1/2018. számú iránymutatás a rendelet 42. és 43 cikkével összhangban történő tanúsításról és a tanúsítási szempontok meghatározásáról

3.0. változat

2019. június 4.

Elfogadva

Korábbi változatok

3.0. változat	2019. június 4.	A 2. melléklet belefoglalása a dokumentumba (a 2. melléklet 2.0 változatát a nyilvános konzultációt követően 2019. június 4-én fogadták el)
2.1. változat	2019. április 9.	Az iránymutatás helyesbítésének elfogadása (45. bekezdés)
2.0. változat	2019. január 23.	Az iránymutatás elfogadása a nyilvános konzultációt követően – Ugyanebben az időpontban elfogadták a 2. mellékletet (1.0 változat) nyilvános konzultációra
1.0. változat	2018. május 25.	Az iránymutatás elfogadása nyilvános konzultációra

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 irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet 70. cikke (1) bekezdésének e) pontjára,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére,

tekintettel a Testület 2018. május 25-i eljárási szabályzatának 12. és 22. cikkére,

figyelembe véve az iránymutatásról szóló, 2018. május 30. és 2018. július 12. közötti, valamint a 2. mellékletről szóló 2019. február 15. és március 29. közötti nyilvános konzultáció eredményét az általános adatvédelmi rendelet 70. cikke (4) bekezdésének megfelelően,

ELFOGADTA A KÖVETKEZŐ IRÁNYMUTATÁST.

1 BEVEZETÉS

1. Az általános adatvédelmi rendelet ((EU) 2016/679 rendelet) biztosítja az európai adatvédelem korszerűsített elszámoltathatósági és alapjogi megfelelési keretét. Az általános adatvédelmi rendelet rendelkezéseinek való megfelelést elősegítő intézkedések ezen új keretrendszer központi elemét képezik. Az intézkedések között szerepelnek konkrét körülményekre vonatkozó kötelező követelmények (többek között adatvédelmi tisztviselők kinevezése és adatvédelmi hatásvizsgálatok elvégzése) és önkéntes intézkedések, például magatartási kódexek és tanúsítási mechanizmusok.

2. Az általános adatvédelmi rendelet elfogadását megelőzően a 29. cikk alapján létrehozott munkacsoport kimondta, hogy a tanúsítás az adatvédelmi elszámoltathatósági keret fontos eleme lehet.1 Egyértelmű szabályokat kell meghatározni a tanúsításra vonatkozó követelmények tekintetében, hogy a tanúsítvány megbízhatóan tanúsítsa az adatvédelmi szabályozásnak történő megfelelést.2 Az általános adatvédelmi rendelet 42. cikke jogalapot biztosít az ilyen szabályok kidolgozásához.

3. Az általános adatvédelmi rendelet 42. cikkének (1) bekezdése a következőképpen rendelkezik:

   „A tagállamok, a felügyeleti hatóságok, a[z Európai Adatvédelmi] Testület, valamint a Bizottság – különösen uniós szinten – ösztönzik olyan adatvédelmi tanúsítási mechanizmusok, valamint adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő

[1] A 29. cikk alapján létrehozott munkacsoport 3/2010. sz. véleménye az elszámoltathatóság elvéről, WP173, 2010. július 13., 69-71. bekezdés.
[2] A 29. cikk alapján létrehozott munkacsoport 3/2010. sz. véleménye az elszámoltathatóság elvéről, WP173, 69. bekezdés.

vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek e rendelet előírásainak. Figyelembe kell venni a mikro-, kis- és középvállalkozások sajátos igényeit."

4. A tanúsítási mechanizmusok3 javíthatják az átláthatóságot az érintettek számára, valamint a vállalkozások – például az adatkezelők és az adatfeldolgozók – közötti kapcsolatok tekintetében is. Az általános adatvédelmi rendelet (100) preambulumbekezdése kimondja, hogy a tanúsítási mechanizmusok létrehozása nyomán javulhat az átláthatóság és a rendeletnek való megfelelés, valamint lehetővé válik az érintettek számára az adott termékek és szolgáltatások adatvédelmi szintjének értékelése.4

5. Az általános adatvédelmi rendelet az adatkezelők és az adatfeldolgozók tekintetében nem állapít meg tanúsítási jogot vagy kötelezettséget; a 42. cikk (3) bekezdése értelmében a tanúsítás önkéntes eljárás, amely segíti az általános adatvédelmi rendeletnek való megfelelés bizonyítását. A rendelet felszólítja a tagállamokat és a felügyeleti hatóságokat, hogy ösztönözzék a tanúsítási mechanizmusok létrehozását, és meg kell határozniuk, hogy milyen szerepet játszanak az érdekelt felek a tanúsítási eljárásban és életciklusban.

6. Emellett a jóváhagyott tanúsítási mechanizmusokhoz való igazodást a felügyeleti hatóságoknak súlyosító vagy enyhítő tényezőként kell figyelembe venniük, amikor arról határoznak, hogy kiszabnak-e közigazgatási bírságot, és ha igen, milyen összegben (a 83. cikk (2) bekezdésének j) pontja).5

1.1 Az iránymutatás hatálya

7. Ezen iránymutatás hatálya korlátozott; nem szolgál az általános adatvédelmi rendelet szerinti tanúsításra vonatkozó kézikönyvként. Ezen iránymutatás elsődleges célja azon átfogó követelmények és szempontok meghatározása, amelyek irányadóak lehetnek az általános adatvédelmi rendelet 42. és 43. cikke szerint kialakított tanúsítási mechanizmusok valamennyi típusára. E célból az iránymutatás:

    - kifejti a tanúsítás – mint elszámoltathatósági eszköz – mögött álló elgondolást;
    - kifejti a 42. és 43. cikk szerinti tanúsítási rendelkezések kulcsfogalmait; valamint
    - ismerteti, hogy mire terjedhet ki a 42. és 43. cikk szerinti tanúsítás és mi a tanúsítás célja;
    - elősegíti, hogy a tanúsítás eredménye könnyen érthető, egyértelmű, a lehető legjobban reprodukálható és összehasonlítható legyen, függetlenül a tanúsítótól (összehasonlíthatóság).

[3] Ebben az iránymutatásban a „tanúsítási mechanizmusok" kifejezés a tanúsítási mechanizmusokat, valamint az adatvédelmi bélyegzőket és jelöléseket jelenti együttesen (lásd az 1.3.2. szakaszt).
[4] Az általános adatvédelmi rendelet (100) preambulumbekezdése kimondja, hogy „az átláthatóság és az e rendeletnek való megfelelés elősegítése érdekében ösztönözni kell a tanúsítási mechanizmusok létrehozását, amelyek lehetővé teszik az érintettek számára, hogy gyorsan értékelni tudják az adott termékek és szolgáltatások adatvédelmi szintjét."
[5] Lásd a 29. cikk szerinti munkacsoport iránymutatását a 2016/679 rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról (WP 253).

8. Az általános adatvédelmi rendelet számos különböző lehetőséget biztosít a tagállamok és a felügyeleti hatóságok számára a 42. és 43. cikk végrehajtására. Ezen iránymutatás tanáccsal szolgál a 42. és 43. cikk rendelkezéseinek értelmezésével és végrehajtásával kapcsolatban, valamint segíti a tagállamokat, a felügyeleti hatóságokat és a nemzeti akkreditáló testületeket az általános adatvédelmi rendelet szerinti tanúsítási mechanizmusokra vonatkozó egységesebb, összehangolt megközelítés kidolgozásában.

9. Az iránymutatásban szereplő tanácsok a következőknek szólnak:

    - az illetékes felügyelő hatóságoknak és az Európai Adatvédelmi Testületnek a tanúsítási szempontoknak a 42. cikk (5) bekezdésével, az 58. cikk (3) bekezdésének f) pontjával, valamint a 70. cikk (1) bekezdésének o) pontjával összhangban történő jóváhagyása tekintetében;

    - a tanúsító szervezeteknek, amikor kidolgozzák és felülvizsgálják a tanúsítási szempontokat, mielőtt a 42. cikk (5) cikkének megfelelően jóváhagyás céljából benyújtanák azokat az illetékes felügyeleti hatósághoz;

    - az Európai Adatvédelmi Testületnek az 42. cikk (5) bekezdése és a 70. cikk (1) bekezdésének o) pontja szerinti európai adatvédelmi bélyegző jóváhagyása tekintetében;

    - a felügyeleti hatóságoknak saját tanúsítási szempontjaik kidolgozása tekintetében;

    - az Európai Bizottságnak, amely a 43. cikk (8) bekezdése értelmében felhatalmazással rendelkezik arra, hogy felhatalmazáson alapuló jogi aktusokat fogadjon el a tanúsítási mechanizmusok tekintetében figyelembe veendő követelmények meghatározása céljából;

    - az Európai Adatvédelmi Testületnek, amikor a 70. cikk (1) bekezdésének q) pontjával és a 43. cikk (8) bekezdésével összhangban véleményezi az Európai Bizottság számára a tanúsítási követelményeket;

    - a nemzeti akkreditáló testületeknek, amelyeknek a tanúsító szervezetek akkreditálása tekintetében figyelembe kell venniük az EN-ISO/IEC 17065/2012 szabvány szerinti tanúsítási követelményeket és a 43. cikk szerinti kiegészítő követelményeket; valamint

    - az adatkezelőknek és az adatfeldolgozóknak az általános adatvédelmi rendeletnek való megfelelésre vonatkozó saját stratégiájuk meghatározása, valamint a tanúsítás, mint a megfelelés bizonyítására szolgáló eszköz mérlegelése tekintetében.

10. Az Európai Adatvédelmi Testület külön iránymutatást fog közzétenni azon szempontok azonosításáról, amelyek a tanúsítási mechanizmusoknak a harmadik országokba vagy a nemzetközi szervezetek részére való továbbítás eszközeiként való jóváhagyására vonatkoznak a 42. cikk (2) bekezdésének megfelelően.

1.2 A tanúsítás általános adatvédelmi rendelet szerinti célja

11. A 42. cikk (1) bekezdése úgy rendelkezik, hogy olyan tanúsítási mechanizmusokat kell létrehozni, „amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek e rendelet előírásainak.”

12. Az általános adatvédelmi rendelet példákat említ azokra az esetekre, amikor a jóváhagyott tanúsítási mechanizmusok az adatkezelők és adatfeldolgozók kötelezettségeknek való megfelelését bizonyító eszközként alkalmazhatók az alábbiakkal összefüggésben:

    - megfelelő technikai és szervezési intézkedések végrehajtása és bizonyítása a 24. cikk (1) és (3) bekezdése, a 25. cikk, valamint a 32. cikk (1) és (3) bekezdése szerint;
    - megfelelő garanciák a 28. cikk (1) bekezdése szerint (az adatfeldolgozótól az adatkezelőnek), valamint a 28. cikk (4) és (5) bekezdése szerint (a további adatfeldolgozótól a fő adatfeldolgozónak).

13. Mivel a tanúsítás önmagában nem bizonyítja a szabályoknak való megfelelést, hanem a megfelelés bizonyítására felhasználható elem, ezért átlátható módon kell elkészíteni. A megfelelés bizonyításához alátámasztó dokumentumok, különösen írott jelentések szükségesek, amelyek nem csupán megismétlik a megfelelés tényét, hanem részletesen ismertetik, hogy miként teljesülnek a szempontok, ha pedig kezdetben nem teljesülnek, akkor ismerteti a korrekciós intézkedéseket és azok megfelelőségét, ezáltal indokolja a tanúsítvány kiadását és fenntartását. Ez vonatkozik a tanúsítvány kiadására, megújítására vagy visszavonására irányuló egyedi határozat felépítésére is. A határozatban ismertetni kell a szempontok alkalmazásából fakadó indokokat, érveket és bizonyítékokat, valamint a tanúsítási eljárás során összegyűjtött tények vagy premisszák alapján hozott következtetéseket vagy ítéleteket.

1.3 Kulcsfogalmak

14. A következő szakaszok ismertetik a 42. és 43. cikkben szereplő kulcsfogalmakat. Értelmezik az alapvető kifejezéseket és a tanúsítás hatályát az általános adatvédelmi rendelet szerint.

1.3.1 A „tanúsítás” kifejezés értelmezése

15. Az általános adatvédelmi rendelet nem határozza meg a tanúsítás fogalmát. A Nemzetközi Szabványügyi Szervezet (ISO) általánosan elfogadott fogalommeghatározása szerint a tanúsítás azt jelenti, hogy egy független szerv írásos biztosítékot (tanúsítványt) nyújt arról, hogy egy adott termék, szolgáltatás vagy rendszer megfelel bizonyos konkrét követelményeknek. A tanúsításra harmadik fél általi megfelelőségértékelésként, a tanúsító szervezetekre pedig megfelelőségértékelő szervezetként is hivatkoznak. Az „ISO/IEC 17000:2004 – Megfelelőségértékelés. Szakszótár és általános elvek” című szabvány (amelyre az ISO17065 szabvány hivatkozik) szerint a tanúsítvány egy termékekhez, folyamatokhoz és szolgáltatásokhoz kapcsolódó harmadik fél által kiadott igazolás.

16. Az igazolás egy olyan nyilatkozat, amelyet egy felülvizsgálatot követő határozat alapján állítanak ki arról, hogy a meghatározott követelmények bizonyítottan teljesülnek (5.2. szakasz, ISO 17000: 2004).

17. Az általános adatvédelmi rendelet 42. és 43. cikke szerinti tanúsítással összefüggésben a „tanúsítvány" az adatkezelők és adatfeldolgozók által végzett adatkezelési műveletekkel kapcsolatos, harmadik fél által kiadott igazolás.

1.3.2 Tanúsítási mechanizmusok, bélyegzők és jelölések

18. Az általános adatvédelmi rendelet nem határozza meg a „tanúsítási mechanizmusok, bélyegzők és jelölések" fogalmát, és ezeket a kifejezéseket együttesen használja. A tanúsítvány egy megfelelőségi nyilatkozat. A bélyegző vagy jelölés annak jelölésére szolgál, hogy a tanúsítási eljárás pozitív eredménnyel zárult. A bélyegző vagy jelölés általában egy olyan logót vagy szimbólumot jelent, melynek jelenléte (a tanúsítvánnyal együtt) azt jelzi, hogy a tanúsítás tárgyát egy tanúsítási eljárás keretében független értékelésnek vetették alá, és megfelel a normatív dokumentumokban – például rendeletekben, szabványokban vagy műszaki előírásokban – meghatározott vonatkozó követelményeknek. Az általános adatvédelmi rendelt szerinti tanúsítással összefüggésben ezeket a követelményeket az EN-ISO/IEC 17065/2012 szabványban foglalt, a tanúsító szervezetek akkreditációjára vonatkozó szabályokat kiegészítő további követelmények, valamint az illetékes felügyelő hatóság vagy a Testület által jóváhagyott tanúsítási szempontok határozzák meg. Az általános adatvédelmi rendelet szerinti tanúsítvány, bélyegző vagy jelölés csak azt követően állítható ki, hogy egy akkreditált tanúsító szervezet vagy illetékes felügyeleti hatóság a bizonyítékok független értékelése révén megállapította, hogy a tanúsítási szempontok teljesülnek.

19. A táblázat egy általános példán szemlélteti a tanúsítás folyamatát.

A kérelem adatkezelő vagy adatfeldolgozó általi benyújtása	**A tanúsító szervezet általi hivatalos ellenőrzés**	**Vizsgálat – Előzetes értékelés**	**Vizsgálat – Az értékelés tárgyának értékelése**	**Vizsgálat – Az eredmények validálása**	**Az illetékes felügyeleti hatóság tájékoztatása**	**Tanúsítvány**	**Nyomon követés**	**A tanúsítvány megújítása**
Egyértelmű-e és teljes-e az értékelés tárgyának leírása, beleértve a kapcsolódási pontokat is?	Elfogadható-e az értékelés tárgyának leírása?	Melyek az alkalmazandó szempontok?	Megfelel-e a szempontoknak az értékelés tárgya?	Meghatározták-e az értékelés tárgyára vonatkozóan az összes meghatározott releváns kritériumot?	Feltüntették-e a tanúsítvány megadásának vagy visszavonásának okait?	Kiadható-e a tanúsítvány?	Továbbra is megfelel-e a szempontoknak az értékelés tárgya?	Továbbra is megfelel-e a tanúsítási szempontoknak az adatkezelés?
Lehet-e hozzáférést biztosítani az értékelés tárgyát képező adatkezelési tevékenységekhez?	Minden dokumentum teljes és naprakész?	Melyek az alkalmazandó értékelési módszerek?	Megfelelően dokumentálva van-e az értékelés tárgya?	Megfelelően dokumentálták-e az értékelést?		Közzétehetőek-e a jelentések?	Helyesen használják-e a tanúsítványt / bélyegzőt / jelölést?	Kielégítően kezelték-e a fejlesztendő területeket?
42. cikk, (6) bekezdés	43. cikk, (4) bekezdés	43. cikk, (4) bekezdés	42. cikk, (5) bekezdés; 43. cikk, (4) bekezdés	43. cikk, (4) bekezdés	43. cikk, (1) bekezdés; 43. cikk, (5) bekezdés	43. cikk, (1) bekezdés; 42. cikk, (7) bekezdés	42. cikk, (7) bekezdés	42. cikk, (7) bekezdés

2 A FELÜGYELETI HATÓSÁGOK SZEREPE

20. A 42. cikk (5) bekezdése úgy rendelkezik, hogy tanúsítványt egy tanúsító szervezet vagy az illetékes felügyeleti hatóság állítja ki. Az általános adatvédelmi rendelet nem teszi a felügyeleti hatóságok kötelező feladatává a tanúsítványok kiállítását. Ehelyett több különböző modellt tesz lehetővé. Például a felügyeleti hatóságok az alábbi lehetőségek közül választhatnak egyet vagy többet:

    - saját maguk állítják ki a tanúsítványt saját tanúsítási rendszerük alapján;
    - saját maguk állítják ki a tanúsítványt saját tanúsítási rendszerük alapján, de az értékelési folyamat egészével vagy egy részével harmadik felet bíznak meg;
    - saját tanúsítási rendszert hoznak létre, és tanúsítási szervezeteket bíznak meg a tanúsítási eljárás lefolytatásával és a tanúsítvány kibocsátásával; valamint
    - tanúsítási mechanizmusok kialakítására ösztönzik a piacot.

21. A felügyeleti hatóságnak ezenfelül figyelembe kell vennie, hogy az akkreditációs mechanizmusokra vonatkozó nemzeti döntések értelmében milyen szerepkört tölt be, különösen akkor, ha a felügyeleti hatóság felhatalmazást kapott arra, hogy maga végezze el a tanúsító szervezeteknek az általános adatvédelmi rendelet 43. cikkének (1) bekezdése szerinti akkreditálását. Ezért az egyes felügyeleti hatóságok döntik el, hogy milyen megközelítést alkalmaznak annak érdekében, hogy teljesüljön a tanúsítás általános adatvédelmi rendelet szerinti átfogó célja. Ennek meghatározásához az 57. és 58. cikkben szereplő feladatokon és hatáskörökön felül azt is figyelembe kell venni, hogy a tanúsítás a közigazgatási bírságok megállapítása szempontjából is jelentőséggel bír, valamint általában véve a megfelelés bizonyításának egyik eszköze.

2.1 A felügyeleti hatóság, mint tanúsító szervezet

22. Amennyiben a felügyeleti hatóság úgy dönt, hogy maga végzi a tanúsítást, akkor gondosan meg kell fontolnia az általános adatvédelmi rendelet által rá rótt feladatok tekintetében betöltött szerepkörét. Egyértelműnek kell lennie, hogy feladatai ellátása során milyen szerepkört lát el. Az esetleges összeférhetetlenség elkerülése érdekében különös gondossággal kell eljárnia a vizsgálati és végrehajtási hatáskörök szétválasztása tekintetében.

23. Amennyiben tanúsító szervezetként tevékenykedik, a felügyeleti hatóságnak gondoskodnia kell megfelelő tanúsítási mechanizmus létrehozásáról, valamint ki kell dolgoznia saját tanúsítási szempontjait vagy el kell fogadnia a már kialakított tanúsítási szempontokat. Ezenfelül a tanúsítványokat kiállító felügyeleti hatóságok kötelesek rendszeres időközönként felülvizsgálni a tanúsítványokat (57. cikk (1) bekezdés o) pont), valamint hatáskörükben áll visszavonni azokat, ha a tanúsítás feltételei nem vagy már nem teljesülnek (58. cikk (2) bekezdés h) pont). E követelmények teljesítése érdekében célszerű meghatározni a tanúsítási eljárásra és folyamatra vonatkozó követelményeket, és – amennyiben egyéb jogszabály (például a nemzeti jog) másként nem rendelkezik – a tanúsítás elvégzésére vonatkozó, jogilag érvényesíthető szerződést kötni az egyes kérelmező szervezetekkel. Biztosítani kell, hogy a tanúsítási megállapodás értelmében a kérelmezőnek meg kelljen felelnie legalább azoknak

tanúsítási szempontoknak, amelyek tartalmazzák az értékelés lefolytatásához, a szempontoknak való megfelelés nyomon követéséhez, az információkhoz és/vagy a helyiségekhez való hozzáférést is magában foglaló rendszeres felülvizsgálat elvégzéséhez, a jelentések és az eredmények dokumentálásához és közzétételéhez, valamint a panaszok kivizsgáláshoz szükséges feltételeket. Elvárható továbbá, hogy a felülvizsgálati hatóságok a 43. cikk (2) bekezdésében foglalt követelményeken felül a tanúsító szervezetek akkreditálására vonatkozó iránymutatásban szereplő követelményeket is teljesítsék.

2.2 A felügyeleti hatóság további feladatai a tanúsítással összefüggésben

24. Azokban a tagállamokban, ahol a tanúsító szervezetek megkezdik működésüket, a felügyelő hatóság saját tevékenységeitől függetlenül a következő hatáskörökkel és feladatokkal rendelkezik:

    - a tanúsítási rendszer szempontjainak értékelése és döntéstervezet kidolgozása (a 42. cikk (5) bekezdése);
    - a döntéstervezet közlése a Testülettel, ha a felügyeleti hatóság a tanúsítási szempontok jóváhagyását tervezi (a 64. cikk (1) bekezdésének c) pontja és a 64. cikk (7) bekezdése), valamint a Testület véleményének figyelembevétele (a 64. cikk (1) bekezdésének c) pontja és 70. cikk (1) bekezdésének t) pontja)
    - az akkreditálást és tanúsítást megelőzően (a 42. cikk (5) bekezdése és a 43. cikk (2) bekezdésének b) pontja) a tanúsítási szempontok jóváhagyása (az 58. cikk (3) bekezdésének f) pontja);
    - a tanúsítási szempontok közzététele (a 43. cikk (6) bekezdése);
    - illetékes hatóságként való eljárás azon uniós szintű tanúsítási rendszerek tekintetében, amelyek eredményeként az Európai Adatvédelmi Testület által jóváhagyott európai adatvédelmi bélyegző állítható ki (a 42. cikk (5) bekezdése és 70. cikk (1) bekezdésének o) pontja); valamint
    - arra, hogy utasítsa a tanúsító szervezetet, hogy a) ne adjon ki tanúsítványt; vagy b) visszavonja a tanúsítványt, amennyiben a tanúsításra (a tanúsítási eljárásokra vagy a szempontokra) vonatkozó követelmények nem vagy már nem teljesülnek (az 58. cikk (2) bekezdésének h) pontja).

25. Az általános adatvédelmi rendelet értelmében a tanúsítási szempontok jóváhagyása a felügyeleti hatóságok feladata, a szempontok kidolgozása azonban nem. Ahhoz, hogy a 42. cikk (5) bekezdése értelmében jóváhagyhassa a tanúsítási szempontokat, a felügyeleti hatóságnak tisztában kell lennie az elvárásokkal, különösen az általános adatvédelmi rendeletnek való megfelelés bizonyításának hatályát és tartalmát illetően, valamint a rendelet alkalmazásának nyomon követésére és érvényesítésére vonatkozó feladata tekintetében. A melléklet iránymutatást ad annak érdekében, hogy a szempontok jóváhagyás céljából végzett értékelése összehangolt megközelítés szerint történjen.

26. A 43. cikk (1) bekezdése előírja a tanúsító szervezetek számára, hogy a tanúsítványok kiállítása vagy megújítása előtt tájékoztassák felügyeleti hatóságukat annak érdekében, hogy az illetékes felügyeleti hatóság gyakorolhassa az 58. cikk (2) bekezdésének h) pontja szerinti korrekciós hatáskörét. A 43. cikk (5) bekezdése továbbá előírja, hogy a tanúsító szervezeteknek közölniük az illetékes felügyeleti hatósággal a kért tanúsítvány megadásának vagy visszavonásának okait. Bár az általános adatvédelmi rendelet lehetővé teszi a felügyeleti hatóságok számára annak meghatározását, hogy a gyakorlatban milyen módon történjen az ilyen információk beérkezése, nyugtázása, ellenőrzése és kezelése (ez magában foglalhat például olyan technológiai megoldásokat, amelyek lehetővé teszik a tanúsító szervezetek számára a jelentéstételt), ugyanakkor a 43. cikk (1) bekezdésének értelmében bevezethetők olyan szempontok és eljárások, amelyek a tanúsító szervezet által az egyes sikeres tanúsítási projektekre vonatkozóan szolgáltatott információk és jelentések feldolgozására szolgálnak. Ezen információk alapján a felügyeleti hatóság gyakorolhatja azt a hatáskörét, amelynek értelmében utasíthatja a tanúsító szervezetet az általános adatvédelmi rendelet szerinti tanúsítvány visszavonására vagy kiállításának megtagadására (az 58. cikk (2) bekezdésének h) pontja szerint), valamint a tanúsítás követelményei és szempontjai alkalmazásának nyomon követésére és kikényszerítésére (az 57. cikk (1) bekezdésének a) pontja és az 58. cikk (2) bekezdésének h) pontja értelmében). Ez elősegíti a harmonizált megközelítést és a különböző tanúsító szervezetek által végzett tanúsítás összehasonlíthatóságát, valamint azt, hogy a felügyeleti hatóságok információkkal rendelkezzenek egy adott szervezet tanúsítási státuszára vonatkozóan.

3 A TANÚSÍTÓ SZERVEZET SZEREPE

27. A tanúsító szervezet feladata tanúsítványok kiállítása, felülvizsgálata, megújítása és visszavonása (42. cikk (5) és (7) bekezdés) egy tanúsítási mechanizmus és jóváhagyott szempontok alapján (43. cikk (1) bekezdés). Ez a tanúsítási szempontok és eljárások meghatározására és kidolgozására kötelezi a tanúsító szervezetet vagy a tanúsítási rendszer tulajdonosát, ideértve a megfelelés nyomon követésére, a felülvizsgálatra, a panaszok kezelésére és a visszavonásra vonatkozó eljárásokat. A tanúsítványok, bélyegzők vagy a jelöléseket kiállítására vonatkozó szabályokra és eljárásokra irányuló akkreditációs folyamat részeként felülvizsgálják a tanúsítási szempontokat (a 43. cikk (2) bekezdésének c) pontja).

28. A 43. cikk értelmében egy tanúsító szervezet csak megfelelő tanúsítási mechanizmus és tanúsítási szempontok megléte esetén akkreditálható. Egy tanúsító szervezet tevékenységét nagyban befolyásolja a tanúsítási szempontok alkalmazási köre és típusa, amely kihat a tanúsítási eljárásokra. Egyes konkrét szempontok például konkrét értékelési módszereket – például helyszíni vizsgálatot vagy a magatartási kódex felülvizsgálatát – tehetnek szükségessé. Ezen eljárások megléte az akkreditáció kötelező előfeltétele, és azokat az akkreditációról szóló iránymutatás részletesen ismerteti.

29. Az általános adatvédelmi rendelet értelmében a tanúsító szervezeteknek a felügyeleti hatóságok rendelkezésére kell bocsátaniuk a tanúsítási mechanizmus alkalmazásának nyomon követéséhez szükséges információkat, különösen az egyéni tanúsítványok tekintetében (a 42. cikk (7) bekezdése, a 43. cikk (5) bekezdése és az 58. cikk (2) bekezdésének h) pontja).

4 A TANÚSÍTÁSI SZEMPONTOK JÓVÁHAGYÁSA

30. A tanúsítási szempontok a tanúsítási mechanizmus szerves részét képezik. Ezért az általános adatvédelmi rendelet értelmében az illetékes felügyeleti hatóságnak jóvá kell hagynia a tanúsítási mechanizmus részét képező tanúsítási szempontokat (a 42. cikk (5) bekezdése és a 43. cikk (2) bekezdésének b) pontja). Az európai adatvédelmi bélyegző esetében az Európai Adatvédelmi Testület hagyja jóvá a tanúsítási szempontokat (a 42. cikk (5) bekezdése és a 70. cikk (1) bekezdésének o) pontja). A tanúsítási szempontok jóváhagyásának két módja van, amelyeket az alábbiakban ismertetünk.

31. Az Európai Adatvédelmi Testület szerint a tanúsítási szempontok jóváhagyásának célja, hogy:

    - megfelelően tükrözze azokat a követelményeket és elveket, amelyeket személyes adatok védelmére vonatkozóan az (EU) 2016/679 rendelet fogalmaz meg a természetes személyek védelme érdekében; valamint
    - elősegítse az általános adatvédelmi rendelet következetes alkalmazását.

32. A tanúsítási szempontok akkor hagyhatóak jóvá, ha maradéktalanul tükrözik az általános adatvédelmi rendelet azon követelményét, amely szerint a tanúsítási mechanizmusnak lehetővé kell tennie az adatkezelők és adatfeldolgozók számára az általános adatvédelmi rendeletnek való megfelelés bizonyítását.

4.1 A szempontok illetékes felügyeleti hatóság általi jóváhagyása

33. Az illetékes felügyeleti hatóságnak egy tanúsító szervezet akkreditációjának eljárását megelőzően vagy annak folyamán kell jóváhagynia a tanúsítási szempontokat. Amennyiben ugyanazon tanúsító szervezet az ISO 17065 szabványnak megfelelően aktualizálja vagy kiegészíti szempontrendszereit, a módosított tanúsítási mechanizmusok alkalmazása előtt ezeket szintén jóvá kell hagyatni (a 42. cikk (5) bekezdése és a 43. cikk (2) bekezdésének b) pontja). A felügyeleti hatóságok a minősítési szempontok jóváhagyására irányuló kérelmeket tisztességes és megkülönböztetésmentes módon, a teljesítendő általános feltételeket és a jóváhagyási folyamat leírását meghatározó, nyilvánosan elérhető eljárás szerint kezelik.

34. Egy tanúsító szervezet az adott tagállam felügyeleti hatósága által jóváhagyott szempontoknak megfelelően csak az adott tagállamban állíthat ki tanúsítványt. Másképpen fogalmazva a tanúsítási szempontokat azon tagállam illetékes felügyeleti hatóságának kell jóváhagynia, ahol a tanúsító szervezet tanúsítási tevékenységet kíván végezni és akkreditációt kíván szerezni. A következő szakasz ismerteti az európai szintű tanúsítási rendszereket.

4.2 Az európai adatvédelmi bélyegzőre vonatkozó szempontok Európai Adatvédelmi Testület általi jóváhagyása

35. A tanúsító szervezet az Európai Adatvédelmi Testület által az európai adatvédelmi bélyegzőre vonatkozóan jóváhagyott szempontok alapján is kiállíthat tanúsítványt. Ha az Európai Adatvédelmi Testület a 63. cikknek megfelelően jóváhagyja a tanúsítási szempontokat, ennek

eredményeképpen európai adatvédelmi bélyegző adható ki (a 42. cikk (5) bekezdése). A meglévő tanúsítási és akkreditációs egyezmények fényében az Európai Adatvédelmi Testület elismeri, hogy el kell kerülni az adatvédelmi tanúsítási piac széttagolódását. A Testület megjegyzi, hogy a 42. cikk (1) bekezdése értelmében a tagállamoknak, a felügyeleti hatóságoknak, a Testületnek és a Bizottságnak ösztönözniük kell a tanúsítási mechanizmusok létrehozását, különösen uniós szinten.

4.2.1 Jóváhagyási kérelem

36. A szempontoknak az Európai Adatvédelmi Testület általi jóváhagyására irányuló, a 42. cikk (5) bekezdésének és a 70. cikk (1) bekezdése o) pontjának megfelelő kérelmet az illetékes felügyeleti hatóságon keresztül kell benyújtani, és annak fel kell tüntetnie, hogy a rendszer tulajdonosa, illetve a kérelmező vagy akkreditált tanúsító szervezet az adatkezelőkre és -feldolgozókra vonatkozó tanúsítási mechanizmus keretében valamennyi tagállamban alkalmazni kívánja a szempontokat. Amennyiben az illetékes felügyeleti hatóság úgy ítéli meg, hogy a szempontok alkalmasak az Európai Adatvédelmi Testület általi jóváhagyásra, tervezetet nyújt be az Európai Adatvédelmi Testületnek.

37. A szempontok jóváhagyására irányuló kérelem benyújtásának helyét az alapján választják meg, hogy hol van tanúsítási rendszer tulajdonosának vagy a tanúsító szervezetnek a székhelye.

38. Ha egy tanúsító szervezet kérelmet nyújt be, akkor ezt általában az akkreditálásra irányuló kérelemhez kapcsolódó folyamat részeként teszi, vagy akkor, amikor az adott tagállam illetékes felügyeleti hatósága vagy nemzeti akkreditáló testülete már akkreditálta a szervezetet. Amennyiben a tanúsító szervezet már megszerezte az általános adatvédelmi rendelet szerinti tanúsítási mechanizmus alkalmazására jogosító akkreditációt, akkor ennek köszönhetően egyszerűbbé válhat a jóváhagyási eljárás.

4.2.2 Az európai adatvédelmi bélyegzővel kapcsolatos szempontok

39. Az Európai Adatvédelmi Testület összehangolja az értékelési folyamatot, és az előírásoknak megfelelően jóváhagyja az európai adatvédelmi bélyegzővel kapcsolatos szempontokat. Az értékelés tárgyát képező területek többek között a következők: a szempontok alkalmazási köre és alkalmassága arra, hogy egy közös tanúsítvány alapjául szolgáljanak. Amennyiben az Európai Adatvédelmi Testület jóváhagyja a szempontokat, a mechanizmussal kapcsolatos panaszok kezelése és a többi felügyeleti hatóság tájékoztatása azon tagállam illetékes felügyeleti hatóságának feladata, amelyben a tanúsító szervezet Európai Unióban létesített székhelye található. A felügyeleti hatóság hatáskörrel rendelkezik arra is, hogy intézkedéseket hozzon a tanúsító szervezettel szemben. Ilyen esetben az illetékes felügyeleti hatóság értesíti a többi felügyeleti hatóságot és az Európai Adatvédelmi Testületet.

40. A közös tanúsítás tanúsítási szempontjait unió szintű igény esetén kell kialakítani, és ezen igények kielégítésére külön mechanizmust kell létrehozni. Az uniós tanúsítási mechanizmusoknak valamennyi tagállamban alkalmazhatónak kell lenniük. A 42. cikk (5) bekezdése értelmében az európai adatvédelmi bélyegzőre vonatkozó mechanizmust és az azzal kapcsolatos szempontokat úgy kell kialakítani, hogy lehetővé tegyék a nemzeti

ágazatspecifikus – pl. az iskolákban végzett adatkezelésre vonatkozó – szabályok figyelembevételét, valamint az egész Unióban alkalmazhatóak legyenek.

41. Példa: Egy Unióban élő érintettek számára képzést biztosító nemzetközi iskola székhelye „A" tagállamban található. Az iskola az uniós szintű tanúsítási rendszer segítségével kívánja igazolni, hogy az általa alkalmazott online jelentkezési eljárás megfelel az előírásoknak, és európai adatvédelmi bélyegzőt kíván kapni. Ez az iskola egy olyan tanúsító szervezettel szeretné elvégeztetni az adatkezelési műveleteire vonatkozó tanúsítást, amelynek székhelye „B" tagállamban található. A bélyegzővel kapcsolatos, a vonatkozó mechanizmus keretében kialakított és lefektetett szempontoknak alkalmasaknak kell lenniük arra, hogy figyelembe vegyék az iskolákra az „A" tagállamban alkalmazandó szabályokat. A szempontoknak azt is elő kell írniuk, hogy az iskola az online jelentkezési eljárás során információval szolgáljon az adott tagállam – más tagállamokétól esetleg eltérő – adatvédelmi követelményeiről, és figyelembe vegye azokat. Ilyen eltérések lehetnek például a következő területeken: a jelentkezés során benyújtandó személyes adatok (például az óvodai osztályzatok vagy teszteredmények), a pénzügyi vagy biometrikus adatok megőrzési ideje, gyűjtése vagy kezelése tekintetében fennálló eltérések, további adatkezelési korlátozások.

    - Az európai adatvédelmi bélyegző mechanizmusának jóváhagyásához többek között a következő magas szintű szempontoknak kell teljesülniük:
        - a Testületnek jóvá kell hagynia a szempontokat;
        - lehetővé kell tennie a joghatóságok közötti alkalmazást oly módon, hogy az adott esetben tükrözze a nemzeti jogszabályi követelményeket és ágazatspecifikus szabályokat;
        -
    - olyan harmonizált szempontokat kell meghatározni, amelyek rugalmasan alakíthatók annak érdekében, hogy tükrözzék a nemzeti jogszabályi követelményeket;
        - a tanúsítási mechanizmus leírásának meg kell határoznia a következőket:
        - a tanúsítási megállapodások, elismerve a páneurópai követelményeket;
        - olyan eljárások, amelyek lehetővé teszik a nemzeti eltérések figyelembevételét és kezelését, valamint biztosítják, hogy a bélyegző segítse az általános adatvédelmi rendeletnek való megfelelés bizonyítását; valamint
        - az összes érintett felügyeleti hatóságnak címzett jelentések nyelve.

42. A melléklet az európai adatvédelmi bélyegző szempontjaira vonatkozó tanácsokat is tartalmaz.

4.2.3 Az akkreditáció szerepe

43. A 4.2.1. pontban említettek szerint, amennyiben a Testület úgy ítéli meg, hogy a szempontok alkalmasak arra, hogy azok alapján közös tanúsítványt adjanak ki, és ennek megfelelően a 42.

cikk (5) bekezdése szerint jóváhagyja azokat, akkor a tanúsító szervezetek akkreditációt szerezhetnek arra, hogy e szempontok alapján az egész Unióban tanúsítást végezzenek.

44. Nem adható ki európai adatvédelmi bélyegző olyan rendszerek keretében, amelyeket csak egyes tagállamokban kívánnak alkalmazni. Az európai adatvédelmi bélyegző kiadására feljogosító akkreditáció feltétele a rendszert működtetni kívánó tanúsító szervezet – vagyis a tanúsítványok kiadásáért, valamint az alszervezetei és leányvállalatai által más tagállamokban végzett tanúsítási tevékenységek irányításért felelős szervezet – székhelye szerinti tagállamban való akkreditáció. Amennyiben különböző egységek vagy irodák önállóan szervezik vagy folytatják le a tanúsítást,, akkor minden egyes ilyen egységnek vagy irodának külön akkreditációt kell szereznie abban a tagállamban, ahol található. Más szóval, csak akkor elegendő a tanúsító szervezet székhelye szerinti tagállamban akkreditációt szerezni, ha kizárólag az adott székhelyen működő központ állít ki tanúsítványokat Ezzel szemben, ha a tanúsító szervezet egyéb szervezeti egységei is kiállítanak tanúsítványokat, akkor ezeket az intézményeket is akkreditálni kell.

45. Következésképpen, ha egy tanúsító szervezet nem szerezte meg az európai adatvédelmi bélyegző kiadására jogosító akkreditációt, akkor nem alkalmazhatja az Európai Adatvédelmi Testület által jóváhagyott szempontokat és nem adhat ki európai adatvédelmi bélyegzőt.

5 A TANÚSÍTÁSI SZEMPONTOK KIDOLGOZÁSA

46. Az általános adatvédelmi rendelet meghatározta a tanúsítási szempontok kidolgozásának keretét. Mivel a tanúsítási eljárásra vonatkozó alapvető követelményeket a 42. és a 43. cikk tárgyalja, valamint alapvető szempontokat is meghatároz a tanúsítási eljárások tekintetében, a tanúsítási szempontok alapját az általános adatvédelmi rendelet elveiből és szabályaiból kell levezetni, és elő kell segíteni azok teljesülését.

47. A tanúsítási szempontok kidolgozása során a tanúsítási szempontok igazolhatóságára, jelentőségére és megfelelőségére kell összpontosítani, hogy alkalmasak legyenek a rendeletnek való megfelelés igazolására. A tanúsítási szempontokat úgy kell megfogalmazni, hogy világosak és érthetőek legyenek, valamint lehetővé tegyék a gyakorlati alkalmazást.

48. A tanúsítási szempontok kidolgozása során az adatkezelési műveletek értékelésének elősegítése céljából adott esetben figyelembe kell venni többek között a következő megfelelési vonatkozásokat:

    - az adatkezelés jogszerűsége a 6. cikknek megfelelően;
    - az adatok kezelésére vonatkozó elvek az 5. cikknek megfelelően;
    - az érintettek jogai a 12–23. cikknek megfelelően;
    - az adatvédelmi incidensek bejelentésére vonatkozó kötelezettség a 33. cikknek megfelelően;
    - a beépített és alapértelmezett adatvédelemre vonatkozó kötelezettség, a 25. cikknek megfelelően;

- adott esetben sor került-e a 35. cikk (7) bekezdésének d) pontja szerinti adatvédelmi hatásvizsgálatra; valamint
- a 32. cikk alapján meghozott technikai és szervezeti intézkedések.

49. A szempontok eltérő mértékben tükrözhetik ezeket a megfontolásokat a tanúsítás hatókörétől függően, amely kiterjedhet többek között az adatkezelési művelet(ek) típusára vagy a tanúsítás tárgyát képező területre (pl. egészségügy).

5.1 Miről adható ki tanúsítvány az általános adatvédelmi rendelet alapján?

50. Az Európai Adatvédelmi Testület véleménye szerint az általános adatvédelmi rendelet tágan határozza meg, hogy miről adható ki tanúsítvány, feltéve, hogy a tanúsítás elsődleges célja segíteni annak bizonyítását, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek a rendelet előírásainak (42. cikk (1) bekezdés).

51. Az adatkezelési művelet értékelésekor adott esetben a következő három alapvető elemet kell figyelembe venni:

    1. személyes adatok (az általános adatvédelmi rendelet tárgyi hatálya);
    2. műszaki rendszerek – a személyes adatok kezeléséhez használt infrastruktúra, például a hardverek és a szoftverek; valamint
    3. az adatkezelési művelet(ek)hez kapcsolódó folyamatok és eljárások.

52. A műveletek során használt valamennyi összetevőt értékelni kell a meghatározott szempontok alapján. Legalább négy különböző lényeges tényező befolyásolhatja az értékelést: 1. az adatkezelő vagy -feldolgozó szervezeti felépítése és jogi struktúrája; 2. az adatkezelési művelet(ek)ben részt vevő szervezeti egység, környezet és személyek; 3. az értékelés tárgyát képező elemek műszaki leírása; és végül 4. az adatkezelési műveletet támogató informatikai infrastruktúra, beleértve az operációs rendszereket, virtuális rendszereket, adatbázisokat, hitelesítési és engedélyezési rendszereket, útválasztókat és tűzfalakat, tárolórendszereket, kommunikációs infrastruktúrát, illetve az internethez való hozzáférést és a kapcsolódó technikai intézkedéseket.

53. Mind a három alapvető elem jelentőséggel bír a tanúsítási eljárások és szempontok kialakítása során. A tanúsítás céljától függően ezeket az alapvető elemeket eltérő mértékben vehetik figyelembe. Egyes esetekben például bizonyos összetevőket figyelmen kívül lehet hagyni, ha úgy ítélik meg, hogy azok a tanúsítás tárgya szempontjából nem relevánsak.

54. Az általános adatvédelmi rendelet további iránymutatást tartalmaz annak pontos meghatározása érdekében, hogy miről adható ki tanúsítvány a rendelet értelmében. A 42. cikk (7) bekezdéséből következik, hogy az általános adatvédelmi rendelet szerinti tanúsítványokat csak az adatkezelők és adatfeldolgozók számára állítják ki, ami kizárja például az adatvédelmi tisztviselők tanúsítását. A 43. cikk (1) bekezdésének b) pontja az ISO 17065 szabványra hivatkozik, amely a termékek, folyamatok és szolgáltatások megfelelőségét értékelő végző szervezetek akkreditálásáról rendelkezik. Az ISO 17065 szabvány terminológiájában egy

adatkezelési művelet vagy műveletek eredményeként termék vagy szolgáltatás jöhet létre, így ez tanúsítás tárgya lehet. Például a munkavállalók adatainak a bérszámfejtés vagy a szabadságok kezelése céljából történő kezelése az általános adatvédelmi rendelet értelmében műveletek összességének minősül, és ez az ISO terminológiája szerinti terméket, folyamatot vagy szolgáltatást eredményezhet.

55. E megfontolások alapján az Európai Adatvédelmi Testület úgy véli, hogy az általános adatvédelmi rendelet szerinti tanúsítás tárgyát az adatkezelési műveletek vagy műveletsorozatok képezik. Ezeket alkothatják szervezeti intézkedésnek számító irányítási folyamatok, amelyek ezáltal egy adatkezelési művelet szerves részét képezik (például a panaszkezelésre létrehozott irányítási folyamat az alkalmazottak adatainak bérszámfejtés céljából való kezelése részeként).

56. Annak értékeléséhez, hogy az adatkezelési művelet megfelel-e a tanúsítási szempontoknak, meg kell adni egy felhasználási esetet. Például attól függ, hogy egy adatkezelési művelet elvégzéséhez használt műszaki infrastruktúra megfelelő-e, hogy milyen kategóriájú adatok kezelésére hozták létre. A szervezeti intézkedések az adatok kategóriájától és mennyiségétől, valamint az adatkezeléshez használt műszaki infrastruktúrától függnek, figyelembe véve az adatkezelés jellegét, alkalmazási körét, tartalmát és céljait, valamint az érintettek jogait és szabadságait érintő kockázatokat.

57. Szem előtt kell tartani továbbá azt is, hogy az informatikai alkalmazások között még akkor is jelentős eltérés lehet, ha azonos adatkezelési célt szolgálnak. Ezért ezt figyelembe kell venni a tanúsítási mechanizmusok alkalmazási körének meghatározása és a tanúsítási szempontok kidolgozása során, azaz a tanúsítás és a szempontok alkalmazási köre nem lehet olyan szűk, hogy kizárja az eltérő kialakítású informatikai alkalmazásokat.

5.2 A tanúsítás tárgyának meghatározása

58. A tanúsítási mechanizmus alkalmazási körét meg kell különböztetni a tanúsítási mechanizmus keretében végzett egyedi tanúsítási projekt tárgyától, másképpen az értékelés tárgyától. A tanúsítási mechanizmus alkalmazási körét vagy általában, vagy az adatkezelési műveletek egy adott típusára vagy területére vonatkozóan lehet meghatározni, ezáltal pedig már azonosítható a tanúsítási mechanizmus alkalmazási körébe tartozó tanúsítás tárgya (például a digitális páncélszekrényben tárolt személyes adatok biztonságos tárolása és védelme). Mindenesetre megbízható és releváns megfelelőségi értékelés csak akkor végezhető, ha a tanúsítási projekt egyedi tárgya pontosan le van írva. Világosan ismertetni kell először azt, hogy mely adatkezelési műveletek képezik a tanúsítás tárgyát, majd azt, hogy melyek az értékelés alapvető elemei, azaz mely adatokat, folyamatokat és műszaki infrastruktúrát kell értékelni, és melyeket nem. Ennek során mindig figyelembe kell venni és ismertetni kell az egyéb folyamatokhoz való kapcsolódási pontokat is. Egyértelmű, hogy az értékelés ismeretlen dolgokra nem terjedhet ki, ezért azokról tanúsítvány sem adható ki. A tanúsítás egyedi tárgyának mindenképpen relevánsnak kell lennie a tanúsítás üzenete vagy az azzal kapcsolatos állítás szempontjából, és nem lehet félrevezető a felhasználók, a fogyasztók vagy a vásárlók számára.

59. [1. példa]

Egy bank egy honlapon keresztül internetes banki szolgáltatásokat kínál ügyfeleinek. E szolgáltatás lehetővé teszi átutalások indítását, részvényvásárlást, állandó megbízások kezdeményezését és a számla kezelését. A bank egy általános alkalmazási körű, általános szempontokon alapuló adatvédelmi tanúsítási mechanizmus révén az alábbiakról kíván tanúsítványt szerezni:

a) Biztonságos bejelentkezés

A biztonságos bejelentkezés olyan adatkezelési művelet, amely a végfelhasználó számára érthető és adatvédelmi szempontból releváns, mivel fontos szerepet játszik az érintett személyes adatok biztonságának garantálásában. Ezért ez az adatkezelési művelet szükséges a biztonságos bejelentkezéshez, és így az értékelés érdemi tárgyának, ha a tanúsítvány egyértelműen jelzi, hogy csak a bejelentkezéshez kapcsolódó adatkezelési műveletre vonatkozik.

b) Ügyféloldali webes felület

Bár az ügyféloldali webes felület adatvédelmi szempontból releváns lehet, a végfelhasználók számára nem értelmezhető, ezért nem lehet az értékelés érdemi tárgya. A felhasználók számára továbbá nem egyértelmű, hogy a honlapon nyújtott mely szolgáltatásra, és ezáltal mely adatkezelési műveletekre terjed ki a tanúsítás.

c) Internetes banki szolgáltatások

Az ügyféloldali webes felület és a feldolgozó oldali funkciók a banki szolgáltatások keretében végzett adatkezelési műveletek, amelyek az internetes a felhasználók számára relevánsak lehetnek. Ebben az összefüggésben mindkettőnek szerepelnie kell az értékelés tárgyai között. Ezzel szemben nem kell szerepelniük az értékelés tárgyai között azoknak az adatkezelési műveleteknek, amelyek nem kapcsolódnak közvetlenül az online banki szolgáltatáshoz – ilyenek például a pénzmosás megelőzése céljából végzett adatkezelési műveletek.

Mindazonáltal a bank által a honlapján kínált online banki szolgáltatások más szolgáltatásokat is magukban foglalhatnak, amelyek viszont külön adatkezelési műveleteket tesznek szükségessé. Ilyen egyéb szolgáltatás lehet például egy biztosítási termék értékesítése. Mivel ez a kiegészítő szolgáltatás nem kapcsolódik közvetlenül az online banki szolgáltatások nyújtásához, elhagyható az értékelés tárgyai közül. Ha ez a kiegészítő szolgáltatás (biztosítás) nem szerepel az értékelés tárgyai között, a honlap e szolgáltatáshoz kapcsolódó felületeire akkor is kiterjed az értékelés, ezért ezekről leírást kell készíteni annak érdekében, hogy egyértelműen el lehessen különíteni egymástól a szolgáltatásokat. Ez a leírás elengedhetetlen ahhoz, hogy azonosítani és értékelni lehessen a két szolgáltatás közötti esetleges adatáramlást.

60. [2. példa]

A bank ügyfeleinek olyan szolgáltatást nyújt, amely lehetővé teszi számukra a különböző számlákhoz és hitelkártyákhoz kapcsolódó, több bankból származó információk összesítését (a számlák összesítése). A bank az általános adatvédelmi rendelet szerinti tanúsítványt kíván szerezni e szolgáltatására vonatkozóan. Az illetékes felügyeleti hatóság jóváhagyta az ilyen

típusú tevékenységre vonatkozó tanúsítási szempontokat. A tanúsítási mechanizmus alkalmazási köre kizárólag a következő megfelelési vonatkozásokra terjed ki:

- a felhasználó hitelesítése; valamint
- az összesítendő adatok más bankoktól/szolgáltatásoktól való megszerzésének elfogadható módjai.

Mivel e tanúsítási mechanizmus alkalmazási köre már önmagában meghatározza az értékelés tárgyát, az értékelés tárgyát érdemben nem lehet a javasoltnál szűkebbre szabni, és a tanúsítást csak adott funkciókra vagy egyetlen adatkezelési műveletre elvégezni. Ilyen esetekben az értékelés tárgya megegyezik az adott alkalmazási körrel.

5.3 Elemzési módszerek és az értékelés módszertana

61. Az adatkezelési műveletek megfelelőségének igazolását segítő megfelelőségértékeléshez azonosítani kell és meg kell határozni az elemzési módszereket és az értékelés módszertanát. Számít az is, hogy az értékeléshez szükséges információkat csak dokumentumokból gyűjtik-e össze (ami önmagában nem elegendő), vagy aktívan a helyszínen, valamint közvetlen vagy közvetett hozzáféréssel szerzik-e meg. Az adatgyűjtés módja befolyásolja a tanúsítás jelentőségét, ezért azt meg kell határozni és le kell írni.

    A tanúsítványok kiállítására és rendszeres felülvizsgálatára vonatkozó eljárások keretében azonosítani kell azt az értékelési szintet (az értékelés mélységét és részletességét), amely a tanúsítási szempontoknak való megfeleléshez szükséges, valamint biztosítani kell a következőket:

    - tájékoztatás az alkalmazott értékelési módszerekről és a – például a helyszíni ellenőrzések során vagy dokumentumokból – összegyűjtött adatokról, valamint azok pontos leírása,
    - az adatkezelési műveletekre (adatok, rendszerek, folyamatok) és az adatkezelés céljára vonatkozó értékelési módszerek,
    - az adatkategóriák és az adatvédelmi szükségletek meghatározása, valamint annak pontosítása, hogy bevonnak-e adatfeldolgozókat vagy harmadik feleket,
    - a szerepek azonosítása, valamint a szerepek és a felelősségi körök szerint meghatározott hozzáférés-ellenőrzési mechanizmus megléte.

62. Az értékelés mélysége befolyásolja a tanúsítás jelentőségét és értékét. Ha gyakorlati okokból vagy a költségek csökkentése érdekében kevésbé mélyreható értékelést végeznek, akkor csökken az adatvédelmi tanúsítvány jelentősége. Az értékelés részletességével kapcsolatos döntések azonban meghaladhatják a kérelmező pénzügyi lehetőségeit, és gyakran az értékelők és az ellenőrök képességét is. A megfelelőség érdemi tanúsításához nem feltétlenül szükséges minden esetben nagyon részletes elemzést készíteni az alkalmazott informatikai rendszerekről.

5.4 Az értékelés dokumentálása

63. A tanúsításról alapos és átfogó dokumentációt kell készíteni. Dokumentáció hiányában nem végezhető megfelelő értékelés. A tanúsítási dokumentáció alapvetően azt a célt szolgálja, hogy átláthatóságot biztosítson a tanúsítási mechanizmus szerinti értékelési folyamat során. A dokumentáció választ ad a jogszabályokban meghatározott követelményekkel kapcsolatos kérdésekre. A tanúsítási mechanizmusoknak elő kell írniuk szabványos dokumentálási módszerek alkalmazását. Ezt követően az értékelés révén lehetővé válik, hogy a tanúsítási dokumentációt összehasonlítsák a tényleges helyszíni állapottal és a tanúsítási szempontokkal.

64. A tanúsítás tárgyáról és az alkalmazott módszertanról szóló átfogó dokumentáció az átláthatóságot szolgálja. A 43. cikk (2) bekezdésének c) pontja értelmében a tanúsítási mechanizmusoknak olyan eljárásokat kell létrehozniuk, amelyek lehetővé teszik a tanúsítványok felülvizsgálatát. A részletes dokumentáció lehet a legmegfelelőbb kommunikációs eszköz annak érdekében, hogy a felügyeleti hatóság fel tudja mérni, hogy hivatalos vizsgálatokban figyelembe lehet-e venni a tanúsítványt, és ha igen, milyen mértékben. Az értékelés során készített dokumentációnak ezért három fő szempontra kell összpontosítania:

    - az alkalmazott értékelési módszerek következetessége és koherenciája;
    - olyan értékelési módszerek, amelyek célja igazolni, hogy a tanúsítás tárgya megfelel a tanúsítási szempontoknak és így a rendeletnek; valamint
    - az értékelés eredményeinek független és pártatlan tanúsító szervezet általi validálása.

5.5 Az eredmények dokumentálása

65. A (100) preambulumbekezdés ismerteti a tanúsítás bevezetésének céljait.

„Az átláthatóság és az e rendeletnek való megfelelés elősegítése érdekében ösztönözni kell olyan tanúsítási mechanizmusok, és adatvédelmi bélyegzők illetve jelölések létrehozását, amelyek lehetővé teszik az érintettek számára, hogy gyorsan értékelni tudják az adott termékek és szolgáltatások adatvédelmi szintjét.”

66. A jobb átláthatóság érdekében fontos a dokumentálás és az eredményekről nyújtott tájékoztatás. A – fogyasztóként vagy vásárlóként fellépő – érintetteknek szóló tanúsítási mechanizmusokat, bélyegzőket vagy jelöléseket alkalmazó tanúsító szervezeteknek könnyen hozzáférhető, érthető és érdemi információt kell nyújtaniuk arról, hogy a tanúsítás mely adatkezelési műveletekre terjedt ki. Ennek a nyilvános tájékoztatásnak legalább a következőket kell tartalmaznia:

    - az értékelés tárgyának leírása;
    - hivatkozás az értékelés konkrét tárgyára vonatkozó, jóváhagyott szempontokra;
    - a szempontok értékelésének módszertana (helyszíni értékelés, dokumentáció stb.); valamint
    - a tanúsítvány érvényességének időtartama; valamint

- lehetővé kell tennie a felügyeleti hatóságok és a nyilvánosság számára az eredmények összehasonlítását.

6 IRÁNYMUTATÁS A TANÚSÍTÁSI SZEMPONTOK MEGHATÁROZÁSÁHOZ

67. A tanúsítási szempontok a tanúsítási mechanizmus szerves részét képezik. A tanúsítási eljárás követelményeket fogalmaz meg arra vonatkozóan, hogy az egyedi tanúsítási projektekhez kapcsolódó értékelés keretében ki, milyen mértékben és milyen részletességgel értékeli az értékelés konkrét tárgyát. Az értékelés tárgyaként megadott konkrét adatkezelési művelet értékelése során a tanúsítási szempontok szolgálnak összehasonlítási alapként. Ez, a tanúsítási szempontok meghatározására vonatkozó iránymutatás általános tanácsokkal szolgál, ezáltal megkönnyíti a tanúsítási szempontok jóváhagyás céljából végzett értékelését.

    - A tanúsítási szempontok jóváhagyásakor vagy meghatározásakor a következő általános megfontolásokat kell figyelembe venni. A tanúsítási szempontokra vonatkozó követelmények:
    - legyenek egységesek és ellenőrizhetők,
    - legyenek ellenőrizhetők, hogy megkönnyítsék az adatkezelési műveletek általános adatvédelmi rendelet szerinti értékelését, különösen azáltal, hogy meghatározzák a célkitűzéseket és végrehajtási iránymutatást adnak azok elérése érdekében;
    - legyenek relevánsak a célcsoport szempontjából (pl. „B2B”, azaz vállalkozások közötti, és „B2C”, azaz vállalkozások és fogyasztók közötti kapcsolatok);
    - vegyék figyelembe és adott esetben legyenek interoperábilisak más szabványokkal (többek között az ISO-szabványokkal és a nemzeti szintű szabványokkal); valamint
    - legyenek rugalmasak és méretezhetőek annak érdekében, hogy lehetővé tegyék a különböző típusú és méretű szervezetek – köztük a mikro-, kis- és középvállalkozások – 42. cikk (1) bekezdése szerinti értékelését, valamint a (77) preambulumbekezdés szerinti kockázatalapú megközelítés alkalmazását.

68. Egy kis helyi vállalat, mint például egy kiskereskedő, általában kevésbé összetett adatkezelési műveleteket végez, mint egy nagy multinacionális vállalat. Habár az adatkezelési műveletek jogszerűségére vonatkozó követelmények azonosak, figyelembe kell venni az adatkezelés körét és összetettségét is; következésképpen a tanúsítási mechanizmusoknak és a tanúsítási szempontoknak méretezhetőnek kell lenniük, hogy illeszkedjenek az adott adatkezelési tevékenységhez.

6.1 Már meglévő szabványok

69. A tanúsító szervezeteknek ügyelniük kell arra, hogy a konkrét szempontok miként veszik figyelembe a már meglévő eszközöket, például a magatartási kódexeket, a műszaki szabványokat, vagy a nemzeti szabályozási és jogi kezdeményezéseket. Az ideális az, ha a szempontok interoperábilisak a meglévő szabványokkal, mivel ez segítheti az adatkezelőt vagy az adatfeldolgozót az általános adatvédelmi rendelet szerinti kötelezettségeik teljesítésében. Míg az ágazati szabványok gyakran arra összpontosítanak, hogy a szervezet milyen védelmi és biztonsági intézkedéseket alkalmaz a fenyegetésekkel szemben, addig az általános adatvédelmi rendelet középpontjában a természetes személyek alapvető jogainak védelme áll. Ezt a különböző nézőpontot figyelembe kell venni a szempontok kialakításakor, illetve az ágazati szabványokon alapuló szempontok vagy tanúsítási mechanizmusok jóváhagyásakor.

6.2 A szempontok meghatározása

70. A tanúsítási szempontoknak meg kell felelniük a tanúsítási mechanizmus vagy rendszer tanúsítási nyilatkozatának (üzenet vagy állítás), valamint az abban megfogalmazott elvárásoknak. Már a tanúsítási mechanizmus neve is kijelölheti az alkalmazási kört, és befolyásolhatja a szempontok meghatározására.

71. [3. példa]

    Egy „HealthPrivacyMark” elnevezésű mechanizmus alkalmazási körének az egészségügyi ágazatra kell korlátozódnia. A bélyegző neve azt sugallja, hogy megvizsgálták az egészségügyi adatokkal kapcsolatos adatvédelmi előírásoknak való megfelelést. Ennek megfelelően ennek a mechanizmusnak alkalmasnak kell lennie az erre az ágazatra vonatkozó adatvédelmi követelmények értékelésére.

72. [4. példa]

    Egy olyan mechanizmusnak, amely az adatkezelési irányítási rendszer által végzett adatkezelési műveletek tanúsítására vonatkozik, meg kell határoznia azokat a szempontokat, amelyek lehetővé teszik az irányítási folyamatok és az azokat támogató technikai és szervezeti intézkedések elismerését és értékelését.

73. [5. példa]

    Egy felhőalapú számítástechnikához kapcsolódó mechanizmus szempontjainak figyelembe kell venniük a felhőalapú szolgáltatások használatához szükséges különleges műszaki követelményeket. Ha például a szervereket az Unión kívül használják, a szempontoknak figyelembe kell venniük az általános adatvédelmi rendelet V. fejezetében foglalt, az adatok harmadik országokba irányuló továbbítására vonatkozó feltételeket.

74. Azoknak a szempontoknak, amelyeket úgy alakítottak ki, hogy az értékelés különféletárgyaihoz illeszkedjenek és különböző ágazatokban és/vagy tagállamokban is alkalmazhatóak legyenek az alábbi követelményeknek kell megfelelniük: alkalmazhatónak kell lenniük különböző esetekre; lehetővé kell tenniük a kis, közepes vagy nagy adatkezelési műveletekhez illeszkedő intézkedések azonosítását, és az általános adatvédelmi rendelettel összhangban figyelembe kell venniük a természetes személyek jogait és szabadságait érintő, különböző valószínűségű és súlyú kockázatokat; Következésképpen a szempontokat kiegészítő (például a dokumentálásra, a tesztelésre vagy az értékelés módszerére és mélységre vonatkozó)

tanúsítási eljárásoknak meg kell felelniük ezeknek az elvárásoknak, valamint lehetővé kell tenniük és szabályozniuk kell például a vonatkozó szempontok egyedi tanúsítási projektek keretében való alkalmazását. A szempontoknak segíteniük kell annak értékelését, hogy a megfelelő technikai és szervezeti intézkedések végrehajtása kellően biztosított-e.

6.3 A tanúsítási szempontok időtállósága

75. Habár a tanúsítási szempontoknak hosszú távon is megbízhatónak kell lenniük, azokat nem kell kőbe vésni, hanem felül kell vizsgálni, például az alábbi esetekben:

    - ha a jogi keret módosul;
    - ha a feltételeket és rendelkezéseket az Európai Bíróság ítéletei értelmezik; vagy
    - műszaki haladás történt.

Az Európai Adatvédelmi Testület részéről

az elnök

(Andrea Jelinek)

1. MELLÉKLET: A FELÜGYELETI HATÓSÁGOKNAK AZ ÁLTALÁNOS ADATVÉDELMI RENDELET SZERINTI TANÚSÍTÁSSAL KAPCSOLATOS FELADATAI ÉS HATÁSKÖRE

	Rendelkezések	Követelmények
Feladatok	43. cikk, (6) bekezdés	Előírja, hogy a felügyeleti hatóság könnyen hozzáférhető formában közzétegye és a Testület részére továbbítsa a 42. cikk (5) bekezdésében említett szempontokat.
	57. cikk, (1) bekezdés, n) pont	Előírja, hogy a felügyelő hatóság a 42. cikk (5) bekezdésének megfelelően jóváhagyja a tanúsítási szempontokat.
	57. cikk, (1) bekezdés, o) pont	Úgy rendelkezik, hogy a felügyelő hatóság adott esetben (vagyis amennyiben tanúsítványokat állít ki) rendszeres időközönként felülvizsgálja a 42. cikk (7) bekezdésének megfelelően kiállított tanúsítványokat.
	64. cikk, (1) bekezdés, c) pont	Előírja, hogy a felügyelő hatóság a 42. cikk (5) bekezdés említett tanúsítási szempontok jóváhagyása során közölje a határozattervezetet a Testülettel.
Hatáskörök	58. cikk, (1) bekezdés, c) pont	Kimondja, hogy a felügyelő hatóság hatáskörrel rendelkezik arra, hogy elvégezze a 42. cikk (7) bekezdésének megfelelően kiadott tanúsítványok felülvizsgálatát.
	58. cikk, (2) bekezdés, h) pont	Kimondja, hogy a felügyeleti hatóság hatáskörrel rendelkezik arra, hogy visszavonja a tanúsítványt vagy utasítsa a tanúsító szervezetet egy tanúsítvány visszavonására, vagy utasítsa a tanúsító szervezetet, hogy ne állítson ki tanúsítványt.
	58. cikk, (3) bekezdés, e) pont.	Kimondja, hogy a felügyeleti hatóság hatáskörrel rendelkezik a tanúsító szervezetek akkreditálására.
	58. cikk, (3) bekezdés, f) pont	Kimondja, hogy a felügyeleti hatóság hatáskörrel rendelkezik tanúsítványok kiállítására és a tanúsítási szempontok jóváhagyására.

2. MELLÉKLET

1 BEVEZETÉS

A 2. melléklet iránymutatást ad a 42. cikk (5) bekezdése szerinti tanúsítási szempontok felülvizsgálatához és értékeléséhez. Meghatározza azokat a kérdésköröket, amelyeket az adatvédelmi felügyeleti hatóságok és az Európai Adatvédelmi Testület a tanúsítási mechanizmus részét képező tanúsítási szempontok jóváhagyása során figyelembe vesznek és alkalmaznak. A kérdéseket figyelembe kell venniük azoknak a tanúsító szerveknek és rendszertulajdonosoknak, akik vagy amelyek ilyen szempontokat kívánnak kidolgozni és jóváhagyásra benyújtani. A felsorolás nem teljes, csak a figyelembe veendő kérdések minimális körét mutatja be. Nem minden kérdés alkalmazandó; mindazonáltal azokat figyelembe kell venni a szempontok kidolgozása során, és ismertetni kell, hogy egyes szempontok miért nem terjednek ki a bizonyos területekre. Néhány kérdés ismétlődik, mivel különböző nézőpontokra utalnak. Ezt az iránymutatást az általános adatvédelmi rendelet és – adott esetben – a nemzeti jogszabályok által előírt jogi követelményeknek megfelelően kell figyelembe venni.

2 A TANÚSÍTÁSI MECHANIZMUS ALKALMAZÁSI KÖRE ÉS AZ ÉRTÉKELÉS CÉLJA

a) A leírás alapján egyértelmű-e a tanúsítási mechanizmus alkalmazási köre (amelyre vonatkozóan az adatvédelmi szempontokat alkalmazni kell)?

b) A tanúsítási mechanizmus alkalmazási köre érdemi-e a célközönség számára, és nem lehet-e félrevezető?

- *Példa: A „Megbízható vállalkozás” („Trusted Company”) bélyegző arra utal, hogy egy egész vállalat adatkezelési tevékenységét auditálták, holott ténylegesen csak meghatározott adatkezelési műveletek – például az online fizetési eljárás – tartoznak tanúsítási kötelezettség alá. Az alkalmazási kör ezért félrevezető.*

c) A tanúsítási mechanizmus alkalmazási köre tükrözi-e az adatkezelési műveletek minden lényeges szempontját?

- *Példa: „Az egészségügyi adatok védelmét tanúsító jelölés” („Privacy Health Mark”) az egészséggel kapcsolatos minden értékelési adatot magában kell, hogy foglaljon a 9. cikk szerinti követelmények teljesítése érdekében.*

d) A tanúsítási mechanizmus alkalmazási köre lehetővé teszi-e az érdemi adatvédelmi tanúsítást, figyelembe véve a kapcsolódó adatkezelési műveletek jellegét, tartalmát és kockázatát?

- *Példa: Ha a tanúsítási mechanizmus alkalmazási köre csak az adatkezelési műveletek olyan konkrét szempontjaira összpontosít, mint például az adatgyűjtés, míg a további adatkezelési műveletekre nem (ideértve például a reklámprofilok létrehozása vagy az érintettek jogainak kezelése céljából végzett adatfeldolgozást), az alkalmazási kör nem lenne érdemi az érintettek számára.*

e) A tanúsítási mechanizmus hatálya az alkalmazás helye szerinti országban végzett személyesadat-kezelésre terjed-e ki, vagy határon átnyúló adatkezelésre és/vagy -továbbításra vonatkozik?

f) A tanúsítási szempontok kellő részletességgel leírják-e, hogy hogyan kell meghatározni az értékelés célját?

- *Példa: Az általános alkalmazási körrel rendelkező adatvédelmi bélyegző („Privacy Seal"), amely csak „a tanúsítás tárgyát képező adatkezelés pontos megjelölését" írja elő, de az értékelés céljának meghatározásához és leírásához nem nyújt elég útmutatást.*
- *Példa: „A személyes adatok biztonságos tárolását tanúsító bélyegző" („Privacy Vault Seal") (specifikus) alkalmazási köre a biztonságos tárolás kezelését szolgálja. Annak részletesen ismertetnie kell azokat a követelményeket, amelyek az ezen alkalmazási kör teljesítéséhez szükséges szempontoknak való megfelelést célozzák, például a biztonságos tárhely fogalommeghatározása, a rendszerkövetelmények, a kötelező technikai és szervezési intézkedések. Ebben az esetben az alkalmazási körből egyértelműen meghatározható az értékelés célja.*

(1) A tanúsítási szempontok megkövetelik-e, hogy az értékelés céljára vonatkozó leírás magában foglalja az összes vonatkozó adatkezelési művelet azonosítását, az adatáramlások szemléltetését, továbbá meghatározza az értékelés céljának alkalmazási területét?

- *Példa: A tanúsítási mechanizmus az általános adatvédelmi rendelet alapján tanúsítja az adatkezelők adatkezelési műveleteit anélkül, hogy részletesebben meghatározná az alkalmazási területet (általános hatály). A mechanizmus által alkalmazott szempontok alapján a kérelmező adatkezelőnek meg kell határoznia a célzott adatkezelési műveletet az adattípus, -rendszer és -folyamat tekintetében.*

(2) A tanúsítási szempontok alapján a kérelmezőnek egyértelművé kell-e tennie, hogy az értékelés tárgyát képező adatkezelés mikor kezdődik és mikor ér véget? A tanúsítási szempontok megkövetelik-e, hogy az értékelés célja kiterjedjen azokra az interfészekre is, amelyek tekintetében az egymástól kölcsönösen függő adatkezelési műveletek nem képezik az értékelés céljának részét? Ez kellően indokolt-e?

- *Példa: Az értékelés célja, amely kell részletességgel leírja a valamely webalapú szolgáltatásra vonatkozó adatkezelési műveletet, ideértve a felhasználók nyilvántartásba vételét, a szolgáltatásnyújtást, a számlázást, a IP-címek naplózását, a felhasználók és harmadik felek rendelkezésére álló interfészeket, a tárhelyet biztosító szerver kivételével (az adatkezelésre és a technikai és szervezési intézkedésekre vonatkozó megállapodásokra azonban kitérve).*

g) Biztosítják-e a tanúsítási szempontok azt, hogy az (egyedi) értékelési célok érthetőek legyenek a célközönség számára, ideértve adott esetben az érintetteket is?

3 ÁLTALÁNOS KÖVETELMÉNYEK

a) A tanúsítási szempontok katalógusában (azaz a tanúsítási szempontok teljes körű felsorolásában) szereplő összes fogalmat megfelelően azonosították, elmagyarázták és ismertették-e?

b) Azonosítottak-e minden normatív hivatkozást?

c) A tanúsítási szempontok magukban foglalják-e a tanúsítási mechanizmus hatálya alá tartozó adatvédelmi kötelezettségek, eljárások és adatkezelés meghatározását?

4 ADATKEZELÉSI MŰVELET – A 42. CIKK (1) BEKEZDÉSE

A tanúsítási mechanizmus alkalmazási köre tekintetében (általános vagy konkrét) a tanúsítási szempontok foglalkoznak-e az adatkezelési műveletek (adatok, rendszerek és eljárások) valamennyi releváns elemével?

a) Megkövetelik-e a tanúsítási szempontok az adatkezelés érvényes jogalapjának azonosítását az értékelés célja tekintetében?

b) Ami az értékelés célját illeti, elismerik-e a tanúsítási szempontok az adatkezelés érintett szakaszait és az adatok teljes életciklusát, beleértve a törlést és az anonimizálást?

c) Az értékelés célja tekintetében megkövetelik-e a tanúsítási szempontok az adatok hordozhatóságát?

d) Az értékelés célja tekintetében lehetővé teszik-e a tanúsítási szempontok a különleges adatkezelési műveletek – például az automatizált döntéshozatal, a profilalkotás – azonosítását és az azokra való hivatkozást?

e) Az értékelés célja tekintetében lehetővé teszik-e a tanúsítási szempontok különleges adatkategóriák azonosítását?

f) A tanúsítási szempontok lehetővé teszik-e és előírják-e az egyes adatkezelési műveletek kockázatértékelését, valamint az érintettek jogainak és szabadságainak védelmét garantáló szükségleteinek felmérését?

g) A tanúsítási szempontok lehetővé teszik-e és előírják-e a természetes személyek jogait és szabadságait érintő kockázatok megfelelő figyelembevételét?

…

5 AZ ADATKEZELÉS JOGSZERŰSÉGE

a) A tanúsítási szempontok előírják-e az egyes adatkezelési műveletek jogszerűségének ellenőrzését az adatkezelés célját és szükségességét tekintve?

b) A tanúsítási szempontok előírják-e az egyes adatkezelési műveletek jogalapjára vonatkozó valamennyi követelmény ellenőrzését?

6 ELVEK – 5. CIKK

a) A tanúsítási szempontok megfelelően kezelik-e az 5. cikk szerinti valamennyi adatvédelmi elvet?

b) A tanúsítási szempontok előírják-e az adattakarékosság szemléltetését az egyes értékelési célok tetkintetében?

…

7 AZ ADATKEZELŐK ÉS AZ ADATFELDOLGOZÓK ÁLTALÁNOS KÖTELEZETTSÉGEI

a) A tanúsítási szempontok előírják-e az adatkezelők és az adatfeldolgozók közötti szerződéses megállapodások meglétének igazolását?

b) Alávetik-e értékelésnek az adatkezelők és az adatfeldolgozók közötti megállapodásokat?

c) A tanúsítási szempontok tükrözik-e az adatkezelő IV. fejezet szerinti kötelezettségeit?

d) A tanúsítási szempontok előírják-e az adatkezelő által a 24. cikk (1) bekezdése alapján végzett technikai és szervezeti intézkedések felülvizsgálatának és frissítésének igazolását?

e) A tanúsítási szempontok közé tartozik-e annak ellenőrzése, hogy a szervezet értékelte-e egy, a 37. cikk által előírt adatvédelmi tisztviselő kijelölésének szükségességét? Adott esetben az adatvédelmi tisztviselő megfelel-e a 37–39. cikk szerinti követelményeknek?

f) A tanúsítási szempontok ellenőrzik-e azt, hogy kötelező-e nyilvántartást vezetni az adatkezelési tevékenységekről a 30. cikk (5) bekezdésével összhangban, valamint megfelelően eleget tesznek-e a 30. cikkben említett követelményeknek?

8 AZ ÉRINTETTEK JOGAI

a) A tanúsítási szempontok megfelelően foglalkoznak-e az érintettek tájékoztatáshoz való jogával, és előírják-e megfelelő intézkedések bevezetését?

b) A tanúsítási szempontok előírják-e azt, hogy az érintettek számára megfelelő vagy akár nagyobb mértékben biztosítani kell, hogy hozzáférhessenek az adataikhoz és azok felett rendelkezhessenek, ideértve az adathordozhatóságot is?

c) A tanúsítási szempontok megkövetelik-e olyan intézkedések bevezetését, amelyek lehetővé teszik az adatkezelési műveletbe való beavatkozást az érintettek jogainak biztosítása érdekében, továbbá lehetővé teszik a javítást, törlést vagy korlátozást?

…

9 A TERMÉSZETES SZEMÉLYEK JOGAIT ÉS SZABADSÁGAIT ÉRINTŐ KOCKÁZATOK

a) A tanúsítási szempontok lehetővé teszik-e és előírják-e a természetes személyek jogait és szabadságait érintő kockázatok értékelését?

b) A tanúsítási szempontok biztosítanak-e vagy előírnak-e elismert kockázatértékelési módszert? Amennyiben igen, arányos-e ez a módszer?

c) A tanúsítási szempontok lehetővé teszik-e és előírják-e annak értékelését, hogy a tervezett adatkezelési műveletek milyen hatást gyakorolnak a természetes személyek jogaira és szabadságaira?

d) A tanúsítási szempontok előírnak-e előzetes konzultációt az adatvédelmi hatásvizsgálat eredményei szerint f fennmaradó azon kockázatokról, amelyeket nem lehetne csökkenteni?

10 A VÉDELMET GARANTÁLÓ TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK

a) A tanúsítási szempontok előírják-e az adatkezelési műveletek bizalmas jellegével kapcsolatos technikai és szervezési intézkedések alkalmazását?

b) A tanúsítási szempontok előírják-e az adatkezelési műveletek integritásával kapcsolatos technikai és szervezési intézkedések alkalmazását?

c) A tanúsítási szempontok előírják-e az adatkezelési műveletek hozzáférhetőségével kapcsolatos technikai és szervezési intézkedések alkalmazását?

d) A tanúsítási szempontok előírják-e olyan intézkedések alkalmazását, amelyek biztosítják az adatkezelési műveletek átláthatóságát a következők tekintetében:

e) elszámoltathatóság;

f) az érintettek jogai;

g) az egyes adatkezelési műveletek értékelése (pl. az algoritmusok átláthatósága tekintetében)?

h) A tanúsítási szempontok előírják-e az érintettek jogait garantáló technikai és szervezési intézkedések alkalmazását, például az információszolgáltatási képességet vagy az adathordozhatóságot?

i) A tanúsítási szempontok megkövetelik-e olyan technikai és szervezési intézkedések alkalmazását, amelyek lehetővé teszik az adatkezelési műveletbe való beavatkozást az érintettek jogainak biztosítása érdekében, továbbá lehetővé teszik a javítást, törlést vagy korlátozást?

j) A tanúsítási szempontok előírják-e olyan intézkedések alkalmazását, amelyek lehetővé teszik az adatkezelési műveletbe való beavatkozást a rendszer vagy a folyamat javítása vagy ellenőrzése céljából?

k) A tanúsítási szempontok megkövetelik-e olyan technikai és szervezési intézkedések alkalmazását, amelyek biztosítják az adatminimalizálást, például az adatok és az érintettek közötti kapcsolat megszüntetését vagy ezek elkülönítését, az adatrendszerek anonimizálását vagy álnevesítését vagy elszigetelését?

l) A tanúsítási szempontok előírják-e az alapértelmezett adatvédelmet biztosító technikai intézkedések bevezetését?

m) A tanúsítási szempontok megkövetelik-e a beépített adatvédelmet biztosító technikai és szervezési intézkedések alkalmazását, például egy olyan adatvédelmi irányítási rendszer bevezetését, amely az adatvédelmi követelményeket szemlélteti, azokról tájékoztatást nyújt, gondoskodik a követelmények végrehajtásáról és annak ellenőrzéséről?

n) A tanúsítási szempontok megkövetelik-e olyan technikai és szervezési intézkedések alkalmazását, amelyek a személyes adatokhoz állandó vagy rendszeres hozzáféréssel rendelkező személyzet számára megfelelő, rendszeres képzést és oktatást biztosítanak?

o) A tanúsítási szempontok előírják-e az intézkedések felülvizsgálatát?

p) A tanúsítási szempontok előírják-e az önértékelést/belső ellenőrzést?

q) A tanúsítási szempontok előírnak-e intézkedéseket annak biztosítására, hogy a személyes adatok megsértésével kapcsolatos értesítési feladatokat kellő időben és körben elvégezzék?

r) A tanúsítási szempontok megkövetelik-e a biztonsági események kezelésére szolgáló eljárások bevezetését és ellenőrzését?

s) A tanúsítási szempontok előírják-e az adatvédelem és a technológia fejlődésével kapcsolatos kérdések nyomon követését, valamint szükség esetén a rendszer frissítését?

…

11 AZ ADATVÉDELMET SZOLGÁLÓ EGYÉB KÜLÖNLEGES JELLEMZŐK

a) A tanúsítási szempontok előírják-e az adatvédelmet javító technikák végrehajtását? Ezek közé tartozhatnak az olyan szempontok is, amelyek az adatvédelem fokozását célozzák a személyes adatok és/vagy az adatvédelmi kockázat megszüntetése vagy csökkentése útján.

- *Példa: Az olyan tanúsítási szempontok, amelyek megkövetelik az összekapcsolhatatlanság javítását oly módon, hogy felhasználó-központú személyazonosság-kezelést (például attribútum-alapú hitelesítési adatokat) alkalmaznak a szervezetközpontú személyazonosság-kezelés helyett, az adatvédelmet javító technikáknak tekinthetők.*

b) A tanúsítási szempontok előírják-e az önrendelkezés és a választás megkönnyítése érdekében olyan intézkedések végrehajtását, amelyek az érintetteknek megfelelőbb lehetőségeket biztosítanak arra, hogy rendelkezhessenek adataik felett ?

…

12 A SZEMÉLYES ADATOK TOVÁBBÍTÁSÁVAL KAPCSOLATOS MEGFELELŐ BIZTOSÍTÉKOK MEGLÉTÉT IGAZOLÓ TANÚSÍTÁSI SZEMPONTOK

Ezekkel a tanúsítási szempontokkal a 42. cikk (2) bekezdésről szóló, hamarosan közzéteendő iránymutatás foglalkozik majd.

13 AZ EURÓPAI ADATVÉDELMI BÉLYEGZŐVEL KAPCSOLATOS TOVÁBBI TANÚSÍTÁSI SZEMPONTOK

a) Tervezik-e a tanúsítási szempontok valamennyi tagállamra történő kiterjesztését?

b) A tanúsítási szempontok alkalmasak-e arra, hogy figyelembe vegyék az egyes tagállamok adatvédelmi jogszabályait vagy forgatókönyveit?

c) A tanúsítási szempontok előírják-e az egyes értékelési célok értékelését az ágazatspecifikus tagállami adatvédelmi jogszabályok fényében?

d) A tanúsítási szempontok értelmében az adatkezelő vagy az adatfeldolgozó köteles-e a tagállamok hivatalos nyelvein megküldeni az érintetteknek és az érdekelt feleknek

e) az adatkezelésről/az értékelés céljáról szóló tájékoztatást?

f) az adatkezelés/az értékelés céljának dokumentációját?

g) az értékelés eredményeit?

…

14 A TANÚSÍTÁSI SZEMPONTOK ÁTFOGÓ ÉRTÉKELÉSE

a) A tanúsítási szempontok teljes mértékben lefedik-e a tanúsítási mechanizmus alkalmazási körét (azaz átfogó tanúsítási szempontokról van-e szó), megfelelő garanciát nyújtva a tanúsítás megbízhatóságának biztosításához?

- *Példa: Amennyiben a tanúsítási mechanizmus alkalmazási köre az egészségügyi adatokkal kapcsolatos adatkezelési műveletekre összpontosít, magas szintű adatvédelmet kell biztosítani olyan tanúsítási szempontok meghatározásával, amelyek biztosítják például a részletes értékelést, valamint a beépített adatvédelem és az alapértelmezett adatvédelem elvének alkalmazását.*

b) Arányosak-e a tanúsítási szempontok a tanúsítási mechanizmus alkalmazási körében elvégzendő adatkezelési művelet méretével, az információk érzékenységével és az adatkezelési kockázattal?

c) Valószínűsíthető-e, hogy a tanúsítási szempontoknak köszönhetően az adatkezelők és -feldolgozók jobban megfelelnek az adatvédelmi szabályoknak?

d) A tanúsítási szempontok az érintettek javát szolgálják-e majd a tájékoztatáshoz való jogukat illetően, ideértve a kívánt eredmények magyarázatát is az érintettek számára?