A Testület véleménye (64. cikk)

27/2024. sz. vélemény a Brand Compliance tanúsítási szempontokról a Testület által az általános adatvédelmi rendelet 42. cikkének (5) bekezdése szerint európai adatvédelmi bélyegző formájában történő jóváhagyásuk tekintetében

Elfogadás időpontja: 2024. december 2.

TARTALOMJEGYZÉK

Az Európai Adatvédelmi Testület

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: „általános adatvédelmi rendelet") 63. cikkére, 64. cikkének (2) bekezdésre és 42. cikkére,

tekintettel az Európai Gazdasági Térségről (a továbbiakban: „EGT") szóló megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával[1] módosított XI. mellékletére és 37. jegyzőkönyvére,

tekintettel eljárási szabályzata 10. és 22. cikkére,

(1) A tagállamok, a felügyeleti hatóságok, az Európai Adatvédelmi Testület (a továbbiakban: a „Testület"), valamint a Bizottság – különösen uniós szinten – ösztönzik olyan adatvédelmi tanúsítási mechanizmusok (a továbbiakban: tanúsítási mechanizmusok), valamint adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek az általános adatvédelmi rendelet előírásainak, figyelembe véve a mikro-, kis- és középvállalkozások sajátos igényeit.[2] Ezenfelül a tanúsítási mechanizmusok létrehozása elősegítheti az átláthatóságot és lehetővé teszi az érintettek számára, hogy értékeljék az adott termékek és szolgáltatások adatvédelmi szintjét.[3]

(2) A tanúsítási szempontok a tanúsítási mechanizmus szerves részét képezik. Következésképpen az általános adatvédelmi rendelet előírja, hogy a nemzeti tanúsítási mechanizmus szempontjait az illetékes felügyeleti hatóságnak (az általános adatvédelmi rendelet 42. cikkének (5) bekezdése és 43. cikke (2) bekezdésének b) pontja), illetve európai adatvédelmi bélyegző esetében az Európai Adatvédelmi Testületnek (az általános adatvédelmi rendelet 42. cikkének (5) bekezdése és 70. cikke (1) bekezdésének o) pontja) jóvá kell hagynia.

(3) Amennyiben valamely felügyeleti hatóság az általános adatvédelmi rendelet 42. cikkének (5) bekezdése alapján európai adatvédelmi bélyegzőnek az Európai Adatvédelmi Testület általi jóváhagyását kívánja javasolni, a felügyeleti hatóságnak jeleznie kell a rendszer tulajdonosának azon szándékát, hogy valamennyi tagállamban felkínálja a tanúsítási mechanizmust. Ebben az esetben az Európai Adatvédelmi Testület fő feladata az általános adatvédelmi rendelet következetes alkalmazásának biztosítása az általános adatvédelmi rendelet 63., 64. és 65. cikkében említett egységességi mechanizmus révén. Ennek keretében az általános adatvédelmi rendelet 64. cikkének (2) bekezdése szerint az Európai Adatvédelmi Testület jóváhagyja a tanúsítási szempontokat.

(4) E vélemény célja az általános adatvédelmi rendelet következetes alkalmazásának biztosítása, többek között a felügyeleti hatóságok, az adatkezelők és az adatfeldolgozók által, figyelembe véve azokat az alapvető elemeket, amelyeket a tanúsítási mechanizmusoknak ki kell dolgozniuk. Az Európai Adatvédelmi Testület értékelése különösen „a rendelet 42. és 43 cikkével összhangban történő

[1] A jelen véleményben a „tagállamokra" történő bármely hivatkozást egyben az „EGT-tagállamokra" történő hivatkozásként kell érteni.

[2] Az általános adatvédelmi rendelet 42. cikkének (1) bekezdése.

[3] Az általános adatvédelmi rendelet (100) preambulumbekezdése.

tanúsításról és a tanúsítási szempontok meghatározásáról szóló 1/2018. számú iránymutatás” (a továbbiakban: „iránymutatás”) és annak Függeléke„a tanúsítási szempontok értékeléséről szóló útmutatás” (a továbbiakban: „Függelék”) alapján történik.

(5) Ennek megfelelően az Európai Adatvédelmi Testület elismeri, hogy minden egyes tanúsítási mechanizmussal külön kell foglalkozni, és az nem érinti a többi tanúsítási mechanizmus értékelését.

(6) A tanúsítási mechanizmus lehetővé teszi az adatkezelők és adatfeldolgozók számára, hogy bizonyítsák az általános adatvédelmi rendeletnek való megfelelőségüket. Ezért a szempontoknak megfelelően tükrözniük kell a személyes adatok védelmére vonatkozóan az általános adatvédelmi rendeletben meghatározott követelményeket és elveket, és hozzá kell járulniuk e rendelet következetes alkalmazásához.

(7) Ugyanakkor a rendszer tulajdonosának biztosítania kell a tanúsítási mechanizmusnak a belefoglalt vagy alkalmazott ISO-szabványokkal és tanúsítási gyakorlatokkal való összhangját és az azoknak való megfelelést.

(8) Ennek eredményeként a tanúsítványoknak hozzáadott értéket kell teremteniük az adatkezelők és az adatfeldolgozók számára azáltal, hogy hozzájárulnak olyan szabványosított és meghatározott szervezeti és technikai intézkedések végrehajtásához, amelyek bizonyíthatóan megkönnyítik és javítják az adatkezelési műveletek általános adatvédelmi rendeletnek való megfelelését, figyelembe véve az ágazat specifikus követelményeket.

(9) Az Európai Adatvédelmi Testület üdvözli a rendszertulajdonosok arra irányuló erőfeszítéseit, hogy olyan tanúsítási mechanizmusokat dolgozzanak ki, amelyek gyakorlatias és potenciálisan költséghatékony eszközök az általános adatvédelmi rendelettel való nagyobb összhang biztosítása, valamint az érintettek magánélethez és adatvédelemhez való jogának az átláthatóság növelése révén történő előmozdítása érdekében.

(10) Az Európai Adatvédelmi Testület emlékeztet arra, hogy a tanúsítványok önkéntes elszámoltathatósági eszközök, és hogy a tanúsítási mechanizmushoz való csatlakozás nem csökkenti az adatkezelőknek vagy az adatfeldolgozóknak az általános adatvédelmi rendeletnek való megfeleléssel kapcsolatos felelősségét, és nem akadályozza meg a felügyeleti hatóságokat abban, hogy ellássák, illetve gyakorolják az általános adatvédelmi rendelet és a vonatkozó nemzeti jogszabályok szerinti feladataikat és hatásköreiket.

(11) Ebben a véleményben az Európai Adatvédelmi Testület olyan kérdésekkel foglalkozik, mint a szempontok hatálya, a szempontok alkalmazhatósága és relevanciája valamennyi tagállamban.

(12) Ez a vélemény a tanúsítási szempontokra összpontosít. Amennyiben az Európai Adatvédelmi Testület magas szintű tájékoztatást kér az értékelési módszerekről annak érdekében, hogy az erről szóló véleményével összefüggésben alaposan értékelni tudja a szempontok ellenőrizhetőségét, ez utóbbi nem jelenti az ilyen értékelési módszerek jóváhagyását.

(13) Az Európai Adatvédelmi Testület a véleményét az általános adatvédelmi rendelet – a Testület eljárási szabályzata 10. cikkének (2) bekezdésével összefüggésben értelmezett – 64. cikkének (2) bekezdése alapján az azt követő munkanaptól számított nyolc héten belül fogadja el, hogy az elnök és az illetékes felügyeleti hatóságok úgy határoztak, hogy a dokumentáció hiánytalan. Az ügy összetettségére figyelemmel ez a határidő az elnök határozatával további hat héttel meghosszabbítható. Ha az Európai Adatvédelmi Testület véleményében arra a következtetésre jut, hogy a szempontok nem hagyhatók jóvá, a felügyeleti hatóság újból benyújthatja a szempontokat jóváhagyásra, amennyiben az Európai Adatvédelmi Testület eredeti véleményében megfogalmazott aggályokat kezelik.

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

1 A TÉNYÁLLÁS RÖVID ISMERTETÉSE

1. A GDPR 42. cikkének (5) bekezdésével és az iránymutatásokkal összhangban a „GDPR Certification Standard and Criteria, BC 5701:2024, Version 0.7” (a továbbiakban: „tanúsítási szempontok tervezete”, „tanúsítási szempontok” vagy „kritériumok”) tervezetét a Brand Compliance B.V., egy hollandiai jogi személy (a továbbiakban: „a rendszer tulajdonosa”) dolgozta ki, és nyújtotta be az Autoriteit Persoonsgegevens-nek, az illetékes holland felügyeleti hatóságnak (a továbbiakban: „NL SA”).

2. Hollandia felügyeleti hatósága 2024. szeptember 26-án benyújtotta a tanúsítási szempontok tervezetét az Európai Adatvédelmi Testületnek az általános adatvédelmi rendelet 64. cikkének (2) bekezdése szerinti jóváhagyásra. A dokumentáció hiánytalanságáról szóló határozat meghozatalára 2024. november 12-én került sor.

3. A Brand Compliance tanúsítási mechanizmus nem az általános adatvédelmi rendelet 46. cikke (2) bekezdésének f) pontja szerinti, a személyes adatok nemzetközi továbbítására vonatkozó tanúsítvány, és ezért nem nyújt megfelelő garanciákat a személyes adatoknak a 46. cikk (2) bekezdésének f) pontjában említett feltételek szerinti, harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása keretében. A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására ugyanis csak az általános adatvédelmi rendelet V. fejezetében foglalt rendelkezések tiszteletben tartásával kerülhet sor.

2 ÉRTÉKELÉS

4. Az Európai Adatvédelmi Testület az iránymutatás 2. mellékletében (a továbbiakban: „melléklet”) és annak kiegészítésében előirányzott struktúrával összhangban végezte el a tanúsítási szempontok értékelését az általános adatvédelmi rendelet 42. cikkének (5) bekezdése szerinti jóváhagyásukhoz.

2.1 A tanúsítási mechanizmus hatálya és az értékelés célja (ToE)

5. A Brand Compliance tanúsítási mechanizmus az Európai Unióban (EU) vagy az Európai Gazdasági Térségben (EGT) letelepedett adatkezelők vagy adatfeldolgozók által személyes adatokon végzett adatkezelési műveletek tanúsítására vonatkozó tanúsítási szempontokat tartalmaz.

6. E tanúsítási mechanizmus fő kritériumai hat követelménycsoportra oszlanak, nevezetesen a következőkre: Az adatkezelés háttere, beleértve a vonatkozó uniós vagy tagállami jognak való megfelelést (1. csoport), Szervezeti keretfeltételek (2. csoport), Az adatkezelési tevékenységek alapjai, beleértve a személyes adatok kezelésére vonatkozó elveket (3. csoport), Technikai és szervezeti védelem (4. csoport), Műveleti végrehajtás, beleértve az érintettek jogait (5. csoport), és Irányítási rendszer (6. csoport).

7. E rendszer keretében a tanúsítást kérelmezőknek adatkezelőknek vagy adatfeldolgozóknak kell lenniük. Ide tartoznak azok az adatfeldolgozók is, akiket az általános adatvédelmi rendelet 4. cikkének (7) bekezdése értelmében az adott adatkezelő közvetlenül bíz meg személyes adatok kezelésével,

valamint al-adatfeldolgozók is. A (részben) al-adatfeldolgozásként végzett feldolgozási műveleteket az adatfeldolgozó szervezeti kapacitásának keretében tanúsítják.

8. A Testület megjegyzi, hogy a tanúsítási mechanizmus nem használható olyan adatkezelési műveletek tanúsítására, amelyek esetében két vagy több adatkezelő közösen határozza meg a célokat és az eszközöket a GDPR 26. cikkének (1) bekezdése szerint (közös adatkezelők). A tanúsítási mechanizmus nem használható az EU-n vagy az EGT-n kívül található szervezetek által végzett adatkezelési műveletek tanúsítására. Ezen túlmenően a tanúsítási mechanizmus nem használható a GDPR 42. cikkének (2) bekezdése és 46. cikke (2) bekezdésének f) pontja értelmében vett adattovábbítási eszközként.

2.2 Adatkezelési műveletek

9. A tanúsítási mechanizmus a személyes adatok kezelésére a szervezet típusától és méretétől függetlenül, valamint az általa nyújtott termékek vagy szolgáltatások jellegétől függetlenül alkalmazható. Ezért a tanúsítási mechanizmus hatálya nem korlátozódik bizonyos típusú adatkezelési műveletekre, és lehetővé teszi az adatkezelő vagy a feldolgozó által végzett bármely adatkezelési művelet tanúsítását. Ennek következtében alapvető fontosságú, hogy a módszertani követelményeket betartsák, mivel csak így biztosítható a tanúsítási szempontok egységes alkalmazása és a különböző tanúsítási eljárásokban a vizsgálatok összehasonlítható szintje. A cél a kiadott tanúsítványok és eredményeik összehasonlíthatóságának és reprodukálhatóságának biztosítása.

2.3 Az adatkezelés jogszerűsége

10. A tanúsítási szempontok előírják annak vizsgálatát, hogy az adatkezelő adatkezelési műveletei megfelelnek-e az általános adatvédelmi rendelet 6. cikke (a tanúsítási szempontok 6.1.2. szakasza) és adott esetben a 9. cikke (a tanúsítási szempontok 6.1.2. szakaszának h) pontja), valamint a 10. cikke (a tanúsítási szempontok 6.1.2. szakaszának i) pontja) rendelkezéseinek. Bár az adatkezelés jogszerűsége elvének tiszteletben tartása az adatkezelő kötelezettsége, az adatfeldolgozónak továbbra is be kell tartania az ezzel kapcsolatos különleges követelményeket (a tanúsítási szempontok 6.2. szakasza). Ezek a követelmények különösen annak biztosítására irányulnak, hogy az adatkezelésre vonatkozó felhatalmazás jogszerűen származzon az adatkezelőtől, és hogy az adatfeldolgozó támogassa az adatkezelőt a GDPR betartásában, beleértve a jogszerűség elvét is.

2.4 Az adatkezelésre vonatkozó alapelvek

11. A tanúsítási szempontok konkrét követelményeket állapítanak meg az általános adatvédelmi rendelet 5. cikke értelmében vett adatkezeléssel kapcsolatos valamennyi alapelv értékelésére vonatkozóan (a tanúsítási szempontok 6. szakasza). Ami az adatfeldolgozókra vonatkozó követelményeket illeti, ebben az összefüggésben külön tanúsítási szempontokat kell értékelni (a tanúsítási szempontok 6.2. szakasza). Amint azt korábban említettük, az adatfeldolgozókra vonatkozó követelmények elsődleges célja, hogy támogassák az adatkezelőt az alapelveknek való megfelelés végrehajtásában.

2.5 Az adatkezelők és az adatfeldolgozók általános kötelezettségei

12. A tanúsítási szempontok tükrözik az adatkezelők és az adatfeldolgozók közötti kapcsolatot. A tanúsítási szempontok különösen arra kötelezik az adatkezelőket és az adatfeldolgozókat, hogy feleljenek meg az adatkezelési tevékenységek kiszervezésével kapcsolatos követelményeknek, amely többek között magában foglalja az általános adatvédelmi rendelet 28. cikkének (3) bekezdésében

foglalt rendelkezések betartását (a tanúsítási szempontok 8.5. szakasza). Amennyiben adatfeldolgozókról van szó, azoknak meg kell felelniük az adatkezelő felügyelete alatt történő adatkezelésre vonatkozó konkrét követelményeknek is (a tanúsítási szempontok 8.6. szakasza). Emellett további követelményeket állapítanak meg az al-feldolgozás körülményeinek figyelembevétele érdekében (a tanúsítási szempontok 6.2.e. szakasza és különösen 8.6. g. szakasza).

13. A szempontok az általános adatvédelmi rendelet 30. cikkével összhangban ellenőrzik az adatkezelési tevékenységek nyilvántartásának tartalmát (a tanúsítási szempontok 5.4 szakasza). Ebben az összefüggésben az általános adatvédelmi rendelet 30. cikkének (1) és (2) bekezdésével összhangban különbséget kell tenni az adatkezelők és az adatfeldolgozók adatkezelési tevékenységeire vonatkozó nyilvántartás kötelező tartalma között.

14. A tanúsítási szempontok előírják, hogy a kérelmezőknek az általános adatvédelmi rendelet 37. cikkével összhangban adatvédelmi tisztviselőt kell kinevezniük. A tanúsítási szempontok biztosítják továbbá, hogy az általános adatvédelmi rendelet 37–39. cikke szerinti követelmények teljesüljenek (a tanúsítási szempontok 5.3.2. szakasza).

15. Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése és 24. cikke szerinti elszámoltathatóság alapelvével kapcsolatban követelményeket állapítanak meg az adatvédelmi és jelentéstételi mechanizmusok megszervezésére (a tanúsítási szempontok 5.1. és 5.3. szakasza), valamint az adatvédelmi politikák végrehajtására (a tanúsítási szempontok 5.2. szakasza) vonatkozóan.

2.6 Az érintettek jogai

16. A tanúsítási szempontok az általános adatvédelmi rendelet III. fejezetével összhangban megfelelő követelményeket határoznak meg az érintettek jogaira vonatkozóan. Először az átlátható tájékoztatásra, a kommunikációra és az érintettek jogainak gyakorlásának módjaira vonatkozó követelményekkel foglalkoznak, majd ezt követi a vonatkozó érintetti jogok részletes vizsgálata (a tanúsítási szempontok 8.4. szakasza). Ami az adatfeldolgozókra vonatkozó követelményeket illeti, a segítségnyújtási kötelezettségekre vonatkozóan külön rendelkezések kerülnek meghatározásra (a tanúsítási szempontok 8.4.11. szakasza).

2.7 A jogokat és szabadságokat érintő kockázatok

17. A szempontok előírják, hogy az adatkezelőnek tisztában kell lennie az értékelés célját képező adatkezelés tekintetében a természetes személyek jogait és szabadságait érintő lehetséges kockázatokkal. Ha a személyes adatok kezelése valószínűleg magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, több tanúsítási szempont biztosítja, hogy a kérelmező bizonyítsa, hogy a GDPR 35. cikkében foglalt követelmények teljesülnek (a tanúsítási szempontok 7.3. szakasza). Emellett konkrét követelményeket is előírnak az adatfeldolgozóknak az általános adatvédelmi rendelet 35. cikke szerinti segítségnyújtási kötelezettségeire vonatkozóan.

2.8 Védelmet garantáló technikai és szervezési intézkedések

18. A tanúsítási szempontok előírják a kezelt személyes adatok bizalmas jellegét, integritását és pontosságát, valamint az adatkezelési rendszer ellenálló képességét biztosító információbiztonsági szabványon alapuló technikai és szervezeti intézkedések alkalmazását. A tanúsítási szempontok az általános adatvédelmi rendelet 25. cikkével összhangban előírják a beépített és alapértelmezett

adatvédelem megvalósítását célzó intézkedések alkalmazását is (a tanúsítási szempontok 7.4. szakasza). A tanúsítási szempontok az általános adatvédelmi rendelet 33. és 34. cikkével összhangban konkrét követelményeket határoznak meg az adatkezelők számára az adatvédelmi incidens felügyeleti hatóság részére történő bejelentésének értékelése, valamint szükség esetén az adatvédelmi incidensről az érintett tájékoztatása tekintetében (a tanúsítási szempontok 8.8. szakasza). Ebben az összefüggésben az adatfeldolgozókra vonatkozó konkrét kötelezettségek is meghatározásra kerültek, különösen az adatvédelmi incidens azonosítását és az adatkezelővel való kommunikációt illetően (a tanúsítási szempontok 8.8.1. és 8.8.4. szakasza).

2.9 A személyes adatok továbbításával kapcsolatos megfelelő biztosítékok meglétét igazoló szempontok

19. A szempontok előírják a személyes adatok harmadik országokba és nemzetközi szervezetek részére történő, az értékelés célját képező valamennyi továbbításának azonosítását, valamint az általános adatvédelmi rendelet V. fejezete szerinti megfelelő garanciákat nyújtó adattovábbítási mechanizmussal kapcsolatos döntés alátámasztását (a tanúsítási szempontok 8.7 szakasza). A tanúsítási szempontok eljárást írnak elő a tervezett adattovábbítások értékelésére, például azok jogszerűségének ellenőrzésére.

3 AZ EURÓPAI ADATVÉDELMI BÉLYEGZŐVEL KAPCSOLATOS TOVÁBBI SZEMPONTOK

20. Az iránymutatás szerint az értékelésnek ki kell terjednie arra a kérdésre is, hogy „a szempontok alkalmasak-e arra, hogy figyelembe vegyék az egyes tagállamok adatvédelmi jogszabályait vagy forgatókönyveit”. A tanúsítási szempontok 4.3 szakasza előírja, hogy a kérelmezőnek meg kell felelnie az alkalmazandó nemzeti és vonatkozó ágazat specifikus adatvédelmi jogszabályoknak. A szervezetnek megfelelően és átfogóan azonosítania, elemeznie és dokumentálnia kell a személyes adatoknak az értékelés cél keretében történő kezelésére alkalmazandó vonatkozó tagállami vagy ágazat specifikus jogszabályokat és rendelkezéseket. A dokumentációban azonosítani kell az értékelés célja szempontjából releváns nemzeti vagy ágazat specifikus jogi keret kidolgozásáért felelős személy(eke)t és jogi szakértelmüket. A Testület továbbá tudomásul veszi, hogy e jogi keret azonosításának és kidolgozásának megfelelőségét a tanúsító szervezet határozza meg.

4 KÖVETKEZTETÉSEK / AJÁNLÁSOK

21. Következtetésként az Európai Adatvédelmi Testület úgy véli, hogy a Brand Compliance tanúsítási szempontok összhangban vannak az általános adatvédelmi rendelettel, és azokat a Testületnek az általános adatvédelmi rendelet 70. cikke (1) bekezdésének o) pontjában meghatározott feladata alapján jóváhagyja, aminek eredményeképpen közös tanúsítvány (európai adatvédelmi pecsét) állítható ki.

22. Az Európai Adatvédelmi Testület a 42. cikk (8) bekezdése szerint bejegyzi a „GDPR Certification Standard and Criteria, BC 5701:2024, Version 0.7” tanúsítási mechanizmust a tanúsítási mechanizmusok, illetve adatvédelmi bélyegzők és jelölések nyilvános nyilvántartásába.

5 ZÁRÓ MEGJEGYZÉSEK

23. Ennek a véleménynek a holland felügyeleti hatóság a címzettje, és a véleményt az általános adatvédelmi rendelet 64. cikke (5) bekezdésének b) pontja alapján nyilvánosságra hozták.

Az Európai Adatvédelmi Testület nevében

az elnök
Anu Talus