Az GPDR 43. cikke szerinti tanúsító szervezet (adatvédelmi tanúsító szervezet) akkreditálása során alkalmazandó, az ISO/IEC 17065/2012 szabványt kiegészítő, az általános adatvédelmi rendelet 43. cikk (1) bekezdés b) pontja szerinti követelmények

Magyarország

Bevezetés

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) jelen dokumentumban állapítja meg a tanúsító szervezetek által teljesítendő kiegészítő követelményeket az ISO/IEC 17065/2012 szabvány, valamint az általános adatvédelmi rendelet[1] (a továbbiakban: GDPR) 43. cikk (1) bekezdés b) pontjával és 43. cikk (3) bekezdésével összhangban.

Ezt a dokumentumot az ISO/IEC 17065/2012 szabvánnyal együtt kell értelmezni. A szakaszok száma megfelel az ISO/IEC 17065/2012 szabványban használt számozásnak.

0 Előszó

Magyarországon a 2018. évi XXXVIII. törvénnyel módosított, a nemzeti akkreditálásról szóló 2015. évi CXXIV. törvény (a továbbiakban: NAH tv.) alapján a GDPR szerinti tanúsító szervezet akkreditációját a Nemzeti Akkreditáló Hatóság (a továbbiakban: NAH) végzi.

Az említett jogszabály 5. § (1) bekezdése alapján akkreditálási, bővítési eljárás iránti kérelmet a természetes személy, vagy a GDPR 43. cikke szerinti tanúsító szervezet (a továbbiakban: adatvédelmi tanúsító szervezet) elektronikus úton köteles benyújtani az akkreditáló szervhez. Az 5. § (4) bekezdés úgy rendelkezik, hogy az akkreditálást azon adatvédelmi tanúsító szervezet kérheti, amely megfelel az általános adatvédelmi rendeletben meghatározott szervezeti, személyi és működési követelményeknek. A 6. § (1) és (2a) bekezdések úgy rendelkeznek, hogy az akkreditálási eljárás értékelési és döntéshozatali szakaszból áll. Adatvédelmi tanúsító szervezet akkreditálási eljárásában és az akkreditált státusz területének bővítési eljárásában az értékelési szakasz során a GDPR 43. cikk (2) bekezdés *a)* és *e)* pontjában meghatározott követelményeknek való megfelelés és 43. cikk (3) bekezdése szerint meghatározott szempontok mint szakkérdések tekintetében a NAIH-ot szakhatóságként kell bevonni. A NAIH szakhatósági eljárásának ügyintézési határideje ötven nap.[2] Az akkreditálási eljárásért, az akkreditált státusz területének bővítési eljárásáért, a kérelemre indult felügyeleti vizsgálati eljárásért, továbbá a külföldi akkreditált státusz elismerési eljárásáért igazgatási szolgáltatási díjat kell fizetni. A NAIH mint szakhatóság eljárásáért az igazgatási szolgáltatási díjat az adatvédelmi tanúsító szervezet akkreditálási eljárásában, az akkreditált státusz

[1] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

[2] 2015. évi CXXIV. törvény 6. § (5a) bekezdés

területének bővítési eljárásában és a kérelemre indult felügyeleti vizsgálati eljárásban fizetett igazgatási szolgáltatási díj részeként, azzal együtt kell megfizetni.[3]

Az akkreditálási eljárás további részleteit a 2015. évi CXXXIV. törvény és az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény tartalmazzák.

A tanúsító szervezetek akkreditálásával kapcsolatos együttműködési és szervezési kérdéseket a NAIH és a NAH közötti kötelező erejű együttműködési megállapodás tartalmazza, amelyet mindkét szervezet közzétesz nyilvánosan elérhető módon a honlapján.

1 Alkalmazási kör

Ez a dokumentum az ISO/IEC 17065/2012 szabványt kiegészítő követelményeket állapít meg, az adatvédelmi tanúsító szervezetek szakértelmének, következetes működésének és pártatlanságának értékeléséhez.

Az ISO/IEC 17065/2012 alkalmazási körének összhangban kell állnia az általános adatvédelmi rendelettel. Az Európai Adatvédelmi Testület akkreditációra és tanúsításra vonatkozó iránymutatásai további tájékoztatást nyújtanak. A NAH és a NAIH 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 adatfeldolgozók adatkezelési műveleteire alkalmazandó.

2 Normatív hivatkozások

A GDPR 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 dokumentum 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. A tájékozódás megkönnyítése céljából az e dokumentumban használt főbb fogalommeghatározások az alábbiak.

- Tanúsítás, adatvédelmi tanúsítás vagy GDPR tanúsítás: annak értékelése és független harmadik fél általi igazolása, hogy a tanúsítási kritériumok teljesítése bizonyításra került egy adatkezelő vagy adatfeldolgozó adatkezelési műveletei tekintetében.

[3] 2015. évi CXXIV. törvény 7. § (1) és (2) bekezdés

- Akkreditáció: a tanúsító szervezet tevékenységéhez kapcsolódó harmadik fél általi hitelesítés. A sikeres tanúsító szervezet értékelési eljárás eredménye (az akkreditációs eljárás részeként).
- Nemzeti akkreditáló testület: egy tagállam egyetlen olyan testülete, amely az államtól származtatott hatáskörében elvégzi az akkreditálást az Európai Parlament és a Tanács 765/2008/EK rendelete értelmében. Magyarországon a nemzeti akkreditáló testület a Nemzeti Akkreditáló Hatóság (a továbbiakban: NAH).
- Akkreditáló testület: a testület, amely az akkreditálást végzi. Ebben a dokumentumban ez a kifejezés a NAH-ot jelöli.
- Tanúsító szervezet: tanúsítási rendszert működtető, harmadik felek körébe tartozó megfelelőségértékelő szervezet.
- Tanúsítási szempontok: azok a szempontok, amelyek alapján egy szervezet adatkezelésének megfelelőségét egy adott tanúsítási mechanizmusban ellenőrzik.
- Tanúsítási rendszer: meghatározott termékekre, folyamatokra és szolgáltatásokra vonatkozó tanúsítási rendszer, amelyre ugyanazokat a meghatározott követelményeket, egyedi szabályokat és eljárásokat kell alkalmazni. Beletartoznak a tanúsítási szempontok és az értékelési módszertan.
- Tanúsítási mechanizmus: egy jóváhagyott tanúsítási rendszer, amely elérhető a kérelmező számára. Egy akkreditált tanúsítási szervezet által, jóváhagyott szempontok és értékelési módszertan alapján nyújtott szolgáltatás. Az a rendszer, amely alapján egy adatkezelőt vagy adatfeldolgozót tanúsítanak.
- Értékelés tárgya: a tanúsítás tárgya. A GDPR tanúsítás esetében a releváns adatkezelési műveletek, amelyeknek az értékelésére és tanúsítására az adatkezelő vagy adatfeldolgozó a kérelmet benyújtja.
- Kérelmező: az a szervezet, amely az adatkezelési műveleteinek tanúsítására a kérelmet benyújtotta.
- Ügyfél: az a szervezet, amelyet tanúsítottak (korábban kérelmező).

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 NAH és a NAIH felé, hogy olyan naprakész eljárásokkal rendelkeznek, amelyek bizonyítják az akkreditáció feltételeiben meghatározott jogi kötelezettségeknek – ezen belül a GDPR alkalmazására vonatkozóan meghatározott kiegészítő követelményeknek – való megfelelést.

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 GDPR-nak. A tanúsító szervezetnek bizonyítékot kell szolgáltatnia a megfelelésről, az

akkreditálási folyamat során kért módon. Ennek keretében a tanúsító szervezetnek meg kell erősítenie a NAH felé, hogy nincs folyamatban vele szemben NAIH eljárás.

4.1.2. Tanúsítási megállapodás (TM)

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 általános tanúsítási követelményeknek, mind a NAIH vagy az Európai Adatvédelmi Testület által a GDPR 43.cikk (2) bekezdésének b) pontjával és a 42. cikk (5) bekezdésével összhangban jóváhagyott kritériumoknak;
2. előírják, hogy a kérelmezőnek teljes átláthatóságot kell biztosítania a NAIH számára a tanúsítási eljárás tekintetében, beleértve a GDPR 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 GDPR rendelkezéseinek való megfelelés tekintetében, és nem érintik a NAIH-nak a GDPR 42. cikk (5) bekezdése szerinti feladatait és hatásköreit;
4. előírják, hogy a kérelmezőnek a GDPR 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 figyelembe kell venni és be kell tartani;
6. az ISO/IEC 17065/2012 4.1.2.2. lit. c 1. pontja tekintetében meg kell határozniuk a GDPR 42. cikk (7) és a 43. cikk (4) bekezdésének megfelelő érvényességi, megújítási és visszavonási szabályokat, beleértve azokat a szabályokat is, amelyek a GDPR 42. cikk (7) bekezdésével összhangban megfelelő időközöket határoznak meg az újraértékelés vagy a felülvizsgálat tekintetében (rendszeresség);
7. lehetővé teszik a tanúsító szervezet számára, hogy a GDPR 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 GDPR 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, illetve ha az értékelés tárgyával összefüggő, a NAIH vagy illetékes bíróság által megállapított jogsértésre kerül sor;

11. kötelező értékelési módszereket tartalmaz az értékelés tárgyára vonatkozóan.

4.1.3. Az adatvédelmi bélyegzők és jelölések használata

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

4.2. A pártatlanság kezelése

A NAH-nak, az ISO/IEC 17065/2012 szabványban, különösen annak 3.13. és 4.2. pontjában, valamint a 765/2008/EK rendelet 17. cikk (3) bekezdésében foglalt követelményeken felül biztosítania kell, hogy a tanúsító szervezet:

1. megfelel a NAIH által ebben a dokumentumban megfogalmazott kiegészítő követelményeknek (a GDPR 43. cikk (1) bekezdés b) pontjának megfelelően):

a. a GDPR 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. igazolta / bemutatta, hogy a GDPR 43. cikk (2) bekezdésének e) pontjával összhangban feladataival kapcsolatban nem áll fenn összeférhetetlenség;

2. nem fűzi releváns kapcsolat az általa értékelt kérelmezőhöz (pl. a tanúsító szervezet nem tartozhat ugyanahhoz a cégcsoporthoz, és nem tartozhat semmilyen módon az irányítása alá).

4.3. Felelősség és finanszírozás

Az ISO/IEC 17065/2012 4.3.1. pontjában szereplő előíráson túl a tanúsító szervezet rendszeresen igazolja a NAH felé, hogy megfelelő intézkedéseket (pl. biztosítás vagy tartalékok) tett annak érdekében, hogy megfeleljen a működése szerinti földrajzi régiókban fennálló felelősségviselési kötelezettségének.

4.4. Diszkriminációtól mentes feltételek

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

4.5. Titoktartás

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

4.6. Nyilvánosan hozzáférhető információk

Az ISO/IEC 17065/2012 szabvány 4.6. pontjában előírt követelmény mellett a tanúsító szervezetnek a következőket is igazolnia kell a NAH felé:

- a GDPR 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, feltüntetve a vonatkozó érvényességi időt;
- a GDPR 43. cikk (2) bekezdésének d) pontja értelmében a panaszkezelési eljárásokkal és a fellebbezésekkel kapcsolatos információkat nyilvánosságra hozzák.

5 Szervezeti követelmények, 43. cik (4) bekezdés [„megfelelő értékelés”]

5.1. Szervezeti felépítés és felső vezetőség

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

5.2. A pártatlanság megőrzését biztosító mechanizmusok

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

6 Erőforrásokra vonatkozó követelmények

6.1. A tanúsító szervezet személyzete

Az ISO/IEC 17065/2012 szabvány 6. pontjában előírt követelmény mellett az akkreditáló testületnek biztosítania kell minden tanúsító szervezet esetében, hogy személyzete

1. a GDPR 43. cikk (1) bekezdésének megfelelően bizonyítottan megfelelő és naprakész szakértelemmel (tudással és tapasztalattal) rendelkezik az adatvédelem tekintetében;
2. a GDPR 43. cikk (2) bekezdés a) pontjának megfelelően független, és a tanúsítás tárgyában naprakész szakértelemmel bír, valamint a GDPR 43. cikk (2) bekezdés e) pontjának megfelelően nem áll fenn feladataival kapcsolatban összeférhetetlenség;
3. a GDPR 43. cikk (2) bekezdése b) pontjának megfelelően vállalja, hogy tiszteletben tartja a GDPR 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 6.1.1., 6.1.4. és 6.1.5. kiegészítő követelményben említett területeken, különösen:

A technikai szakértelemmel rendelkező személyzet esetén:

- az érintett technikai szakterületen legalább az európai képesítési keretrendszer[4] 6. szintjének megfelelő képesítést vagy elismert védett címet (pl.: Dipl. Ing.) szerzett az érintett szabályozott szakmában.
- 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 jogi szakértelemmel rendelkező személyzet esetén:

- az EU által vagy államilag elismert egyetemen szerzett, legalább nyolc féléves jogi tanulmányok, ideértve a mesterfokozatú vagy ezzel egyenértékű diplomát (LL.M.) is
- *A tanúsítási döntésekért felelős személyzetnek* az adatvédelmi jog terén szerzett legalább ötéves szakmai – és az elvégzendő feladatokkal összefüggő – tapasztalattal kell rendelkeznie.
- *Az értékelésekért felelős személyzetnek* legalább hároméves, az adatvédelmi jog terén szerzett szakmai tapasztalattal, valamint a hasonló eljárásokkal (pl. tanúsítványokkal/ellenőrzésekkel) kapcsolatos ismeretekkel és gyakorlattal kell rendelkeznie.

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

A szakértelem a megfelelő, releváns szakképesítésre vagy tanfolyamokra vonatkozó dokumentumok (pl. bizonyítvány, oklevél) által igazolható, amelyek a szükséges végzettségeket vagy szakértelmet tanúsítják.

6.2. Az értékeléshez szükséges erőforrások

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

7 Eljárási követelmények[5]

7.1. Általános követelmények

Az ISO/IEC 17065/2012 szabvány 7.1. pontjában előírt követelmények mellett a NAH-nak biztosítania kell az alábbiak teljesülését:

1. A tanúsító szervezetek a kérelem benyújtásakor a GDPR 43. cikk (1) bekezdésének b) pontja szerint teljesítik az illetékes felügyeleti hatóság által megállapított kiegészítő követelményeket annak érdekében, hogy a GDPR 43. cikk

[4] Lás az összehasonlítási módszert a https://ec.europa.eu/ploteus/en/compare? oldalon
[5] GDPR 43. cikk (2) bekezdés c) és d) pont

(2) bekezdésének b) pontjával összhangban a feladatok és kötelezettségek ne vezessenek összeférhetetlenséghez;

2. Értesítik az illetékes felügyeleti hatóságokat azt megelőzően, hogy a tanúsító szervezet megkezdené kihelyezett irodáján keresztül a jóváhagyott európai adatvédelmi bélyegző új tagállamban történő működtetését.

7.2. Kérelem

Az ISO/IEC 17065/2012 7.2. pontjában foglalt követelményeken túlmenően a tanúsító szervezetnek elő kell írnia 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 a felelősségi körüket és feladataikat, továbbá a kérelemnek tartalmaznia kell az érintett adatkezelői/adatfeldolgozói szerződés(eke)t;
3. annak feltüntetése, hogy közös adatkezelők részt vesznek-e az adatkezelésben, és ha a kérelmezők közös adatkezelők, a felelősségi körüket és feladataikat ismertetni kell, továbbá a kérelemnek tartalmaznia kell az általuk elfogadott megállapodást;
4. tájékoztatást kell adnia a kérelmezőnek minden olyan folyamatban lévő vagy korábbi NAIH eljárás tényéről, amelynek az alanya a kérelmező, és amely az értékelés tárgyával összefügg.

7.3. A kérelem vizsgálata

Az ISO/IEC 17065/2012 7.3. pontján túlmenően elő kell írni, hogy a 7.3. e) szakasz elegendő szakértelem meglétére irányuló értékelése kellőképpen vegye figyelembe a 6. cikk alapján az adatvédelem területére vonatkozó technikai és jogi szakértelmet egyaránt.

A kérelem vizsgálatának figyelembe kell vennie az e dokumentum 7.2.4. pontja szerinti adatvédelmi megfelelőségellenőrzést. A tanúsító szervezetnek meg kell győződnie arról, hogy a kérelmező megfelelő jelölt adatvédelmi tanúsításra.

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;
4. továbbá 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, akiket a 6. pontban előírt szakmai követelményeket alkalmazva a tanúsító szervezet elismert. A tanúsító szervezet akkor is megőrzi a felelősséget a döntéshozatalért, amennyiben külső szakértőket alkalmaz.

Az ISO/IEC 17065/2012 7.4.5. pontján túlmenően elő kell írni, hogy a GDPR 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 a kérelmezőt a tanúsítási mechanizmusnak való megfelelés hiányosságairól. Ezen 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 a NAIH számára.

7.5. Felülvizsgálat

Kötelező az ISO/IEC 17065/2012 7.5. pontján túlmenően eljárásokat létrehozni a GDPR 43. cikk (2) bekezdése és a GDPR 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 tanúsítási szervezet köteles részletesen meghatározni az eljárásaiban azt, hogy milyen módon biztosítja az egyes tanúsítási döntések vonatkozásában a függetlenségét és a felelősségét.

Az átláthatóság biztosítása érdekében, az ISO/IEC 17065/2012 által előírt követelményeken kívül, a tanúsító szervezet számára elő kell írni, hogy a jóváhagyás tervezetét, beleértve az

értékelési jelentés összefoglalóját, közvetlenül a tanúsítás kibocsátását vagy megújítását megelőzően a NAIH számára be kell nyújtani. Az összefoglalónak világosan be kell mutatnia, hogy a szempontok milyen módon teljesülnek, ezáltal bemutatva a tanúsítás megadásának vagy fenntartásának indokait. Még amennyiben a NAIH úgy is döntene, hogy a benyújtott információk alapján eljárást indít, ez a tény nem függeszti fel a tanúsítási eljárást.

A kérelmezési szakaszt követően is, a tanúsítvány kibocsátását megelőzően, a tanúsítási szervezetnek elő kell írni, hogy a kérelmezőtől megerősítést kérjen arról, hogy nem áll semmilyen, az értékelés tárgyával vagy a tanúsítás alkalmazási körével összefüggő NAIH vizsgálat vagy eljárás alatt, amely megakadályozhatná a tanúsítvány kibocsátását.

7.7. Tanúsítási dokumentáció

Az ISO/IEC 17065/2012 7.7.1.e) pontján túlmenően és a GDPR 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 verzióstátusszal vagy más hasonló jellemzőkkel együtt).

A tanúsító szervezetet kötelezni kell arra, hogy tanúsítvány kibocsátásakor az ISO/IEC 17065/2012 7.7.1. pontjában említett tanúsítási dokumentáció másolatát a NAIH rendelkezésére bocsássa.

7.8. A tanúsított termékek jegyzéke

Az ISO/IEC 17065/2012 7.8. ponton túlmenően a tanúsító szervezet köteles a tanúsított termékekre, eljárásokra és szolgáltatásokra vonatkozó információkat szervezetén belül és a nyilvánosság számára elérhető módon megőrizni. 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 tanúsítás alkalmazási köre és a tanúsítás (értékelés) tárgyának érthető leírása,
- a vonatkozó tanúsítási kritériumok (beleértve a verziót és a funkcionális státuszt),
- az értékelési módszerek és az elvégzett vizsgálatok, valamint az eredmény(ek).

Az ISO/IEC 17065/2012 7.8. pontján túlmenően és a GDPR 43. cikk (5) bekezdésének megfelelően a tanúsító szervezet közli az illetékes felügyeleti hatóságokkal 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 a GDPR 43. cikke (2) bekezdésének c) pontja szerint elő kell írni, hogy az ellenőrzési időszak során foganatosítsanak rendszeres ellenőrzési intézkedéseket a tanúsítás fenntartásához. A felügyelet gyakoriságának meghatározásakor elsősorban az adatkezeléssel

járó kockázatokat kell figyelembe venni, de minden esetben legalább kétévente sor kell, hogy kerüljön ellenőrzésre.

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:

- bármely magas kockázatú adatvédelmi incidens bekövetkezése, vagy a NAIH vagy illetékes bíróság által megállapított jogsértés, amely kapcsolatban áll az értékelés tárgyával, és amelyet az ügyfél vagy a NAIH jelzett;
- az adatvédelmi jogszabályok módosítása, vagy a tudomány és technológia állásának változása,
- az Európai Bizottság által a GDPR 43. cikk (8) bekezdése és a GDPR 43. cikk (9) bekezdése alapján elfogadott felhatalmazáson alapuló jogi aktusok,
- az Európai Adatvédelmi Testület által elfogadott alkalmazandó dokumentumok, és
- adatvédelemmel kapcsolatos bírósági határozatok.

Az itt meghatározandó módosítási eljárások közé tartozhatnak például a következők: átmeneti időszakok, a NAIH jóváhagyási eljárása, 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. 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 a NAIH-ot és a NAH-ot a meghozott intézkedésekről, valamint a tanúsítás folytatásáról, korlátozásáról, felfüggesztéséről és visszavonásáról.

A GDPR 58. cikk (2) bekezdés h) pontja szerint a tanúsító szervezetnek el kell fogadnia a NAIH 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[6]

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

- ki nyújthat be panaszt vagy kifogást,
- ki kezeli ezeket a tanúsító szervezet részéről,

[6] GDPR 43. cikk (2) bekezdés d) pont

- milyen ellenőrzésekre kerül sor ezzel összefüggésben, továbbá
- 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:

- hogyan és kinek a számára kell ilyen megerősítést adni,
- milyen határidők vonatkoznak erre, továbbá
- ezt követően milyen eljárásokat kell kezdeményezni.

A tanúsító szervezeteknek elő kell írni, hogy a panaszkezelési eljárásukat nyilvánosan és érintettek számára könnyen elérhetővé tegyék.

A tanúsító szervezetnek elő kell írni, hogy a panaszost ésszerű határidőn belül tájékoztassa a panaszkezelés menetéről és eredményéről.

Az ISO/IEC 17065/2012 7.13.1. pontján túlmenően a tanúsító szervezetnek meg kell határoznia, hogyan biztosítja a tanúsítási tevékenységek, valamint 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 meghatároznia 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 a GDPR 58. cikk szerinti akkreditációs eljárás keretében, majd ezt követően a NAIH kérésére a GDPR 58. cikk (1) bekezdésének b) pontja szerinti adatvédelmi felülvizsgálat formájában végzett vizsgálat során vagy a GDPR 42. cikk (7) bekezdése szerint kiadott tanúsítványokra vonatkozóan a GDPR 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[7].

Az átláthatóság érdekében a tanúsító szervezetnek:

- figyelemmel kell kísérnie a megfelelőségértékelés alapjául szolgáló alapelveket (például hivatkozott műszaki szabványok, törvények és rendeletek stb.);
- dokumentálnia kell a megfelelőségértékeléshez alkalmazott ellenőrzések megállapításához használt speciális módszereket;
- dokumentálnia kell a vizsgálati és ellenőrzési tevékenységeket, és a meglévő eljárásokkal kapcsolatban eszközölt javításokat, ideértve ezek indokait és menetrendjét;
- dokumentálnia és ellenőriznie kell a pártatlansággal kapcsolatos követelményeket;
- meg kell indokolnia az egyes tanúsítási mechanizmusokkal kapcsolatban a nyilvántartásban és eljárásban bekövetkező változásokat, a mechanizmusoknak való megfelelés érdekében kialakított intézkedéseket, és az ügyfelekkel kötött tanúsítási megállapodásokban előírt minimális követelményeket.

8.1. Az irányítási rendszerre vonatkozó általános követelmények

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

8.2. Az irányítási rendszerre vonatkozó dokumentáció

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

8.3. Dokumentumok kezelése

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

8.4. Nyilvántartás kezelése

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

8.5. Az irányítás felülvizsgálata

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

8.6. Belső ellenőrzések

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

8.7. Korrekciós intézkedések

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

8.8. Megelőző intézkedések

Az ISO/IEC 17065/2012 követelményei alkalmazandók.

[7] GDPR (100) preambulumbekezdés

9 További kiegészítő követelmények

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 és kérelmezői 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:
   - információkérések, vagy
   - a kapcsolatfelvétel lehetővé tétele egy adott tanúsítással kapcsolatos panasztétel esetében;
2. A kérelmezési eljárás megőrzése a következő célból:
   - a kérelem státuszával és kimenetelével kapcsolatos tájékoztatás;
   - a NAIH által végzett értékelések a következők tekintetében
     a. visszajelzések;
     b. a NAIH határozatai.

9.3.2. Az értékelési tevékenységek dokumentálása

Nincsenek további követelmények.

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.

A releváns panaszt és kifogást meg kell osztani a NAIH-al.

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.