Könyvtárellátó Nonprofit Kft.

Telefon: + 36 1 237 69 00 • Fax: + 36 1 339 4791
Levelezési cím: 1391 Bp., Pf. 204. • www.kello.hu

A Könyvtárellátó Nonprofit Kft.
Ügyvezető Igazgatójának
6/2019. (X.14) számú Ügyvezető Igazgatói Utasítása

A Könyvtárellátó Nonprofit Kft. (a továbbiakban: Társaság) Alapító Okirata 7.3.2. pontjában foglalt felhatalmazás alapján az alábbi utasítást adom ki.

I. Az utasítás tárgya
Az utasítás tárgya a Társaság 2019. október 14. napjától hatályos Adatkezelési Szabályzatának elrendelése

II. Az utasítás személyi hatálya
Az utasítás hatálya kiterjed a Társaság székhelyén, valamint telephelyein foglalkoztatott valamennyi Munkavállalójára

III. Az utasítás munkavállalókkal történő megismertetése, jogkövetkezmények

A jelen utasítást a Társaság vezető beosztású munkavállalói kötelesek a közvetlen irányításuk alá tartozó munkavállalókkal megismertetni és annak rendelkezéseit betartani és betartatni.

Az utasításban foglaltak be nem tartása, szándékos vagy súlyos gondatlansággal történő megszegése lényeges kötelezettségszegésnek minősül, mellyel kapcsolatban az Ügyvezető Igazgató – mint a munkáltatói jog gyakorlója – jogosult a vonatkozó munkajogi rendelkezéseket alkalmazni.

IV. Az utasítás hatálya
A jelen utasítás 2019. október 14. napján lép hatályba és visszavonásig érvényes. A jelen utasítás hatálybalépésével egyidejűleg a 6/2018. (VII.23.) számú Ügyvezetői Igazgatói Utasítás hatályát veszti.

Budapest, 2019. október 14.

.....
Tőczik Zsolt
ügyvezető igazgató

KÖNYVTÁRELLÁTÓ NONPROFIT KFT. 1134 BP. VÁCI ÚT 19. 3.

A

Könyvtárellátó Nonprofit Kft.

ADATKEZELÉSI SZABÁLYZATA

Nagyné Branszeisz Katalin

Folyamatgazda/készítette: Nagyné Branszeisz Katalin általános igazgatási vezető

A Szabályzatot elfogadom, alkalmazását a mai nappal elrendelem.

.....

Tőczik Zsolt
ügyvezető igazgató

KÖNYVTÁRELLÁTÓ NONPROFIT KFT. 1134 BP. VÁCI ÚT 19. 3.

Budapest, 2019. október 14.

Tartalom

1. A szabályzat célja

A Könyvtárellátó Nonprofit Kft. (a továbbiakban: Társaság vagy Adatkezelő) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. tv. (alábbiakban: „**Infotv.**") 25/A. § (3) bekezdése, valamint az Európai Parlament és a Tanács (EU) 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 2016/679. számú Rendelet (általános adatvédelmi rendelet, a továbbiakban: „**GDPR**") rendelkezéseinek végrehajtása érdekében az alábbi szabályzatot fogadja el.

Az adatkezelés az alábbi jogszabályokkal összhangban történik:

- Magyarország Alaptörvénye;
- GDPR;
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény (alábbiakban: „**Ptk.**");
- Info tv.;
- a nemzeti köznevelés tankönyvellátásáról szóló 2013. évi CCXXXII. törvény (alábbiakban: „**Ntt.**");
- a nemzeti köznevelés tankönyvellátásáról szóló 2013. évi CCXXXII. törvény egyes rendelkezéseinek végrehajtásáról, valamint a tankönyvellátásban közreműködők kijelöléséről szóló 501/2013. (XII. 29.) Korm. rendelet;

Jelen szabályzat célja a természetes személyek személyes adatainak kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a személyes adatoknak a Társaság, mint adatkezelő által, vagy nevében végzett bármilyen jellegű kezelése tekintetében a Társaság hatáskörét és felelősségét szabályozza.

2. A szabályzat hatálya

Időbeli hatály

Jelen Szabályzat 2019. október 14. napján lép hatályba.

Személyi hatály

A Szabályzat hatálya kiterjed valamennyi, a Társaság nevében adatkezelési tevékenységet végző személyre. A Társaság munkavállalói adatkezelési tevékenységük során kötelesek a jelen szabályzat rendelkezéseit betartani és kötelesek a saját feladatkörükben minden ésszerű erőfeszítést megtenni annak érdekében, hogy a Társasággal nem munkaviszonyban álló természetes vagy jogi személyek megfelelő garanciát nyújtsanak az adatkezelés GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

3. Meghatározások

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.

Adatkezelés: Személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás terjesztés

vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Adatkezelési célok: az *1. mellékletben* felsorolt adatkezelési célok, amelyekre vonatkozóan a személyes adatok kezelése azonos adatkezelési tevékenységet jelent.

Adatkezelő: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. Társaságnál kezelt adatok tekintetében a Társaság minősül adatkezelőnek.

Adatfeldolgozó: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

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.

DPO: Data Protection Officer, a GDPR 37. cikke szerinti adatvédelmi tisztviselő, aki felelős az Adatkezelési Nyilvántartás (Adatfeldolgozó esetén az Adatfeldolgozási Nyilvántartás) vezetéséért és naprakészen tartásáért, valamint az Egyedi adatkezelési tevékenységek esetén az adatvédelmi incidensek nyilvántartásáért és bejelentéséért. A DPO nevét és pontos elérhetőségét a *2. számú melléklet* tartalmazza.

Adatkezelési tevékenységért felelős szervezeti egység: Az Adatkezelési Nyilvántartásban rögzített minden egyes adatkezelési cél egy-egy olyan működési folyamat része, amelyet a Társaság valamely szabályzata szabályoz. A folyamatgazda ennek keretében az adatkezelési tevékenységért is felelős.

Felügyeleti Hatóság: Magyarország által a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv. Jelen szabályzat hatálybalépésekor a NAIH.

NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság.

Érintett: A jelen Szabályzat alkalmazásában Érintett az a természetes személy, akire vonatkozóan az Adatkezelő személyes adatot kezel.

Tájékoztató: A személyes adatok kezelésére vonatkozóan a GDPR 13. és 14. cikkeiben meghatározott, jelen Szabályzat 4.3. pontjában részletezettek szerint az Érintettek részére kötelező tartalommal rendelkezésre bocsátandó információk összessége.

Adatkezelési Nyilvántartás: A Társaság által az Érintettek vonatkozásában végzett összes adatkezelési tevékenység nyilvántartása a GDPR 30. cikkében meghatározott, jelen Szabályzat 4.5.1. pontjában részletezett tartalommal.

Címzett: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e.

Harmadik fél: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.

4. A szabályzat tartalma

4.1. Alapelvek

A személyes adatok kezelésére vonatkozóan a Társaság a működése során tiszteletben tartja a GDPR-ban meghatározott elveket, azaz

a) a személyes adatokat **jogszerűen** és **tisztességesen**, valamint az Érintett számára **átlátható módon** kezeli;

b) személyes adatokat csak meghatározott, egyértelmű és **jogszerű célból gyűjti és** kezeli;
c) csak az adatkezelés célja szempontjából megfelelő és releváns személyes adatokat kezeli, a szükséges mértékben, biztosítva az **adattakarékosságot**;
d) biztosítja a személyes adatok **pontosságát** és szükség esetén naprakészségét, minden ésszerű intézkedést megtesz annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
e) a személyes adatokat olyan formában tárolja, amely az Érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé, biztosítva a **korlátozott tárolhatóságot**;
f) az **integritás és bizalmas jelleg** alapelvének megfelelő technikai és szervezési intézkedéseket tesz az adatbiztonság érdekében, azaz a személyes adatok kezelése során védi azokat a jogosulatlan vagy jogellenes kezeléssel szemben, a véletlen elvesztéssel szemben, a megsemmisítéssel vagy károsodással szemben;
g) a személyes adatok kezelését az **elszámoltathatóság** alapelvének megfelelően olyan módon végzi, hogy képes legyen a fenti alapelveknek való megfelelés igazolására.

Az egyes adatkezelési tevékenységek a) pont szerinti jogalapjait, b) pont szerint az adatkezelési tevékenység célját, c) pont szerint a kezelt személyes adatok körét, d) pont szerint az adatkezelés időtartamát részletesen az Adatkezelési Nyilvántartás és az annak alapján készített Tájékoztató tartalmazza. Az elszámoltathatóság alapelvének történő megfelelés érdekében a jogszabályi dokumentációs kötelezettségeket a jelen Szabályzat tartalmazza.

4.2. Az adatkezelés jogszerűsége

4.2.1. Jogalapok

Személyes adatot a Társaság a GDPR-nak megfelelően akkor és annyiban kezel jogszerűen, amennyiben az alábbiak legalább egyike teljesül:

a) az Érintett **hozzájárulását** adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez, vagy
b) az adatkezelés olyan **szerződés teljesítéséhez szükséges, amelyben az Érintett az egyik fél**, vagy az a szerződés megkötését megelőzően az Érintett kérésére történő lépések megtételéhez szükséges, vagy
c) az adatkezelés a **Társaságra vonatkozó jogi kötelezettség** teljesítéséhez szükséges; vagy
d) az adatkezelés az Érintett vagy egy másik természetes személy **létfontosságú érdekeinek védelme** miatt szükséges; vagy
e) az adatkezelés **közérdekű vagy az adatkelezőre ruházott közhatalmi jogosítvány** gyakorlásának keretében végzett feladat végrehajtásához szükséges; vagy
f) az adatkezelés a Társaság vagy egy harmadik fél **jogos érdekeinek** érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az Érintett olyan érdekei vagy alapvetői jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az Érintett gyermek.

A Társaság jellemzően a jelen pont a), b), c) és e) alpont alapján végzi az adatkezelési tevékenységét. Az egyes adatkezelési tevékenységek jogalapjait az Adatkezelési Nyilvántartás és az annak alapján készített Tájékoztató tartalmazza.

4.2.2. A jogalapokkal kapcsolatos jogszabályi dokumentációs kötelezettség

Hozzájárulás

Ha az Adatkezelési Nyilvántartás a hozzájárulást jelöli meg az adatkezelés jogalapjaként, akkor az elszámoltathatóság alapelvére tekintettel a Társaságnak, mint adatkezelőnek képesnek kell lennie annak igazolására, hogy az Érintett a személyes adatainak kezeléséhez önkéntes, konkrét és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánításával, például írásbeli – ideértve az elektronikus úton tett-, nyilatkozattal hozzájárult, azaz nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelezte, hogy beleegyezését adta az őt érintő személyes adatok kezeléséhez. Ilyen hozzájárulásnak minősül az is, ha az érintett valamely internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi. A hozzájárulás az ugyanazon cél vagy célok érdekében végzett összes adatkezelési tevékenységre kiterjed. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni.

Hozzájárulás jogalap esetén személyes adat csak az Érintett dokumentált – ideértve az elektronikus utat is – nyilatkozatát követően kezelhető.

Jogos érdek, érdekmérlegelési teszt

Amennyiben az Adatkezelési Nyilvántartás jogos érdeket jelöl meg az adatkezelés jogalapjaként, akkor érdekmérlegelési teszt lefolytatására van szükség. Ennek keretében meg kell határozni, hogy mi alkotja a Társaság, mint adatkezelő vagy a harmadik fél jogszerű érdekét, meg kell vizsgálni, hogy mi alkotja az Érintett olyan érdekeit vagy alapvető jogait és szabadságait, amelyek a személyes adatok védelmét teszi szükségessé. Ezen tényezők alapján előzetes mérlegelést kell végezni, amelynek eredményéhez képest – amennyiben nem egyértelmű – további garanciákat kell társítani az Érintett jogainak védelmében. Az elszámoltathatóság alapelvére tekintettel jogos érdek jogalap esetén személyes adat csak érdekmérlegelés elvégzését és írásbeli dokumentálását követően kezelhető. Az érdekmérlegelési teszteket az adatkezelés megkezdését megelőzően kell elkészíteni a DPO, az IT és az általános igazgatási területek bevonásával. Az elvégzett érdekmérlegelési tesztek írásbeli dokumentációját a DPO őrzi.

4.3. Érintett jogainak védelmére vonatkozó intézkedések

4.3.1. Átlátható tájékoztatáshoz és kommunikációhoz fűződő jog

A Társaság az Érintett részére a személyes adatok kezelésére vonatkozó információkat a jelen Szabályzat rendelkezései szerinti Tájékoztatás formájában tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtja. A tájékoztatást írásban – ideértve az elektronikus utat is – kell megadni a GDPR 12. cikke értelmében.

A tájékoztatás jogának gyakorlása a GDPR 14. cikk (5) bekezdése értelmében abban az esetben, amennyiben a kezelt személyes adatok nem az érintettől származnak, az alábbi esetekben tagadható meg:

a. az Érintett már rendelkezik az információkkal
b. a rendelkezésre bocsátás lehetetlen, aránytalanul nagy erőfeszítést igényel vagy a rendelkezésre bocsátás ténye lehetetlenné tenné vagy veszélyeztetné az adatkezelés céljának elérését (amelyre vonatkozóan az Adatkezelési Nyilvántartás külön jelölést tartalmaz, ha van ilyen). Ilyen esetben a Társaság megfelelő intézkedéseket hoz az Érintett jogainak, illetve jogos érdekeinek védelme érdekében.
c. kifejezett olyan jogszabályi előírás esetén, amely egyidejűleg az Érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről is rendelkezik

d. ha a jogszabályban előírt szakmai titoktartási kötelezettség - ideértve a jogszabályon alapuló titoktartási kötelezettséget is - miatt az adatkezelésnek bizalmasnak kell maradnia (amelyre vonatkozóan az Adatkezelési Nyilvántartás külön jelölést tartalmaz, ha van ilyen).

Tájékoztatáshoz való joggal kapcsolatos jogszabályi dokumentációs kötelezettség, társasági szintű közreműködők

A Tájékoztató az Adatkezelési Nyilvántartás alapján készül. A jogszabálynak megfelelő, a GDPR 13. és 14. cikkében előírt kötelező elemeket tartalmazó Tájékoztatókat a Társaság az internetes honlapján teszi közzé, továbbá a Társaság belső informatikai hálózati rendszerére feltölti.

Amennyiben a Felügyeleti Hatóság további formai vagy tartalmi előírásokat határoz meg a Tájékoztatóra vonatkozóan, különösen, ha szabványosított ikonok által megjelenítendő jogi aktusok kerülnek elfogadásra, a mintát annak megfelelően módosítani szükséges. A módosítás elkészítéséért jelen szabályzat folyamatgazdája felelős.

A Tájékoztatót a személyes adatok kezelésének konkrét körülményeit figyelembe véve az alábbiak szerint kell közölni:

- a személyes adatok megszerzésének időpontjában, ha nem az Érintettől szerezték meg, akkor a megszerzésétől számított ésszerű határidőn, de legkésőbb egy hónapon belül és díjmentesen;
- ha a személyes adatokat az Érintettel való kapcsolattartás céljára használják, legalább az Érintettel való első kapcsolatfelvétel alkalmával;
- ha a Tájékoztatóban szereplőn kívül más címzettel is közlik az adatokat, akkor legkésőbb az ilyen címzettel történő első közléskor;
- ha a megszerzés céljától eltérő (Tájékoztatóban eredetileg nem szereplő) adatkezelést is kíván végezni a Társaság, akkor a további adatkezelést megelőzően.

Az Érintetti kérelemmel kapcsolatos előírások

A GDPR 12. cikke szerint az Érintett a jelen Szabályzat 4.3.2-4.3.7. pontjaiban írt jogainak gyakorlása érdekében jogosult bármely formában kérelmet benyújtani a Társaság részére. Elektronikus formában a kérelem kizárólag az adatvedelem@kello.hu e-mail címre küldhető meg. A Társaság az Érintett jogainak gyakorlására irányuló kérelem teljesítését nem tagadhatja meg, kivéve, ha bizonyítja, hogy az Érintettet nem áll módjában azonosítani.

A kérelem benyújtását és dokumentált érkeztetését követően a DPO a Társaság Általános Igazgatási területének bevonásával haladéktalanul köteles megvizsgálni a kérelmet az alábbiak szerint:

a) az arra jogosult (azonosítható) Érintett nyújtotta-e be a kérelmet,
b) a kérelem melyik érintetti jog gyakorlására vonatkozik,
c) a kérelemben foglaltak teljesítésére vonatkozó intézkedés megtételére az Adatkezelő jogszabály szerint kötelezett-e.

A Társaság köteles elősegíteni az Érintett 4.3.2.-4.3.7. pont szerinti jogainak gyakorlását. Ennélfogva, ha a Társaság ügyvezetésének, vagy eljáró munkavállalójának megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, azaz amennyiben a Társaság által az Adatkezelési Nyilvántartásban rögzített célok szerint egyébként kezelt személyes adatok és az Érintett által a kérelemben sajátjaként megjelölt személyes adatok az azonosítást nem teszik lehetővé, és a Társaság bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az Érintettet, további, az Érintett személyazonosságának megerősítéséhez szükséges információk benyújtását kérheti.

Ilyen esetben a Társaság az Érintett azonosításához szükséges és az Érintett által a jogainak gyakorlása érdekében önkéntesen megadott további kiegészítő információkat a GDPR 11. cikke értelmében az azonosítást követően nem köteles sem rögzíteni sem megőrizni, ha az azonosítás vagy panaszkezelés folyamatában mégis szükségessé válik ezen kiegészítő információk rögzítése, akkor annak kezelésével kapcsolatban a válaszlevélben az Érintettet tájékoztatni szükséges azzal, hogy az ilyen kiegészítő személyes adatok és információk más célra nem használhatók.

A kérelem vizsgálatát követően az adatkezelési tevékenységért felelős szervezeti egység kijelölt munkavállalója a visszajelzés tervezetét – bonyolultabb intézkedést igénylő esetben az intézkedési javaslattal kapcsolatos jegyzőkönyvet – kétség esetén véleményezteti a DPO-val, illetőleg díjmentesen és indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül visszajelzést ad az Érintett számára az alábbiakról:

- intézkedés megtételéről vagy
- az intézkedés elmaradásáról
- az intézkedés elmaradásának (ideértve a határidő meghosszabbítást is) jogszabály szerinti okairól,
- arról, hogy az Érintett panaszt nyújthat be a NAIH-nál és élhet bírósági jogorvoslati jogával,
- ha további kiegészítő információ megadása vált szükségessé a kérelemmel összefüggő azonosítás céljából és a Társaság bármely oknál fogva kezeli az Érintett ilyen kiegészítő személyes adatait, akkor az erre vonatkozó tájékoztatás.

Szükség esetén az egy hónapos határidő további két hónappal meghosszabbítható, figyelembe véve a kérelem összetettségét és a kérelmek számát. A határidő meghosszabbításáról – a késedelem okainak megjelölésével – a kérelem kézhezvételétől számított egy hónapon belül az érintettet tájékoztatni kell.

Szükség esetén a visszajelzéssel egyidejűleg kell értesíteni a címzetteket is.

A kérelem alapján történő intézkedés kizárólag akkor tagadható meg, vagy kizárólag akkor számítható fel ésszerű összegű díj a kért információ illetőleg az intézkedés meghozatalával járó adminisztratív költségekre is figyelemmel, ha a Társaság bizonyítani tudja, hogy a kérelem egyértelműen megalapozatlan (különösen például ismétlődő jellege miatt) vagy túlzó.

A visszajelzés (válaszlevél) illetőleg a címzetti értesítés előkészítéséért a kérelemmel érintett adatkezelési tevékenységéért felelős szervezeti egység vezetője felelős a Társaság Általános Igazgatási Vezetőjének támogatásával.

A DPO nyilvántartást vezet a Társaság vonatkozásában tárgyévben előforduló kérelmekről és címzetti értesítésekről, amely tartalmazza a kérelmek számát érintetti jogonkénti bontásban, és a Társaság által megtett intézkedéseket.

4.3.2. Az Érintett hozzáférési joga

A GDPR 15. cikke alapján az Érintett kérelmezheti a rá vonatkozó személyes adatokhoz való hozzáférést. Az Érintett jogosult arra, hogy kérelmére a Társaságtól visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, akkor jogosult arra, hogy hozzáférést kapjon a személyes adatokhoz és a következő (a Tájékoztatóban egyébként kötelezően rögzítendő) információkhoz:

a) az adatkezelés céljai;

b) az érintett személyes adatok kategóriái;

c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;

d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

e) az Érintett azon joga, hogy kérelmezheti a Társaságtól a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;

f) a Felügyeleti Hatósághoz címzett panasz benyújtásának joga;

g) ha az adatokat nem az Érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;

h) az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír és az Érintettre nézve milyen várható következményekkel jár.

Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az Érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a jogszabály által előírt (GDPR 46. cikk) megfelelő garanciákról.

Az Érintett jogosult arra, hogy a személyes adatok másolatát kérje az Adatkezelőtől. Az Érintett által kért további másolatokért az Adatkezelő az adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel. Ha az Érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az Érintett másként kéri.

A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait. A személyes adat másolata a foglalkoztatási jogviszonyokra illetőleg az ügyfélkapcsolattal összefüggő jogviszonyokra vonatkozóan a (törzs) nyilvántartásban tárolt személyes adatok másolatát jelenti, nem pedig a személyes adat (Adatkezelési Nyilvántartásban és Tájékoztatóban meghatározott célból történő) felhasználásával készült irat vagy bármely – akár elektronikus – dokumentum másolatát.

4.3.3. Helyesbítéshez való jog

A GDPR 16. cikke alapján az Érintett erre vonatkozó kérelme esetén az Adatkezelő köteles indokolatlan késedelem nélkül helyesbíteni 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.

Az Adatkezelő minden olyan címzettet tájékoztat a helyesbítésről (a személyes adatokra mutató linkek vagy e személyes adatok másolatának, másodpéldányának helyesbítése érdekében) akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az Érintettet kérésére az Adatkezelő tájékoztatja e címzettekről.

4.3.4. Törléshez való jog („az elfeledtetéshez való jog")

A GDPR 17. cikke alapján az Érintett jogosult arra, hogy az Adatkezelőtől a rá vonatkozó személyes adatok törlését kérje, az Adatkezelő pedig köteles arra, hogy az Érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az Érintett (akár a kérelemmel egyidejűleg akár attól független formában) visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
c) az Érintett tiltakozik az Adatkezelési Nyilvántartásban rögzített alábbi két jogalap szerinti tevékenységre vonatkozóan:

   c.1) a közérdekből, vagy közhatalmi jogosítvány gyakorlása keretében vagy a jogos érdek érvényesítése érdekéből történő adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy

   c.2) a közvetlen üzletszerzés érdekében történő adatkezelés ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik;

d) a személyes adatokat jogellenesen kezelték;

e) a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy hazai jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

f) a személyes adatok gyűjtésére a közvetlenül a gyermekek számára nyújtott, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Az Adatkezelő minden olyan címzettet tájékoztat a törlésről (a személyes adatokra mutató linkek vagy e személyes adatok másolatának, másodpéldányának törlése érdekében), akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az Érintettet kérésére az Adatkezelő tájékoztatja őt ezen címzettekről.

A törlésre vonatkozó rendelkezéseket nem kell alkalmazni, amennyiben az adatkezelés szükséges,

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából,
- a személyes adatok kezelését előíró valamely jog szerinti kötelezettség teljesítésének való megfelelés (azaz az Adatkezelési Nyilvántartásban jogi kötelezettség jogalappal rögzített tevékenység esetén az adatkezelés céljának megfelelő időtartam alatt), illetve a közérdekből vagy a Társaságra ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából, a népegészségügy területét érintő közérdek alapján,
- a közérdekű archiválás céljából,

tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést, vagy

- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

4.3.5. Az adatkezelés korlátozásához való jog

A korlátozás általában egy átmeneti intézkedés egy érintetti igény elbírálásáig vagy egy intézkedés megtételéig. A GDPR 18. cikke alapján az Érintett kérelmére az Adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) az Érintett vitatja a személyes adatok pontosságát, amely esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az Adatkezelő ellenőrizze a személyes adatok pontosságát;

b) az adatkezelés jogellenes, és az Érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c) az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az Érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d) az Érintett a fenti 4.3.4. c.1) pontban rögzített rendelkezés alapján tiltakozott az adatkezelés ellen; amely esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az Érintett jogos indokaival szemben.

Ha az adatkezelés a fentiek alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az alábbi esetekben lehet kezelni:

- Érintett hozzájárulásával, vagy
- jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy
- más természetes vagy jogi személy jogainak védelme érdekében, vagy
- az Unió, illetve valamely tagállam fontos közérdekéből.

Az Adatkezelő köteles a korlátozás feloldásáról a feloldást megelőzően tájékoztatni az Érintettet, akinek kérése alapján az adatkezelés korlátozásra került.

Az Adatkezelő minden olyan címzettet tájékoztat a korlátozásról, valamint annak feloldásáról (a személyes adatokra mutató linkek vagy e személyes adatok másolatával, másodpéldányával kapcsolatos adatkezelés korlátozása érdekében) akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az Érintettet kérésére az Adatkezelő tájékoztatja őt ezen címzettekről.

4.3.6. Az adathordozhatósághoz való jog

A GDPR 20. cikke alapján az Érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta,

- ha az adatkezelés jogalapja az Érintett hozzájárulása, vagy az Érintettel kötött szerződés teljesítése (az Adatkezelési Nyilvántartásban ezen két jogalap szerint rögzített tevékenységre vonatkozóan)
- és az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog gyakorlása során az Érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

Az adathordozhatóság jogának gyakorlása nem sértheti a törléshez való jogot. Az adathordozás joga nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához (az Adatkezelési Nyilvántartásban ezen jogalap szerint rögzített tevékenységre vonatkozóan) szükséges.

Az adatok hordozhatóságához való jog nem érintheti hátrányosan mások jogait és szabadságait. A személyes adat hordozhatóságára vonatkozó jog a foglalkoztatási jogviszonyokra illetőleg az ügyfélkapcsolattal összefüggő jogviszonyokra vonatkozóan a (törzs) nyilvántartásban tárolt személyes adatok hordozhatóságát (másolatát) jelenti, nem pedig a személyes adat (Adatkezelési Nyilvántartásban és Tájékoztatóban meghatározott célból történő) felhasználásával készült irat vagy bármely – akár elektronikus – dokumentum hordozhatóságát (másolatát).

4.3.7. A tiltakozáshoz való jog

A tiltakozáshoz való jog gyakorlása és a törlés

A GDPR 21. cikke alapján az Érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak (az Adatkezelési Nyilvántartásban alábbi két jogalap szerint rögzített tevékenységre vonatkozóan) közérdekből, vagy közhatalmi jogosítvány gyakorlása érdekében vagy az adatkezelő (harmadik fél) jogos érdekében történő kezelése ellen, ideértve az ezen alapuló profilalkotást is. Ebben az esetben az Adatkezelő a személyes adatokat nem kezelheti tovább, azaz törölni köteles, kivéve, ha az Adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az Érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik (az Adatkezelési Nyilvántartásban direkt marketing célként megjelölt tevékenység esetén), az Érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az Érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

A tiltakozáshoz való jogra legkésőbb az Érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni (ezt a Tájékoztató tartalmazza).

Az információs társadalommal összefüggő szolgáltatások igénybevételéhez kapcsolódóan és a 2002/58/EK irányelvtől eltérve az Érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

Ha a személyes adatok kezelésére közérdekű archiválás céljából tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az Érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

Hozzájárulás visszavonása

A GDPR 7. cikk (3) bekezdése alapján az Érintett jogosult arra, hogy személyes adatainak kezeléséhez adott hozzájárulását bármely időpontban visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt erről az Érintettet tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon jogosult megtenni, mint annak megadását.

4.3.8. Automatizált döntéshozatal, profilalkotás

Az Adatkezelő csak akkor alkalmaz kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntést, amely az Érintette nézve joghatással jár vagy őt hasonlóképpen jelentős mértékben érinti, ha az Adatkezelési Nyilvántartásban rögzített alábbi három jogalap szerinti tevékenységre vonatkozik:

- az Adatkezelő és az Érintett közötti szerződés megkötése vagy teljesítése érdekében szükséges;
- meghozatalát az Adatkezelőre alkalmazandó olyan uniós vagy hazai jog teszi lehetővé, amely az Érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít,
- az Érintett kifejezett hozzájárulásán alapul.

Az automatizált döntés és profilalkotás további követelményeire a GDPR alkalmazandó.

4.4. Az adatvédelmi tisztviselő (DPO)

4.4.1. A DPO kijelölése és feladatai

A Társaság a GDPR 39. Cikk (1) bekezdésben megjelölt feladatok ellátására adatvédelmi tisztviselőt (DPO) jelöl ki.

A DPO feladatai:

a) tájékoztatást és szakmai tanácsot ad a jelen Szabályzat hatálya alá tartozó Adatkezelő és Adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére a GDPR, valamint egyéb uniós vagy hazai adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
b) ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy hazai adatvédelmi rendelkezéseknek való megfelelést, a jelen Szabályzatnak és az adatvédelemmel összefüggő egyéb belső szabályainak történő megfelelést,
c) ellenőrzi az adatkezeléssel kapcsolatos társasági feladatkörök kijelölését, részt vesz a belső audit tevékenységben, javaslatot tesz a személyes adatok védelmével kapcsolatos szabályozásra, módosításra,
d) szervezi és ellenőrzi az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését;
e) szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, nyomon követi annak elvégzését;

f) együttműködik és bármely kérdésben konzultációt folytat a Felügyeleti Hatósággal, kapcsolattartási pontként szolgál a Felügyeleti Hatóság felé, ennek keretében részt vesz az adatvédelmi incidenskezelési tevékenységben.

A DPO feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

4.4.2. Kapcsolattartás a DPO-val

Ha bármely munkavállaló a Társaság működése körében adatkezeléssel összefüggően intézkedést igénylő körülményt észlel az alábbiak szerint kell eljárnia. Ha valamely Érintett adatkezeléssel kapcsolatos kérelmet juttat el hozzá vagy a Társasághoz, köteles értesíteni a DPO-t. Ha adatvédelmi incidensre utaló eseményt tapasztal vagy ezzel kapcsolatban bármely más releváns információhoz jut, haladéktalanul köteles értesíteni a DPO-t, illetőleg köteles továbbítani neki a releváns dokumentumokat és információkat.

4.5. Nyilvántartásokra vonatkozó jogszabályi dokumentációs kötelezettség

Az alábbi nyilvántartások lehetővé teszik, hogy a Felügyeleti Hatóság ellenőrizni tudja a társaság adatkezelési tevékenységét érintő jogszabályi megfelelést. Az Adatkezelő vagy az Adatfeldolgozó megkeresés alapján a Felügyeleti Hatóság részére rendelkezésre bocsátja a nyilvántartást.

A Társaság Nyilvántartásait a DPO vezeti.

4.5.1. Az adatkezelési tevékenységekre vonatkozó jogszabályi kötelezettségek

Adatkezelési Nyilvántartás vezetése és felülvizsgálata

Az Adatkezelő az általa végzett adatkezelési tevékenységekről nyilvántartást vezet a GDPR 30. cikk (1) bekezdése alapján.

Az Adatkezelési Nyilvántartás tartalmát folyamatosan felül kell vizsgálni és naprakészen tartani. Ennek keretében rögzíteni kell az új adatkezelési tevékenységeket, különösen új adatkezelési cél vagy új érintetti kör esetén. Törölni kell a már nem végzett adatkezelési tevékenységeket. Meglévő adatkezelési tevékenység módosulása esetén rögzíteni kell, ha megváltozott az adatkezelési tevékenységért felelős szervezeti egység, az adat tárolásának a helye, az igénybe vett adatfeldolgozó, a címzettek köre, a személyes adatok köre. A 4.3.1. pont szerinti Tájékoztatók az Adatkezelési Nyilvántartás alapján készülnek (a kötelező tartalom az egyes tájékoztatók mintájának csatolmányában egyértelműen megtalálható). Az Adatkezelési Nyilvántartás frissítésével egyidejűleg frissíteni szükséges a vonatkozó Tájékoztatókat is, amelyek alapján szükség szerint ismételten tájékoztatni kell az Érintetteket.

Az adatkezelési tevékenységért felelős szervezeti egység a beépített és alapértelmezett adatvédelem elvét figyelembe véve köteles a személyes adatokkal bármely módon összefüggő tervezett tevékenységeket bejelenteni a DPO-nak, különösen jogszabályváltozás, új belső folyamatok, fejlesztések vagy szolgáltatások esetén.

Adatkezelési Nyilvántartás szerinti törlési kötelezettség

Az Adatkezelő az Adatkezelési Nyilvántartásban rögzített, a személyes adatok kezelésére vonatkozó jogszerű időtartam elteltét követően a személyes adatot törölni köteles.

Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az adatkezelési tevékenység végzéséért felelős szervezeti egység rendszeres felülvizsgálja az általa kezelt személyes adatokat az alábbiak szerint:

- naponta, amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében napokban meghatározott időtartamot rögzít;

- havonta, amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében hónapokban meghatározott időtartamot rögzít;
- negyedévente, amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében a munkaviszony vagy egyéb jogviszony végét rögzíti;
- negyedévente, amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében az elévülési idővel összefüggő időtartamot rögzít;
- a tárgyév végét megelőző negyedéves felülvizsgálat során, amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében a tárgyév végét rögzíti.

A negyedévente történő felülvizsgálat során az adatkezelési tevékenységért felelős szervezeti egység a társasági DPO, valamint szükség szerint az adatfeldolgozó bevonásával törlési bizottságot hoz létre az intézkedések meghatározása érdekében. A törlési intézkedések határidőben történő megtételét anonimizált módon dokumentálni szükséges.

Adatvédelmi hatásvizsgálat

Az adatkezelőnek az adatkezelést megelőzően hatásvizsgálatot kell végeznie a GDPR 35. cikkének megfelelően, a Felügyeleti Hatóság erre vonatkozó jegyzékének figyelembe vételével, ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. A hatásvizsgálat előtt a DPO szakmai tanácsát ki kell kérni.

4.5.2. Az adatfeldolgozói nyilvántartás vezetése és felülvizsgálata

A Társaság illetékes munkavállalói kötelesek gondoskodni arról, és a vonatkozó szerződéses feltételek, megbízói utasítások útján elérni, hogy az Adatfeldolgozó megfelelő nyilvántartást vezessen az Adatkezelő nevében végzett adatkezelési tevékenységekről a GDPR 30. cikk (2) bekezdése alapján. Az adatfeldolgozási nyilvántartást az alapjául szolgáló adatfeldolgozási megállapodások módosulása, megszűnése vagy új adatfeldolgozási megállapodás megkötésével egyidejűleg folyamatosan kell frissíteni a 4.7. pontban írtak szerint.

4.5.3. Nyilvántartás az adatvédelmi incidensekről

A Társaság Nyilvántartást vezet az adatvédelmi incidensekről a GDPR 33. cikk (5) bekezdés alapján, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

Az adatvédelmi incidens nyilvántartást folyamatosan naprakészen kell tartani. A nyilvántartás a hatósági bejelentési kötelezettség alá tartozó és a hatósági bejelentési kötelezettség alá nem tartozó adatvédelmi incidenseket is tartalmazza. Amennyiben a Felügyeleti Hatóság kötelező tartalmi elemeket határoz meg az adatvédelmi incidenskezelési nyilvántartással kapcsolatban, abban az esetben ezzel a tartalommal ki kell egészíteni a nyilvántartást.

4.6. Az adatkezelési tevékenységekre irányadó általános szabályok és a speciális belső szabályok viszonya

4.6.1. Személyes adatok tárolása, felhasználása és áramlása az Adatkezelő működési körén belül illetőleg az adattovábbításra vonatkozó lényeges szempontok

Az Adatkezelő a GDPR alapelveinek megfelelően tárolja, használja fel, és továbbítja a személyes adatokat. A részletes – a beépített és alapértelmezett adatvédelem elvét teljesítő – technikai intézkedéseket és biztonsági előírásokat a Társaság Informatikai Biztonsági Szabályzata tartalmazza.

A szervezési és technikai intézkedéseket az Adatkezelési Nyilvántartás összegzi. A személyes adatok (alap adatbázis) papíralapú tárolása fizikailag az adatkezelési tevékenységért felelős szervezeti egység által meghatározott és az Adatkezelési Nyilvántartásban rögzített helyen történik (I oszlop).

A papíralapú dokumentumok papíralapú vagy elektronikus másolatainak létrehozását (ideértve a személyes adatok e-mailen történő továbbítását is) az adatkezelési tevékenység végzéséért felelős

szervezeti egység vezetője által meghatározott módon az Adatkezelő működési körén belül a feladat elvégzéséhez szükséges mértékben a minimálisra kell szorítani.

Az egyes adatkezelési tevékenységekre irányadó belső szabályzatok „Adatkezelés és adatvédelem" címszó alatt részletezhetik a feladatkörükbe tartozó adatkezeléssel összefüggő tevékenységek adattárolási eljárásait. Az adatkezelési és adatvédelmi rendelkezéseket tartalmazó szabályzatok és a GDPR rendelkezéseinek összhangjával kapcsolatban az elszámoltathatóság alapelvére tekintettel a DPO rendszeres jelentést készít.

4.6.2. Személyes adatok törlésére vonatkozó lényeges szempontok

Az Adatkezelő

- a 4.5.1.2. pontban írtak szerint az Adatkezelési Nyilvántartásban az egyes adatkezelési tevékenységek vonatkozásában az adatkezelés célja tekintetében meghatározott időtartam elteltét vagy
- a 4.3.1.2. pontban írtak szerint az Érintett törlésre irányuló kérelmének (törlési jog gyakorlása vagy tiltakozási jog gyakorlása) teljesítéséről szóló döntést követően

törölni köteles a személyes adatot.

A 4.5.1.2. pont szerinti rendszeres felülvizsgálat körében, valamint a 4.3.1.2. pont szerinti kérelemre adott válaszlevél megküldését megelőzően, az adatkezelési tevékenységért felelős szervezeti egység áttekinti az általa kezelt személyes adatokat, meghatározza a törlendő tételeket és intézkedik a törlés iránt. Az egyes adatkezelési tevékenységekre irányadó belső szabályzatok „Adatkezelés és adatvédelem" címszó alatt részletezhetik a feladatkörükbe tartozó adatkezeléssel összefüggő tevékenységek törlési eljárásait. Az adatkezelési és adatvédelmi rendelkezéseket tartalmazó szabályzatok és a GDPR rendelkezéseinek összhangjával kapcsolatban az elszámoltathatóság alapelvére tekintettel a DPO rendszeres jelentést készít a 4.4.1. b) pont szerinti feladatkörében.

Az ilyen előírásokat tartalmazó dokumentumokról az elszámoltathatóság alapelvére tekintettel a DPO rendszeres jelentést készít az 4.4.1. b) pont szerinti feladatkörében.

4.6.3. Adatbiztonság

A GDPR 32. cikke értelmében az Adatkezelő és az Adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, valamint az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatait figyelembe véve megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Az Adatkezelő és az Adatfeldolgozó egyúttal biztosítja, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező alkalmazottai kizárólag az adatkezelő utasításainak megfelelően kezeljék a személyes adatokat kivéve, ha az ettől való eltérésre uniós vagy hazai jog kötelez.

4.6.4. Az érintetti jogok gyakorlásának Adatkezelő általi elősegítése az egyes belső szabályzatokban

Személyes adatokra vonatkozó adatkezelési tevékenységgel kapcsolatos rendelkezést tartalmazó belső szabályzatban „Adatkezelés és adatvédelem" címszó alatt szükséges meghatározni az alábbiakat:

- a szabályzat szerint végzett adatkezelés célja, azaz az adatkezelési tevékenység Adatkezelési Nyilvántartásban szereplő megjelölése és a (D oszlop szerinti) adatkezelési cél megnevezése,
- mivel az Adatkezelési Nyilvántartás a fenti adatkezelési tevékenységre vonatkozóan meghatározza (a V oszlopban), hogy az Érintett tájékoztatása a szabályzatban történik-e meg, ez esetben a szabályzatban Mellékletként rögzíteni szükséges az előírt Tájékoztatót,
- fentieken kívül, ha az adott adatkezelési tevékenység bonyolultsága indokolja, akkor szükséges részletesen meghatározni a szabályzatban a személyes adatok tárolására, áramlására és továbbítására vonatkozó, valamint a személyes adatok törlésére vonatkozó előírásokat és felelősségi köröket a jelen Szabályzattal összhangban.

4.7. Adatfeldolgozó igénybevételével kapcsolatos általános szabályok és jogszabályi dokumentációs kötelezettség és a közös adatkezelés

A Társaság csak olyan Adatfeldolgozókat vesz igénybe, amelyek megfelelnek a GDPR előírásainak. Az adatfeldolgozási megállapodást írásban kell megkötni az adatfeldolgozó igénybevételére vonatkozó szerződéssel egyidejűleg. Amennyiben a Felügyeleti Hatóság általános szerződési feltételeket határoz meg az adatfeldolgozási megállapodásra vonatkozóan, a Társaság által alkalmazott mintákat megfelelően módosítani szükséges.

A Társaság adatfeldolgozással összefüggésbe hozható beszerzései tekintetében a szerződéskötéssel egyidejűleg adatfeldolgozási megállapodást is kell kötni, amely a beszerzési eljárás során megkötendő szerződés mellékletét képezi.

Az adatfeldolgozással összefüggő szerződéskötések tényét be kell jelenteni a DPO-nak annak érdekében, hogy a 4.5.1 pont szerinti Adatkezelési Nyilvántartás és ezzel egyidejűleg a Tájékoztató, valamint a 4.5.2. pont szerinti Adatfeldolgozási Nyilvántartás jogszerűsége biztosítható legyen a Címzettekre vonatkozó adatok naprakészen tartásával.

Amennyiben a fentiektől eltérően az eset összes körülményét figyelembe véve nem adatfeldolgozásnak hanem közös adatkezelésnek minősül a jogviszony, akkor az Adatkezelő és a további adatkezelők a közöttük létrejött megállapodásban kötelesek meghatározni a GDPR-ban foglalt kötelezettségek teljesítéséért fennálló felelősségük megoszlását, különösen az érintettek jogainak gyakorlásával és tájékoztatásával kapcsolatban. A megállapodásban meg kell jelölni, hogy melyikük tartja a kapcsolatot az Érintettel. A megállapodás lényegéről az Érintetteket tájékoztatni kell. Biztosítani kell az Érintett jogait abban az esetben is, ha azokat a megállapodás feltételeitől függetlenül kívánja gyakorolni.

4.8. Adatvédelmi incidenskezeléssel kapcsolatos szabályok és jogszabályi dokumentációs kötelezettség

4.8.1. Az adatvédelmi incidens nyilvántartása

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között

- személyes adataik feletti rendelkezés elvesztését,
- jogaik korlátozását,
- hátrányos megkülönböztetést,
- személyazonosság-lopást,
- vagy személyazonossággal való visszaélést,
- pénzügyi veszteséget,
- az álnevesítés engedély nélkül történő feloldását,
- a jó hírnév sérelmét,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését,
- vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrányt.

Az adatvédelmi incidensek nyilvántartására a 4.5.3. pont rendelkezései vonatkoznak.

4.8.2. Az adatvédelmi incidens hatósági bejelentése

A GDPR 33. cikke alapján az adatvédelmi incidenst az Adatkezelő a tudomására jutását követően indokolatlan késedelem nélkül, ha lehetséges, legkésőbb 72 órával bejelenti a NAIH részére. A bejelentést, amennyiben ilyen létezik, a NAIH által megadott formában és módon kell megtenni, a NAIH előírásai szerint a www.naih.hu weboldalon az Adatvédelmi Incidensbejelentő Rendszer menüpont alatt. A bejelentéssel egyidejűleg a 4.8.3. pont rendelkezéseinek megfelelő tájékoztatási kötelezettséget is teljesíteni kell.

Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, az elszámoltathatóság elvével összhangban, a bejelentést nem kell megtenni.

Ezt a döntést a Társaság ügyvezetője hozza meg, mérlegelve az eset összes körülményeit.

4.8.3. Az Érintettek tájékoztatása az adatvédelmi incidensről

Az Adatkezelő indokolatlan késedelem nélkül tájékoztatja az Érintettet az adatvédelmi incidensről, **ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve**.

Nem kell értesíteni az Érintettet, ha a következő feltételek bármelyike teljesül:

a) az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazta, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat; vagy

b) az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az Érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg; vagy

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé, amely esetben az Érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az Érintettek hasonlóan hatékony tájékoztatását.

4.8.4. Az adatvédelmi incidens belső bejelentése, kivizsgálása, közbenső döntések

Adatvédelmi incidens észlelése többféle módon történhet:

a) bejelentés – érintett, egyéb felhasználó, adatfeldolgozó – jelzése alapján

b) rendszer biztonsági jelzése alapján

c) külső/belső ellenőrzés eredménye alapján.

A Társaság munkavállalói kötelesek jelenteni a Társaság ügyvezetőjének, vagy közvetlen felettesüknek, vagy a DPO-nak, ha adatvédelmi incidenst, vagy arra utaló eseményt észlelnek. A bejelentés történhet személyesen, telefonon, vagy az adatvedelem@kello. hu e-mail címen.

Rendszer biztonsági jelzése alapján a jelen Szabályzat 3. számú mellékletét képező Informatikai incidenskezelési eljárási rend szerint kell eljárni.

Adatvédelmi incidens esetén a Társaság ügyvezetője a DPO, az informatikai igazgató és az érintett (gazdasági... stb.) szervezeti egység vezetője közreműködésével haladéktalanul megvizsgálja a bejelentést, ennek során azonosítani kell az incidenst, el kell dönteni, hogy valódi incidensről, vagy téves riasztásról van szó. Meg kell vizsgálni és meg kell állapítani:

- az incidens bekövetkezésének és felfedezésének időpontját és helyét
- az incidens leírását, mi történt (tények és körülmények)
- az érintett személyes adatok körét és valószínűsíthető mennyiségét
- az érintett személyek körét és valószínűsíthető számát
- az incidens elhárítása érdekében tett intézkedéseket

- a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedéseket és
- további incidenst megelőző intézkedések megtételét.

Amennyiben a vizsgálat közben egyértelműen megállapítható, hogy informatikai rendszert érintő incidens történt, akkor a vizsgálati eljárást ki kell egészíteni a jelen Szabályzat 3. sz. mellékletét képező Informatikai incidenskezelési eljárási rendben rögzített vizsgálatokkal.

Az adatvédelmi incidens kivizsgálásának összes részletét a DPO köteles rögzíteni a jelen Szabályzat 4. sz. mellékletét képező jegyzőkönyvben.

Adatvédelmi incidens bekövetkezése esetén az érintett rendszereket, személyeket, adatokat be kell határolni és el kell különíteni, továbbá gondoskodni kell az incidens bekövetkezését alátámasztó bizonyítékok begyűjtéséről és megőrzéséről. Ezt követően lehet megkezdeni a károk helyreállítását és a biztonságos működés visszaállítását.

DPO az esemény észlelésétől számított 48 órán belül, de legkésőbb 60 órán belül az eset összes körülményét figyelembe véve döntési javaslatot fogalmaz meg arra vonatkozóan, hogy

- az esemény adatvédelmi incidens-e (lásd 4.8.1. pont),
- amennyiben igen, az adatvédelmi incidens jár-e kockázattal a természetes személyek jogaira és szabadságaira nézve (ez esetben lásd Hatósági bejelentés 4.8.2. pont),
- és ha jár, akkor az magas kockázat-e (ez esetben lásd Hatósági bejelentés 4.8.2 és Érintettek tájékoztatása 4.8.3 pont).

A döntési javaslat megfogalmazása során az eset összes körülményének mérlegelése, valamint az adatvédelmi incidens elhárítására tett intézkedés megtétele érdekében a DPO szükség szerint bevonja a kivizsgálásba az adatvédelmi incidenssel érintett szervezeti egység vezetőjét.

A javaslat alapján haladéktalanul döntést kell hozni arról, hogy kötelező-e a NAIH részére a bejelentés a 4.8.2 pontnak megfelelően, illetőleg kötelező-e az Érintettek tájékoztatása a 4.8.3. pontnak megfelelően.

Minden esetben meg kell határozni az adatvédelmi incidens elhárítására tett intézkedéseket a jogszabályi kötelezettségeknek megfelelő adatkezelési eszközök fenntartása érdekében, amelyet a DPO ellenőriz. Meg kell vizsgálni, hogy milyen megelőző technikai és szervezési intézkedések végrehajtása szükséges a személyes adatok esetleges megsértésének elkerülése érdekében. A feltárt megelőző tevékenységeket (policy, folyamat fejlesztés, képzés, oktatás) végre kell hajtani és dokumentálni kell.

A döntést követően a DPO az adatvédelmi incidens észlelésétől számított lehetőleg legkésőbb **72 órán** belül megteszi a szükséges adminisztratív intézkedéseket (bejelentés, tájékoztatás), és rögzíti az adatvédelmi incidens adatait a nyilvántartásban. Ha nem lehetséges a bejelentés mintában meghatározott információkat egyidejűleg közölni, akkor további indokolatlan késedelem nélkül később részletekben is közölhetők. Ha a bejelentés kötelező és nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

4.9. Jogorvoslat, felelősség és szankciók

Az Érintett által tapasztalt jogellenes adatkezelés esetén polgári pert kezdeményezhet az Adatkezelő ellen. A per elbírálása a törvényszék hatáskörébe tartozik. A per – az Érintett választása szerint – a lakóhelye szerinti törvényszék előtt is megindítható

Bármely Érintett az egyéb közigazgatási vagy bírósági jogorvoslatok sérelme nélkül jogosult arra, hogy panaszt tegyen valamely Felügyeleti Hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha a megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a GDPR-t.

A Magyarországon illetékes Felügyeleti Hatóság megnevezése és elérhetősége a Tájékoztatóban található.

Minden olyan személy, aki a GDPR megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől, vagy az adatfeldolgozótól kártérítésre jogosult.

Az adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért, amelyet a GDPR-t, vagy jelen szabályzatot sértő adatkezelés okozott, kivéve, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

A jelen Szabályzat valamely rendelkezésének be nem tartása esetén a Társaság, mint munkáltató fenntartja a jogot, hogy az esetleges károkozásból eredő költségeket az érintett Munkavállalóra, vagy adatfeldolgozóra tovább terhelje. A jelen szabályzatban foglaltak be nem tartása, szándékos vagy súlyos gondatlansággal történő megszegése lényeges kötelezettségszegésnek minősül, mellyel kapcsolatban az Ügyvezető Igazgató – mint a munkáltatói jog gyakorlója – jogosult a vonatkozó munkajogi rendelkezéseket alkalmazni.

5. Hatályon kívül helyezés

Jelen szabályzat hatálybalépésével egyidejűleg hatályát veszti a Társaság 2018. július 23-i hatállyal kiadott Adatkezelési Szabályzata.

6. Mellékletek

1. melléklet	Adatkezelési célok
2. melléklet	DPO neve és elérhetősége
3. melléklet	Informatikai incidenskezelési eljárási rend
4. melléklet	Jegyzőkönyv adatvédelmi incidensről - minta

1. sz. melléklet – Adatkezelési célok

Adatkezelési célok, melyek érdekében a Társaság a jelen szabályzat hatálya alá tartozó személyek személyes adatait kezeli:

1. Munkaviszony keretében a Társaságot, mint munkáltatót jogszabály alapján biztosított jogosultság, illetve terhelő kötelezettségek teljesítése.

2. Munkaviszony keretében a Társaság által biztosított, béren kívüli juttatás keretében a Társaságot, mint munkáltatót jogszabály, vagy a Társaság belső szabályzata alapján biztosított jogosultság, illetve terhelő kötelezettségek teljesítése.

3. A Társaság által munkavállalói számára biztosított kereskedelmi szolgáltatás igénybevételének keretében a Társaságot jogszabály alapján biztosított jogosultság, illetve terhelő kötelezettségek teljesítése.

4. A Társaság által ellátott közfeladatok teljesítése, azaz a könyvtárak állományi gyarapítása, valamint az országos tankönyvellátás biztosítása keretében a Társaságot jogszabály alapján biztosított jogosultság, illetve terhelő kötelezettségek teljesítése.

5. A Társaság által külső ügyfelek, partnerek számára biztosított kereskedelmi szolgáltatás igénybevételének keretében a Társaságot jogszabály alapján biztosított jogosultság, illetve terhelő kötelezettségek teljesítése.

6. A Társaság által külső ügyfelek számára biztosított hírlevél szolgáltatás igénybevételének keretében a Társaságot jogszabály alapján biztosított jogosultság, illetve terhelő kötelezettségek teljesítése.

2. sz. melléklet – DPO neve és elérhetősége

A Társaság képviselője adatkezelési kérdésekben az alábbiak szerint megnevezett adatvédelmi tisztviselő.

Az adatvédelmi tisztviselő elérhetőségei:

Név:	Rigó István
Székhely:	1134 Budapest, Váci út 19.
Postacím:	1391 Budapest, Pf.: 204.
Telefon:	+36 1 237-6900
E-mail:	adatvedelem@kello.hu

Informatikai incidenskezelési eljárási rend

Az informatikai vagyontárgy, vagy adatvagyon szándékos vagy véletlen sérülése esetén KELLO IT felkészülten, gyorsan és hatékonyan kell, hogy reagáljon az esemény üzletfolytonosságra gyakorolt hatásának minimalizálása céljából. Jelen dokumentum a KELLO által követett információbiztonság kezelési folyamatot ismerteti.

Informatikai incidens jelentése

Az információbiztonság incidens olyan lényeges nemkívánatos esemény, amely kritikus vagy érzékeny információk vagy vagyontárgyak integritását vagy rendelkezésre állását veszélyezteti. Az incidensek alááshatják az operatív tevékenységeket, súlyos anyagi kárt okoznak, érzékeny adatokkal kapcsolatos jogi kérdéseket vetnek fel, a Társaság információs vagyontárgyaival való visszaélést valósítanak meg, ronthatják az ügyfelek fennálló bizalmát, vagy csökkenthetik a bevételeket. Ide tartoznak a technológiai / kibertámadások vagy behatolások, a fizikai feltörés, adatvagyon eltulajdonítása, valamint a szellemi tulajdon engedély nélküli kiszolgáltatása.

Minden esemény és incidens dokumentálására és besorolására meghatározott folyamatnak megfelelően kerül sor. Az adott eset súlyosságától függően kerül meghatározásra, hogy elindítják-e az Információbiztonság incidenskezelési folyamatot.

Incidenskezelési folyamat

Az incidenskezelési tevékenység célja az incidensek üzletmenetre gyakorolt hátrányos következményeinek lehető legrövidebb időn belüli megszüntetése. Ezt a tevékenységet a KELLO informatikai üzemeltetésben részt vevő munkatársai végzik, szükség esetén további támogatók igénybe vételével.

Rögzítés

Minden IT biztonsággal kapcsolatos incidens adatait incidens riport kezelő nyomtatványon kell rögzíteni. Az incidensek bejelentése kétféle módon történhet

- Felhasználó általi bejelentés
- Informatikai üzemeltető személyzet általi észlelt incidens

Felhasználó általi bejelentés

Amennyiben az incidens bekövetkezését a felhasználó észleli, és az incidens nem akadályozza meg a felhasználót az informatika@kello.hu email címre történő bejelentésben, akkor a rögzítést a megadott email címen keresztül elvégezheti. Amennyiben erre nincs módja, abban az esetben tájékoztatja az informatikai igazgatót.

Informatikai üzemeltető személyzet általi rögzítés

Amennyiben az incidens bekövetkezését nem a felhasználó, hanem az informatikai üzemeltető személyzet valamely munkatársa – például a felügyeleti rendszer riasztása alapján – észleli, akkor az incidens riport kezelő nyomtatványon történő rögzítést saját maga köteles haladéktalanul elvégezni és továbbítani az informatikai igazgatónak.

Informatikai incidensek értékelési fázisai

Üzleti hatás vs. Bekövetkezési valószínűség	Hatás: Jelentős	Hatás: Közepes	Hatás: Alacsony
Valószínűség: Magas	1	1	3
Valószínűség: Közepes	1	2	3
Valószínűség: Alacsony	2	3	3

Kezdeti értékelés/besorolás

Az Információbiztonság incidens súlyosság szerinti besorolási mátrixa kockázati alapú megközelítést alkalmaz az események besorolásakor. Az esemény akkor kap „incidens" besorolást, ha valószínűsíthető valamely információs vagyontárgy sérülése, ami KELLO egészére általánosságban hatással lehet. Az incidens elsődleges besorolását a KELLO IT szakértői végzik el. Az incidens besorolásának módosítását/emelését az Incidenskezelési csoport végezheti el.

Az információbiztonság incidensek három, súlyosság szerinti besorolási szintje az Incidens besorolási és jelentési adatlap alapján

1. szintű információbiztonság incidensek

Az 1. szintű információbiztonság incidens jellemzően nagyszámú felhasználót / ügyfelet érint, jelentős mértékű az anyagi és/vagy hírnév kockázata. Az I. szintű információbiztonság incidensek jelentősnek minősülnek.

Ezek - jellemzően- az alábbiak:

- Bizonyíthatóan vagy gyaníthatóan többszörösen elkövetett identitáslopás vagy -csalás
- Behatolás észlelése vagy weboldal feltörése
- Érzékeny (írott, hangrögzítéses vagy elektronikus) információk engedély nélküli kiszolgáltatása
- Információk nem szándékos kiszolgáltatása
- Érzékeny információt tartalmazó, elvesztett vagy ellopott, titkosítatlan adathordozó vagy mobil eszköz
- Rossz helyre irányított tömeges üzenetek
- Érzékeny dokumentumok nem megfelelő megsemmisítése vagy tárolása

2. szintű információbiztonság incidensek

A 2. szintű információbiztonság incidensek mérsékeltnek minősülnek.

Ezek - jellemzően- az alábbiak:

- Bizonyított identitáslopás vagy -csalás elszigetelt esetei
- Rossz helyre irányított üzenetek

- Nem kezelt vírusok és/vagy férgek megjelenése
- Az érzékeny (írott, hangrögzítéses vagy elektronikus) dokumentumot nem a megfelelő fél kapta

3. szintű információbiztonság incidensek

A 3. szintű információbiztonság incidensek minimálisnak minősülnek.

Ezek - jellemzően- az alábbiak:

- Információs vagyontárgyakon észlelt rendszerteszt, rendszervizsgálat, és/vagy hasonló tevékenységek
- Lehetséges behatolás észlelése
- Titkosított laptop / mobil eszköz elvesztése
- Számítógépes vírusok és/vagy férgek (Az alkalmazott antivírus program vagy egyéb feltelepített szoftver könnyen észleli és kezeli)
- Pszichológiai manipulációra vagy adathalászatra irányuló kísérletek

Intézkedési terv

Felfedezés

Sorszám	Tevékenység	Leírás	Felelős
1	esemény felfedezése	Információbiztonsági incidenseket, azok észlelését vagy egyéb anomáliákat jelenteni kell az incidens jelentési eljárások használatával	Eseményrögzítő
1.01	kezdeti értékelés	Az esemény jelentése után kezdeti értékelést kell végrehajtani a részletek jobb megértése, a lehetséges hatások és a kezdeti súlyosság érdekében	KELLO IT
1.02	Döntési pont: Információ-biztonsági esemény? (I/N)	Meghatározni, az eseményt információbiztonságiként, ha az összegyűjtött adatok alapján erre lehet következtetni	KELLO IT
1.03	Információ-biztonsági esemény eljárások	Amennyiben biztonsági esemény tényét megerősítették követni kell a megfelelő alkalmazandó kezelési eljárásokat (AHU, AGT)	KELLO IT
1.04	Átadás Incidens kezelési eljárásba	Kövesse az Incidens kezelési eljárást az esemény kezeléséhez	KELLO IT
1.05	Döntési pont: BC/DR esemény? (I/N)	Meghatározni az eseményt BC/DR eseményként, ha az összegyűjtőt információk alapján erre lehet következtetni, a BCP dokumentumok alapján .	Informatikai igazgató
1.06	Döntési pont: Jogsértési értesítés? (I/N)	Meghatározni az eseményt Jogi eseményként, ha az összegyűjtőt információk alapján arra lehet következtetni, hogy ügyfél, vagy vállalti bizalmas adatok kompromittálódása történt (vagy annak gyanúja merült fel). Jogi Szervezet részletes tájékoztatása szükséges.	Informatikai igazgató
1.07	Átadás Jogi eljárásba	A jogi osztály által meghatározott speciális eljárás követése.	Jogi személyzet
1.08	Döntési pont: Csalási esemény? (I/N)	Meghatározni az eseményt csalási eseményként, ha az összegyűjtőt információk alapján arra lehet következtetni, hogy csalás történt vagy erre utaló gyanú merült fel, vagy ehhez köthető riasztás történt.	Jogi személyzet

1.09	Átadás családkezelési eljárásba	Az esemény részletes ismertetése a családkezelő csoporttal, hogy követni tudják az előre meghatározott eljárásrendet.	Jogi személyzet
1.10	Döntési pont: Panaszkezelési eljárás? (I/N)	Amennyiben az esemény egy ügyfél panaszt eredményez tájékoztatni, kell a.....	Jogi személyzet
1.11	Átadás Panaszkezelési eljárásba	Az esemény részletes ismertetése a Panaszirodával, hogy megkezdhessék az előre meghatározott eljárásokat.	
1.12	Döntési pont: Fizikai biztonságot érintő esemény? (I/N)	Amennyiben az esemény a fizikai biztonságot érinti, értesíteni kell az épületüzemeltetésért felelős szervezetet.	Informatikai igazgató
1.13	Átadás fizikai biztonságot érintő eljárásba	Részletes információ szolgáltatása a biztonsági szolgálatnak, hogy megkezdhessék az előírt eljárásokat.	Üzemeltetés vezető
1.14	Döntési pont: Egyéb releváns esemény?	Ha a fent felsoroltakból sehova sem sorolható, meghatározni a kezelést.	Informatikai igazgató
1.15	Átadás egyéb eljárásba.	Az összegyűjtött információk alapján meghatározni, hogy szükség van-e más funkcióra, vagy csoportokra a kezeléshez.	Informatikai igazgató
1.16	Esemény lezárása	Ha az esemény nem felel meg a biztonsági esemény definíciójának (false pozitív), vagy a támogató folyamatok (Átadási Pontok) megoldásának, zárja le az eseményt.	Folyamat tulajdonos
1.17	Döntési pont:	Az Eseményrögzítő vagy Folyamat tulajdonos minden korábbi bejelentett folyamatból (Átadási Pontok) képes beadni az eseményt a folyamatba, ha alapos okkal feltételezhető, hogy az eseményt az ISIRT kezeli, és az esemény az elején újraértékelésre kerül az értékelési fázisban.	Folyamat tulajdonos
1.18	Biztonsági újraértékelés szükséges?	Az újraértékelés lehetséges kritériumai: • Megerősített vagy feltételezett kompromittálódás a titoktartásra, az integritásra vagy a rendelkezésre állásra • Leállások, adatvesztés vagy jogosulatlan módosítások a kritikus üzleti rendszerekben, alkalmazásokban vagy adatokban • Az esemény nagyszámú érintett félre vonatkozik, és közzétételre vagy értesítésre lehet szükség • Az esemény illegális vagy rosszindulatú tevékenység;	Informatikai igazgató

Értékelés

Sorszám	Tevékenység	Leírás	Felelős
2	Újraértékelés	Ha az esemény olyan kritériumokat tartalmaz, amelyek potenciálisan eszkalálódhatnak egy incidensé, abban az esetben újra kell értékelnie az eseményt az információ biztonsági incidens súlyossági besorolási mátrixával.	Informatikai Igazgató
2.1	Incidens osztályozása	Az újraértékelési tevékenységből gyűjtött információk felhasználásával osztályozza az incidens szintet az információbiztonsági esemény súlyossági besorolási mátrixával.	Informatikai Igazgató
2.2	Döntési pont: Biztonsági Incidens?	Az összegyűjtött információk és az újbóli értékelés alapján határozza meg, hogy az eseményt incidensként kell kezelni.	Informatikai Igazgató
2.3	Incidens bejelentése	Az eseményt incidensnek nyilvánítsa, megjelöli/kijelöli a megfelelő incidens felelőst	Informatikai Igazgató
2.4	Lezárás, vagy kezelés biztonsági eseményként.	Ha az esemény nem incidens, akkor az 1.02 lépéstől követnie kell az információbiztonsági eseményt	Informatikai Igazgató

Kezelés

Sorszám	Tevékenység	Leírás	Felelős
3	Elhárításban résztvevők meghatározása	Jelölje ki az incidens elhárítására a megfelelő személyeket. Győződjön meg róla, hogy a szerepek és a felelősségi körök egyértelműek és érthetőek.	Informatikai igazgató
3.1	Helyzetértékelés	Információgyűjtés, amennyire csak lehetséges, és értékelje annak hatását a szervezetre.	Informatikai igazgató
3.2	Végrehajtási metódus kiválasztása	Ki kell dolgozni végrehajtási metódust, amely meghatározza azokat a lépéseket / teendőket amelyek az alábbiakhoz szükségesek: • Az események titkosságának fenntartása • Az érintett adatok azonosítása • Feltartóztatás • Felszámolás • Helyreállítás • Kivizsgálás • Bizonyítékok elmentése	Informatikai igazgató

3.3	Feltartóztatás	• Az elszigetelés és stratégiák azonosítása és dokumentálása • Határozza meg, hogy milyen bizonyítékokkal kell kezelni / vizsgálati szempontból megfelelő eljárásokat követelni • végezze el az esemény részletes technikai elemzését • Határozza meg a további veszélyeztetett gépek / adatok észlelésének módját • Határozza meg a kompromittálódás irányát (ha lehetséges) tiltsa le a hozzáférést	Technikai elemző
3.4	Felszámolás	• Az felszámolási/törlési stratégia meghatározása • Határozza meg a kiváltó okot • Távolítsa el az aktív támadási irányt (ha lehetséges) • azonosítani és eltávolítani a kompromittálódott eszközöket • Javítani vagy mérsékelni a kihasznált sérülékenységet • A tevékenységek prioritás meghatározása	Technikai elemző
3.5	Visszaállítás	A helyreállítási tevékenységeknek tartalmazniuk kell: • Az eseménnyel kompromittálódott hitelesítő adatok cseréje • Ha az esemény egy sérülékenység miatt következett be, ellenőrizze, hogy az érintett eszközök már nem érzékenyek a sérülékenységre • A rendszerek teljes működési képességének visszaállítása	Technikai elemző
3.6	Kivizsgálás	• Határozza meg, hogy milyen bizonyítékokat kell kezelni és vizsgálati szempontból milyen eljárásokra van szükség • Végrehajtja a vizsgálati eljárásokat az esetek kivizsgálásával kapcsolatos bizonyítékok összegyűjtésére és megőrzésére	Technikai elemző
3.7	Bizonyítékgyűjtés	• egyértelműen dokumentálja, hogy az összes bizonyíték, beleértve a veszélyeztetett rendszereket, megmaradt • A bizonyítékokat olyan eljárások szerint kell összegyűjteni, amelyek megfelelnek a jogi személyzet és a megfelelő bűnüldöző szervek által folytatott korábbi megbeszélésekből származó valamennyi vonatkozó törvénynek és rendeletnek, hogy minden bizonyíték a bíróság előtt elfogadható legyen • A bizonyítékokat az esetek kivizsgálása során meg kell őrizni és dokumentálni kell.	Technikai elemző
3.8	Döntési pont: Külső erőforrás igénybevétele? (I/N)	Határozza meg, hogy külső szervezeteket kell-e bevonni az elszigetelésre, megsemmisítésre és helyreállításra.	Informatikai igazgató

3.9	Külső erőforrások bevonásának eljárása	• Vegye fel a kapcsolatot a megfelelő szervezetekkel (csak az előre ellenőrzött cégek jogosultak a belső szakemberek helyett eljárni) • A kijelölt kapcsolattartó nyomon követi az elsődleges és támogató egyének haladását, szoros kapcsolatot tart velük, figyelve a határidőket és együtt működést.	Informatikai igazgató
4	Belső kommunikációs protokoll	A hivatalos (és esetlegesen szükséges) kommunikáció a management tájékoztatása. Jogi szervezet értékeli az elszigetelési, felszámolási és helyreállítási terveket a megfelelő kommunikációs módszer és tartalom meghatározására. Ezek a tevékenységek magukban foglalhatják: • A szabályozási hatások azonosítása • kommunikációs módszerek meghatározása • Külső felekre vonatkozó tájékoztatások (szabályozók, bűnüldözési hatóságok) • E-mail értesítés az érintett felhasználóknak;	Jogi személyzet
4.1	Döntési pont: Végrehajtási terv kész? (I/N)	Ellenőrizni, hogy a 3.2 pontban felsorolt tevékenységek befejeződtek-e.	Incidensgazda
4.2	Incidens végrehajtási tervének lezárása	Ha a végrehajtási terv sikeresen befejezett zárja le az incidenst.	Incidensgazda

Lezárás

Sorszám	Tevékenység	Leírás	Felelős
5	Gyökér ok elemzés	• Elemezze az esetleges kivizsgálás során összegyűjtött összes információt, és határozza meg az eset kiváltó okait. • Biztosítani kell a helyzet tényleges megértését, az azonosított esemény alapjául szolgáló okokat, a hasonló esemény bekövetkezte esélyének minimalizálására, valamint az erőforrások hatékony felhasználására. • Azonosítsa a környezetben lévő támadás / sebezhetőségre érzékeny egyéb eszközöket a gyökér ok meghatározása alapján	Incidensgazda

5.1	Tanulságok megállapítása	Szűrje le a tanulságokat összpontosítson az alábbiakra: • Mit lehet jobban tenni? • Az üzleti tevékenység javításához szükséges változtatások és / vagy műszaki környezetben • Azonosítani kell a kulcsfontosságú kérdéseket, hogy megakadályozza az eset megismétlődését. • Milyen policy vagy folyamati fejlesztések valósíthatók meg (üzleti, technikai vagy maga az incidensfolyamat)? • Milyen biztonsági ellenőrzéseket kell felülvizsgálni a hatékonyság és az alkalmazhatóság szempontjából? • Milyen képzésre vagy oktatásra lenne szükség a tudatosság növelése érdekében? • Van-e hosszú távú kármentesítési tevékenység, amelyhez szükség lehet a projektmenedzsment bevonására, például egy alkalmazás módosítására vagy egy folyamat támogatási eszköz beszerzésére? • Mi az, ami jól működött az esemény során, és fel kell venni az incidensek kezelésének folyamataiba? • Van-e olyan esemény, amelynek hasonló/azonos gyökér oka van, amely egy rendszerszintű problémát jelez?	Incidensgazda
5.2	policy vagy folyamatfejlesztés	felülvizsgálhatja a kapcsolódó tevékenységeket az azonosított irányelvek vagy folyamatok fejlesztési terveinek frissítéséhez annak érdekében, hogy csökkentse a hasonló esemény megismétlődési valószínűségét.	Folyamatgazda
5.3	Biztonsági incidens lezárása	Zártnak nyilvánítsuk az incidenset, amikor valamennyi kiemelkedő feladat dokumentálva van, és minden csapattag egyetért abban, hogy az eset lezárulhat. Biztosítsa a következőket: • Az incidensről szóló jelentések részleteit és a dokumentált bizonyítékokat a teljesség érdekében ellenőrizték • Az eseményhez kapcsolódó összes (hardver, szoftver, jogi, stb.) költség dokumentált	Incidensgazda

Incidens riport kezelő nyomtatvány (mellékelve)

KÖNYVTÁRELLÁTÓ NONPROFIT KFT. I 1134 BUDAPEST, VÁCI ÚT 19. I LEVELEZÉSI CÍM: 1391 BUDAPEST, PF.204. I TEL.: +36 1 237 6900 I FAX: +36 1 339 4791

KELLO Informatika		
Incidens Jelentés	Bizonylat azonosító:	Verziószám: V1.0
	Kiadás dátuma: 2017.07.23.	

Incidens Riport: Tárgy

A hiba leírása	
A hiba hatása mely szolgáltatásokat érintette, milyen mértékben	
A hiba oka:	
A hiba jövőbeni elkerülésére tett intézkedések:	
A hiba észlelésének időpontja	
A hiba elhárításának időpontja	

Budapest,

.....

Könyvtárellátó Nonprofit Kft.

Telefon: + 36 1 237 69 00 • Fax: + 36 1 339 4791
Levelezési cím: 1391 Bp., Pf. 204. • www.kello.hu

Jegyzőkönyv száma: ...../201.....

Jegyzőkönyv adatvédelmi incidensről

az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/J. § (1) bekezdés alapján amely készült 20..... év ..... hó ..... napján, a Könyvtárellátó Nonprofit Kft. székhelyén, a ..... hivatalos helyiségében.

Jelen vannak (név és beosztás):

....
....
....

A jelenlevők rögzítik, hogy az Infotv. alapján a Könyvtárellátó az általa kezelt adatokkal összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és a kezelésükre tett intézkedéseket köteles rögzíteni, melyre tekintettel a jelen jegyzőkönyvet veszik fel.

1. Időpontok

Az adatvédelmi incidens időpontja: .....
Az incidensről való tudomásra jutás/felfedezés időpontja: .....
Az incidens Könyvtárellátó részére történő bejelentésének időpontja: .....
Az incidens észlelésének módja: .....

2. Az adatvédelmi incidens körülményei

(az incidens részletes leírása, hogy mi történt (tények és körülmények), az érintett(ek) leírása, milyen személyes adatokat érintett sz incidens, az adatvédelmi incidens oka)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Könyvtárellátó Nonprofit Kft.

Telefon: + 36 1 237 69 00 • Fax: + 36 1 339 4791
Levelezési cím: 1391 Bp., Pf. 204. • www.kello.hu

3. Az adatvédelmi incidenssel érintett személyes adatok köre és mennyisége

.....
.....
.....

4. Az adatvédelmi incidenssel érintettek köre és száma

(az érintett adatalanyok részletes leírása, az érintettek becsült száma)

.....
.....
.....

5. Következmények

(az adatvédelmi incidens hatásai (mik az adatvédelmi incidens – valószínű – kockázatai, következményei)

.....
.....
.....

6. Az incidens orvoslására megtett vagy tervezett intézkedések

(beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is)

.....
.....
.....

7. Az adatvédelmi incidenssel kapcsolatos egyéb adatok

(kockázat besorolása, NAIH felé történő bejelentés (max. 72 óra) mellőzésének/szükségességének indoklása, érintett tájékoztatása vagy a tájékoztatás mellőzésének indoklása)

.....
.....
.....

Aláírások: