Az általános adatvédelmi rendelet 41. cikke szerinti, a magatartási kódexnek való megfelelést ellenőrző szervezetek akkreditációs követelményei

Magyarország

Tartalomjegyzék

1. Bevezetés

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet, a továbbiakban: GDPR) 41. cikkének (1) bekezdése szerint a 40. cikk szerinti magatartási kódexnek való megfelelés ellenőrzését olyan szervezet végezheti, amely megfelelő szintű szakértelemmel rendelkezik a kódex tárgyával kapcsolatosan és amelyet az illetékes felügyeleti hatóság e célra akkreditált.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 38. § (2a) bekezdése szerint a Magyarország joghatósága alá tartozó természetes és jogi személyek tekintetében a felügyeleti hatóság számára a GDPR-ban meghatározott feladatokat és hatásköröket a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) gyakorolja a GDPR és az Infotv. rendelkezései szerint.

A GDPR 41. cikkének (2) bekezdése alapján a magatartási kódexet kidolgozó adatkezelők vagy az adatfeldolgozók kategóriáit képviselő egyesületek és egyéb szervezetek (a továbbiakban: a kódex felelősei) javaslatokat tesznek a kódexnek való megfelelést ellenőrző szervezet működésére vonatkozóan azért, hogy ezen ellenőrző szervezetet az illetékes felügyeleti hatóság e célból akkreditálja. E cikk értelmében az ellenőrző szervezetnek:

a) az illetékes felügyeleti hatóság számára kielégítő módon bizonyítania kell *függetlenségét* és *szakértelmét* a kódex által szabályozott tárgykörrel kapcsolatban;
b) olyan *eljárásokat* kell kialakítania, amelyek lehetővé teszik annak értékelését, hogy az érintett adatkezelők és adatfeldolgozók a kódex *előírásait betartják és megfelelően alkalmazzák*-e. A kialakított eljárásoknak továbbá lehetővé kell tenniük, hogy az ellenőrző szerv nyomon követhesse azt, hogy az adatkezelők és adatfeldolgozók a kódex rendelkezéseinek megfelelnek-e, továbbá, hogy a működésüket rendszeresen képes legyen felülvizsgálni;
c) *eljárásokat kell kialakítania a kódex megsértésével* vagy a kódex adatkezelő vagy adatfeldolgozó általi végrehajtásának módjával *kapcsolatos panaszok kezelésére*, és ezeket az eljárásokat és struktúrákat átláthatóvá kell tennie az érintettek és a nyilvánosság számára; végül
d) az illetékes felügyeleti hatóság számára kielégítően bizonyítania kell, hogy feladatai és kötelezettségei végrehajtása *nem eredményez összeférhetetlenséget*.

A GDPR és az Infotv. fenti rendelkezései alapján a NAIH a magatartási kódexet ellenőrző szervezetek alábbi akkreditációs követelményeit teszi közzé. Ezeket az akkreditációs követelményeket az Európai Adatvédelmi Testületnek az általános adatvédelmi rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről szóló 1/2019. sz. iránymutatásával együtt kell értelmezni.[1]

2. Eljárási szabályok és a kérelem díjai

Az Infotv. 64/A. § (1) bekezdés b) pontja alapján a NAIH az adatkezelés engedélyezésére irányuló eljárást folytat le, ha a GDPR 41. cikke szerinti ellenőrző szervezet akkreditációja iránti kérelmet nyújtanak be.

---

[1] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_hu.pdf

A kérelemnek az általános közigazgatási rendtartásról szóló 2016. évi CL. törvényben (a továbbiakban: Ákr.) foglalt rendelkezéseken túl tartalmaznia kell azokat az adatokat, amelyek igazolják, hogy a GDPR 41. cikk (2) bekezdésében, valamint a NAIH által kiadott jelen akkreditációs követelményekben meghatározott feltételek teljesülnek.

Az Infotv. 64/B. §-a szerint az adatkezelési engedélyezési eljárás lefolytatásáért a 25/2018. (IX. 3.) számú igazságügyi miniszteri rendeletben (a továbbiakban: miniszteri rendelet) meghatározott igazgatási szolgáltatási díjat kell fizetni. A miniszteri rendelet 1. § b) pontja alapján a GDPR 41. § szerinti ellenőrző tevékenységet végző szervezet akkreditációja iránti kérelem igazgatási szolgáltatási díja 530.000 Ft. A díjat a kérelem előterjesztésével egyidejűleg kell befizetni a NAIH Magyar Államkincstárnál vezetett következő bankszámlájára: 10032000-00319425-000000000.

A GDPR 41. cikke szerinti ellenőrző szervezet akkreditációja iránti kérelem kapcsán meginduló engedélyezési hatósági eljárásban a határidő száznyolcvan nap az Infotv. 64/C. § (1) bekezdés a) pontja alapján. Amennyiben az engedélyezési eljárás határon átnyúló jellegű, a NAIH felfüggeszti azt a GDPR 60. cikk (3)-(5) bekezdése szerinti együttműködési eljárás és a GDPR 63-66. cikke szerinti egységességi mechanizmus időtartamára, azzal, hogy a NAIH a felfüggesztés időtartama alatt is végrehajtja az együttműködési eljárásban és az egységességi mechanizmus során szükséges eljárási cselekményeket.

Az ellenőrző szervezeti tevékenység akkreditálása iránti kérelem benyújtása esetén a NAIH a hatósági eljárásban a szükséges számú alkalommal felhívhatja a kérelmezőt a kérelem vagy annak részét képező szabályzat-tervezetek módosítására, kiegészítésére azok jóváhagyása és az engedély megadása érdekében.

Az akkreditáció időtartamát első alkalommal három évben kell megállapítani, amelynek lejárta előtt felülvizsgálatra kerül sor annak megállapítása érdekében, hogy az ellenőrző szervezet továbbra is megfelel-e az akkreditációs követelményeknek. Ez az előírás nem érinti a kódexfelelősök azon lehetőségét, hogy magában a kódexben esetleg erre vonatkozóan rövidebb időtartamot írjanak elő.

A NAIH hatósági eljárásban dönt az Ákr. vonatkozó rendelkezései szerint az ellenőrző szervezet akkreditációjáról. Az akkreditáció pontos időtartamát a döntésről szóló határozatban kell meghatározni. Ha a határozatban meghatározott határidő az akkreditáció megújítása iránti kérelem nélkül jár le, az ellenőrző szervezet akkreditációja automatikusan megszűnik.

Annak ellenőrzése érdekében, hogy az ellenőrző szervezet megfelel-e az akkreditációs követelményeknek és ellenőrzési feladatait a GDPR-nak megfelelően látja-e el, a NAIH fenntartja magának a jogot, hogy az akkreditáció felülvizsgálatát az adott időtartam lejárta előtt kezdeményezze. Erre különösen abban az esetben lehet szükség, ha a NAIH olyan fennálló kockázati vagy egyéb tényezőkről szerez tudomást, amelyek befolyásolhatják vagy veszélyeztethetik az ellenőrző szervezet jelen akkreditációs követelményeknek vagy az ellenőrzési kötelezettségeinek való megfelelését, vagy egyébként az ellenőrző szervezet által a GDPR érvényesülésének elősegítésére elfogadott intézkedések érvényesülését.

Az ellenőrző szervezetet az akkreditáció időtartamára kell akkreditálni, kivéve, ha a NAIH által végzett felülvizsgálat megállapítja, hogy az ellenőrző szervezet már nem felel meg az akkreditációs követelményeknek, vagy nem képes ellenőrzési kötelezettségeinek eleget tenni, vagy az általa hozott intézkedések sértik a GDPR rendelkezéseit.

Az akkreditáció megújítása iránti kérelmet legalább az akkreditáció határidejének lejárta előtt száznyolcvan nappal kell benyújtani a NAIH-hoz az Infotv. 64/C. §-ában meghatározott határidő betartása érdekében. A megújítás iránti eljárásra a miniszteri rendelet 1. § b) pontja szerinti, az igazgatási szolgáltatási díjra vonatkozó szabályokat alkalmazni kell.

Amennyiben az akkreditációs idő megújítás iránti kérelem nélkül jár le, az ellenőrző szervezet a GDPR-ban, az Infotv.-ben és a jelen akkreditációs követelményekben meghatározott hatásköreit a továbbiakban nem gyakorolhatja.

A magatartási kódex tekintetében új vagy további ellenőrző szervezet létrehozása szükségessé teszi, hogy az új szervezetet az akkreditációs követelményekkel összhangban külön engedélyezési eljárásban értékeljék. Erre az akkreditációs eljárásra a miniszteri rendelet 1. § b) pontjában meghatározott igazgatási szolgáltatási díjra vonatkozó szabályokat alkalmazni kell.

Mivel a magatartási kódex hatálya alá tartozó ágazat(ok) sajátosságait a NAIH az akkreditáció során figyelembe veszi, ezért külön akkreditációs kérelmet kell benyújtani a NAIH-hoz abban az esetben, ha egy adott kódexnek való megfelelés ellenőrzésére akkreditált szervezet más kódex tekintetében is el kíván látni ellenőrzési feladatokat. Erre az akkreditációs eljárásra a miniszteri rendelet 1. § b) pontjában foglaltak szerinti igazgatási szolgáltatási díjra vonatkozó szabályokat alkalmazni kell.

3. A kérelemmel kapcsolatos tartalmi követelmények

Az ellenőrző szervezet akkreditációja iránti kérelmet az azt alátámasztó valamennyi dokumentummal együtt a NAIH-hoz kell benyújtani. A hivatalos benyújtáshoz és levelezéshez a következő elérhetőségek vehetők igénybe:

Postai úton: 1363 Budapest, Pf.: 9.
Hivatali kapun keresztül: rövid név: NAIH, KRID: 429616918

A kérelmet magyar nyelven kell benyújtani, és csatolni kell hozzá az akkreditációs követelmények teljesülését alátámasztó, igazoló dokumentumokat. A kérelemnek a következő információkat mindenképpen tartalmaznia kell:

a) A kérelmező azonosítására szolgáló adatok; ha a kérelmező társaság, egyesület, alapítvány vagy más szervezet, a jogi képviselőt és az ellenőrző tevékenység keretein belül hozott döntések meghozataláért felelős személy(eke)t azonosító adatok;
b) A kérelmező adóazonosítója, továbbá gazdasági társaságok esetében a cégjegyzékszám;
c) A kérelmező lakóhelyére, vagy ha a kérelmező gazdasági társaság, egyesület, alapítvány vagy más szervezet a bejegyzett székhelyére vonatkozó adatok. Ez mindkét esetben az Európai Gazdasági Térségben kell, hogy megtalálható legyen;
d) Az alapító okirat és az alapszabály másolata, gazdasági társaságok, egyesületek, alapítványok és egyéb szervezetek esetében;
e) Az alkalmazottak száma és szerepe;
f) Az akkreditációs kérelemmel kapcsolatos kommunikáció során használandó elérhetőségek;
g) Az ellenőrző szervezet típusának meghatározása (azaz, hogy belső vagy külső);
h) Azon magatartási kódex meghatározása, amelynek tekintetében az akkreditációt kérik;
i) Az adatkezelők, adatfeldolgozók kategóriáinak és azon ágazatoknak a megjelölése, amelyekért az ellenőrző szervezet felelős;
j) Azon területi hatálynak a meghatározása, amelynek keretei között az ellenőrző szervezet az ellenőrzési tevékenységét gyakorolja, beleértve a magatartási kódex nemzeti vagy határon átnyúló (transznacionális) alkalmazási körét is.

Ha egynél több ellenőrző szervezet kér akkreditációt a magatartási kódexhez, akkor a GDPR 41. cikk (2) bekezdésében meghatározott követelmények teljesítésének bizonyítása mellett a

kérelmezőknek a kérelemben ismertetniük kell az akkreditációt kérő ellenőrző szervezeteknek az esetleges kompetencia- és felelősség elosztására vonatkozó információkat is. Meg kell tehát tudni különböztetni az egyes ellenőrző szervezetek hatáskörét és ezekkel kapcsolatos felelősségét. E tekintetben a kérelemnek tartalmaznia kell egy listát vagy útmutatót az ellenőrzési tevékenységgel kapcsolatos hatásköreik megosztásáról, és jeleznie kell, hogy melyik ellenőrző szervezet a kódexet alkalmazó mely tagokért felelős. A kérelemben ismertetni kell az ehhez szükséges struktúrákat, üzleti folyamatokat és egyéb szervezeti intézkedéseket is.

Az akkreditációs kérelemhez csatolni kell az összes annak bizonyításához szükséges dokumentumot, hogy a jelen akkreditációs követelményekben lefektetett előírások teljesülnek.

Az akkreditációs eljárás során az ellenőrző szervezetnek tudnia kell azt bizonyítani, hogy képes ellenőrzési tevékenységeit a GDPR 40. és 41. cikkeinek, valamint ezen akkreditációs követelményeknek megfelelően gyakorolni.

4. Jogállás

A jogi személy ellenőrző szervezetnek az Európai Gazdasági Térség területén bejegyzett székhellyel kell rendelkeznie. Amennyiben az ellenőrző szervezet természetes személy, ahhoz, hogy szakmai tevékenységét ellenőrző szervezetként gyakorolhassa, szintén az Európai Gazdasági Térség területén lévő székhellyel vagy lakóhellyel kell rendelkeznie.

Az ellenőrzési tevékenységet végezheti a kódexfelelőstől szervezetileg elkülönült külső szervezet (külső ellenőrző szervezet) vagy az végezhető a kódex felelősének belső szervezeti egységeként (belső ellenőrző szervezet). A belső ellenőrző szervezetek további intézkedéseket hoznak a kódexfelelős szervezeti struktúráján belüli elkülönülés biztosítása érdekében (további részletekért lásd jelen dokumentum 5. pontját).

Ha az ellenőrző szervezet természetes személy, bizonyítania kell tudni azt, hogy rendelkezik az ellenőrző szervezeti feladatok teljes körű ellátásához szükséges humán, pénzügyi és egyéb erőforrásokkal valamint eljárási renddel. Ezek kapcsán különösen azt kell tudnia biztosítani, hogy a természetes személy ellenőrző szervezet hirtelen, átmeneti vagy tartós elveszítéséhez vezető, előre nem látható esemény bekövetkezése esetén az ellenőrzési tevékenységek megszakítás nélkül tudjanak folytatódni.

5. Függetlenség

A GDPR 41. cikk (2) bekezdésének a) pontjával összhangban az ellenőrző szervezetnek bizonyítania kell, hogy mindenkor biztosított a kódex tagjaitól, a kódex felelősétől, valamint a szakmai iparágtól és a magatartási kódex ágazatától való függetlensége. E tekintetben azt is bizonyítania kell, hogy rendelkezik a függetlenségével kapcsolatos kockázatok hatékony kezeléséhez szükséges megfelelő eljárásokkal és szervezési intézkedésekkel. A függetlenség csak akkor lehetséges, ha ezek garantálják a pártatlanságot, az objektivitást és a belső integritást.

A függetlenség jogi, gazdasági, személyes és ténybeli szempontokat is magában foglal. A következő rendelkezésekkel összhangban az ellenőrző szervezetnek megfelelő intézkedéseket kell tennie minden olyan közvetlen vagy közvetett, kereskedelmi, pénzügyi vagy egyéb beavatkozás megakadályozására, amely veszélyezteti vagy veszélyeztetheti az ellenőrző szervezet függetlenségét és pártatlanságát.

Az ellenőrző szervezet nem fogadhat el utasításokat feladatai ellátásával kapcsolatban, és sem közvetve, sem közvetlenül nem befolyásolható feladatai ellátásában. Ezenkívül az ellenőrző szervezetet sem a kódex felelőse, sem a kódex tagjai nem büntethetik ellenőrzési feladatai ellátásáért.

5.1. A szervezeti struktúra függetlensége

Belső ellenőrző szervezetek nem hozhatók létre a kódexhez csatlakozó egyes tagok szervezetein belül. Az ellenőrző tevékenységet ebben az esetben kizárólag a kódexfelelős elkülönült belső szervezeti egysége végezheti, továbbá ez esetben bizonyítania is kell a feladatai ellátása tekintetében való függetlenségét, amit dokumentált belső szabályzatokkal és eljárásrenddel kell alátámasztania.

Különösen azt kell bizonyítani, hogy a belső ellenőrző szervezet strukturálisan elkülönül a kódexfelelős egyéb területeitől a felső vezetés alatti szintig bezárólag. E tekintetben az ellenőrző szervezetnek saját személyzettel kell rendelkeznie, továbbá feladatai, elszámoltathatósága és jelentéstételi rendszere tekintetében el kell különülnie a kódex felelősének egyéb területeitől. A belső ellenőrző szervezetnek a szervezet egyéb területeitől elkülönült irányítással kell rendelkeznie. A belső ellenőrző szervezet közvetlenül a kódexfelelős szervezetén belüli legmagasabb vezetői szintnek tartozik beszámolási kötelezettséggel. Biztosítani kell továbbá, hogy sem a kódex felelőse, sem a kódex tagjai ne gyakorolhassanak semmilyen befolyást az ellenőrző szervezetre.

Amennyiben az ellenőrzési tevékenységet a kódexfelelős struktúrájától elkülönült külső ellenőrző szervezet végzi, úgy bizonyítani kell, hogy az ellenőrző szervezet nem kínál a kódex felelőse vagy a kódex tagjai, illetve a kódex hatálya alá tartozó szakma, iparág vagy ágazat számára olyan terméket, illetve nem kínál olyan szolgáltatást, amely aláásható annak autonómiáját, függetlenségét és pártatlanságát, illetve ellenőrzési feladatainak tényleges ellátását.

Az ellenőrző szervezet például a következő dokumentumokkal igazolhatja szervezeti függetlenségét:

- *Az ellenőrző szervezet és a kódexfelelős alapító okirata és alapszabálya;*
- *Az ellenőrző szervezet ellenőrzési tevékenységekkel kapcsolatos döntéshozatalért felelős személyzetének tagságára, kinevezésére, javadalmazására és hivatali idejére vonatkozó szabályok és eljárások;*
- *Az ellenőrző szervezet és a kódexfelelős vagy a kódexet benyújtó egyesület/szervezet közötti üzleti, pénzügyi, szerződéses vagy egyéb kapcsolatokat igazoló dokumentumok.*

5.2. Pénzügyi függetlenség

Az ellenőrző szervezetnek bizonyítania kell, hogy rendelkezik a feladatai hatékony ellátásához és kötelezettségei teljesítéséhez szükséges pénzügyi forrásokkal. Az ellenőrző szervezetnek rendelkeznie kell a hosszú távú pénzügyi stabilitás biztosításához szükséges pénzügyi forrásokkal. Ezenkívül, ha a kódex egy vagy több tagja kilép a magatartási kódexből, ez nem veszélyeztetheti az ellenőrző szervezet finanszírozását.

Az ellenőrző szervezetnek képesnek kell lennie arra, hogy pénzügyi forrásait önállóan és függetlenül kezelje, a kódex felelőse, a kódex tagjai vagy a kódex hatálya alá tartozó szakma, iparág vagy ágazat beavatkozása, nyomásgyakorlása vagy ellenőrzése nélkül.

Az ellenőrző szervezetnek bizonyítania kell, hogy finanszírozási mechanizmusai nem ássák alá ellenőrzési funkcióinak autonómiáját, függetlenségét és pártatlanságát, és hogy azokkal kapcsolatban képes elszámolni. Ha az ellenőrző szervezet a kódex felelősének belső szervezeti egységeként működik, külön költségvetést kell elkülöníteni részére.

Az ellenőrző szervezet például a következő dokumentumokkal igazolhatja pénzügyi függetlenségét:

- *A finanszírozás forrásaira vonatkozó dokumentáció benyújtása a NAIH-hoz a megfelelő pénzügyi források igazolásaként;*
- *A tevékenységeiből eredő pénzügyi kockázatértékelés;*
- *Belső eljárások a függetlenséget veszélyeztető vagy kizáró körülmények elkerülésének biztosítása és kellő céltartalékok képzése érdekében a tevékenységeiből származó fennmaradó pénzügyi kockázatok kezelése céljából (pl. pénzügyi veszteségre vonatkozó felelősségbiztosítás megkötése, tartalékok képzése).*

5.3. A személyzet függetlensége

Az ellenőrző szervezetnek tudnia kell azt bizonyítani, hogy rendelkezik a feladatai hatékony ellátásához szükséges megfelelő humán, műszaki és logisztikai erőforrásokkal. Ezeknek az erőforrásoknak lehetővé kell tenniük az ellenőrző szervezet számára, hogy ellenőrzési feladatait teljesen önállóan, függetlenül és pártatlanul lássa el. Az erőforrásoknak arányosnak kell lenniük a kódex-tagok várható számával és méreteivel, valamint a vonatkozó adatkezelés(ek) összetettségével, mértékével és kockázataival. Az ellenőrző szervezet személyzete az ellenőrzési tevékenységgel kapcsolatos feladatok ellátása során hozott döntéseiért felelősséggel tartozik.

Az ellenőrző szervezetnek bizonyítania kell, hogy tapasztalt személyzettel rendelkezik. E személyzetnek minden esetben az ellenőrző szervezet kizárólagos felügyelete és irányítása alatt kell állnia, és feladataik ellátása során különleges titoktartási kötelezettségek vonatkoznak rájuk. Az ellenőrző szervezetnek elegendő számú, megfelelően képzett személlyel (belső személyzettel vagy külső szolgáltatókkal) kell rendelkeznie, és megfelelő javadalmazást kell biztosítania alkalmazottai számára.

Az ellenőrző szervezetnek az ellenőrzési feladatai ellátása során felelősséget kell vállalnia saját személyzetéért. Az ellenőrző szervezetnek a döntéseit saját felelősségére és utasítások nélkül kell meghoznia. A kódex felelőse és tagjai nem utasíthatják az ellenőrző szervezetet az adott kódex előírásainak ellenőrzésére vonatkozóan.

Amennyiben az ellenőrző szervezet olyan külső személyzetet és alvállalkozókat vesz igénybe, akiket kifejezetten megbíztak az egyedi ellenőrzési tevékenységek elvégzésével, intézkedéseket kell hozni annak biztosítására, hogy az ilyen személyzet és vállalkozók rendelkezzenek a szükséges szakértelemmel, kompetenciákkal és megbízhatósággal, különös tekintettel a kódex tárgya kapcsán. A döntéshozatali hatáskör és ezzel járó tevékenységek azonban senkire nem ruházhatók át.

Az ellenőrző szervezetnek megfelelő és elegendő technikai erőforrással kell rendelkeznie feladatai szakszerű és biztonságos ellátásához. A technikai erőforrások megfelelőségét folyamatosan ellenőrizni kell.

Az ellenőrző szervezet a személyzeti függetlenségét, például a következő dokumentumokkal bizonyíthatja:

- *Konkrét szervezeti és irányítási modellek és működési eljárások kidolgozásával és bemutatásával, amelyek biztosítják, hogy az ellenőrző szervezet elkülönülten működik a kódex felelősétől és a kódex tagjaitól;*
- *A külső személyzet és alvállalkozók bevonására és igénybevételére vonatkozó dokumentált eljárások és szervezeti szabályok;*
- *Dokumentált eljárások és szervezeti szabályok a külső személyzet és alvállalkozók szakértelmének, kompetenciáinak és megbízhatóságának biztosítása érdekében;*

- *Szerződéses vagy egyéb jogi eszközök, amelyek részletezik a vonatkozó felelősségi köröket, beleértve az adatok és információk bizalmas kezelésére vonatkozó előírásokat.*

5.4. A döntéshozatali folyamatok függetlensége

Az ellenőrző szervezetnek döntései és intézkedései tekintetében függetlennek kell lennie. Az ellenőrző szervezet függetlenül jár el a kódexet alkalmazó adatkezelővel vagy adatfeldolgozóval szembeni szankciók megválasztása és alkalmazása során.

Az ellenőrző szervezet által ellenőrzési feladatai részeként hozott döntéseket nem kell jóváhagynia semmilyen más szervnek, szövetségnek vagy szervezetnek, ideértve a kódex felelősét, a kódex tagjait vagy azt a szakmát, iparágat vagy ágazatot, amelyre a kódex vonatkozik. Ez a függetlenség biztosítja, hogy az ellenőrző szervezet elszámoltatható legyen döntéseiért és intézkedéseiért.

Az ellenőrző szervezet például a következő dokumentumokkal bizonyíthatja a döntéshozatali függetlenségét és a tevékenységeiért való elszámoltathatóságát:

- *A döntéshozatali eljárásokra vonatkozó dokumentáció;*
- *A megfelelő szerepstruktúrákra és jelentéstételi mechanizmusokra vonatkozó dokumentáció.*
- *Olyan belső szabályzatok kidolgozása, amelyek növelik a személyzet tudatosságát az irányítási struktúrával és az alkalmazott eljárásokkal kapcsolatban.*

6. Szakértelem

A GDPR 41. cikk (2) bekezdésének a) pontjával összhangban az ellenőrző szervezetnek az illetékes felügyeleti hatóság számára kielégítő módon bizonyítania kell szakértelmét a kódex tárgyával kapcsolatban.

Az ellenőrző szervezetnek megfelelő szakértelemmel kell rendelkeznie ahhoz, hogy az egyedi magatartási kódex figyelembevételével pontosan és hatékonyan láthassa el ellenőrzési feladatait. A személyzet szakértelmének rendelkezésre állását a következő témakörökben kell igazolni:

a) Megfelelő ismeretek és tapasztalat az adatvédelmi jog területén;
b) Mérnöki/műszaki szakértelem az adatvédelem területén, ha ez a kódex alkalmazási köre miatt szükséges;
c) Mélyreható ismeretek a magatartási kódex tárgya kapcsán, az annak hatálya alá tartozó adatkezelési műveletekben és kapcsolódó kockázati tényezőkben, valamint az e területen zajló folyamatokban;
d) Mélyreható ismeretek és szakértelem a felügyeleti és kontrollfunkciók ellátása terén (például az audit vagy minőség-ellenőrzési ágazatban);
e) A szakértelmet rendszeres képzési tevékenységek keretében kell fejleszteni, figyelembe véve az alkalmazandó jogszabályok fejlődését és az ágazatban alkalmazott technológiát.

Az ellenőrzési tevékenységért felelős személyzetnek jogi és műszaki szakértelemmel és képesítéssel kell rendelkeznie, de ezeket nem feltétlenül egy személynek kell megtestesítenie:

- A jogi szakértő személyzetnek legalább mesterfokozatú (MA) általános egyetemi jogi végzettséggel vagy ezzel egyenértékű jogi diplomával kell rendelkeznie.
- A mérnöki/műszaki szakértő személyzetnek legalább alapfokozatú (BSc) egyetemi végzettséggel vagy azzal egyenértékű diplomával kell rendelkeznie a számítástechnika vagy az információs rendszerek területén.

Az ellenőrző szervezet vezetéséért felelős személyzetnek szakképesítéssel és releváns szakmai tapasztalattal kell rendelkeznie a jog, a technológia és a magatartási kódex által lefedett ágazat területén, de ezeket nem feltétlenül kell egy személynek megtestesítenie.

A részletesebb szakértelemre vonatkozó követelmények magában a magatartási kódexben határozhatók meg és az akkreditáció részének tekinthetők.

Az ellenőrző szervezet például a következő bizonyítékokkal támaszthatja alá szakértelmét:

- *A személyzet önéletrajzai, bizonyítványok, képesítések, egyetemi diplomák, posztgraduális mesterfokozatok, tudományos fokozatok (PhD-k), egyéb szakmai képesítések másolatai és releváns munkatapasztalat igazolása;*
- *Tudományos közlemények és az adott területen szerzett szakmai tapasztalat, tanulmány vagy kutatás bármely más bizonyítékának becsatolása;*
- *A fenti követelményeket figyelembe vevő felvételi folyamatokra vonatkozó eljárásrend, dokumentáció.*

7. Létrehozott eljárások és szervezeti struktúra

Az általános adatvédelmi rendelet 41. cikk (2) bekezdés b) pontja szerint az ellenőrző szervezetnek tudnia kell azt bizonyítani, hogy olyan eljárásokat dolgozott ki, amelyek révén meg tudja állapítani, hogy az érintett adatkezelők és adatfeldolgozók alkalmasak-e a kódex alkalmazására, ellenőrizni tudja, hogy az érintett adatkezelők és adatfeldolgozók betartják-e a kódex rendelkezéseit, valamint rendszeres időközönként felül tudja vizsgálni a kódex működését.

Ezeket az eljárásokat a kezelt adatok kategóriáira, az adatfeldolgozás összetettségére és az érintetteket érintő kockázatokra, a kódex tagjainak típusára és (várható) számára, a kódex alkalmazásának földrajzi hatályára, a beérkezett panaszokra és a megállapított jogsértésekre tekintettel kell meghatározni. Az ellenőrző szervezetnek ellenőrzési feladatai megkezdése előtt meg kell határoznia tevékenységei alapját és hatókörét, hogy a kódexhez csatlakozó tagok előtt is biztosítani tudja az átláthatóságot.

7.1. A magatartási kódexhez való csatlakozás iránti kérelmek jóváhagyása

Az ellenőrző szervezetnek rendelkeznie kell a kódex alkalmazásának ellenőrzésére szolgáló eljárással, amelynek keretében értékeli, hogy a kódex tagja képes-e megfelelni a kódex előírásainak és végrehajtani azokat. Az ellenőrző szervezet e célból kialakított eljárásainak biztosítaniuk kell, hogy az adatkezelők és adatfeldolgozók magatartási kódexhez való csatlakozás iránti kérelmeit észszerű időn belül bírálják el.

7.2. A magatartási kódexnek való megfelelés nyomon követésére szolgáló eljárások

Az ellenőrző szervezetnek ellenőrzési eljárásokat kell kidolgoznia annak figyelemmel kísérésére, hogy a kódex tagjai megfelelnek-e a magatartási kódex előírásainak. A kódex évente ellenőrzött tagjai számának lehetővé kell tennie következtetések levonását arra vonatkozóan, hogy a kódex tagjai milyen mértékben hajtják végre a magatartási kódex előírásait.

Az ellenőrző szervezetnek egyedi ellenőrzési módszertannal kell rendelkeznie, különös tekintettel az alkalmazandó ellenőrzés típusára (önértékelés, auditok, előzetes értesítéssel vagy anélküli, helyszíni és távoli vizsgálatok, kérdőívek, rendszeres jelentéstétel stb.), az ellenőrizendő kritériumokra, valamint a megállapítások dokumentálása és kezelésükre vonatkozó intézkedések kapcsán.

Minden ellenőrzési eljárást konkrét és dokumentált előzetes utasításokba foglalt, az ellenőrzés tárgyára és hatókörére vonatkozó részleteket, továbbá a lefolytatáshoz szükséges időkeret, határidők és a szükséges technikai erőforrások elosztását is tartalmazó belső döntésnek kell megelőznie. Az ellenőrzés eredményeit tartalmazó jelentést ésszerű határidőn belül meg kell küldeni az ellenőrzött adatkezelőnek vagy adatfeldolgozónak, minden egyes megállapítás és észrevétel indokaival és azokat alátámasztó bizonyítékokkal együtt. Az ellenőrzött kódex-tag az ellenőrzés megállapításainak és következtetéseinek kézhezvételét követően azzal kapcsolatban jogosult észrevételeket tenni.

Az ellenőrző szervezetnek előre meghatározott és észszerű határidőkön belül kiszabható megfelelő korrekciós intézkedéseket és szankciókat kell elfogadnia – beleértve az érintett adatkezelő vagy adatfeldolgozó felfüggesztését vagy kizárását a kódexből –, annak érdekében, hogy orvosolja a magatartási kódex előírásainak tagok általi megsértését, és megakadályozza azok újbóli előfordulását. Ezen korrekciós intézkedéseknek összhangban kell lenniük azokkal a kódex megsértése esetén előírt reparatív intézkedésekkel, amelyeket magában a kódexben határoztak meg.

Az ellenőrizendő kódex-tagok száma és kiválasztása az adatkezelés kapcsán felmért kockázati tényezőkön és azok változásán, a panaszokon, a kódex-tagok számán, a magatartási kódex területi hatályán és a vonatkozó adatvédelmi jogi szabályozás változásán is alapulhat. Az ellenőrzési eljárás történhet felmérések vagy helyszíni ellenőrzés útján is. A rendszeres vizsgálatok során végzett rutinszerű ellenőrzés mellett konkrét eseményekkel kapcsolatos ellenőrzések is végezhetők.

A kódex tagjainak teljes körű együttműködésükkel kell biztosítani azt, hogy az ellenőrző szervezet hatékonyan le tudja folytatni az ellenőrzési tevékenysége keretein belül a vizsgálatokat.

Az eljárásrend előírhatja az elvégzett ellenőrzésekről szóló jelentések közzétételét, vagy az ellenőrző szervezet által végzett tevékenységekről és a vonatkozó megállapításokról szóló rendszeres vagy összefoglaló jelentések közzétételét.

7.3. A magatartási kódex alkalmasságának ellenőrzése

Az ellenőrző szervezet részt vesz a magatartási kódex felülvizsgálatában, amely magában foglalhat rendszeres vagy konkrét eseményhez kapcsolódó koncepcionális felülvizsgálatokat annak biztosítása érdekében, hogy a magatartási kódex előírásai végrehajthatóak, kellően pontosak és egyértelműen megszövegezettek legyenek, megfeleljenek a mindenkori szabályozási követelményeknek és a gyakorlatban is elfogadottak legyenek. A kódex felülvizsgálata során figyelembe kell venni azokat az új technológiai fejlesztéseket is, amelyek hatással lehetnek a kódex tagjai által végzett és a kódex által szabályozott adatkezelésekre, illetve a kódex vonatkozó rendelkezéseire.

Amennyiben az ellenőrző szervezet hiányosságokat állapít meg, ezekről értesíti a kódex felelősét, továbbá a magatartási kódex rendszeres felülvizsgálatának részeként is javasolhatja a vonatkozó előírás(ok) felülvizsgálatát. Amennyiben ez lehetséges, úgy már az értesítés is tartalmazhat javaslatokat a feltárt hibák kiküszöbölésére. A magatartási kódex szövegének felülvizsgálata a kódexfelelős feladata és felelőssége.

7.4. A bizalmasság biztosítására szolgáló eljárások

Az ellenőrző szervezetnek dokumentált eljárásrenddel kell rendelkeznie az általa kezelt adatok és információk bizalmasságának garantálására. Az ellenőrző szervezet által ellenőrzési tevékenységei

részeként, különösen a kódex tagjaitól vagy szerződéses partnereitől (pl. ügyfelektől) kapott valamennyi információt, beleértve az ilyen információk forrásait is, bizalmasan kell kezelnie, kivéve, ha az ellenőrző szervezetet jogszabály írja elő az információk közzétételére, vagy erre szerződés felhatalmazza.

Az ellenőrző szervezet köteles a bizalmas információkat is közölni a NAIH-al annak érdekében, hogy segítse a felügyeleti hatósági tevékenységének ellátását.

Az ellenőrző szervezetnek bizonyítania kell, hogy dokumentált eljárásrenddel rendelkezik a nevében eljáró harmadik feleken keresztül történő titoktartás biztosítására is.

7.5. Beszámolás az ellenőrző tevékenységről a felügyeleti hatóság számára rendszeres és alkalmi jelleggel

A GDPR 41. cikk (4) bekezdése alapján az ellenőrző szervezet köteles írásban, rendszeres időközönként, de legalább évente egyszer tájékoztatni a NAIH-ot a kódex tagok általi megsértése esetén tett intézkedéseiről és a megtett intézkedések indokairól. Ezt megteheti összefoglaló beszámoló formájában is.

Az ellenőrző szervezetnek igazolnia kell, hogy rendelkezik külön eljárásrenddel arra az esetre, hogy indokolatlan késedelem nélkül tájékoztassa a NAIH-ot a megtett intézkedésekről és az azokat alátámasztó okokról olyan jogsértések esetén, amelyek az érintett tag felfüggesztését vagy a magatartási kódexből való kizárását vonják maguk után.

Az ellenőrző szervezet írásban értesíti a NAIH-ot minden olyan változásról, amely lényegesen befolyásolhatja az ellenőrző szervezet ellenőrzési tevékenységét.

Az ellenőrző szervezet indokolatlan késedelem nélkül tájékoztatja a NAIH-ot az ellenőrző szervezet minden olyan lényeges változásáról (különösen a struktúrát vagy a szervezetet illetően), amely megkérdőjelezheti annak függetlenségét, szakértelmét és összeférhetetlenségtől való mentességét, vagy hátrányosan befolyásolhatja annak teljes körű működését.

8. Panaszkezelési mechanizmusok

Az általános adatvédelmi rendelet 41. cikk (2) bekezdésének c) pontja szerint az ellenőrző szervezetnek eljárásokkal és struktúrákkal kell rendelkeznie a kódex megsértésével vagy a kódex adatkezelő vagy adatfeldolgozó általi alkalmazásának módjával kapcsolatos panaszok kezelésére, valamint ezen eljárásokat és struktúrákat az érintettek és a nyilvánosság számára átláthatóvá kell tennie.

8.1. Az érintettek és egyéb érintett szervezetek panaszai

A panaszkezelési mechanizmusnak biztosítania kell, hogy az adatkezelés érintettje vagy bármely olyan személy, aki ugyanilyen módon bizonyítani tudja jogos érdekét, jogosult legyen panaszt benyújtani az ellenőrző szervezethez a releváns tények és az állítólagos jogsértés rövid leírását tartalmazó kérelem benyújtásával.

Ezek a mechanizmusok nem érintik az érintettek azon jogát, hogy a GDPR 77. és 79. cikkei, valamint az Infotv. 22. § és 23. §-ai alapján a NAIH-nál panaszt tegyenek vagy a bíróságnál peres eljárást indítsanak.

Az ellenőrző szervezetnek bizonyítania kell, hogy a panaszok fogadására, kivizsgálására és elbírálására szolgáló eljárások és struktúrák megfelelő keretrendszerével rendelkezik. Ezeknek az eljárásoknak átláthatónak, könnyen érthetőnek és a nyilvánosság számára könnyen hozzáférhetőnek kell lenniük. Az ellenőrző szervezetnek megfelelő forrásokkal kell rendelkeznie a panaszok hatékony kezelésének biztosítása érdekében. Az ellenőrző szervezet nyilvánosan hozzáférhetővé teheti határozatait vagy az azokkal kapcsolatos információkat.

Az ellenőrző szervezetnek bizonyítania kell, hogy képes a magatartási kódexben meghatározott azon korrekciós intézkedés(eke)t eszközölni – beleértve a szankciókat is –, amelyek alkalmasak a tagok által elkövetett jogsértések orvoslására és azok újbóli előfordulásának megelőzésére. A szóban forgó intézkedések magukban foglalják az érintett tag felfüggesztését vagy kizárását a kódexből, figyelembe véve a megállapított jogsértések súlyosságát.

A panaszkezelési eljárásnak elő kell írnia, hogy az ellenőrző szervezetnek ésszerű határidőn belül tájékoztatnia kell a panaszost panasza kapcsán indított eljárás előrehaladásáról és eredményéről. Az erre vonatkozó határidő nem haladhatja meg a 3 hónapot. Az ellenőrző szervezet minden szükséges esetben rendszeresen tájékoztatja az érintettet a panasz kapcsán indult eljárásról. Minden döntést megfelelően indokolni kell.

8.2. A panaszkezelési eljárás átláthatósága

Az ellenőrző szervezet sikeres akkreditációját követően a panasztételi eljárás leírását mind az ellenőrző szervezetnek, mind a kódex tagjainak közzé kell tenniük olyan formában, amely a nyilvánosság számára általánosan és könnyen hozzáférhető.

Az eljárás könnyen hozzáférhető, például, ha:

- *Közzétették az ellenőrző szervezet és a kódex tagjainak honlapjain;*
- *A panaszok benyújtásához könnyen hozzáférhető és kitölthető formanyomtatvány/sablon áll rendelkezésre.*

8.3. A felügyeleti hatósággal való kapcsolattartás a panaszokra vonatkozóan

Az ellenőrző szervezet nyilvántartást vezet valamennyi panaszról és azok kapcsán megtett korrekciós intézkedésekről, ideértve a szankciókat is, valamint rendszeresen frissíti e nyilvántartását. Ehhez a NAIH részére bármikor hozzáférést kell biztosítani.

9. Összeférhetetlenség

A GDPR 41. cikk (2) bekezdés d) pontja alapján az ellenőrző szervezet akkor akkreditálható magatartási kódex betartásának ellenőrzésére, ha a szervezet a NAIH számára hitelt érdemlően bizonyította, hogy feladatai és kötelezettségei végzése nem eredményez összeférhetetlenséget.

9.1. Az összeférhetetlenség elkerülésére szolgáló belső folyamatok

Az összeférhetetlenség elkerülése érdekében az ellenőrző szervezetnek különösen mentesnek kell lennie külső (közvetlen vagy közvetett) befolyástól, és ezért nem kérhet és nem fogadhat el utasításokat semmilyen személytől vagy szervezettől.

Az ellenőrző szervezetet a feladatai ellátása során megfelelően védeni kell a kódex felelőse, más érintett szervek vagy a kódex tagjai által alkalmazott szankciókkal vagy beavatkozásokkal szemben, függetlenül azok belső vagy külső jellegétől.

Az ellenőrző szervezetnek belső eljárással kell rendelkeznie a személyzetével vagy magával az ellenőrző szervezettel kapcsolatos összeférhetetlenségek elkerülésére és kezelésére. Az összeférhetetlenség elkerülését szolgáló eljárások és intézkedések biztosítják, hogy az ellenőrző szervezet tartózkodjon a feladataival és kötelezettségeivel összeegyeztethetetlen cselekedetektől. Az ellenőrző szervezet alkalmazottai írásban jelentik az esetleges összeférhetetlenségeket vagy a függetlenséget fenyegető veszélyeket.

Az ellenőrző szervezetnek saját külön személyi állománnyal kell rendelkeznie. Az állomány kiválasztásának folyamatát magának az ellenőrző szervezetnek vagy más, a kódextől független szervezetnek kell lefolytatnia. A szóban forgó személyzet kizárólag e szervezetek irányítása alatt állhat.

Az ellenőrző szervezet nem fogadhat el olyan szolgáltatásokat a kódex felelősétől, a kódex tagjaitól vagy más harmadik felektől, amelyek veszélyeztethetik a függetlenségét vagy összeférhetetlenséget idézhetnek elő. Elvben nem áll fenn összeférhetetlenség, ha a szolgáltatások olyan nem felügyeleti típusú, hanem tisztán adminisztratív, szervezési segítségnyújtási vagy támogató jellegű tevékenységek, amelyek nem befolyásolják az ellenőrző szervezet pártatlanságát és döntéseit: pl. informatikai támogatás, bérszámfejtés, titkársági munka, takarítási szolgáltatások stb.

Az ellenőrző szervezet az összeférhetetlenség kezelését például a következők révén tudja bizonyítani:

- *A döntésre jogosult személyzet kiválasztására vonatkozó eljárások;*
- *A vonatkozó javadalmazási szabályok;*
- *A kinevezés megújításának feltételei a személyzet hivatali idejének lejártakor.*

9.2. Egyes tevékenységek és folyamatok kiszervezése

Az ellenőrző tevékenység egyes részei és folyamatai kiszervezhetők külső szolgáltatóknak, feltéve, hogy az ellenőrző szervezet bizonyítani tudja, hogy a kiszervezésre vonatkozóan dokumentált eljárásrenddel és struktúrákkal rendelkezik, továbbá a kiszervezés nem veszélyezteti a függetlenségét és nem ad alapot összeférhetetlenségre.

Az ellenőrző szervezetnek tudnia kell azt biztosítani, hogy az ellenőrzési tevékenységeinek a kiszervezése esetén a külső szolgáltató is azonos módon meg tud felelni azoknak a követelményeknek, amelyek egyébként az ellenőrző szervezetre vonatkoznának. A kiszervezés nem eredményezheti azonban az ellenőrzési tevékenységgel kapcsolatos felelősség átruházását a külső szolgáltatóra. Az ellenőrző szervezet végső soron továbbra is a NAIH-nak, mint az illetékes felügyeleti hatóságnak tartozik minden esetben elszámolási kötelezettséggel.

Abban az esetben, ha az ellenőrző szervezet az ellenőrzési tevékenység egyes tevékenységeit és folyamatait külső szolgáltatóhoz kívánja kiszervezni, úgy az ellenőrző szervezetnek dokumentált kiszervezési eljárással kell rendelkeznie. Az ellenőrző szervezetnek jogilag kötelező erejű, végrehajtható írásbeli megállapodással kell rendelkeznie minden egyes kiszervezett szolgáltatóval. A megállapodásban foglaltaknak biztosítaniuk kell a külső szolgáltató által alkalmazott személyzet szakértelmét és függetlenségét, valamint a pártatlanságot, a titoktartást és az összeférhetetlenség tilalmát.

A kiszervezési megállapodás tervezett vagy várható felmondása esetén az ellenőrző szervezetnek biztosítania kell a kiszervezett tevékenységek és folyamatok folytonosságát és minőségét a felmondás után is.

Az ellenőrző szervezet például a következő dokumentumokkal tudja igazolni kiszervezett tevékenységei megfelelőségét:

- *A kiszervezett tevékenységekhez használt adatfeldolgozói szerződés mintája.*
- *Bármely releváns dokumentum, amely tanúsítja a szolgáltató függetlenségét, szakértelmét és a kiszervezett tevékenységgel kapcsolatos összeférhetetlenség hiányát.*
- *Adatvédelmi és / vagy titoktartási megállapodás sablonja.*