Az általános adatvédelmi rendelet ((EU) 2016/679 rendelet) 43. cikke szerinti tanúsító szervezetek akkreditálásáról szóló 4/2018. számú iránymutatások

Translations proofread by EDPB Members.

This language version has not yet been proofread.

3.0. változat

2019. június 4.

Elfogadva

Korábbi változatok

3.0. változat	2019. június 4.	Az 1. melléklet belefoglalása a dokumentumba (az 1. melléklet 2.0. változatát a nyilvános konzultációt követően 2019. június 4-én fogadták el)
(2.0. változat)	2018. december 4.	Az iránymutatások elfogadása a nyilvános konzultációt követően – Ugyanebben az időpontban elfogadták az 1. mellékletet (1.0. változat) nyilvános konzultációra
1.0. változat	2018. február 6.	A 29. cikk alapján létrehozott munkacsoport által elfogadott iránymutatások (a nyilvános konzultációra szánt változat). Ezt a változatot az Európai Adatvédelmi Testület 2018. május 25-én hagyta jóvá.

Tartalomjegyzék

Az Európai Adatvédelmi Testület

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) pontja értelmében

figyelembe véve az iránymutatásokról 2018. februárban és a mellékletről 2018. december 14. és 2019. február 1. között tartott nyilvános konzultáció eredményét az általános adatvédelmi rendelet 70. cikke (4) bekezdésének megfelelően,

ELFOGADTA A KÖVETKEZŐ IRÁNYMUTATÁSOKAT

1 BEVEZETÉS

1. A 2018. május 25-én hatályba lépő általános adatvédelmi rendelet (az (EU) 2016/679 rendelet) korszerűsített, elszámoltathatóságra és alapvető jogokra épülő megfelelőségi keretet biztosít az adatvédelemre vonatkozóan Európában. Az általános adatvédelmi rendelet rendelkezéseinek való megfelelést elősegítő számos intézkedés központi szerepet játszik ebben az új keretrendszerben. Ezek magukban foglalják az egyedi körülmények között kötelező követelményeket (ideértve az adatvédelmi tisztviselők kinevezését és az adatvédelmi hatásvizsgálatok elvégzését), valamint az önkéntes – például a magatartási kódexeket és a tanúsítási mechanizmusokat érintő – intézkedéseket.

2. A tanúsítási mechanizmusok, valamint adatvédelmi bélyegzők, illetve jelölések létrehozása érdekében az általános adatvédelmi rendelet 43. cikkének (1) bekezdése előírja, hogy a tagállamoknak biztosítaniuk kell, hogy a 42. cikk (1) bekezdése értelmében tanúsítványt kibocsátó tanúsító szervezetek akkreditálva legyenek az illetékes felügyeleti hatóság vagy a nemzeti akkreditáló testület vagy mindkettő által. Ha az akkreditációt a nemzeti akkreditáló testület az ISO/IEC 17065/2012 szabvány szerint végzi, akkor az illetékes felügyeleti hatóság által megállapított kiegészítő követelményeket is alkalmazni kell.

3. A megfelelő tanúsítási mechanizmusok elősegíthetik az általános adatvédelmi rendeletnek való megfelelést és növelhetik az átláthatóságot az érintettek számára és a vállalatközi kapcsolatok terén, például az adatkezelők és az adatfeldolgozók között. Az adatkezelőket és adatfeldolgozókat független harmadik fél hitelesíti az adatkezelési műveleteik megfelelésének bizonyítása érdekében[1].

4. Ebben az összefüggésben az Európai Adatvédelmi Testület elismeri, hogy szükség van akkreditációval kapcsolatos iránymutatások biztosítására. Az akkreditáció különös értéke és

[1] Az általános adatvédelmi rendelet (100) preambulumbekezdése szerint a tanúsítási mechanizmusok létrehozása elősegítheti az átláthatóságot és a rendeletnek való megfelelést, valamint lehetővé teszi az érintettek számára, hogy értékeljék az adott termékek és szolgáltatások adatvédelmi szintjét.

célja abban rejlik, hogy a tanúsító szervezetek alkalmasságáról hiteles nyilatkozatot biztosít, amely lehetővé teszi a tanúsítási mechanizmusba vetett bizalom növelését.

5. Az iránymutatások célja, hogy segítséget nyújtsanak az általános adatvédelmi rendelet 43. cikkében foglalt rendelkezések értelmezéséhez és végrehajtásához. Különösen arra irányulnak, hogy segítsenek a tagállamoknak, a felügyeleti hatóságoknak és a nemzeti akkreditáló testületeknek a tanúsítványt kibocsátó tanúsító szervezetek akkreditálásának következetes és összehangolt alapjait kialakítani az általános adatvédelmi rendeletnek megfelelően.

2 AZ IRÁNYMUTATÁSOK ALKALMAZÁSI KÖRE

6. Ezek az iránymutatások:

- meghatározzák az akkreditáció célját az általános adatvédelmi rendelettel összefüggésben;
- ismertetik a tanúsító szervezetek számára a 43. cikk (1) bekezdésével összhangban rendelkezésre álló akkreditációs lehetőségeket, és azonosítják a kulcsfontosságú kérdéseket;
- keretet biztosítanak a kiegészítő akkreditációs követelmények megállapításához, amikor az akkreditációt a nemzeti akkreditáló testület kezeli; továbbá
- keretet biztosítanak az akkreditációs követelmények megállapításához, amikor az akkreditációt a felügyeleti hatóság kezeli.

7. Az iránymutatások nem szolgálnak eljárási kézikönyvként a tanúsító szervezetek akkreditálásához az általános adatvédelmi rendelettel összhangban. Továbbá nem jelentetnek meg új technikai szabványt a tanúsító szervezetek akkreditálására az általános adatvédelmi rendelet alkalmazásában.

8. Az iránymutatások címzettjei:

- a tagállamok, amelyeknek biztosítaniuk kell, hogy a tanúsító szervezeteket a felügyeleti hatóság és/vagy a nemzeti akkreditáló testület akkreditálja;
- a 43. cikk (1) bekezdésének b) pontja értelmében tanúsító szervezetek akkreditációját végző nemzeti akkreditáló testületek;
- az ISO/IEC 17065/2012 szabványban[2] szereplőkön túl a „kiegészítő követelményeket” meghatározó illetékes felügyeleti hatóság, ha az akkreditációt a nemzeti akkreditáló testület végzi a 43. cikk (1) bekezdésének b) pontja értelmében;
- az Európai Adatvédelmi Testület, ha az illetékes felügyeleti hatóság akkreditációs követelményeiről véleményt ad ki vagy jóváhagyja őket a 43. cikk (3) bekezdése, a 70. cikk (1) bekezdésének p) pontja és a 64. cikk (1) bekezdésének c) pontja értelmében;
- az akkreditációs követelményeket meghatározó illetékes felügyeleti hatóság, amennyiben az akkreditációt a felügyeleti hatóság végzi a 43. cikk (1) bekezdésének a) pontja értelmében;
- más érdekelt felek, például a leendő tanúsító szervezetek vagy tanúsítási rendszerek tulajdonosai, amelyek tanúsítási kritériumokat és eljárásokat biztosítanak[3].

[2] Nemzetközi Szabványügyi Szervezet: Megfelelőségértékelés – A termékek, folyamatok és szolgáltatások tanúsítását végző szervezetekre vonatkozó követelmények.

9. Fogalommeghatározások

10. Az alábbi fogalommeghatározások célja az akkreditációs folyamat alapvető elemei közös megértésének elősegítése. Ezeket referenciapontoknak kell tekinteni, és nem vetnek fel kétségeket arra vonatkozóan, hogy megtámadhatatlanok. A jelen fogalommeghatározások a meglévő szabályozási kereteken és szabványokon alapulnak, különösen az általános adatvédelmi rendelet vonatkozó rendelkezésein és az ISO/IEC 17065/2012 szabvány előírásain.

11. Ezen iránymutatások alkalmazásában az alábbi fogalommeghatározásokat kell alkalmazni:

12. „*akkreditáció*": a tanúsító szervezetek akkreditációjáról a 3. pontban (Az „akkreditáció" fogalmának értelmezése az általános adatvédelmi rendelet 43. cikkének alkalmazásában) található bővebb információ;

13. „*kiegészítő követelmények*": az illetékes felügyeleti hatóság által megállapított kiegészítő követelmények, amelyeknek az akkreditáció során meg kell felelni[4];

14. „*tanúsítás*": annak értékelése és független harmadik fél általi igazolása[5], hogy a tanúsítási kritériumok teljesítése bizonyítva lett;

15. „*tanúsító szervezet*": tanúsítási mechanizmust[6] működtető, harmadik felek körébe tartozó megfelelőségértékelő[7] szervezet[8];

16. „*tanúsítási rendszer*": meghatározott termékekre, folyamatokra és szolgáltatásokra vonatkozó tanúsítási rendszer, amelyre ugyanazokat a meghatározott követelményeket, egyedi szabályokat és eljárásokat kell alkalmazni[9];

17. azok a kritériumok, amelyek szerint a tanúsítást (megfelelőségértékelés) elvégzik; „nemzeti akkreditáló testület"[10];

---

[3] A rendszerek tulajdonosai olyan azonosítható szervezetek, amelyek tanúsítási kritériumokat és követelményeket állapítanak meg, amelyek szerint a megfelelőség értékelésre kerül. Az akkreditáció a tanúsítási rendszer követelményeinek való megfelelés értékelését végző szervezeté (a 43. cikk (4) bekezdése), amely a tanúsítványok kiadásával is foglalkozik (azaz a tanúsító szervezeté, más néven a megfelelőségértékelő szervezeté). Az értékeléseket végző szervezet lehet ugyanaz a szervezet, amely kifejlesztette és tulajdonosa a rendszernek, de lehetnek olyan megállapodások is, ahol egy szervezet tulajdonosa a rendszernek, és egy másik (vagy több) szervezet végzi el az értékelést.

[4] A 43. cikk (1), (3) és (6) bekezdése.

[5] Fontos megjegyezni, hogy az ISO 17000 szabvány szerint a harmadik fél által kiadott igazolás (tanúsítvány) „a megfelelőségértékelés minden tárgyára alkalmazandó" (5.5.) „kivéve a megfelelőségértékelő szervezetekre, amelyek esetében az akkreditációt kell alkalmazni" (5.6.). Az általános adatvédelmi rendelet 42. cikkének (1) és (5) bekezdése

[6] Lásd az általános adatvédelmi rendelet 42. cikkének (1) bekezdése és 42. cikkének (5) bekezdése.

[7] A harmadik fél általi megfelelőségértékelési tevékenységet olyan szervezet végzi, amely független a tárgyat biztosító személytől vagy szervezettől, valamint az adott tárgyat érintő felhasználói érdekektől, vö. az ISO 17000 szabvány 2.4. pontjával.

[8] Lásd az ISO 17000 szabvány 2.5. pontját: „megfelelőségértékelési szolgáltatásokat végző szervezet"; az ISO 17011 szabványt: „megfelelőségértékelési szolgáltatásokat végző szervezet, amely képezheti az akkreditáció tárgyát"; az ISO 17065 szabvány 3.12. pontját.

[9] Lásd a 3.9. pontot az ISO 17065 szabvány B. mellékletével összefüggésben értelmezve.

18. „kritériumok” vagy „tanúsítási kritériumok”: a 765/2008/EK európai parlamenti és tanácsi rendelet szerint kinevezett egyetlen tagállami szerv, amely akkreditációt végez az államtól kapott jogkörénél fogva[11].

3 AZ „AKKREDITÁCIÓ” FOGALMÁNAK ÉRTELMEZÉSE AZ ÁLTALÁNOS ADATVÉDELMI RENDELET 43. CIKKÉNEK ALKALMAZÁSÁBAN

19. Az általános adatvédelmi rendeletben nem kerül meghatározásra az „akkreditáció” fogalma. A 765/2008/EK rendelet 2. cikkének (10) bekezdése – amely meghatározza az akkreditációra vonatkozó általános követelményeket – az akkreditációt a következőképp definiálja:

20. „a nemzeti akkreditáló testület tanúsítása arról, hogy egy megfelelőségértékelő szervezet megfelel a meghatározott megfelelőségértékelési tevékenységek ellátásához a harmonizált szabványokban megállapított követelményeknek és amennyiben alkalmazandó, bármely további követelménynek, beleértve a vonatkozó ágazati szabályozásokban meghatározottakat is”

21. Az ISO/IEC 17011 szabvány értelmében

22. „az akkreditáció olyan megfelelőségértékelő szervezethez kapcsolódó harmadik fél általi hitelesítésre utal, amely hivatalosan igazolja a megfelelőségértékelési feladatok elvégzésére irányuló illetékességet.”

23. A 43. cikk (1) bekezdése előírja, hogy:

24. „Az illetékes felügyeleti hatóság 57. és 58. cikk alapján fennálló feladat- és hatásköreinek sérelme nélkül a tanúsítvány kiállítását és megújítását – a felügyeleti hatóság a célból való tájékoztatását követően, hogy az szükség esetén gyakorolhassa az 58. cikk (2) bekezdésének h) pontja szerinti hatáskörét – olyan tanúsító szervezet végzi, amely az adatvédelem terén megfelelő szakértelemmel rendelkezik. A tagállamok biztosítják, hogy e tanúsító szervezetek akkreditációját az alábbiak közül egy vagy mindkettő elvégezte:

    (a) az a felügyeleti hatóság, amelyik az 55. vagy az 56. cikk alapján illetékes;
    (b) az EN-ISO/IEC 17065/2012 szabványnak megfelelően, a 765/2008/EK európai parlamenti és tanácsi rendelettel, valamint az 55. vagy az 56. cikk alapján illetékes a felügyeleti hatóság által megállapított kiegészítő követelményekkel összhangban megnevezett nemzeti akkreditáló testület.”

25. Az általános adatvédelmi rendelet tekintetében az akkreditációs követelmények az alábbiakra épülnek:

) Az ISO/IEC 17065/2012 szabvány és a 43. cikk (1) bekezdésének b) pontja szerinti illetékes felügyeleti hatóság által megállapított „kiegészítő követelmények”, amennyiben az akkreditációt a nemzeti akkreditáló testület és a felügyeleti hatóság maga végzi el.

26. Mindkét esetben a konszolidált követelményeknek ki kell terjedniük a 43. cikk (2) bekezdésében említett követelményekre.

---

[10] Lásd a 42. cikk (5) bekezdését.
[11] Lásd a 765/2008/EK rendelet 2. cikkének (11) bekezdését.

27. Az Európai Adatvédelmi Testület elismeri, hogy az akkreditálás célja, hogy hiteles nyilatkozatot nyújtson egy szervezet alkalmasságáról, miszerint képes tanúsítást (megfelelőségértékelési tevékenységeket) végezni[12]. Az általános adatvédelmi rendelet szerinti akkreditáció alatt a következőket kell érteni:

28. a nemzeti akkreditáló testület és/vagy a felügyeleti hatóság által biztosított igazolás[13], hogy a tanúsító szervezet[14] az általános adatvédelmi rendelet 42. és a 43. cikke értelmében tanúsítás elvégzésére jogosult, figyelembe véve az ISO/IEC 17065/2012 szabványt és a felügyeleti hatóság és/vagy az igazgatótanács által megállapított kiegészítő követelményeket.

4 AKKREDITÁCIÓ AZ ÁLTALÁNOS ADATVÉDELMI RENDELET 43. CIKKÉNEK (1) BEKEZDÉSÉVEL ÖSSZHANGBAN

29. A 43. cikk (1) bekezdése elismeri, hogy számos lehetőség létezik a tanúsító szervezetek akkreditációjára. Az általános adatvédelmi rendelet értelmében a felügyeleti hatóságok és a tagállamok kötelesek meghatározni a tanúsító szervezetek akkreditációjának folyamatát. A következő szakaszban meghatározásra kerülnek a 43. cikkben előírt akkreditációs lehetőségek.

4.1 A tagállamok szerepköre

30. A 43. cikk (1) bekezdése előírja a tagállamok számára, hogy *biztosítsák* a tanúsító testületek akkreditálását, de lehetővé teszi minden tagállam számára, hogy maga határozza meg az akkreditációhoz vezető értékelés elvégzéséért felelős személyt. A 43. cikk (1) bekezdése alapján három lehetőség áll rendelkezésre; az akkreditációt elvégezheti:

(1) kizárólag a felügyeleti hatóság, saját követelményei alapján;
(2) kizárólag a 765/2008/EK rendelet, valamint az ISO/IEC 17065/2012 szabvány szerint megnevezett nemzeti akkreditáló testület, továbbá az illetékes felügyeleti hatóság által megállapított kiegészítő követelményekkel összhangban; vagy
(3) mind a felügyeleti hatóság, mind a nemzeti akkreditáló testület (és a fenti 2. pontban felsorolt követelményeknek megfelelően).

31. Az egyes tagállamok feladata annak eldöntése, hogy a nemzeti akkreditáló testület vagy a felügyeleti hatóság, avagy mindkettő együttesen végzi-e ezeket az akkreditációs tevékenységeket, de mindenképpen biztosítania kell a megfelelő erőforrásokat[15].

4.2 Kölcsönhatás a 765/2008/EK rendelettel

32. Az Európai Adatvédelmi Testület megjegyzi, hogy a 765/2008/EK rendelet 2. cikke (11) bekezdésének meghatározása szerint a nemzeti akkreditáló testület „egy tagállam *egyetlen* olyan testülete, amely az államtól származtatott hatáskörében elvégzi az akkreditálást”.

33. A 2. cikk (11) bekezdése ellentétesnek tekinthető az általános adatvédelmi rendelet 43. cikkének (1) bekezdésével, amely lehetővé teszi a tagállam nemzeti akkreditáló testületétől

[12] Vö. a 765/2008/EK rendelet (15) preambulumbekezdésével.
[13] Vö. a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról szóló, 2008. július 9-i 765/2008/EK európai parlamenti és tanácsi rendelet 2. cikkének (10) bekezdésével.
[14] Vö. az ISO 17011 szabvány szerinti „akkreditáció” kifejezés meghatározásával.
[15] Lásd a 765/2008/EK rendelet 4. cikkének (9) bekezdését.

eltérő szervezet általi akkreditációt. Az Európai Adatvédelmi Testület úgy véli, hogy az uniós jogszabályok célja az volt, hogy eltérjenek attól az általános elvtől, hogy az akkreditációt kizárólag a nemzeti akkreditáló hatóság végezze, azáltal hogy a felügyeleti hatóságoknak ugyanolyan jogkört biztosítanak a tanúsító szervezetek akkreditációja tekintetében. Ezért a 43. cikk (1) bekezdése lex specialis a 765/2008/EK rendelet 2. cikkének (11) bekezdésével szemben.

4.3 A nemzeti akkreditáló testület szerepköre

34. A 43. cikk (1) bekezdésének b) pontja előírja, hogy a nemzeti akkreditáló testület tanúsító szervezeteket akkreditál az ISO/IEC 17065/2012 szabvány és az illetékes felügyeleti hatóság által megállapított kiegészítő követelmények alapján.

35. Az egyértelműség kedvéért az Európai Adatvédelmi Testület megjegyzi, hogy a 43. cikk (3) bekezdése b) pontjának első albekezdésére való konkrét hivatkozás azt jelenti, hogy azok a követelmények a 43. cikk (1) bekezdésének b) pontja értelmében az illetékes felügyeleti hatóság által megállapított kiegészítő követelményekre, valamint a 43. cikk (2) bekezdésben előírt követelményekre mutatnak.

36. Az akkreditálás folyamata során a nemzeti akkreditáló testületeknek alkalmazniuk kell a felügyeleti hatóságok által nyújtandó kiegészítő követelményeket.

37. Az ISO/IEC 17065/2012 szabvány alapján annak az általános adatvédelmi rendelethez nem kapcsolódó tanúsítási rendszerekre meglévő akkreditációval rendelkező tanúsító szervezetnek, amely szeretné kiterjeszteni akkreditációs hatáskörét az általános adatvédelmi rendeletnek megfelelően kibocsátott tanúsítványokra, meg kell felelnie a felügyeleti hatóság kiegészítő követelményeinek, ha az akkreditációt a nemzeti akkreditáló testület kezeli. Ha az általános adatvédelmi rendelet szerinti tanúsításra vonatkozó akkreditációt csak az illetékes felügyeleti hatóság nyújtja, az akkreditációra pályázó tanúsító szervezetnek meg kell felelnie az adott felügyeleti hatóság által meghatározott követelményeknek.

4.4 A felügyeleti hatóság szerepköre

38. Az Európai Adatvédelmi Testület megjegyzi, hogy az 57. cikk (1) bekezdésének q) pontja előírja, hogy a felügyeleti hatóságnak a 43. cikknek megfelelően el *kell* végeznie a tanúsító szervezet akkreditálását „felügyeleti hatósági feladatként” az 57. cikk értelmében, továbbá az 58. cikk (3) bekezdésének e) pontja előírja, hogy a felügyeleti hatóság hitelesítő és tanácsadói jogkörrel rendelkezik a 43. cikk szerinti tanúsító szervezetek akkreditálása tekintetében. A 43. cikk (1) bekezdésének megfogalmazása bizonyos rugalmasságot biztosít, és a felügyeleti hatóság akkreditációs funkcióját csak adott esetben kell feladatként értelmezni. A tagállami jog ezt a pontot tisztázhatja. A nemzeti akkreditáló testület akkreditációs folyamata során azonban a tanúsító szervezeteknek a 43. cikk (2) bekezdésének a) pontja értelmében bizonyítaniuk kell függetlenségüket és szakértelmüket az illetékes felügyeleti hatóság előtt az általuk biztosított tanúsítási mechanizmus tárgyára vonatkozóan[16].

39. Ha egy tagállam előírja, hogy a tanúsító szervezeteket a felügyeleti hatóságnak kell akkreditálnia, a felügyeleti hatóságnak akkreditációs követelményeket kell megállapítania, beleértve, de nem kizárólagosan a 43. cikk (2) bekezdésében meghatározott

[16] A felügyeleti hatóság által a 43. cikk (1) bekezdésének b) pontja alapján megállapított kiegészítő követelményeknek tartalmazniuk kell a függetlenségre és szakértelemre vonatkozó követelményeket. Lásd még az iránymutatások 1. mellékletét.

követelményeket. A nemzeti akkreditáló testületek által végzett, tanúsító szervezetek akkreditációjával kapcsolatos kötelezettségekhez képest a 43. cikk kevesebb utasítást ad az akkreditáció követelményeivel kapcsolatban arra az esetre, ha a felügyeleti hatóság maga végzi el az akkreditációt. Az akkreditáció harmonizált megközelítéséhez való hozzájárulás érdekében a felügyeleti hatóság által alkalmazott akkreditációs kritériumoknak az ISO/IEC 17065 szabványon kell alapulniuk, és ki kell egészíteni azokkal a kiegészítő követelményekkel, amelyeket a felügyeleti hatóság a 43. cikk (1) bekezdésének b) pontja értelmében állapít meg. Az Európai Adatvédelmi Testület megjegyzi, hogy a 43. cikk (2) bekezdésének a)–e) pontjai tükrözik és meghatározzák az ISO 17065 szabvány követelményeit, amelyek hozzájárulnak a következetességhez.

40. Ha egy tagállam előírja, hogy a tanúsító szervezeteket a nemzeti akkreditáló testületek akkreditálják, a felügyeleti hatóságnak kiegészítő követelményeket kell megállapítania a 765/2008/EK rendeletben előirányzott akkreditációs egyezmények kiegészítéseként (amelynek 3–14. cikke a szervezetre és a megfelelőségértékelő szervezetek akkreditációjának működtetésére vonatkozik), valamint a tanúsító szervezetek módszereit és eljárásait leíró technikai szabályokat. Ennek fényében a 765/2008/EK rendelet további iránymutatást nyújt: A 2. cikk (10) bekezdése meghatározza az akkreditációt, és utal „harmonizált szabványokra” és „bármely további követelményre, beleértve a vonatkozó ágazati szabályozásokban meghatározottakat is”. Ebből következik, hogy a felügyeleti hatóság által meghatározott kiegészítő követelményeknek egyedi követelményeket kell tartalmazniuk, és többek között a tanúsító szervezetek adatvédelmi szakismerete függetlenségének és szintjének értékelésére kell összpontosítaniuk, például az adatfeldolgozók és adatkezelők személyes adatokkal kapcsolatos feldolgozási műveleteinek értékelésére és hitelesítésére vonatkozó képességük tekintetében a 42. cikk (1) bekezdése értelmében. Ez magában foglalja az ágazati szabályozásokhoz szükséges illetékességet, valamint a természetes személyek alapvető jogainak és szabadságainak védelmét és különösen a személyes adatok védelméhez való jogukat[17]. Ezen iránymutatások melléklete tájékoztatást biztosíthat az illetékes felügyeleti hatóságoknak a „kiegészítő követelmények” meghatározása során a 43. cikk (1) bekezdésének b) pontjával és a 43. cikk (3) bekezdésével összhangban.

41. A 43. cikk (6) bekezdése előírja, hogy „az e cikk (3) bekezdésében említett követelményeket és a 42. cikk (5) bekezdésében említett szempontokat a felügyeleti hatóság könnyen hozzáférhető formában közzéteszi”. Ezért az átláthatóság biztosítása érdekében a felügyeleti hatóság által jóváhagyott összes kritériumot és követelményt közzé kell tenni. A tanúsító szervezetekben a minőség és bizalom tekintetében kívánatos lenne, ha az akkreditációra vonatkozó valamennyi követelmény könnyen hozzáférhető lenne a nyilvánosság számára.

4.5 Tanúsító szervezetként eljáró felügyeleti hatóság

42. A 42. cikk (5) bekezdése előírja, hogy a felügyeleti hatóság tanúsítványokat adhat ki, de az általános adatvédelmi rendelet nem követeli meg, hogy akkreditálva legyen a 765/2008/EK rendeletben foglalt követelmények teljesítéséhez. Az Európai Adatvédelmi Testület megjegyzi, hogy a 43. cikk (1) bekezdésének a) pontja, és különösen az 58. cikk (2) bekezdésének h) pontja, valamint (3) bekezdésének a) és e)–f) pontjai feljogosítják a felügyeleti hatóságokat mind az akkreditáció, mind a tanúsítás elvégzésére, a tanácsadásra, és adott esetben a tanúsítványok visszavonására, vagy a tanúsító szervezetek utasítására, hogy ne adjanak ki tanúsítványt.

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

43. Lehetnek olyan helyzetek, amikor az akkreditációs és tanúsítási szerepek és feladatok szétválasztása helyénvaló vagy szükséges, például ha egy felügyeleti hatóság és más tanúsító szervezetek együtt léteznek egy tagállamban, és mindkettő ugyanazt a tanúsítványt bocsátja ki. A felügyeleti hatóságoknak ezért elegendő szervezeti intézkedést kell tenniük az általános adatvédelmi rendelet szerinti feladatok elkülönítésére a tanúsítási mechanizmusok rögzítése és megkönnyítése érdekében, miközben óvintézkedéseket tesznek az ilyen feladatokból eredő összeférhetetlenségek elkerülése érdekében. Ezenkívül a tagállamoknak és a felügyeleti hatóságoknak figyelembe kell venniük a harmonizált európai szintet az általános adatvédelmi rendelet szerinti akkreditációval és tanúsítással kapcsolatos nemzeti jog és eljárások kidolgozása során.

4.6 Akkreditációs követelmények

44. Ezen iránymutatások melléklete útmutatást ad a kiegészítő akkreditációs követelmények azonosításához. Azonosítja az általános adatvédelmi rendelet vonatkozó rendelkezéseit és olyan követelményeket javasol, amelyeket a felügyeleti hatóságoknak és a nemzeti akkreditáló testületeknek figyelembe kell venniük az általános adatvédelmi rendeletnek való megfelelés biztosítása érdekében.

45. A fentiek szerint, ahol a tanúsító szervezeteket a nemzeti akkreditáló testületek akkreditálták a 765/2008/EK rendelet értelmében, ott az ISO/IEC 17065/2012 lesz a megfelelő akkreditációs szabvány, kiegészítve a felügyeleti hatóság által megállapított kiegészítő követelményekkel. A 43. cikk (2) bekezdése az ISO/IEC 17065/2012 szabvány általános rendelkezéseit tükrözi, tekintettel az általános adatvédelmi rendelet szerinti alapvető jogok védelmére. A mellékletben szereplő keret a 43. cikk (2) bekezdését és az ISO/IEC 17065/2012 szabványt veszi alapul a tanúsító szervezetek adatvédelmi szakértelmének értékelésével, valamint az azzal kapcsolatos követelmények és további kritériumok azonosításához, hogy képesek-e tiszteletben tartani a természetes személyek jogait és szabadságait a személyes adatok feldolgozásával kapcsolatban, amint azt az általános adatvédelmi rendelet előírja. Az Európai Adatvédelmi Testület megjegyzi, hogy különös hangsúlyt fektet annak biztosítására, hogy a tanúsító szervezetek megfelelő szintű adatvédelmi szakértelemmel rendelkezzenek a 43. cikk (1) bekezdésével összhangban.

46. A felügyeleti hatóság által meghatározott kiegészítő akkreditációs követelmények minden, akkreditációs kérelmet benyújtó tanúsító szervezetre vonatkoznak. Az akkreditáló testület értékelni fogja, hogy a tanúsító szervezet képes-e a tanúsítási tevékenység elvégzésére a kiegészítő követelményeknek és a tanúsítás tárgyának megfelelően. Hivatkozni kell a specifikus ágazatokra vagy tanúsítási területekre, amelyekre vonatkozóan a tanúsító szervezet akkreditált.

47. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az ISO/IEC 17065/2012 szabvány követelményei mellett az adatvédelem területén különleges szakértelemre van szükség, ha más külső szervek, például laboratóriumok vagy könyvvizsgálók is részt vesznek a tanúsítási tevékenységek elvégzésében az akkreditált tanúsító szervezet képviseletében. Ezekben az esetekben e külső szerveknek az általános adatvédelmi rendelet szerinti akkreditálása nem lehetséges. Annak érdekében azonban, hogy az említett szervezetek alkalmasak legyenek az akkreditált tanúsító szervezetek képviseletében a tevékenységek elvégzésére, az akkreditált tanúsító szervezetnek biztosítania kell, hogy akkreditált szervezethez méltón rendelkezik a szükséges adatvédelmi szakismerettel, és ezt bizonyítania kell a külső testület esetében az elvégzett tevékenység vonatkozásában.

48. Az ezen iránymutatások mellékletében bemutatott kiegészítő akkreditációs követelmények meghatározásának kerete nem minősül eljárási kézikönyvnek a nemzeti akkreditáló testület vagy a felügyeleti hatóság által végzett akkreditációs folyamathoz. Iránymutatást ad a felépítésre és a módszertanra vonatkozóan, eszköztárat biztosítva ezáltal a felügyeleti hatóságoknak, hogy azonosítani tudják az akkreditációra vonatkozó kiegészítő követelményeket.

1. MELLÉKLET

Az 1. melléklet útmutatást nyújt az ISO/IEC 17065/2012 tekintetében, valamint az általános adatvédelmi rendelet 43. cikke (1) bekezdésének b) pontjával és az általános adatvédelmi rendelet 43. cikke (3) bekezdésével összhangban megállapított kiegészítő követelmények meghatározásához.

Ez a melléklet ismerteti azokat a kívánatos követelményeket, amelyeket az adatvédelmi felügyeleti hatóságnak meg kell határoznia, és a tanúsító szervezetekre vonatkozóan a nemzeti akkreditáló testület vagy az illetékes felügyeleti hatóság által végzett akkreditáció során alkalmazni kell[18]. Ezeket a kiegészítő követelményeket a 64. cikk (1) bekezdésének c) pontja szerinti jóváhagyás előtt közölni kell az Európai Adatvédelmi Testülettel.

Ezt a mellékletet az ISO/IEC 17065/2012 szabvánnyal együtt kell értelmezni. A szakaszok számozása megfelel az ISO/IEC 17065/2012 szabványban használt számozásnak. Ha a felügyeleti hatóságok a 43. cikk (1) bekezdésének a) pontja alapján akkreditációt végeznek, a helyes gyakorlat az lenne, ha ezt a megközelítést alkalmaznák, amennyiben ez kivitelezhető. Ez elő fogja segíteni az EU-n belüli akkreditáció harmonizálását.

Az alábbi útmutatás sérelme nélkül vagy az ISO/IEC 17065/2012 szabvány bármelyik elemére vonatkozó útmutatás hiányában az illetékes felügyeleti hatóság ezekre az elemekre vonatkozóan további kiegészítő követelményeket fogalmazhat meg, ha azok összhangban vannak a nemzeti joggal.

0 ELŐTAG

[Ez a szakasz az adott esetben a nemzeti akkreditáló testület és az adatvédelmi felügyeleti hatóság között esetlegesen létrejött együttműködés feltételeire hivatkozik, amelyek például arra vonatkoznak, hogy kinek a feladata legyen a kérelmek fogadása, vagy hogy milyen módon szervezzék meg – az akkreditációs folyamaton belül – a jóváhagyott kritériumok elismerését.]

1 ALKALMAZÁSI KÖR[19]

Az ISO/IEC 17065/2012 alkalmazási körének összhangban kell állnia az általános adatvédelmi rendelettel. Az akkreditációra és a tanúsításra vonatkozó iránymutatások további tájékoztatást nyújtanak. A nemzeti akkreditáló testület és az illetékes felügyeleti hatóság által az akkreditációs folyamat során végzett értékelés során figyelembe kell venni a tanúsítási mechanizmus alkalmazási körét (például: felhőalapú szolgáltatások adatkezelési műveleteinek tanúsítása), különös tekintettel a kritériumokra, a szakértelemre és az értékelés módszertanára. Az ISO/IEC 17065/2012 termékekre, eljárásokra és szolgáltatásokra kiterjedő széles alkalmazási köre nem csökkentheti vagy nem írhatja felül az általános adatvédelmi rendelet követelményeit, például a tanúsítási mechanizmus nem szorítkozhat kizárólag az irányítási mechanizmusra, hanem ki kell terjednie a személyes adatok kezelésére, azaz az adatkezelési műveletekre is. A 42. cikk (1) bekezdésének értelmében az általános adatvédelmi rendelet szerinti tanúsítás csak az adatkezelők és -feldolgozók adatkezelési műveleteire alkalmazandó.

[18] A tanúsítási kritériumokra vonatkozó jóváhagyási eljárásról a tanúsítási iránymutatások 4. szakasza nyújt tájékoztatást.

[19] A számozás az ISO/IEC 17065/2012 számozására vonatkozik.

2 RENDELKEZŐ HIVATKOZÁSOK

Az általános adatvédelmi rendelet elsőbbséget élvez az ISO/IEC 17065/2012 szabvánnyal szemben. Ha a kiegészítő követelményekben vagy a tanúsítási mechanizmus keretében más ISO-szabványokra történik hivatkozás, akkor azokat az általános adatvédelmi rendeletben meghatározott követelményekkel összhangban kell értelmezni.

3 KIFEJEZÉSEK ÉS FOGALOMMEGHATÁROZÁSOK

E melléklet összefüggésében az akkreditációra vonatkozó iránymutatás (WP 261) és a tanúsításra vonatkozó iránymutatás (1/2018 EDPB) fogalmai és meghatározásai alkalmazandók, és elsőbbséget élveznek az ISO fogalommeghatározásaival szemben.

4 AZ AKKREDITÁCIÓRA VONATKOZÓ ÁLTALÁNOS KÖVETELMÉNYEK

4.1 Jogi és szerződéses kérdések

4.1.1 Jogi felelősség

A tanúsító szervezeteknek (mindenkor) képesnek kell lenniük annak bizonyítására a nemzeti akkreditáló testület vagy az illetékes felügyeleti hatóság számára, hogy olyan naprakész eljárásokkal rendelkeznek, amelyek bizonyítják az akkreditáció feltételeiben meghatározott jogi kötelezettségeknek – ezen belül a 2016/679/EK rendelet alkalmazására vonatkozóan meghatározott kiegészítő követelményeknek – való megfelelést. Megjegyzendő, hogy mivel a tanúsító szervezetek maguk is adatkezelők/adatfeldolgozók, tanúsítási eljárásuk részeként képesnek kell lenniük annak bizonyítására, hogy a kifejezetten az ügyfélszervezetek személyes adatainak kezelésére alkalmazott eljárásaik és intézkedéseik megfelelnek a 2016/679/EK rendeletnek.

Az illetékes felügyeleti hatóságok dönthetnek úgy, hogy további követelményeket és eljárásokat vezetnek be annak akkreditáció előtti ellenőrzésére, hogy a tanúsító szervezetek megfelelnek-e az általános adatvédelmi rendeletnek.

4.1.2 Tanúsítási megállapodás

A tanúsítási megállapodás minimumkövetelményeit az alábbi pontok egészítik ki:

A tanúsító szervezetnek az ISO/IEC 17065/2012 szabvány követelményein túl igazolnia kell, hogy tanúsítási megállapodásai:

1. előírják, hogy a kérelmezőnek minden esetben meg kell felelnie mind az ISO/IEC 17065/2012 4.1.2.2. lit. a. pontjában meghatározott tanúsítási követelményeknek, valamint az illetékes felügyeleti hatóság vagy az Európai Adatvédelmi Testület által a 43. cikk (2) bekezdésének b) pontjával és a 42. cikk (5) bekezdésével összhangban jóváhagyott kritériumoknak;
2. előírják, hogy a kérelmezőnek teljes átláthatóságot kell biztosítania az illetékes felügyeleti hatóság számára a tanúsítási eljárás tekintetében, beleértve a 42. cikk (7) bekezdése és az 58. cikk (1) bekezdésének c) pontja szerinti adatvédelmi megfeleléssel kapcsolatos, szerződéses feltételek alapján bizalmas kérdéseket is;
3. nem csökkentik a kérelmező felelősségét a 2016/679/EK rendelet rendelkezéseinek való megfelelés tekintetében, és nem érintik a 42. cikk (5) bekezdése szerint illetékes felügyeleti hatóságok feladatait és hatásköreit;

4. előírják, hogy a kérelmezőnek a 42. cikk (6) bekezdésének megfelelően a tanúsító szervezet számára minden olyan információt meg kell adnia és minden olyan adatkezelési tevékenységéhez hozzáférést kell biztosítania, amely a tanúsítási eljárás lefolytatásához szükséges;
5. előírják, hogy a kérelmezőnek tiszteletben kell tartania a vonatkozó határidőket és eljárásokat. A tanúsítási megállapodásnak elő kell írnia, hogy a – például a tanúsítási programból vagy egyéb rendelkezésekből származó – határidőket és eljárásokat követni kell és be kell tartani;
6. az ISO/IEC 17065/2012 4.1.2.2. lit. c 1. pontja tekintetében meg kell határozniuk a 42. cikk (7) bekezdése és a 43. cikk (4) bekezdésének megfelelő érvényességi, megújítási és visszavonási szabályokat, beleértve azokat a szabályokat is, amelyek a 42. cikk (7) bekezdésével összhangban megfelelő időközöket határoznak meg az újraértékelés vagy a felülvizsgálat (rendszeressége) tekintetében;
7. lehetővé teszik a tanúsító szervezet számára, hogy a 42. cikk (8) bekezdése és a 43. cikk (5) bekezdése szerinti tanúsításhoz szükséges valamennyi információt közzétegye;
8. szabályokat tartalmaznak a 4.1.2.2 lit. c 2. szerinti panaszok kivizsgálásához szükséges óvintézkedésekről, továbbá a lit. j. szakaszban a 43. cikk (2) bekezdésének d) pontjával összhangban explicit módon nyilatkozni kell a panaszkezelés struktúrájáról és eljárásáról;
9. az ISO/IEC 17065/2012 4.1.2.2. pontjában említett minimumkövetelmények mellett, az ügyfelet érintő következményeket is figyelembe kell venni abban az esetben, ha a tanúsító szervezetre vonatkozó akkreditáció visszavonásából vagy felfüggesztéséből származó következmények érintik az ügyfelet;
10. előírják a kérelmező számára, hogy tájékoztassa a tanúsító szervezetet abban az esetben, ha a tényleges vagy jogi helyzetét, illetve a tanúsítás által érintett termékeit, eljárásait és szolgáltatásait érintő jelentős változásokra kerül sor.

4.1.3 Az adatvédelmi bélyegzők és jelölések használata

A tanúsítványokat, bélyegzőket és jelöléseket csak a 42. és a 43. cikknek, valamint az akkreditációra és a tanúsításra vonatkozó iránymutatásoknak megfelelően lehet használni.

4.2 A pártatlanság kezelése

Az akkreditáló testület az ISO/IEC 17065/2012 4.2. pontjában foglalt követelményen felül biztosítja az alábbiak teljesülését:

1. a tanúsító szervezet megfelel az illetékes felügyeleti hatóság kiegészítő követelményeinek (a 43. cikk (1) bekezdésének b) pontjának megfelelően);
    a. a 43. cikk (2) bekezdésének a) pontjával összhangban külön bizonyítékot szolgáltat arra nézve, hogy független. Ez különösen a tanúsító szervezet finanszírozására vonatkozó bizonyítékokat érinti, amilyen mértékben az a pártatlanság biztosításához kapcsolódik;
    b. a 43. cikk (2) bekezdésének e) pontjával összhangban feladataival kapcsolatban nem áll fenn összeférhetetlenség;
2. a tanúsító szervezetet nem fűzi releváns kapcsolat az általa értékelt ügyfélhez.

4.3 Felelősség és finanszírozás

Az akkreditáló testület az ISO/IEC 17065/2012 4.3.1. pontjában szereplő előíráson túl rendszeresen biztosítja, hogy a tanúsító szervezet megfelelő intézkedések (pl. biztosítás vagy tartalékok) révén megfeleljen a működése szerinti földrajzi régiókban fennálló felelősségviselési kötelezettségének.

4.4 Megkülönböztetésmentes feltételek

A felügyeleti hatóság a nemzeti joggal összhangban további követelményeket határozhat meg.

4.5 Titoktartás

A felügyeleti hatóság a nemzeti joggal összhangban további követelményeket határozhat meg.

4.6 Nyilvános információk

Az akkreditáló testület az ISO/IEC 17065/2012 szabvány 4.6. pontjában előírt követelmény mellett előírja, hogy a tanúsító szervezetnek legalább a következőket biztosítania kell:

1. a 42. cikk (5) bekezdésének értelmében alkalmazott jóváhagyott szempontok valamennyi (aktuális és korábbi) változatát közzéteszik és a nyilvánosság számára könnyen hozzáférhetővé teszik, az összes tanúsítási eljárással egyetemben, általában feltüntetve az adott érvényességi időt;
2. a 43. cikk (2) bekezdésének d) pontja értelmében a panaszkezelési eljárásokkal és a fellebbezésekkel kapcsolatos információkat nyilvánosságra hozzák.

5 STRUKTURÁLIS KÖVETELMÉNYEK, 43. CIKK (4) BEKEZDÉS [„MEGFELELŐ” ÉRTÉKELÉS]

5.1 Szervezeti felépítés és felső vezetés

A felügyeleti hatóság további követelményeket határozhat meg.

5.2 A pártatlanság megőrzését biztosító mechanizmusok

A felügyeleti hatóság további követelményeket határozhat meg.

6 ERŐFORRÁSOKRA VONATKOZÓ KÖVETELMÉNYEK

6.1 A tanúsító szervezet személyzete

Az akkreditáló testület az ISO/IEC 17065/2012 szabvány 6. pontjában előírt követelmény mellett előírja minden tanúsító szervezetnek annak biztosítását, hogy személyzete:

1. a 43. cikk (1) bekezdésének megfelelően bizonyítottan megfelelő és naprakész szakértelemmel (tudással és tapasztalattal) rendelkezik az adatvédelem tekintetében;
2. a 43. cikk (2) bekezdése a) pontjának megfelelően független, és a tanúsítás tárgyában naprakész szakértelemmel bír, valamint a 43. cikk (2) bekezdése e) pontjának megfelelően nem áll fenn feladataival kapcsolatban összeférhetetlenség;
3. a 43. cikk (2) bekezdése b) pontjának megfelelően vállalja, hogy tiszteletben tartja a 42. cikk (5) bekezdésében említett szempontokat;
4. releváns és megfelelő ismeretekkel és tapasztalattal rendelkezik az adatvédelmi jogszabályok alkalmazása terén;
5. releváns és megfelelő ismeretekkel és tapasztalattal rendelkezik az érintett technikai és szervezeti adatvédelmi intézkedések terén;
6. képes bizonyítani, hogy tapasztalattal rendelkezik a fenti 6.1.1., 6.1.4. és 6.1.5. kiegészítő követelményben említett területeken, különösen

a technikai szakértelemmel rendelkező személyzet esetében:

- az érintett technikai szakterületen legalább az európai képesítési keretrendszer[20] 6. szintjének megfelelő képesítést vagy elismert védett címet (pl.: Dipl. Ing.) szerzett az érintett szabályozott szakmában, vagy jelentős szakmai tapasztalattal rendelkezik.
- A *tanúsítási döntésekért felelős személyzetnek* jelentős szakmai tapasztalattal kell rendelkeznie az adatvédelmi intézkedések meghatározása és végrehajtása terén.
- *Az értékelésekért felelős személyzetnek* az adatvédelmi technológia terén szerzett szakmai tapasztalattal, valamint a hasonló eljárásokkal (pl. tanúsítványokkal/ellenőrzésekkel) kapcsolatos ismeretekkel és gyakorlattal kell rendelkeznie, valamint adott esetben szerepelnie kell az érintett szakmai nyilvántartásban.

A személyzetnek bizonyítania kell, hogy a technikai és ellenőrzési készségek tekintetében az adott szakterületre vonatkozó ismereteit folyamatos szakmai fejlődés révén naprakészen tartja.

a jogi szakértelemmel rendelkező személyzet esetében:

- az EU által vagy államilag elismert egyetemen szerzett, legalább nyolc féléves jogi tanulmányok, ideértve a mesterfokozatú vagy ezzel egyenértékű diplomát (LL.M.) is, vagy jelentős szakmai tapasztalat.
- *A tanúsítási döntésekért felelős személyzetnek* az adatvédelmi jog terén szerzett jelentős szakmai tapasztalattal valamint a tagállam által előírt bejegyzett státusszal kell rendelkeznie.
- *Az értékelésekért felelős személyzetnek* legalább kétéves, az adatvédelmi jog terén szerzett szakmai tapasztalattal, valamint a hasonló eljárásokkal (pl. tanúsítványokkal/ellenőrzésekkel) kapcsolatos ismeretekkel és gyakorlattal kell rendelkeznie, és szerepelnie kell az esetleges tagállami előírásoknak megfelelő szakmai nyilvántartásban.
    - A személyzetnek bizonyítania kell, hogy a technikai és ellenőrzési készségek tekintetében az adott szakterületre vonatkozó ismereteit folyamatos szakmai fejlődés révén naprakészen tartja.

6.2 Az értékeléshez szükséges erőforrások

A felügyeleti hatóság a nemzeti joggal összhangban további követelményeket határozhat meg.

7 ELJÁRÁSI KÖVETELMÉNYEK – A 43. CIKK (2) BEKEZDÉSÉNEK C) ÉS D) PONTJA

7.1 Általános követelmények

Az akkreditáló testületnek az ISO/IEC 17065/2012 szabvány 7.1. pontjában előírt követelmény mellett biztosítania kell az alábbiak teljesülését:

1. A tanúsító szervezetek a kérelem benyújtásakor a 43. cikk (1) bekezdésének b) pontja szerint teljesítik az illetékes felügyeleti hatóság által megállapított kiegészítő követelményeket annak érdekében, hogy a 43. cikk (2) bekezdésének b) pontjával összhangban a feladatok és kötelezettségek ne vezessenek összeférhetetlenséghez.
2. Értesítik az érintett illetékes felügyeleti hatóságot azt megelőzően, hogy a tanúsító szervezet megkezdené kihelyezett irodáján keresztül a jóváhagyott európai adatvédelmi bélyegző új tagállamban történő működtetését.

[20] Lásd a képesítési keretrendszer összehasonlító eszközét: https://ec.europa.eu/ploteus/en/compare?

7.2 Kérelem

Az ISO/IEC 17065/2012 7.2. pontján túlmenően elő kell írni a következőket:

1. a tanúsítás tárgyának (az értékelés tárgyának) részletes leírása/ismertetése a kérelemben. Ideértendők az interfészek és a más rendszerekbe és szervezetekhez való továbbítások, protokollok és egyéb biztosítékok is;
2. annak feltüntetése a kérelemben, hogy alkalmaznak-e adatfeldolgozókat, és amennyiben a kérelmezők adatfeldolgozók, ismertetni kell felelősségi körüket és feladataikat, továbbá a kérelemnek tartalmaznia kell az érintett adatkezelői/adatfeldolgozói szerződés(eke)t.

7.3 A kérelem vizsgálata

Az ISO/IEC 17065/2012 7.3. pontján túlmenően elő kell írni a következőket:

1. az értékelés tárgyára vonatkozó kötelező értékelési módszereket meghatározása a tanúsítási megállapodásban;
2. a 7.3. e) szakasz elegendő szakértelem meglétére irányuló értékelése kellőképpen vegye figyelembe az adatvédelem területére vonatkozó technikai és jogi szakértelmet egyaránt.

7.4 Értékelés

Az ISO/IEC 17065/2012 7.4. pontján túlmenően a tanúsítási mechanizmusoknak olyan kielégítő értékelési módszereket kell ismertetniük, amelyek lehetővé teszik annak vizsgálatát, hogy az adatkezelési művelet(ek) megfelel(nek)-e a tanúsítási kritériumoknak, például adott esetben:

1. annak vizsgálatára szolgáló módszert, hogy az adatkezelési műveletek céljukat és az adott érintetteket tekintve mennyiben szükségesek és arányosak;
2. olyan módszert, amellyel megvizsgálható az adatkezelő és az adatfeldolgozó által az általános adatvédelmi rendelet 30., 32. és 35. és 36. cikkéből adódó jogkövetkezmények, továbbá az általános adatvédelmi rendelet 24., 25. és 32. cikkéből következő technikai és szervezeti intézkedések meghatározása tekintetében figyelembe vett összes kockázat kiterjedése, összetétele és értékelése, valamint
3. olyan módszert, amellyel megvizsgálhatók azok a jogorvoslati lehetőségek – ideértve a garanciákat, biztosítékokat és eljárásokat is –, amelyek biztosítják a tanúsítás tárgya által végzendő adatkezeléssel összefüggésben a személyes adatok védelmét, valamint bizonyítják a kritériumokban meghatározott jogi kötelezettségek teljesülését; továbbá
4. a módszerek és megállapítások dokumentálását.

A tanúsító szervezet számára elő kell írni, hogy ezek az értékelési módszerek szabványosak és általánosan alkalmazhatók legyenek. Ez azt jelenti, hogy amennyiben az értékelés tárgyai egymáshoz hasonlóak, akkor hasonló értékelési módszert kell alkalmazni ezekre. A tanúsító szervezetnek a fenti eljárástól való bármiféle eltérést indokolnia kell.

Az ISO/IEC 17065/2012 7.4.2. pontján túlmenően lehetővé kell tenni, hogy az értékelést a tanúsító szervezet által elismert külső szakértők végezzék.

Az ISO/IEC 17065/2012 7.4.5. pontján túlmenően elő kell írni, hogy az általános adatvédelmi rendelet 42. és 43. cikkének megfelelő, a tanúsítás tárgyát részben már lefedő adatvédelmi tanúsítvány belefoglalható a jelenlegi tanúsításba. Ez azonban nem elegendő ahhoz, hogy teljesen kiváltsa a (részleges) értékeléseket. A tanúsító szervezet köteles ellenőrizni a kritériumoknak való megfelelést. Az elismeréshez minden esetben teljes értékelési jelentés elérhetővé tételére vagy olyan információkra van szükség, amelyek lehetővé teszik a korábbi tanúsítási tevékenységnek és annak

eredményeinek értékelését. A tanúsító nyilatkozat vagy a hasonló tanúsítási tanúsítvány nem tekinthető elégségesnek ahhoz, hogy a jelentést kiváltsa.

Az ISO/IEC 17065/2012 7.4.6. pontján túlmenően elő kell írni, hogy a tanúsító szervezet a tanúsítási mechanizmusában részletesen meghatározza, hogy a 7.4.6. pontban előírt információk hogyan tájékoztatják az ügyfelet (a tanúsítás kérelmezőjét) a tanúsítási mechanizmusnak való megfelelés hiányosságairól. Ezzel összefüggésben meg kell határozni legalább az ilyen tájékoztatás jellegét és időzítését.

Az ISO/IEC 17065/2012 7.4.9. pontján túlmenően elő kell írni, hogy kérésre a dokumentációt teljes mértékben elérhetővé tegyék az adatvédelmi felügyeleti hatóság számára.

7.5 Felülvizsgálat

Az ISO/IEC 17065/2012 7.5. pontján túlmenően kötelező eljárásokat létrehozni a 43. cikk (2) bekezdése és a 43. cikk (3) bekezdése szerinti tanúsítások kiadására, rendszeres felülvizsgálatára és visszavonására.

7.6 Tanúsítási döntés

Az ISO/IEC 17065/2012 7.6.1. pontján túlmenően a tanúsító szervezetnek eljárásaiban részletesen meg kell határoznia, hogy az egyes tanúsítási döntések tekintetében hogyan biztosított a függetlensége és felelőssége.

7.7 Tanúsítási dokumentáció

Az ISO/IEC 17065/2012 7.7.1.e) pontján túlmenően és az általános adatvédelmi rendelet 42. cikkének (7) bekezdésével összhangban elő kell írni, hogy a tanúsítványok érvényességi ideje nem haladhatja meg a három évet.

Az ISO/IEC 17065/2012 7.7.1.e) pontján túlmenően elő kell írni a 7.9. szakasz szerinti tervezett ellenőrzés időtartamának dokumentálását is.

Az ISO/IEC 17065/2012 szabvány 7.7.1.f pontján túlmenően a tanúsító szervezetet kötelezni kell arra, hogy a tanúsítási dokumentációban nevezze meg a tanúsítás tárgyát (adott esetben a verziótátusszal vagy más hasonló jellemzőkkel együtt).

7.8 A tanúsított termékek jegyzéke

Az ISO/IEC 17065/2012 7.8. ponton túlmenően a tanúsító szervezetet kötelezni kell arra, hogy a tanúsított termékekre, eljárásokra és szolgáltatásokra vonatkozó információkat szervezetén belül és a nyilvánosság számára elérhető módon megőrizze. A tanúsító szervezet összefoglalót készít az értékelő jelentésről a nyilvánosság számára. Ennek az összefoglalónak az a célja, hogy átláthatóbbá tegye, hogy mire vonatkozott a tanúsítás és ezt milyen módon értékelték. Az összefoglaló többek között a következők magyarázatát foglalja magában:

(a) a tanúsítás alkalmazási köre és a tanúsítás tárgyának érthető leírása,

(b) a vonatkozó tanúsítási kritériumok (beleértve a verziót és a funkcionális státuszt),

(c) az értékelési módszerek és az elvégzett vizsgálatok, valamint

(d) az eredmény(ek).

Az ISO/IEC 17065/2012 7.8. pontján túlmenően és az általános adatvédelmi rendelet 43. cikke (5) bekezdésének megfelelően a tanúsító szervezet közli az illetékes felügyeleti hatósággal a kért tanúsítvány megadásának vagy visszavonásának okait.

7.9 Felügyelet

Az ISO/IEC 17065/2012 szabvány 7.9.1., 7.9.2. és 7.9.3. pontján túlmenően, valamint az általános adatvédelmi rendelet 43. cikke (2) bekezdésének c) pontja szerint elő kell írni, hogy az ellenőrzési időszak során foganatosítsanak rendszeres ellenőrzési intézkedéseket a tanúsítás fenntartásához.

7.10 A tanúsítást érintő változások

Az EN ISO/IEC 17065/2012 szabvány 7.10.1. és 7.10.2. pontján túlmenően a tanúsító szervezetnek a tanúsítást érintő következő változásokat kell figyelembe vennie: az adatvédelmi jogszabályok módosítása, az Európai Bizottság által a 43. cikk (8) bekezdése és a 43. cikk (9) bekezdése alapján elfogadott felhatalmazáson alapuló jogi aktusok, az Európai Adatvédelmi Testület határozatai és az adatvédelemmel kapcsolatos bírósági határozatok. Az itt meghatározandó módosítási eljárások közé tartozhatnak például a következők: átmeneti időszakok, az illetékes felügyeleti hatósággal kialakítandó jóváhagyási eljárás, a tanúsítás vonatkozó tárgyának újraértékelése és a tanúsítvány visszavonására vonatkozó megfelelő intézkedések, amennyiben a tanúsított adatkezelési művelet már nem felel meg az aktualizált kritériumoknak.

7.11 A tanúsítás megszüntetése, korlátozása, felfüggesztése vagy visszavonása

Az ISO/IEC 17065/2012 7.11.1. pontján túlmenően a tanúsító szervezetet kötelezni kell arra, hogy adott esetben haladéktalanul írásban tájékoztassa az illetékes felügyeleti hatóságot és a nemzeti akkreditáló testületet a meghozott intézkedésekről, valamint a tanúsítás folytatásáról, korlátozásáról, felfüggesztéséről és visszavonásáról.

Az 58. cikk (2) bekezdésének h) pontja szerint a tanúsító szervezetnek el kell fogadnia az illetékes felügyeleti hatóság arra vonatkozóan hozott határozatait és utasításait, hogy vonják vissza vagy ne adják ki a tanúsítást egy ügyfélnek (a kérelmezőnek), ha a tanúsítás feltételei nem vagy már nem teljesülnek.

7.12 Nyilvántartások

A tanúsító szervezetet kötelezni kell arra, hogy minden dokumentációt hiánytalanul, érthető formában, naprakészen és ellenőrizhető módon megőrizzen.

7.13 Panaszok és fellebbezések – a 43. cikk (2) bekezdésének d) pontja

Az ISO/IEC 17065/2012 7.13.1. pontján túlmenően elő kell írni, hogy a tanúsító szervezet határozza meg a következőket:

(a) ki nyújthat be panaszt vagy kifogást,

(b) ki kezeli ezeket a tanúsító szervezet részéről,

(c) milyen ellenőrzésekre kerül sor ezzel összefüggésben, továbbá

(d) milyen lehetőségek vannak az érdekelt felekkel folytatott konzultációra.

Az ISO/IEC 17065/2012 7.13.2. pontján túlmenően elő kell írni, hogy a tanúsító szervezetnek meg kell határoznia a következőket:

(a) hogyan és kinek a számára kell ilyen megerősítést adni,

(b) milyen határidők vonatkoznak erre, továbbá

(c) ezt követően milyen eljárásokat kell kezdeményezni.

Az ISO/IEC 17065/2012 7.13.1. pontján túlmenően a tanúsító szervezetnek meg kell határoznia, hogyan biztosítják a tanúsítási tevékenységeknek és a fellebbezések és panaszok kezelésének szétválasztását.

8 AZ IRÁNYÍTÁSI RENDSZERRE VONATKOZÓ KÖVETELMÉNYEK

Az irányítási rendszerre vonatkozóan az ISO/IEC 17065/2012 8. fejezete azt az általános követelményt rögzíti, hogy az akkreditált tanúsító szervezet által alkalmazott tanúsítási mechanizmus alkalmazási körébe tartozó, korábbi fejezetekből eredő valamennyi követelmény végrehajtása tekintetében biztosítani kell a dokumentációt, az értékelést, az ellenőrzést és a független felügyeletet.

Az irányítás alapelve egy olyan rendszer meghatározása, amely révén eredményes és hatékony módon rögzíthető annak célja, azaz a tanúsítási szolgáltatások végrehajtása – megfelelő előírások alkalmazásával. Ehhez az szükséges, hogy a tanúsító szervezet az akkreditációs követelményeket átlátható és ellenőrizhető módon érvényesítse, és azoknak mindenkor megfeleljen.

E célból az irányítási rendszernek módszertant kell meg kell határoznia az e követelményeknek az adatvédelmi szabályokkal összhangban történő megvalósítására és ellenőrzésére, valamint ezeknek az akkreditált szervezetek vonatkozásában való ellenőrzésére.

Biztosítani kell ezen irányítási elvek és azok dokumentált végrehajtása tekintetében az átláthatóságot, és azokat közölni kell az akkreditált tanúsító szervezettel az 58. cikk szerinti akkreditációs eljárás keretében, majd ezt követően az adatvédelmi felügyeleti hatóság kérésére az 58. cikk (1) bekezdésének b) pontja szerinti adatvédelmi felülvizsgálat formájában végzett vizsgálat során vagy a 42. cikk (7) bekezdése szerint kiadott tanúsítványokra vonatkozóan az 58. cikk (1) bekezdésének c) pontja alapján végzett felülvizsgálat során bármikor.

Az akkreditált tanúsító szervezetnek állandó jelleggel és folyamatosan közzé kell tennie, hogy melyik tanúsítást milyen alapon (vagy milyen tanúsítási mechanizmusok vagy rendszerek révén) végezték el, illetve mennyi ideig, milyen keretek között és milyen feltételek mellett érvényesek a tanúsítványok ((100) preambulumbekezdés).

8.1 Az irányítási rendszerre vonatkozó általános követelmények

Az illetékes felügyeleti hatóság további kiegészítő követelményeket határozhat meg és alkalmazhat, ha ezek összhangban állnak a nemzeti joggal.

8.2 Az irányítási rendszerre vonatkozó dokumentáció

Az illetékes felügyeleti hatóság további kiegészítő követelményeket határozhat meg és alkalmazhat, ha ezek összhangban állnak a nemzeti joggal.

8.3 A dokumentumok kezelése

Az illetékes felügyeleti hatóság további kiegészítő követelményeket határozhat meg és alkalmazhat, ha ezek összhangban állnak a nemzeti joggal.

8.4 A nyilvántartás kezelése

Az illetékes felügyeleti hatóság további kiegészítő követelményeket határozhat meg és alkalmazhat, ha ezek összhangban állnak a nemzeti joggal.

8.5 Az irányítás felülvizsgálata

Az illetékes felügyeleti hatóság további kiegészítő követelményeket határozhat meg és alkalmazhat, ha ezek összhangban állnak a nemzeti joggal.

8.6 Belső ellenőrzések

Az illetékes felügyeleti hatóság további kiegészítő követelményeket határozhat meg és alkalmazhat, ha ezek összhangban állnak a nemzeti joggal.

8.7 Korrekciós intézkedések

Az illetékes felügyeleti hatóság további kiegészítő követelményeket határozhat meg és alkalmazhat, ha ezek összhangban állnak a nemzeti joggal.

8.8 Megelőző intézkedések

Az illetékes felügyeleti hatóság további kiegészítő követelményeket határozhat meg és alkalmazhat, ha ezek összhangban állnak a nemzeti joggal.

9 TOVÁBBI KIEGÉSZÍTŐ KÖVETELMÉNYEK21

9.1 Az értékelési módszerek aktualizálása

A tanúsító szervezet eljárásokat dolgoz ki annak érdekében, hogy iránymutatást nyújtson a 7.4. pont szerinti értékelés keretében alkalmazandó értékelési módszerek aktualizálásához. Az aktualizálást a jogi keretet, a vonatkozó kockázat(ok)at, a technika állását, valamint a technikai és szervezési intézkedések végrehajtási költségeit érintő változásokkal összefüggésben kell elvégezni.

9.2 A szakértelem megőrzése

A tanúsító szervezeteknek a 9.1. pontban felsorolt fejleményeket figyelembe véve eljárásokat kell kidolgozniuk alkalmazottaik arra irányuló képzésének biztosítása érdekében, hogy készségeik naprakészek legyenek.

9.3 Felelősségi körök és hatáskörök

9.3.1 A tanúsító szervezet és az ügyfelei közötti kommunikáció

Eljárásokat kell meghatározni a tanúsító szervezet és az ügyfelei közötti megfelelő eljárások és kommunikációs struktúrák kialakítása céljából. Ezeknek ki kell terjedniük az alábbiakra:

1. Az akkreditált tanúsító szervezet által a feladatokról és felelősségi körökről fenntartott dokumentáció, amely a következő célokra szolgál:
    a. információkérések, vagy
    b. a kapcsolatfelvétel lehetővé tétele egy adott tanúsítással kapcsolatos panasztétel esetében.
2. A kérelmezési eljárás megőrzése a következő célból:
    a. a kérelem státuszával kapcsolatos tájékoztatás;
    b. az illetékes felügyeleti hatóság végzett értékelések a következők tekintetében:
        i. visszajelzések;
        ii. az illetékes felügyeleti hatóság határozatai.

9.3.2 Az értékelési tevékenységek dokumentálása

A felügyeleti hatóság további követelményeket határozhat meg.

9.3.3 A panaszkezelésre vonatkozó irányítás

Az irányítási rendszer szerves részeként panaszkezelési rendszert kell létrehozni, amelynek különösen az ISO/IEC 17065/2012 szabvány 4.1.2.2 lit. c), 4.1.2.2 lit. j), 4.6 lit. d) and 7.13 pontjának követelményeit kell teljesítenie.

---

[21] Az illetékes felügyeleti hatóság további kiegészítő követelményeket határozhat meg és alkalmazhat, ha ezek összhangban állnak a nemzeti joggal.

A releváns panaszt és kifogást meg kell osztani az illetékes felügyeleti hatósággal.

9.3.4 A visszavonásra vonatkozó irányítás

Az akkreditáció felfüggesztése vagy visszavonása esetén alkalmazandó eljárásokat be kell építeni a tanúsító szervezet irányítási rendszerébe, ideértve az ügyfelek értesítését is.