az alkalmazandó titoktartási megfontolások tiszteletben tartása mellett).

2.2.1.2. A FISA 702. szakaszának újbóli engedélyezése

A FISA 702. szakasza lehetővé teszi a külföldi hírszerzési információk gyűjtését olyan nem amerikai személyek megcélzása révén, akikről megalapozottan feltételezhető, hogy az Egyesült Államokon kívül tartózkodnak. Az információszerzés a Külföldi Hírszerzést Felügyelő Bíróságnak (FISC) benyújtott és az általa jóváhagyott éves tanúsítások alapján történik. Ezek a tanúsítások meghatározzák a gyűjtendő külföldi hírszerzési információk konkrét kategóriáit. 2023. július 21-én az ODNI bejelentette, hogy a FISA 702. szakasza alapján három jóváhagyott tanúsítás létezik, amelyek a külföldi hírszerzés alábbi kategóriáira terjednek ki: 1) külföldi kormányok és kapcsolódó szervezetek, 2) a terrorizmus elleni küzdelem és 3) a fegyverek elterjedése elleni küzdelem[44]. A tanúsításokat emellett a FISC által jóváhagyott célzott és minimalizálási eljárásoknak kell kísérniük[45]. A célkiválasztás mindenekelőtt úgy történik, hogy felkérik az „elektronikus hírközlési szolgáltató” FISA-definíciójának megfelelő egyesült államokbeli vállalatokat, hogy tegyék közzé az elektronikus hírközlési adatokat egyes „választóknak” – amelyek egy adott kommunikációs fiókot, pl. telefonszámot vagy e-mail-címet azonosítanak – vagy „választóktól” küldött kommunikációra vonatkozóan. Az Egyesült Államok kormánya számos anyagot tett közzé a FISA 702. szakaszával kapcsolatban, hogy tájékoztassa a nyilvánosságot a megfigyelési programok működéséről, az alkalmazandó követelményekről és a magánélet védelme érdekében tett intézkedésekről, valamint a FISC szerepéről[46].

Egy hatályvesztésre vonatkozó rendelkezés értelmében a FISA 702. szakasza 2023 végén hatályát veszti, kivéve, ha azt a Kongresszus újra engedélyezi. Az ideiglenes, változtatás nélküli újbóli engedélyezést követően a Kongresszus 2024. április 19-én elfogadta a hírszerzés reformjáról és Amerika biztonságáról szóló törvényt (RISAA), amely két évre újra engedélyezte a FISA 702. szakaszát, és számos változtatást vezetett be. Ezek nagy vonalakban két csoportra oszthatók: 1) a FISA 702. szakasza alapján engedélyezett megfigyelési tevékenységek körének megváltozása és 2) intézményi és eljárási változások.

A FISA 702. szakasza alapján engedélyezett megfigyelési tevékenységek körének változásai

A RISAA három fő módosítást vezetett be a FISA 702. szakasza alapján végezhető megfigyelési tevékenységek körét illetően.

Először is, véglegesen megtiltotta az ún. említésalapú információgyűjtést[47]. Ez olyan üzenetek gyűjtésére vonatkozik, amelyek esetében a 702. szakasz szerinti választó (például egy e-mail-cím) nem az üzenet küldője vagy címzettje mezőben szerepel, hanem magában az üzenetben (pl. olyan e-mail-üzenetek, amelyeket nem a kiválasztott e-mail-címre vagy a kiválasztott e-mail-címről küldenek, hanem az e-mail szövegében szerepel a kiválasztott e-mail-cím). Bár az ilyen információgyűjtést a FISA 2018. évi módosítását követően már megszüntették, a FISA a

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] Az ilyen eljárások korlátozzák az egyes külföldi hírszerzési célokra vonatkozó adatgyűjtést, korlátozzák az olyan adatbázisokhoz való hozzáférést, amelyekben a FISA 702. szakasza alapján megszerzett információkat tárolnak (ideértve a hozzáférés ellenőrzését), és korlátozzák az ilyen információk felhasználását, megőrzését és terjesztését.

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

[47] A RISAA 22. szakasza.

FISC és a Kongresszus bevonásával zajló egyedi engedélyezési eljárásnak megfelelően továbbra is lehetőséget biztosított az említésalapú információgyűjtés jövőbeli újraindítására. A RISAA legutóbbi módosítása megszüntette ezt a lehetőséget.

Másodszor, a külföldi hírszerzési információk fogalommeghatározását kiterjesztették a kábítószer elleni küzdelemmel kapcsolatos információkra[48]. A felülvizsgálati ülésen az Egyesült Államok hatóságai kifejtették, hogy ezt a jelenlegi fentanil-válságra, valamint a nemzetközi kábítószer-kereskedők és -gyártók által jelentett növekvő nemzetbiztonsági fenyegetésekre való tekintettel vezették be. Ennek fényében megerősítést nyert, hogy ez a fogalom a 14086. sz. elnöki rendeletben felsorolt számos jogszerű célkitűzés – azaz az Egyesült Államok vagy szövetségesei nemzetbiztonságára aktuális vagy potenciális fenyegetést jelentő külföldi szervezetek képességeinek, szándékainak vagy tevékenységeinek megértése vagy értékelése, a globális biztonságot érintő transznacionális fenyegetések megértése vagy értékelése, beleértve a közegészségügyi kockázatokat, valamint a transznacionális bűnügyi fenyegetésekkel szembeni védelem[49] – körébe tartozik.

Harmadszor, a RISAA kiterjesztette az „elektronikus hírközlési szolgáltató” fogalommeghatározását, és ezáltal kibővítette az olyan vállalatok körét, amelyek a FISA 702. szakasza alapján adatszolgáltatásra kötelezhetők[50]. A fogalommeghatározás immár magában foglalja az olyan berendezésekhez való hozzáféréssel rendelkező egyéb szolgáltatókat, amelyeket vezetékesen vagy elektronikusan üzenetek továbbítására vagy tárolására használnak vagy használhatnak, ugyanakkor kifejezetten kizárja a nyilvános szálláshelyeket, lakásokat, közösségi létesítményeket és vendéglátási létesítményeket. Az Igazságügyi Minisztérium a Kongresszushoz intézett levelében erre a módosításra olyan technikai módosításként hivatkozott, amelynek célja, hogy lefedje az olyan „rendkívül kis” számú technológiai vállalatokat, amelyekre a FISC és a Külföldi Hírszerzést Felügyelő Fellebbviteli Bíróság (FISCR) közelmúltbeli határozatai szerint nem terjedt ki az „elektronikus hírközlési szolgáltató” korábbi fogalommeghatározása[51]. Az Igazságügyi Minisztérium ugyanebben a levélben kötelezettséget vállalt arra, hogy szűkíti ezt a kört, és ezt a fogalommeghatározást kizárólag a FISC-határozathoz vezető jogvita tárgyát képező szolgáltatótípusra alkalmazza. Következésképpen az érintett vállalatokat megnevezik egy, a Kongresszusnak szánt, minősített mellékletben. Több nem kormányzati szervezet, köztük azok, amelyek a felülvizsgálat részeként visszajelzést adtak, aggodalmát fejezte ki a fogalommeghatározás ilyen kiterjesztéssel kapcsolatban, és azzal érvelt, hogy az potenciálisan számos egyesült államokbeli vállalkozást érinthet (mivel közülük sokan nyújtanak valamilyen típusú szolgáltatást, és hozzáférnek kommunikációs berendezésekhez). Az ilyen aggályokra való tekintettel a Hírszerzési Közösség támogatásával újabb módosítást javasoltak a 2025-ös pénzügyi évre vonatkozó hírszerzési engedélyezési törvény tervezetében, amelyet jelenleg a Kongresszus tárgyal. Ez a módosítás – amennyiben a Kongresszus elfogadja – biztosítaná, hogy az „elektronikus hírközlési szolgáltató” fogalommeghatározása alá tartozó további vállalatok köre csak a FISC fent említett határozataiban említett vállalatokra korlátozódjon. A törvénytervezetben az is szerepel, hogy az ilyen vállalatoknak címzett irányelveket jelenteni

48 A RISAA 23. szakasza.

49 A 14086. sz. elnöki rendelet 2. szakasza (b) pontja (ii) alpontja (A) szakaszának (2), (3) és (10) pontja.

50 A RISAA 25. szakasza.

51 https://www.justice.gov/opa/media/1348621/dl?inline. Lásd a FISC 2022. évi határozatát (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) és a Külföldi Hírszerzést Felügyelő Fellebbviteli Bíróság e határozatot helybenhagyó ítéletét (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

kell a FISC-nek, hogy az felülvizsgálhassa, hogy az adott vállalat valóban a fogalommeghatározás alá tartozik-e. A Kongresszushoz intézett levelében az Igazságügyi Minisztérium kötelezettséget vállalt arra, hogy hathavonta jelentést tesz a Kongresszusnak az aktualizált fogalommeghatározás alkalmazásáról annak érdekében, hogy a Kongresszus megfelelő felügyeletet gyakorolhasson a fogalommeghatározás szűk körű alkalmazása tekintetében.

Fontos megjegyezni, hogy az Egyesült Államok hatóságai és a PCLOB a felülvizsgálati ülésen megerősítették, hogy a 14086. sz. elnöki rendelet valamennyi biztosítéka továbbra is teljes mértékben alkalmazandó a FISA 702. szakasza szerinti valamennyi adatgyűjtésre és -felhasználásra, e módosításokat követően is. Így, bár a RISAA némileg kiszélesíti azon vállalatok körét, amelyek esetében végzést adhatnak ki, nem korlátozza a jogok gyakorlását. Mindazonáltal fontos lesz a további (jogalkotási és jelentéstételi) fejlemények nyomon követése, valamint az ilyen új szabályok gyakorlati alkalmazásáról szóló tájékozódás. Idetartozik például a külföldi hírszerzési információk és az elektronikus hírközlési szolgáltató fogalommeghatározásának kibővítése által a FISA 702. szakasza szerinti célpontok számára gyakorolt hatás (az ODNI által évente közöltek szerint, lásd alább az átláthatóság tekintetében). A FISA 702. szakaszáról szóló közelmúltbeli PCLOB-jelentést utánkövető jövőbeli jelentésnek (lásd alább) különösen informatívnak kell lennie e tekintetben.

Intézményi és eljárási változások

Ami az intézményi és eljárási változásokat illeti, a RISAA számos olyan eljárást kodifikált, amelyet a gyakorlatban már követtek, és új biztosítékokat vezetett be. Míg ezek közül néhány csak egyesült államokbeli személyeket érint, számos változás nagyobb védelmet biztosít mind az egyesült államokbeli, mind a nem egyesült államokbeli személyek számára, akiknek az adatai a FISA 702. szakasza[52] alapján gyűjthetők, és ezért ezek a változások relevánsak az adatvédelmi keret működése szempontjából.

Először is, számos további elszámoltathatósági, felügyeleti és jelentéstételi követelményt vezettek be. Mindenekelőtt, az FBI személyzetének már évente képzésben kell részesülnie a FISA 702. szakasza alapján megszerzett információk lekérdezésére vonatkozó szabályokról[53]. Az FBI köteles továbbá beszámolni a Kongresszusnak a lekérdezési tevékenységéről (pl. a „kötegelt technológiákat” alkalmazó lekérdezések számáról, azaz egyetlen lekérdezés részeként több lekérdezési kifejezés futtatásáról), valamint a lekérdezésre vonatkozó jogi követelményeknek való megfelelés biztosítása érdekében bevezetett elszámoltathatósági intézkedésekről (a RISAA 11–12. szakasza). Ezenkívül az Igazságügyi Minisztérium főellenőre köteles jelentést készíteni arról, hogy az FBI megfelel-e a lekérdezési követelményeknek (a RISAA 9. szakasza). Általánosabban fogalmazva, a FISC előtti eljárások átláthatóságának növelése érdekében az ODNI-nak és a főügyésznek már 180 napon belül le kell zárnia a FISC-határozatok minősítésének feloldására irányuló felülvizsgálatot (a RISAA

[52] Emellett a RISAA bevezetett néhány változtatást a FISA 105. szakasza szerinti hagyományos, egyedi elektronikus megfigyelés tekintetében (a FISC által kiadott parancs alapján, ha teljesül az alapos gyanúra vonatkozó követelmény). Ahhoz, hogy egy hírszerző ügynökség egyedi elektronikus megfigyelésre vonatkozó végzést kérjen a főügyésztől, már eskü alatt tett nyilatkozatra van szükség, amely igazolja azt a meggyőződést, hogy teljesülnek a FISA 105. szakaszában foglalt feltételek (a RISAA 6. szakaszának (a) pontja). A külföldi hatalmak vagy a külföldi hatalmak ügynökei tekintetében az elektronikus megfigyelés lehetséges időtartamát 120 napról egy évre hosszabbították meg (a RISAA 6. szakaszának (g) pontja).

[53] A RISAA 2. szakaszának (d) pontja.

7. szakasza). Emellett a FISC és a Külföldi Hírszerzést Felügyelő Fellebbviteli Bíróság (FISCR, ahol fellebbezéssel lehet élni a FISC határozataival szemben) előtti valamennyi tárgyalás átiratát meg kell őrizni és továbbítani kell a Kongresszusnak (a RISAA 8. szakasza).

Másodszor, a RISAA további korlátozásokat vezetett be a FISA 702. szakasza alapján gyűjtött adatok FBI általi felhasználására vonatkozóan. A RISAA 2. szakaszának (d) pontja úgy rendelkezik, hogy az FBI a „kötegelt technológiát" alkalmazó lekérdezést csak ügyvédi jóváhagyását követően végezheti el, kivéve, ha rendkívüli körülmények állnak fenn. Emellett az FBI már nem ellenőrizheti automatikusan a FISA 702. szakasza alapján megszerzett nem minimalizált információkat, és ehelyett biztosítania kell, hogy az elemzőknek kifejezetten dönteniük kelljen az ilyen információkban való keresésről. A RISAA azt is megtiltotta az FBI-nak, hogy olyan lekérdezéseket végezzen, amelyek egyedüli célja a bűncselekményre vonatkozó bizonyítékok felkutatása és kinyerése (kivéve, ha megalapozottan feltételezhető, hogy segíthetnek az életveszély vagy a súlyos testi sérülés mérséklésében vagy bekövetkeztének elhárításában, vagy szükség esetén a peres eljárások során a nyilvánosságra hozatali kötelezettségek teljesítésében[54]). Ezenkívül megtiltotta az FBI számára a nem minimalizált adatok elemző adattárakba történő bevitelét, kivéve, ha a célszemély érintett valamely nemzetbiztonsági vizsgálatban[55].

Harmadszor, egyes, az *amicus curiae* FISC előtti státuszára és szerepére vonatkozó rendelkezések módosultak[56]. Az *amicus curiae* olyan szakértő, aki segíti a Bíróságot (és a FISCR-t) a magánélethez és a polgári szabadságjogokhoz kapcsolódó ügyekben, vagy segít tisztázni a technológiai kérdéseket egy adott kormány kérelmével kapcsolatban. Míg a FISA korábban előírta, hogy az *amicus curiae-nak* szakértelemmel kell rendelkeznie a magánélet védelme és a polgári szabadságjogok, a hírszerzési információk gyűjtése és a kommunikációs technológia terén vagy más releváns területeken, most főszabály szerint a magánélethez való jog/a polgári szabadságjogok, illetve a hírszerzési információk gyűjtése terén szerzett szakértelmet követel meg. A Bíróságnak már eddig is volt lehetősége arra, hogy minden általa megfelelőnek ítélt esetben *amicus curiae-t* nevezzen ki, és ezt kötelező is volt megtennie, amikor új vagy jelentős jogértelmezéssel foglalkozott. Az újbóli engedélyezést követően a FISC-nek most minden alkalommal, amikor a FISA 702. szakasza szerinti tanúsítások és kísérő eljárások (pl. célzási eljárások) jóváhagyására kérik, *amicus curiae-t* kell kineveznie, kivéve, ha úgy találja, hogy ez nem lenne megfelelő, vagy valószínűleg indokolatlan késedelemhez vezetne[57]. Ezenkívül a Bíróság ahelyett, hogy csak egyet nevezne ki, már dönthet úgy, hogy egy vagy több *amicus curiae-t* nevez ki. Egyértelművé tették azt is, hogy az *amicus curiae* által szolgáltatandó információknak „a bíróság által meghatározott konkrét kérdésekre kell korlátozódniuk", bár azok a területek, amelyekkel kapcsolatban az *amicus curiae* észrevételeket tehet, széles körűek maradtak (azaz az egyesült államokbeli személyek magánéletének és polgári szabadságjogainak védelmével kapcsolatos jogi érvek és információk, hírszerzési adatgyűjtés és kommunikációs technológia vagy bármely más releváns terület).

---

54 A RISAA 3. szakaszának (a) pontja.

55 A RISAA 3. szakaszának (b) pontja. Amennyiben rendkívüli körülmények miatt szükséges, az FBI igazgatója dönthet az e rendelkezés alóli kivételről, amelyről értesíteni kell a Kongresszust.

56 Az egyértelműség érdekében ezek a módosítások nem érintik a különleges főtanácsnokoknak a DPRC előtti jogállását és szerepét, amint azt az Egyesült Államok a felülvizsgálati ülésen megerősítette.

57 A RISAA 5. szakaszának (b) pontja.

Végezetül a RISAA 18. szakasza létrehoz egy „FISA-reformbizottságot” – amely többek között a Kongresszus tagjaiból, a PCLOB elnökéből, a nemzeti hírszerzés főigazgató-helyetteséből és a főügyészhelyettesből, valamint a Kongresszus által kinevezendő további tagokból áll[58] –, hogy további FISA-reformokat javasoljon.

A Bizottság szorosan nyomon fogja követni a FISA 702. szakaszával kapcsolatos további fejleményeket, többek között a PCLOB felügyeleti tevékenységével (lásd alább), a reformbizottság munkájával és a FISA közelgő, két év utáni felülvizsgálatával összefüggésben.

2.2.1.3. Felügyeleti tevékenységek a gyakorlatban: számadatok és tendenciák

A nemzetbiztonsági megfigyelési jogosultságok Hírszerző Közösség általi, a 2023. naptári évre vonatkozó használatáról szóló éves ODNI statisztikai átláthatósági jelentés (amelyet 2024 áprilisában tettek közzé)[59] azt mutatja, hogy a FISA 702. szakasza szerinti célpontok száma a 2022. naptári évi 245 073-ról a 2023-as naptári évben 268 590-re nőtt. A jelentés kifejti, hogy a célpontok számának ingadozása különböző okokra vezethető vissza, ideértve az operatív prioritások változásait, a globális eseményeket, a műszaki képességeket, a célmagatartást és a távközlési ágazat változásait. A jelentésből az is kiderül, hogy a FISA 402. szakasza (a kimenő és bejövő hívások adatait rögzítő eszközök) alapján nem került sor nem egyesült államokbeli személyek megfigyelésére (2021-ben ez a szám 1, 2022-ben pedig 0 volt), míg a FISA 501. szakasza (a közös fuvarozók, gépjármű-bérbeadó létesítmények vagy fizikai raktározási létesítmények üzleti nyilvántartásaihoz való hozzáférés) alapján hat (2021-ben 13, 2022-ben pedig 11) célpont vonatkozásában hat végzést adtak ki (szemben a 2021. évi és 2022. évi 11 végzéssel), amelyek 5 412 egyedi azonosítót érintettek (szemben a 2021. évi 23 157 és a 2022. évi 55 431 egyedi azonosítóval), amelyeket az ilyen végzések alapján gyűjtött információk megosztására használtak.

Az Igazságügyi Minisztérium által a külföldi hírszerzési megfigyelésről szóló törvénynek megfelelően a Kongresszus számára készített éves jelentés szerint a 2023-as naptári évben 327 kérelmet nyújtottak be a FISC-hez a FISA 105., illetve 302. szakasza szerinti, külföldi hírszerzési célú elektronikus megfigyelés és/vagy fizikai keresés céljából[60]. A célszemélyek teljes száma 500 és 999 között volt. Ami a nemzetbiztonsági leveleket (NSL) illeti, a jelentés szerint (kivéve a csak előfizetői információkra vonatkozó kéréseket) 10 115 megkeresést adtak ki nem egyesült államokbeli személyeket érintő információkra vonatkozóan, és ezek keretében 3 033 különböző nem egyesült államokbeli személyre vonatkozóan kértek információt[61].

Számos, az adatvédelmi keret alapján tanúsított vállalat (pl. Google, Meta) él az Egyesült Államok joga által biztosított azon lehetőséggel, hogy olyan átláthatósági jelentéseket tegyen közzé, amelyek tájékoztatást nyújtanak az adott jelentéstételi időszakban hozzájuk beérkezett FISA- és NSL-kérelmek számáról. E jelentés elkészítésekor a FISA 2023 júliusa utáni kérelmeire vonatkozó statisztikák még nem álltak rendelkezésre. A Google például arról számolt be, hogy 2023 júliusa és decembere között 500–999 NSL-kérést kapott, amelyek

58 A 18. szakasz kifejezetten előírja a Kongresszuson kívüli képviselők részvételét.

59 https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

60 https://www.justice.gov/nsd/media/1350236/dl?inline.

61 Ezek a számok az előző jelentéstételi évhez (2022) képest nagyrészt változatlanok. Összehasonlításképpen 2022-ben 317 végleges kérelem érkezett a FISC-hez a külföldi hírszerzési célokból végzett elektronikus megfigyelés és/vagy fizikai keresés vonatkozásában. Az elektronikus megfigyelést elrendelő végzések által érintett célszemélyek teljes száma 0 és 499 között volt. Az FBI 2022-ben 9 103 NSL információkérést nyújtott be nem amerikai személyekre vonatkozóan (kivéve a kizárólag előfizetői információkra vonatkozó kéréseket). Forrás: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.

2 000–2 499 fiókot érintettek[62]. A Meta arról számolt be, hogy ugyanebben a jelentéstételi időszakban 0–499 NSL-kérelmet kapott, amelyek 500–999 fiókot érintettek[63]. Ezek a számok az elmúlt években nagyrészt változatlanok. Az átláthatóság további növelése érdekében egyes vállalatok (pl. a Google) a titoktartási korlátozások feloldását követően proaktívan közzéteszik az általuk kapott NSL-eket[64].

2.2.1.4. Egyéb fejlemények

A felülvizsgálat előkészítésével összefüggésben több nem kormányzati szervezet kérdéseket vetett fel az Egyesült Államok hírszerző ügynökségei által kereskedelmi szervezetektől, különösen adatközvetítőktől való adatvásárlás révén történő adatgyűjtés új formáival kapcsolatban. Kifejtették, hogy bár az ezen az alapon gyűjtött adatokat továbbra is más követelményeknek megfelelően kell feldolgozni, többek között a 12333. elnöki rendelet alapján[65], az ilyen adatszerzésre a FISA és a 14086. sz. elnöki rendelet keretein kívül kerül sor.

E tekintetben emlékeztetni kell arra, hogy az adatok harmadik felekkel való önkéntes megosztásának minden típusára számos részletes feltétel vonatkozik az adatvédelmi keret alapján. Először is, a tanúsított szervezet nem oszthat meg adatokat harmadik féllel (amely nem ügynökként/feldolgozóként jár el) anélkül, hogy az érintett magánszemélyeket értesítené és választást kínálna számukra[66]. Másodszor, *az újbóli adattovábbításért való elszámoltathatóság elvével* összhangban az újbóli adattovábbításra kizárólag (1) korlátozott és meghatározott célból, (2) az EU–USA adatvédelmi kerete által tanúsított szervezet és a harmadik fél közötti szerződés alapján és (3) csak akkor kerülhet sor, ha a szerződés előírja a harmadik fél számára, hogy ugyanolyan szintű védelmet nyújtson, mint amilyent az elvek garantálnak[67].

Továbbá, amint azt a felülvizsgálati ülésen is megvitatták, az FTC végrehajtási intézkedéseket hozott az érzékeny fogyasztói adatokat értékesítő adatközvetítőkkel szemben. Például az *X-Mode* és jogutódja, az *Outlogic* ellen indított ügyben az FTC 2024. január 9-én határozatot fogadott el, amelyben megtiltotta a vállalat számára, hogy földrajzi helymeghatározási adatokat adjon el harmadik feleknek, és előírta a jogellenesen használt és megosztott adatok törlését. Az FTC vizsgálata többek között azt állapította meg, hogy a vállalat nem tájékoztatta teljes körűen a magánszemélyeket földrajzi helymeghatározási adataik felhasználásáról és értékesítéséről, nem vezetett be olyan intézkedéseket, amelyek lehetővé tették a magánszemélyek számára, hogy elutasítsák a nyomon követést, lehetővé tette az adatok potenciálisan diszkriminatív célokra történő felhasználását, és nem korlátozta az ilyen információk harmadik felek általi felhasználását[68]. A Bizottság arra számít, hogy az FTC ugyanezt a megközelítést fogja alkalmazni, ha az adatvédelmi keret alapján tanúsított vállalatok a fent említett rendelkezéseket megsértve osztanának meg adatokat.

62 https://transparencyreport.google.com/user-data/us-national-security.
63 https://transparency.meta.com/reports/government-data-requests/country/US/.
64 https://transparencyreport.google.com/user-data/us-national-security.
65 Lásd például a 12333. sz. elnöki rendelet adatgyűjtési technikákról szóló 2.4. szakaszát.
66 Lásd a megfelelőségi határozat (40) preambulumbekezdését.
67 Lásd a megfelelőségi határozat (38) preambulumbekezdését.
68 https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

Végezetül érdemes megemlíteni, hogy az ODNI 2024 májusában megjelentette a Hírszerző Közösség kereskedelmileg elérhető információkra vonatkozó szakpolitikai keretét[69]. Ez a keret számos olyan elvet és követelményt határoz meg, amelyeket a hírszerző ügynökségeknek követniük kell, többek között a magánélet védelmével és a polgári szabadságjogokkal kapcsolatos kockázatok minimalizálása érdekében, amikor valamely kereskedelmi ügylettel összefüggésben információkat szereznek és használnak fel.

2.2.2. Független felügyelet

Az Egyesült Államok hírszerző ügynökségeinek tevékenységét különböző szervek felügyelik, ideértve a magánélet védelmével és a polgári szabadságjogokkal foglalkozó tisztviselőket, a főfelügyelőket, a Kongresszust és a PCLOB-t. Mindenekelőtt a 14086. sz. elnöki rendelet megköveteli, hogy minden hírszerző ügynökség rendelkezzen magas szintű jogi, felügyeleti és megfelelési tisztviselőkkel az alkalmazandó egyesült államokbeli jogszabályoknak való megfelelés biztosítása érdekében. Ezt a felügyeleti feladatot a kijelölt megfelelési szerepkörrel rendelkező tisztviselők, az adatvédelmi és polgári szabadságjogi tisztviselők, valamint a főellenőrök[70] töltik be. El kell látniuk a jelfelderítési tevékenységek rendszeres felügyeletét, és biztosítaniuk kell, hogy minden meg nem felelést orvosoljanak. A hírszerző ügynökségeknek felügyeleti feladataik ellátása érdekében biztosítaniuk kell az ilyen tisztviselők számára az összes releváns információhoz való hozzáférést, és nem tehetnek semmilyen intézkedést felügyeleti tevékenységük akadályozására vagy nem megfelelő befolyásolására.

A felülvizsgálati ülésen részt vett az ODNI keretében a Hírszerzési Közösség Főellenőri Hivatalának (ICIG) Főtanácsadói Hivatala, amely teljes hatáskörrel rendelkezik a Hírszerző Közösség egésze felett, és jogosult kivizsgálni a jogellenes magatartásra vagy a hatalommal való visszaélésre vonatkozó állításokkal kapcsolatos panaszokat vagy információkat. Megerősítette, hogy az ICIG a felügyeleti tevékenysége részeként rendszeresen ellenőrzi a 14086. sz. elnöki rendeletnek való megfelelést. Utalt továbbá a Hírszerzési Közösség más főellenőreinek közelmúltbeli felügyeleti tevékenységére, amelyet rendszeres jelentések részleteznek. Például a Kongresszusnak címzett, 2023. április–szeptemberi féléves jelentésében[71] az NSA főfelügyelője tájékoztatást adott az NSA célkiválasztási döntésekre és megkeresésekre vonatkozó belső ellenőrzési keretének értékeléséről. Megállapította, hogy ez a keret megfelelően működik annak érdekében, hogy biztosítsa a polgári szabadságjogok és a magánélet védelmét szolgáló törvényeknek, irányelveknek és politikáknak való megfelelést. Ugyanez a jelentés említést tesz egy olyan vizsgálatról is, amely feltárta, hogy az NSA egyik alkalmazottja jogosulatlan célokra használt egy jelfelderítési eszközt.

---

69 https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. A hírszerző ügynökségeknek 2024 augusztusa óta meg kell felelniük a keretnek.

70 Minden hírszerző ügynökségnek van egy, a törvény erejénél fogva független főellenőre, aki felelős az adott ügynökség által nemzetbiztonsági célból végzett tevékenységekkel kapcsolatos ellenőrzések és vizsgálatok lefolytatásáért. Hozzáférnek minden releváns (többek között minősített) anyaghoz, szükség esetén határozottal, és tanúvallomást vehetnek fel. A főellenőrök büntetőeljárást kezdeményeznek a feltételezett bűncselekmények esetében, és korrekciós intézkedésekre vonatkozó ajánlásokat tesznek az ügynökségek vezetőinek. Bár ajánlásaik nem kötelező erejűek, jelentéseiket – többek között a nyomonkövetési intézkedésekről (vagy azok hiányáról) szóló jelentéseket – általában nyilvánosságra hozzák és megküldik a Kongresszusnak. Lásd e tekintetben a megfelelőségi határozat 136. lábjegyzetét a főellenőr szerepéről.

71 https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

A 14086. sz. elnöki rendelet értelmében a PCLOB-t[72] konkrét felügyeleti feladatokkal bízták meg[73]. A PCLOB elnöke és három tagja részt vett a felülvizsgálati ülésen, és tájékoztatott arról, hogy a PCLOB 2023 áprilisában tanácsot adott a hírszerző ügynökségeknek a 14086. sz. elnöki rendeletet végrehajtó politikáik és eljárásaik tervezetével kapcsolatban, és részt vett az adatvédelmi felülvizsgálati bíróság (DPRC) bíráinak és különleges főtanácsnokainak kinevezéséről folytatott konzultációban. A PCLOB továbbá felügyeleti projektet indított annak érdekében, hogy 1) felülvizsgálja a hírszerző ügynökségek által elfogadott aktualizált politikák és eljárások végrehajtását az elnöki rendelettel való összhang biztosítása érdekében, és 2) évente felülvizsgálja az új jogorvoslati mechanizmus működését (lásd alább)[74]. A PCLOB tagjai megerősítették, hogy a PCLOB a közeljövőben mindkét felülvizsgálatot el kívánja végezni. A jogorvoslatot illetően kifejtették, hogy panasz hiányában a PCLOB felülvizsgálata a mechanizmus létrehozása érdekében bevezetett politikákra és eljárásokra fog összpontosítani.

Ami az egyéb felügyeleti tevékenységeket illeti, a PCLOB 2023. szeptember 28-án jelentést[75] adott ki a FISA 702. szakaszáról. Ez a jelentés egy korábbi, 2014. évi jelentés nyomon követése, és naprakész ténybeli és jogi információkat tartalmaz a FISA 702. szakasza szerinti megfigyelési programok működéséről. A jelentés emellett ajánlásokat tartalmaz az alkalmazandó követelményeknek való, hírszerző ügynökségek általi megfelelésről, valamint javaslatokat tesz a Kongresszusnak a FISA 702. szakasza több aspektusának további megerősítése érdekében az újbóli engedélyezéssel összefüggésben (többek között a 14086. sz. elnöki rendeletben felsorolt megfigyelési tevékenységeket alátámasztó jogszerű célkitűzések kodifikálásával)[76]. A felülvizsgálati ülésen a PCLOB arról tájékoztatott, hogy hamarosan választ vár a hírszerző ügynökségektől az ajánlásainak végrehajtásáról, és felhasználja ezeket a válaszokat a jövőbeli nyomonkövetési jelentéshez. Az egyéb folyamatban lévő felügyeleti projektek közé tartozik egy, a belföldi terrorizmus elleni küzdelemmel, valamint annak a magánéletre és a polgári szabadságjogokra gyakorolt hatásával, valamint egy, a nyílt forráskódú vagy kereskedelmi forgalomban elérhető adatok FBI általi gyűjtésével foglalkozó projekt[77].

Végezetül a felülvizsgálat keretében megkérdezett nem kormányzati szervezetek aggodalmukat fejezték ki azzal kapcsolatban, hogy a PCLOB több tagjának megbízatása a közeljövőben lejár, és így a PCLOB potenciálisan határozatképtelen lesz. Mindenekelőtt lejárt az elnök megbízatása, és 2025 januárjában lejár az az időszak, amely alatt még betöltheti

---

[72] A PCLOB független ügynökség amely a magánélet és a polgári szabadságjogok védelme érdekében hatáskörrel rendelkezik a terrorizmusellenes politikák és azok végrehajtása terén. Minden releváns (többek között minősített) információhoz hozzáférhet, kihallgatásokat végezhet, és tanúvallomásokat hallgathat meg. Ajánlásokat adhat a bűnüldöző és hírszerző hatóságoknak, és rendszeresen jelentést tesz a Kongresszusnak és az elnöknek. Jelentéseit a lehető legnagyobb mértékben nyilvánosan hozzáférhetővé teszi.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ac93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] A Bizottság megjegyzi, hogy ezen ajánlások közül néhányat beépítettek a RISAA-ba, többek között az említésalapú információgyűjtésre vonatkozó ajánlást és a FISC szakértői (amicus curiae) szerepének megerősítéséről szóló ajánlást.

[77] https://www.pclob.gov/OversightProjects.

pozícióját, egy másik hely betöltetlen, egy harmadik pedig a jövő év januárjában szintén meg fog üresedni. A felülvizsgálati ülésen a tagok kifejtették, hogy nem számítanak a PCLOB határozatképtelenségére, mivel a jelenleg betöltetlen (és a Szenátus általi megerősítésre váró) hely esetében már megtörtént a jelölés[78]. Hangsúlyozták továbbá, hogy még ha a PCLOB el is veszítené határozatképességét, ez nem befolyásolná a felügyeleti projektek végrehajtásának folytatására vonatkozó képességét. Tekintettel azonban arra, hogy a PCLOB fontos szerepet tölt be a 14086. sz. elnöki rendelet végrehajtásának felülvizsgálatában, a Bizottság szorosan nyomon fogja követni a jövőbeli betöltetlen álláshelyek és a jelölések/kinevezések helyzetét.

2.2.3. Jogorvoslat

A 14086. sz. elnöki rendelet, amelyet főügyészi rendelet egészít ki, új jogorvoslati mechanizmust hozott létre a magánszemélyektől érkező, az Egyesült Államok jelfelderítési tevékenységével kapcsolatos minősített panaszok kezelésére és megoldására[79]. Az EU-ban bármely magánszemély jogosult panaszt benyújtani a jogorvoslati mechanizmushoz a jelfelderítési tevékenységekre vonatkozó egyesült államokbeli jogszabályok (pl. a 14086. sz. elnöki rendelet, a FISA 702. szakasza, a 12333. sz. elnöki rendelet) olyan állítólagos megsértése miatt az Egyesült Államokba továbbított személyes adatok tekintetében, amelyek hátrányosan érintik a magánélethez és a polgári szabadságjogokhoz fűződő érdekeit. A magánszemélyek panaszt nyújthatnak be valamely uniós tagállam adatvédelmi hatóságánál, amely az Európai Adatvédelmi Testület titkárságán keresztül továbbítja a panaszt a jogorvoslati mechanizmushoz. A mechanizmus két rétegből áll: a panaszoknak az ODNI CLPO által végzett kezdeti kivizsgálásából, valamint annak lehetőségéből, hogy a magánszemélyek fellebbezhessenek a CLPO határozatával szemben egy független DPRC előtt. Az ODNI CLPO vagy a DPRC általi felülvizsgálat befejezését követően a nemzeti hatóságon keresztül tájékoztatják a magánszemélyeket, hogy „a felülvizsgálat vagy nem állapította meg az érintett jogsértéseket, vagy az ODNI CLPO/a DPRC megfelelő kárenyhítést előíró határozatot hozott”. Az ODNI CLPO és a DPRC határozatai kötelező erejűek a hírszerző ügynökségekre nézve.

A megfelelőségi határozat elfogadása óta további lépések történtek a jogorvoslati mechanizmus teljes körű működőképessé tétele érdekében.

Ami a DPRC létrehozását illeti, 2023. november 14-én nyolc bírót neveztek ki a bíróságra (azaz kettővel többet, mint amit a főügyész rendeletei által – a Szövetségi Rendeletek Kódexe 28. címe 201.3 szakaszának (a) pontjában – kiegészített, 14086. sz. elnöki rendelet minimális létszámként előír)[80]. Kinevezésükre a 14086. sz. elnöki rendeletben meghatározott kritériumok alapján és az abban meghatározott eljárással összhangban került sor, többek között a PCLOB-bal folytatott konzultációt követően[81]. A Szövetségi Kerületi Bíróság és a Fellebbviteli Bíróság korábbi bírái, az Egyesült Államok egy korábbi főügyésze és a PCLOB egy korábbi tagja tartoznak e nyolc bíró közé. Az elnöki rendelet előírásainak megfelelően a bírák legalább fele rendelkezik korábbi bírói tapasztalattal. Ezen túlmenően 2024 áprilisában két különleges főtanácsnokot – a magánélet védelme és a nemzetbiztonság területén egyaránt szakértelemmel rendelkező jogi szakembereket – neveztek ki a magánszemélyek érdekeinek DPRC előtti képviseletére. A felülvizsgálati ülésen megerősítést nyert, hogy valamennyi bíró és különleges

78 https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.

79 A megfelelőségi határozat (176)–(194) preambulumbekezdése.

80 https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.

81 A 14086. sz. elnöki rendelet 3. szakasza (d) pontjának (A) szakasza.

főtanácsnok esetében sor került a legmagasabb szintű biztonsági átvilágításra, és így a DPRC-vel kapcsolatos feladataik ellátása során hozzáférhetnek a minősített anyagokhoz. A DPRC egy sor gyakran ismételt kérdést is közzétett, amelyek további információkkal szolgálnak a szerepéről, függetlenségéről és működéséről[82].

Ami a panaszok kezelését illeti, az ODNI 2022. december 6-án elfogadta a Hírszerző Közösségről szóló 126. irányelvet, amely részletesen szabályozza (határidők kitűzésével, biztonságos elektronikus adattár és kommunikációs csatornák létrehozásával, annak előírásával, hogy a CLPO-nak és a Hírszerző Közösségnek a jogorvoslati mechanizmus éves felülvizsgálatával összefüggésben együtt kell működnie a PCLOB-bal stb.) a panaszok kivizsgálásával és elbírálásával kapcsolatos eljárás különböző szempontjait[83]. Ez az irányelv az Egyesült Államok Hírszerzési Közösségének egészében alkalmazandó, és az egyes hírszerző ügynökségek által a panaszok kezelésével összefüggésben az ODNI CLPO-val való együttműködésükre vonatkozóan elfogadott további belső eljárások egészítik ki (pl. a panaszok és az azokra válaszoló dokumentumok megosztására szolgáló biztonságos adattár fejlesztése, valamint az érintett ügynökségek közötti biztonságos kommunikáció). Az elkövetkező hónapokban a DPRC is részletesebb szabályokat fog kiadni a panaszok kezelésére és más eljárási szempontokra vonatkozóan.

Az Európai Unióban és az Egyesült Államokban számos további intézkedést hoztak a lakosság tájékoztatására, valamint a panaszok benyújtásának és kezelésének megkönnyítésére. Ezek közé tartozik az új jogorvoslati mechanizmusról szóló tájékoztató feljegyzés Európai Adatvédelmi Testület általi elfogadása[84], egy panasznyomtatvány mintája (amelyet valamennyi adatvédelmi hatóság lefordít és közzétesz a nemzeti nyelvein)[85], valamint a nemzeti felügyeleti hatóságok és az Európai Adatvédelmi Testület titkársága közötti együttműködést szabályozó eljárási szabályzat[86]. Hasonlóképpen, az ODNI közzétette a gyakran ismételt kérdéseket és az új jogorvoslati mechanizmusról szóló tájékoztatót, valamint figyelemfelhívó tevékenységeket folytatott[87].

Emellett az elmúlt évben az Európai Adatvédelmi Testület és az érintett amerikai hatóságok szorosan együttműködtek számos operatív kérdésben. Mindenekelőtt – amint azt a felülvizsgálati ülésen megerősítették – titkosított kommunikációs csatornát hoztak létre a panaszok továbbítására az uniós nemzeti hatóságoktól az Európai Adatvédelmi Testület titkárságához, az Európai Adatvédelmi Testület titkárságától az ODNI CLPO-hoz, illetve az Igazságügyi Minisztérium adatvédelmi és polgári szabadságjogi hivatalához (OPCL), valamint az ODNI CLPO és az Egyesült Államok más hatóságai (pl. a DPRC) között. Emellett az ODNI CLPO kifejtette, hogy további belső eljárásokat vezettek be az egyes hírszerző ügynökségeknek az ODNI CLPO-val való együttműködése tekintetében a panaszok kezelésével összefüggésben.

---

82 https://www.justice.gov/opcl/dprc-resources.

83 https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

84 https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_hu.

85 https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_hu.

86 https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_hu.

87 https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf és https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

Végezetül az OPCL, amely adminisztratív támogatást nyújt a DPRC-nek, arról is tájékoztatott, hogy a DPRC-nek saját költségvetési sort biztosítottak, és rendelkezik a feladatai ellátásához szükséges eszközökkel, beleértve a biztonságos számítógépeket és laptopokat, telefonokat stb. Ezenkívül a 14086. sz. elnöki rendelet előírásainak megfelelően a Kereskedelmi Minisztérium megtette a szükséges intézkedéseket – többek között titkosított kommunikációs csatornát hozott létre az ODNI CLPO-val – annak érdekében, hogy nyilvántartást vezessen valamennyi beérkezett minősített panaszról. A Kereskedelmi Minisztérium rendszeresen felveszi a kapcsolatot az ODNI CLPO-val azzal kapcsolatban, hogy feloldották-e az egyéni panaszokkal kapcsolatos információk minősítését. Amennyiben igen, a Kereskedelmi Minisztérium értesíti erről az érintett magánszemélyt, lehetővé téve számára az ilyen információkhoz való hozzáférést.

A felülvizsgálati ülés időpontjáig az uniós felügyeleti hatóságokhoz nem érkezett panasz, ezért az új jogorvoslati mechanizmust még nem aktiválták.

3. KÖVETKEZTETÉS

Az ezen első felülvizsgálat során gyűjtött információk alapján a Bizottság megállapítja, hogy az Egyesült Államok hatóságai bevezették az adatvédelmi keret hatékony működésének biztosításához szükséges struktúrákat és eljárásokat. Ebben az összefüggésben a Bizottság nagyon nagyra értékeli az Egyesült Államok hatóságaival a felülvizsgálat lefolytatása terén folytatott rendkívül jó együttműködést.

Bár ez az első felülvizsgálat természetesen annak ellenőrzésére összpontosított, hogy a keret valamennyi alkotóeleme be lett-e vezetve, a tanúsított vállalatok általi adatfeldolgozásra és a hatóságok adatokhoz való hozzáférésére egyaránt alkalmazandó biztosítékok gyakorlati alkalmazásával kapcsolatos tapasztalatok mindössze egy év működést követően szükségszerűen korlátozottak. A Bizottság ezért az elkövetkező hónapokban és években szorosan nyomon fogja követni a releváns fejleményeket, különös figyelmet fordítva 1) a PCLOB soron következő jelentéseire a 14086. sz. elnöki rendelet végrehajtásáról és a jelfelderítési jogorvoslati mechanizmus, különösen a DPRC működéséről, 2) a FISA 702. szakaszának esetleges további módosításaira, valamint 3) a PCLOB tagjainak a soron következő megüresedő álláshelyek betöltését célzó jelölésére és kinevezésére.

Emellett a folyamatos és hatékony működés biztosítása érdekében a Bizottság fontosnak tartja, hogy:

- amint azt a felülvizsgálati ülésen bejelentették, a Kereskedelmi Minisztérium jobban kihasználja az adatvédelmi keretben biztosított különböző eszközöket egyrészt annak nyomon követésére, hogy a vállalatok betartják-e az elveket, másrészt a részvételre vonatkozó hamis állítások felderítésére,
- az FTC továbbfejlessze proaktív megközelítését annak vizsgálata és érvényesítése tekintetében, hogy a tanúsított vállalatok megfelelnek-e az adatvédelmi keret elveinek, valamint
- a Kereskedelmi Minisztérium, az FTC és az uniós adatvédelmi hatóságok közös iránymutató eszközöket dolgozzanak ki az adatvédelmi keret elvei szerinti

kulcsfontosságú követelményekről, például a HR-adatokról és az újbóli adattovábbításról.

A felülvizsgálat eredményének fényében és a megfelelőségi határozat (211) preambulumbekezdésében foglaltak szerint a Bizottság helyénvalónak tartja, hogy a következő időszakos felülvizsgálatra három év elteltével kerüljön sor. Ez lehetővé tenné, hogy több tapasztalatot szerezzenek az adatvédelmi keret gyakorlati alkalmazásával kapcsolatban, és figyelembe venné a fent említett jövőbeli fejleményeket. A Bizottság ezért a megfelelőségi határozat 3. cikkének (4) bekezdésével összhangban konzultálni fog a jövőbeli felülvizsgálatok rendszerességéről az Európai Adatvédelmi Testülettel és az általános adatvédelmi rendelet 93. cikkének (1) bekezdése alapján létrehozott bizottsággal.