A családsegítő és gyermekjóléti intézményeknek a GDPR-hoz kapcsolódó feladatai
(Emlékeztető a MACSGYOE által szervezett konferencia 2018. 10. 09. napon megtartott előadásáról)

Figyelemfelhívás: Az emlékeztető áttanulmányozása nem pótolja szakember segítségét és a vonatkozó jogszabályok pontos ismeretét. Az emlékeztető szövege a jobb megértést segítő egyszerűsített változat.

Tartalom

Az általános adatvédelmi rendelet elhelyezése a jogforrási hierarchiában 3

Mi a GDPR? 3

Miért volt szükség az általános adatvédelmi rendelet megalkotására? 4

Adatvédelem és adatbiztonság fogalma 4

A személyes adat fogalma 4

Mikor alkalmazzuk, illetve mikor nem alkalmazzuk az általános adatvédelmi rendeletet? 4

Főbb feladatok a GDPR alapján 5

Szükséges-e adatvédelmi tisztviselőt alkalmaznunk? 5

Ki lehet adatvédelmi tisztviselő? 5

Mi az adatvédelmi tisztviselő feladatai: 5

Az adatvédelmi tisztviselő jogállása 6

Kell-e adatkezelési tevékenységek nyilvántartását vezetni? 6

Az adatkezelési tevékenységek nyilvántartásának tartalma 6

Mi a jogalapja az adatkezelésnek? 7

Milyen célból történik az adatkezelés? 8

Meddig kezelhető a személyes adat? 8

Hogyan kezeljük az adatokat? 8

Adatkezelési tájékoztatók elkészítése 8

Meg kell alkotni a belső adatvédelmi és adatbiztonsági szabályzatot? 9

Adatbiztonsági ellenőrzést kell lefolytatni, melynek keretében fel kell mérni az adatkezelési szabályok sérülésének kockázatait és a károsodás lehetséges mértékét 9

Adatvédelmi incidens 10

Az adatvédelmi incidens kockázatosságának, súlyosságának megállapítása 10

Az általános adatvédelmi rendelet elhelyezése a jogforrási hierarchiában

A közösségi jog forrásain belül különbséget kell tenni az ún. elsődleges és másodlagos források között.
Elsődleges jogforrásnak tekintjük:
- az Európai Unióról szóló szerződés (EUSZ);
- az Európai Unió működéséről szóló szerződés (EUMSZ); és ezek jegyzőkönyvei
- az Európai Unió Alapjogi Chartája,
- az Európai Atomenergia-közösséget létrehozó szerződés (Euratom) külön szerződésként még mindig hatályban van;

A Lisszaboni Szerződés hierarchiát állapít meg a másodlagos jog területén, pontos különbséget téve az EUMSZ 289., 290. és 291. cikkében a jogalkotási aktusok, a felhatalmazáson alapuló jogi aktusok és a végrehajtási jogi aktusok között.

Másodlagos jogforrásnak tekintjük:
- az irányelveket,
- rendeleteket,
- ajánlásokat,
- véleményeket,
- határozatokat.

A rendeletek általános hatállyal bírnak, teljes egészében kötelezőek és közvetlenül alkalmazandók. A címzetteknek (magánszemélyeknek, tagállamoknak, uniós intézményeknek) maradéktalanul be kell tartaniuk őket.

Az irányelvek az elérendő célokat tekintve kötelezőek a címzett tagállam (vagy tagállamok, illetve az összes tagállam) számára, a célkitűzések megvalósításának formáját és eszközeit azonban a tagállamok választhatják meg. A nemzeti jogalkotónak átültető jogszabályt (más kifejezéssel „nemzeti végrehajtási intézkedést") kell elfogadnia, amellyel a nemzeti jogszabályokat az irányelvekben megállapított célkitűzésekhez igazítja. Az egyes polgárokat alapvetően csak akkortól illetik meg a jogok, illetve terhelik a kötelezettségek, miután az átültető jogszabályt elfogadták. A tagállamok a nemzeti jogba való átültetés tekintetében bizonyos mérlegelési jogkörrel rendelkeznek, amely lehetővé teszi a nemzeti sajátosságok figyelembevételét. Az átültetést az irányelvben megállapított határidőn belül kell végrehajtani.

A határozat teljes egészében kötelező. Amennyiben címzetteket is megjelölnek (tagállamok, természetes személyek vagy jogi személyek), akkor a határozatok csak rájuk nézve kötelezőek. A magánszemélyek az adott tagállamhoz címzett határozat által biztosított jogaikra csak akkor hivatkozhatnak, ha a tagállam átültető jogszabályt fogadott el. A határozatok az irányelvekre vonatkozó feltételekkel azonos feltételek mellett közvetlenül is alkalmazhatók.

Az ajánlások és a vélemények címzettjeik számára nem keletkeztetnek semmilyen jogot vagy kötelezettséget, de útmutatást adhatnak az uniós jog értelmezésére és tartalmára vonatkozóan.

A GDPR (General Data Protection Regulation) angol mozaikszó) rendelet, így másodlagos jogforrás.

Mi a GDPR?

GDPR = General Data Protection Regulation
AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE 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 (általános adatvédelmi rendelet)

2016. április 27-én fogadták el, 2018. 05. 25. napon lépett hatályba.

Miért volt szükség az általános adatvédelmi rendelet megalkotására?

- A belső piac működéséből eredő gazdasági és társadalmi integráció lényegesen megnövelte a személyes adatok határokon átnyúló áramlását
- A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét.
- A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt.
- A természetes személyek számára biztosítani kell, hogy saját személyes adataik felett maguk rendelkezzenek
- A természetes személyek következetes és magas szintű védelmének biztosítása
- minden tagállamban azonos szintű védelemben kell részesíteni
- A vonatkozó szabályok következetes és egységes alkalmazását
- eltérések megelőzése érdekében rendelettel kell biztosítani a jogbiztonságot és az áttekinthetőséget
- Biztosítani kell minden tagállamban azonos szintű, jogi úton érvényesíthető jogokat és kötelezettségeket, az adatkezelők és adatfeldolgozók számára azonos felelősséget, a személyes adatok kezelésének következetes nyomon követését, valamennyi tagállamban azonos szankciók alkalmazását, és a különböző tagállamok felügyeleti hatóságai közötti hatékony együttműködést

Adatvédelem és adatbiztonság fogalma

Az adatbiztonság az összegyűjtött adatvagyon sérthetetlenségét, integritását, használhatóságát és bizalmasságát lehetővé tevő technológiák és szervezési módszerek összessége.
A fogalom nem azonos az adatvédelem kifejezéssel, amely a személyes adatok kezelésével, védelmével kapcsolatos jogi szabályozás összessége.

A személyes adat fogalma

A „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

A személyes adatok különleges kategóriája:
A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Mikor alkalmazzuk, illetve mikor nem alkalmazzuk az általános adatvédelmi rendeletet?

A főszabály, hogy a személyes adatok kezelésére a gdpr-t alkalmazzuk, azonban vannak kivételek.
A kivételek tárgyalása előtt az **adatkezelés fogalmát** kell tisztázni.
Adatkezelésnek tekintjük a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált formában végzett tevékenységet, műveletek összességét, így az adatok felvételét, gyűjtését, rögzítését, tárolását, rendszerezését, módosítását, átalakítását, továbbítását, törlését, megsemmisítését.

- nemzetbiztonsággal kapcsolatos tevékenységek
- kül- és biztonságpolitika
- a természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett kezelésére, amely így semmilyen szakmai vagy üzleti tevékenységgel nem hozható összefüggésbe

- bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából, ezeken belül ideértve a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése céljából végzett kezelése
- az elhunyt személyekkel kapcsolatos személyes adatokra

Főbb feladatok a GDPR alapján

1. Annak eldöntése kell-e adatvédelmi tisztviselőt kijelölni
2. Szükséges-e adatkezelési tevékenységekről nyilvántartást vezetni?
3. Meg kell határozni az adatkezelési tevékenységeket
4. El kell készíteni az egyes adatkezelési tevékenységekhez az adatkezelési tájékoztatót
5. Meg kell alkotni a belső adatvédelmi és adatbiztonsági szabályzatot
6. Adatbiztonsági ellenőrzést kell lefolytatni, melynek keretében fel kell mérni az adatkezelési szabályok sérülésének kockázatait és a károsodás lehetséges mértékét
7. Tudatosítani kell a dolgozókban az adatkezelés fontosságát, meg kell tanítani a belső adatvédelmi és adatbiztonsági szabályzatot
8. Az adatvédelmi és adatbiztonsági szabályok betartását folyamatosan ellenőrizni kell

Szükséges-e adatvédelmi tisztviselőt alkalmaznunk?

Az adatkezelő adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor:
a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;

b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé;

c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

Ki lehet adatvédelmi tisztviselő?

A gdpr nem határoz meg konkrét szakmai képesítést, hogy ki lehet adatvédelmi tisztviselő, azonban körülírja azokat a feltételeket, aminek meg kell felelni:
- szakmai rátermettség
- a feladatok elvégzésére való alkalmasság
- adatvédelmi jog és gyakorlat szakértő szintű ismerete

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Info tv.) sem határoz meg további feltételeket. A 25/L.§ (2) bekezdése szerint:
az adatvédelmi tisztviselő a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik.

Mi az adatvédelmi tisztviselő feladatai:

- tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére a rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
- ellenőrzi a rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
- együttműködik a felügyeleti hatósággal; és

- az adatkezeléssel összefüggő ügyekben – ideértve a 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Javasolt feladatai:
- közreműködik az adatkezelési tevékenységek nyilvántartásának létrehozásában
- elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot
- elvégzi az intézményen belül a dolgozók oktatását, képzését
- ellenőrzi a szabályoknak a betartását
- kapcsolatot tart a hatóságokkal
- képezi magát
- adatvédelmi incidens felmerülése esetén közreműködik a probléma megtalálásában és megoldásában
- kockázatelemzést végez
- minden személyes adattal kapcsolatos kérdésben az intézmény és az érintettek rendelkezésére áll

Az adatvédelmi tisztviselő jogállása

- Az adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.
- Az adatkezelő támogatja az adatvédelmi tisztviselőt a feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.
- Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el.
- Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja.
- Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel.
- Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.
- Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.
- Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

Kell-e adatkezelési tevékenységek nyilvántartását vezetni?

Minden adatkezelő a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet. Ez nem vonatkozik a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha
- az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár,
- az adatkezelés nem alkalmi jellegű, vagy
- az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére

Az adatkezelési tevékenységek nyilvántartásának tartalma

a) az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
b) az adatkezelés céljai;
c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;

d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
f) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
g) ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

Ahhoz, hogy az adatkezelési tevékenységek nyilvántartását össze tudjuk állítani tisztában kell lenni, hogy
- ki kezeli az adat
- milyen adatot kezel
- mi a jogalapja
- milyen célból kezeli az adatot
- meddig kezeli
- hogyan kezeli az adatokat

Ki kezeli? – adatkezelő
Milyen adatot kezel? – személyes adat fogalma, különleges kategóriája

Mi a jogalapja az adatkezelésnek?

- hozzájárulás
- szerződéses kapcsolat, szerződés előkészítése
- jogi kötelezettség teljesítése
- érintett vagy másik természetes személy létfontosságú érdekeinek védelme
- közérdekű vagy közhatalmi jogosítvány gyakorlása
- adatkezelő, harmadik fél jogos érdeke (kivéve gyermek, közhatalmi szervek

Hozzájárulás
- önkéntesnek kell lennie
- előzetes tájékoztatáson alapul
- igazolni kell tudni

Gyermekek hozzájárulása (8. cikk)
A közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.

Az információs társadalommal összefüggő szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv (19) 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás;
b) „szolgáltatás”: az információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás.
E fogalommeghatározás alkalmazásában:
i. „távolról” azt jelenti, hogy a szolgáltatást a felek egyidejű jelenléte nélkül nyújtják;
ii.„elektronikus úton” azt jelenti, hogy a szolgáltatás kezdőpontjától való elküldése és célállomásán való fogadása adatok feldolgozására (beleértve a digitális tömörítést is) és tárolására szolgáló elektronikus berendezés útján történik, valamint annak elküldése, továbbítása és vétele teljes egészében vezetéken, rádión, optikai vagy egyéb elektromágneses eszköz útján történik;
iii.„a szolgáltatást igénybe vevő egyéni kérelmére” azt jelenti, hogy az adatok továbbításával nyújtott szolgáltatás egyéni kérelemre történik.

Az I. melléklet tartalmazza azoknak a szolgáltatásoknak a tájékoztató jegyzékét, amelyek nem tartoznak e fogalom-meghatározás alá;

A jogi kötelezettség teljesítése és a közérdekű, közhatalmi jogosítvány gyakorlása jogalap esetén lehetővé tette a gdpr, hogy a tagállami jogalkotó ezt tovább cizellálja.

5. § (1) Személyes adat akkor kezelhető, ha
a) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli,
b) az a) pontban meghatározottak hiányában az az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult,
c) az a) pontban meghatározottak hiányában az az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, vagy
d) az a) pontban meghatározottak hiányában a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.

Milyen célból történik az adatkezelés?

Célhoz kötöttség elve érvényesül. Csak meghatározott, egyértelmű, jogszerű célból van lehetőség adatokat kezelni.
Adattakarékosság elve: Csak annyi adatot lehet kezelni, amennyi a cél eléréséhez feltétlenül szükséges.

Meddig kezelhető a személyes adat?

Korlátozott tárolhatóság elve:
A célok eléréséhez szükséges ideig van lehetőség tárolni.
Kötelező adatkezelés, ha az adatokat jogi kötelezettség teljesítése, közérdekű és közhatalmi jogosítvány gyakorlása, törvény, önkormányzati rendelet elrendelése alapján kezeljük.
Kötelező adatkezelés esetében a jogszabály határozza meg az időtartamot.
Amennyiben nem, akkor 3 évente jegyzőkönyv felvétele mellett ellenőrizzük, hogy a célhoz kötöttség elve érvényesül-e.
A jegyzőkönyvet 10 évig őrizzük.

Hogyan kezeljük az adatokat?

Ez már az adatbiztonság kérdése. (lásd később)

Adatkezelési tájékoztatók elkészítése

Mit tartalmaz az adatkezelési tájékoztató?
- adatkezelő adatai, neve, címe, elérhetősége,
- adatvédelmi tisztviselő neve, elérhetősége
- az adott adatkezelési tevékenység megjelölése
- adatok köre
- jogalap
- cél
- időtartam
- kik férhetnek hozzá
- sor kerül-e adattovábbításra
- az érintettek jogai
- jogorvoslati tájékoztatás

Az érintettek jogai:
- tájékoztatáshoz való jog (12. cikk)
(tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva)

- hozzáféréshez való jog (15. cikk) Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon
- tiltakozáshoz való jog (21. cikk)
- helyesbítéshez való jog (16. cikk) Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.
- adathordozhatósághoz való jog (20. cikk)
- elszámoltathatósághoz való jog (5. cikk (2))
- törléshez való jog (elfeledtetéshez való jog) (17. cikk) Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha a GDPR-ban meghatározott indokok valamelyike fennáll
- adatkezelés korlátozásához való jog (18. cikk)
- hozzájárulás visszavonásának a joga (7. cikk (3))

Az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az érintett jogaihoz kapcsolódó kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

Meg kell alkotni a belső adatvédelmi és adatbiztonsági szabályzatot?

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Info tv.) 25/A.§ (3) Ha az adatkezelő adatvédelmi tisztviselő kijelölésére köteles, (…) az adatkezelő belső adatvédelmi és adatbiztonsági szabályzatot alkot meg és alkalmaz.

A szabályzat tartalma nincs meghatározva.

Adatbiztonsági ellenőrzést kell lefolytatni, melynek keretében fel kell mérni az adatkezelési szabályok sérülésének kockázatait és a károsodás lehetséges mértékét

Bizalmasság elve

Az adatok bizalmasságának megvédése, annak garanciája, hogy az adatokhoz jogosulatlanul vagy illetéktelenül nem juthatnak hozzá.

Sértetlenség elve

Az adatok sértetlensége (integritása) azt jelenti, hogy azokat csak az arra jogosultak változtathatják meg.

Rendelkezésre állás elve

Annak a biztosítása, hogy az adatok mindig elérhetőek legyenek, jogtalanul ne semmisítsék meg, ne töröljék azokat.

Az adatbiztonsági ellenőrzés folyamata:

I. A védelmi igény feltárása: ki kell választani az intézmény lényeges adatkezeléssel érintett rendszereit, amelyeket az intézmény védeni akar.
II. Fenyegetettség-elemzés: azoknak a fenyegető tényezőknek a feltárása, amelyek az előbbi adatokra, alkalmazásokra veszélyesek lehetnek.
III. Kockázatelemzés: a fenyegető tényezők hatását kell megvizsgálni az informatikai rendszerre, meghatározni a lehetséges károk bekövetkezésének gyakoriságát és a kárértékeket.
IV. Kockázatkezelés: a megfelelő intézkedések kiválasztása és értékelése a károk csökkentésére.

Adatvédelmi incidens

„Adatvédelmi incidens”: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

Az adatvédelmi incidenst az adatvédelmi tisztviselő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens az adatkezelő tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak (Az Adatvédelmi Incidensbejelentő rendszer elérhetősége: https://naih.hu/adatvedelmi-incidensbejelent--rendszer.html), kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal (ide értve az alacsony kockázatot is) a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Az adatvédelmi incidens kockázatosságának, súlyosságának megállapítása

SE = DPC x EI + CB

Data Processing Context (DPC): A megsérült adatok fajtáinak vizsgálata

Ease of Identification (EI): Az érintett azonosíthatóságának foka

Circumstances of breach (CB): A jogsértés körülményeinek leírása, kiterjesztve a szándékosság vizsgálatára, a biztonság elvesztésére

$SE < 2$	alacsony kockázat	Az érintettekre vagy nincs hatással, vagy legfeljebb néhány kellemetlenséggel találkozhatnak, amelyek minden probléma nélkül leküzdhetők (az információk újbóli bevitele stb.).
$2 \leq SE < 3$	közepes kockázat	Az egyének jelentős nehézségeket tapasztalhatnak, amelyeket képesek lesznek leküzdeni (többletköltségek, szolgáltatásokhoz való hozzáférés megtagadása, félelem, megértés hiánya, stressz, stb.).
$3 \leq SE < 4$	magas kockázat	Az egyének jelentős következményekkel is szembesülhetnek (feketelistázás, vagyoni kár, munkahely elvesztése, egészségromlás stb.).
$4 \leq SE$	nagyon magas kockázat	Az egyének jelentős vagy akár visszafordíthatatlan következményekkel is szembesülhetnek, amelyeket nem lehet, vagy számottevő nehézség árán lehet leküzdeni (pénzügyi nehézségek, például jelentős adósság vagy munkaképtelenség, hosszú távú pszichés vagy fizikai betegségek, halál stb.).