A DRM-PROFESSIONAL CONSULTING KFT.
SZEMÉLYES ADATKEZELÉSI ÉS ADATVÉDELMI SZABÁLYZATA

2021.09.15.

Tartalom

1. Cél

A jelen adatvédelmi szabályzat (a továbbiakban: Szabályzat) célja, hogy szabályozza a **DrM-Professional Consulting Kft.** (továbbiakban: Cég) személyes adatkezelési folyamatait, biztosítva az érintettek jogait, eleget téve az alkalmazandó jogszabályok követelményeinek. A Szabályzat meghatározza és kötelezően előírja az érintett jogainak védelme érdekében a Szabályzat hatálya alá tartozóktól megkövetelt technikai és szervezési intézkedéseket.

A Szabályzat célja a GDPR cégen belül alkalmazandó követelmények meghatározása, ezért a Szabályzat belső dokumentum, az adatvédelmi jogszabályok által megkövetelt részletességű bárki számára elérhető nyilvános információkat az adatvédelmi és adatkezelési tájékoztató tartalmazza.

2. A szabályzat hatálya

2.1. Időbeli hatály

Jelen Szabályzat a GDPR alkalmazásának első napján (2021. szeptember 15.) lép hatályba és mindaddig hatályban marad, amíg a Cég meg nem szűnik vagy hatályon kívül helyezésével új Szabályzatot nem alkot. Jelen szabályzat mellékletei és formanyomtatványai a szabályzat egységes, elválaszthatatlan részét képezik.

2.2. Személyi hatály

A Szabályzat hatálya kiterjed az Adatkezelő nevében adatkezelési tevékenységeket végző személyekre (munkavállalók vagy más munkavégzésre irányuló jogviszonyban álló személyek) az Adatfeldolgozó nevében adatfeldolgozási tevékenységeket végző személyekre (munkavállalók vagy más munkavégzésre irányuló jogviszonyban álló személyek), illetőleg azokra a természetes személyekre, akikkel kapcsolatban az Adatkezelő személyes adatokat kezel vagy feldolgoz (Érintettek).

Az Adatkezelő valamennyi munkavállalója köteles a saját feladatkörében minden ésszerű erőfeszítést megtenni annak érdekében, hogy az Adatkezelővel nem munkaviszonyban álló személyek a jelen szabályzat előírásait magukra nézve kötelezőnek fogadják el, azokat betartsák, illetve szükség esetén betartassák.

2.3. Tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed az adatkezelési célokkal és eszközökkel összefüggésben adatkezelési tevékenységek során kezelt vagy feldolgozott személyes adatokra. Egyedi adatkezelési tevékenységei során kezelt vagy feldolgozott személyes adatokra vonatkozóan kizárólag a kifejezetten jelzett rendelkezések tekintetében kell alkalmazni.

3. Hivatkozások

- 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 (továbbiakban: „GDPR”);
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény („Ptk.”)
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény („Infotv.”)
- a munka törvénykönyvéről szóló 2012. évi I. törvény („Mt.”)

E szabályzat alkalmazásában jogszabálynak minősül az Európai Unió általános hatályú közvetlenül alkalmazandó jogi aktusa is.

4. 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.

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.

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

Adatkezelési tevékenységek: A jelen Szabályzat személyi hatálya alá tartozók által végzett azon adatkezelési tevékenységek, amelyek Céges vagy elkülönült eszközökön adatkezelési cél érdekében történnek, különösen a foglalkoztatással, az általános jogszabályok szerinti irányítási és támogató funkciókkal összefüggésben.

Egyedi adatkezelési tevékenységek: A jelen Szabályzat személyi hatálya alá tartozók által végzett adatkezelési tevékenységek, az adatkezelési céloktól eltérő cél érdekében történnek, különösen a Cég esetleges speciális jogszabályok szerinti szolgáltatási vagy kereskedelmi feladataival összefüggésben az alkalmazott adatkezelési eszközöktől függetlenül. Az Egyedi adatkezelési tevékenységeket végzők az Egyedi adatkezelési tevékenységeik vonatkozásában kötelesek a jelen Szabályzattal összhangban álló jogi és információbiztonsági szabályok szerint kezelni a személyes adatokat.

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.

Vállalkozás: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is.

Felügyeleti Hatóság: egy tagállam által a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv.

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 5.3. pontjában részletezett, NY-03-07 formanyomtatványok szerint az Érintettek részére kötelező tartalommal rendelkezésre bocsátandó információk összessége.

Adatkezelési Nyilvántartás: Az Adatkezelő által az Érintettek vonatkozásában végzett összes adatkezelési tevékenység nyilvántartása a GDPR 30. cikkében meghatározott, jelen Szabályzat 5.5.1. pontjában és a NY-08 formanyomtatványban részletezett tartalommal.

5. A szabályzat tartalma

5.1. Alapelvek

Az Érintettek személyes adataihoz való jogának érvényesítése érdekében a jelen Szabályzat hatálya alá tartozók működése során tiszteletben tartja az adatvédelmi jog – hivatkozásokban lefektetett –alapelveit, azaz

a) a személyes adatokat **jogszerűen** és **tisztességesen**, valamint az Érintett számára **átlátható módon** kezeli;
b) személyes adatokat csak meghatározott, egyértelmű és **jogszerű célhoz kötötten** kezel;
c) csak az adatkezelés célja szempontjából megfelelő és releváns személyes adatokat kezel, 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 adattárolással és adattörléssel kapcsolatos az 5.1 e) pont szerinti szervezési és technikai intézkedéseket vagy az azokra való utalást a jelen Szabályzat tartalmazza. Az adat- és információbiztonsággal kapcsolatos 5.1 f) pont szerinti szervezési és technikai intézkedéseket vagy az azokra való utalást a jelen Szabályzat tartalmazza. Az elszámoltathatóság alapelvének történő megfelelés érdekében a jogszabályi dokumentációs kötelezettségeket a jelen Szabályzat tartalmazza.

5.2. Az adatkezelés jogszerűsége

5.2.1. *Jogalapok*

Személyes adatot az Adatkezelő kizárólag az alábbi esetekben kezel:

a) ha az Érintett **hozzájárulását** adta az adatainak kezeléséhez, vagy
b) ha az adatkezelés olyan **szerződés teljesítéséhez szükséges, amelyben az Érintett az egyik fél**, vagy a szerződés megkötését megelőzően az Érintett kérésére történő lépések megtételéhez szükséges, vagy
c) ha az adatkezelés az **Adatkezelőre vonatkozó jogi kötelezettség** teljesítéséhez szükséges; vagy
d) ha az adatkezelés **közérdekből közhatalmi jogosítvány** gyakorlásának keretében végzett feladat végrehajtásához szükséges; vagy
e) ha az adatkezelés az Érintett vagy egy másik természetes személy **létfontosságú érdekeinek védelme** miatt szükséges; vagy
f) ha az adatkezelés az Adatkezelő vagy egy harmadik fél **jogos érdekeinek** érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az Érintett olyan érdekei,

alapvetői jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az Érintett gyermek.

A DrM-Professional Consulting Kft. jellemzően a jelen pont b), c) pont és f) alpont alapján, kisebb mértékben az a) alpont alapján végzik az adatkezelési tevékenységüket. Az 5.2.1. pont d) és e) alpontok szerinti adatkezelés egyáltalán nem jellemző. Az egyes adatkezelési tevékenységek jogalapjait az Adatkezelési Nyilvántartás és az annak alapján készített Tájékoztató tartalmazza.

5.2.2. *Az A jogalapokkal kapcsolatos jogszabályi dokumentációs kötelezettség*

5.2.2.1. Hozzájárulás

Ha az Adatkezelési Nyilvántartás a hozzájárulást jelöli meg az adatkezelés jogalapjaként, akkor az elszámoltathatóság alapelvére tekintettel az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az Érintett a személyes adatainak kezeléséhez önkéntes, konkrét és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánításával hozzájárult, azaz nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelezte, hogy beleegyezését adta az őt érintő személyes adatok kezeléséhez.

Személyes adatok különleges kategóriáiba tartozó adatokat az Adatkezelő kizárólag az Érintett kifejezett hozzájárulása alapján, illetőleg munkavállaló esetén a foglalkoztatásra, valamint szociális biztonságra és védelemre vonatkozó jogszabályon vagy kollektív szerződésen alapuló jogi kötelezettségei teljesítése érdekében kezel. A jogi kötelezettség teljesítését kivéve hozzájárulás hiányában az Érintett által az Adatkezelő számára megküldött iratot az Adatkezelő másolat készítése nélkül visszaküldi.

Hozzájárulás jogalap esetén személyes adat csak az Érintett dokumentált – ideértve az elektronikus utat is – nyilatkozatát követően kezelhető. A hozzájárulás mintáját a NY-01 formanyomtatvány tartalmazza.

5.2.2.2. 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 az 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 teszt mintáját a NY-02 formanyomtatvány tartalmazza.

5.3. Érintettek jogainak védelmére vonatkozó intézkedések

5.3.1. *Átlátható tájékoztatáshoz és kommunikációhoz fűződő jog*

Az Adatkezelő 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 az alábbi esetekben tagadható meg:

a. az Érintett már rendelkezik az előírt 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) és amelynek érdekében az adatkezelő megfelelő intézkedéseket hozott az Érintett jogos érdekeinek védelme érdekében

c. kifejezett olyan jogszabályi előírás esetén, amely egyidejűleg az Érintett jogos érdekeinek védelméről is rendelkezik
d. ha a jogszabályban előírt szakmai titoktartási kötelezettség vagy jogszabályon alapuló titoktartási kötelezettség miatt az adatkezelésnek bizalmasnak kell maradnia (amelyre vonatkozóan az Adatkezelési Nyilvántartás külön jelölést tartalmaz, ha van ilyen).

5.3.1.1. Tájékoztatáshoz való joggal kapcsolatos jogszabályi dokumentációs kötelezettség, társasági szintű közreműködők

A Tájékoztató az Adatkezelési Nyilvántartás alapján készül (NY-08.) A jogszabálynak megfelelő, a GDPR 13. és 14. cikkében előírt kötelező elemeket tartalmazó Tájékoztatók mintáját a jelen Szabályzat részét képező NY-03-07 „formanyomtatványok tartalmazzák.

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 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 az Adatkezelő, akkor a további adatkezelést megelőzően.

5.3.1.2. Az Érintetti kérelemmel kapcsolatos előírások

A GDPR 12. cikke szerint az Érintett az 5.3.2-5.3.7. pontban írt jogainak gyakorlása érdekében jogosult bármely formában kérelmet benyújtani az Adatkezelő részére. Az Adatkezelő az Érintett 5.3.2.-5.3.7. pontban említett jogainak gyakorlására irányuló kérelem teljesítését nem tagadhatja meg, kivéve, ha bizonyítja, hogy az Érintettet nem áll módjában azonosítani.

A kérelem benyújtását és dokumentált érkeztetését (iktatását) követően az Adatkezelő adatkezelési tevékenységért felelős szervezeti egység kijelölt munkavállalója szükség esetén a társasági adatvédelmi felelős bevonásával illetőleg az Adatkezelő jogi 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.

Az Adatkezelő köteles elősegíteni az Érintett 5.3.2.-5.3.7. pont szerinti jogainak gyakorlását. Ennélfogva, ha az Adatkezelőnek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, azaz amennyiben az Adatkezelő 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 az Adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az Érintettet, további, az Érintett személyazonosságának megerősítéséhez szükséges információk benyújtását kérheti.

Ilyen esetben az Adatkezelő 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, sem egyéb módon kezelni, 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 –véleményezteti a társaság adatvédelmi felelősével, 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 az Adatkezelő 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.

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 az Adatkezelő bizonyítani tudja, hogy a kérelem egyértelműen megalapozatlan vagy (különösen ismétlődő jellege miatt) túlzó.

A visszajelzés (válaszlevél) illetőleg a címzetti értesítés másodhelyi aláírója a kérelemmel megkeresett Adatkezelő adatkezelési tevékenységéért felelős szervezeti egységének vezetője, az első helyi aláíró a kérelemmel megkeresett Adatkezelő jogi vagy biztonsági vagy a HR vezetője. A visszajelzést tartalmazó iratot minden esetben iktatni kell a bejövő kérelem ügyszámára hivatkozással.

Az 5.3.2.-5.3.7. pontokra vonatkozó visszajelzés (válaszlevél az érintett személyes adatkezeléssel összefüggő kérelmére) mintáját a NY-14 formanyomtatvány tartalmazza, az ugyanott említett címzetti értesítések mintáját a NY-15 formanyomtatvány tartalmazza.

5.3.2. *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 az Adatkezelő társaságtól visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, akkor jogosult arra, hogy hozzáérést kapjon a személyes adatokhoz és a következő (A Tájékoztatóban egyébként kötelezően rögzítendő) információkhoz:

a) az adatkezelés céljai;

b) a 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 az alkalmazott logikára illetve az ilyen adatkezelés jelentőségére és az Érintettre nézve várható következményeire vonatkozó információk.

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.

5.3.3. *Helyesbítéshez való jog*

A GDPR 18. 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 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.

5.3.4. *Törléshez 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) ha az Érintett (akár a kérelemmel egyidejűleg akár attól független formában) visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) ha az Érintett tiltakozik az Adatkezelési Nyilvántartásban rögzített alábbi két jogalap szerinti tevékenységre vonatkozóan: a közérdekből, közhatalmi jogosítvány gyakorlása érdekében vagy a jogos érdekből történő adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,

d) ha az Érintett tiltakozik a közvetlen üzletszerzés érdekében történő adatkezelés ellen (az Adatkezelési Nyilvántartásban direkt marketing célként megjelölt tevékenység esetén);

e) ha a személyes adatokat jogellenesen kezelték;

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

g) ha a személyes adatok gyűjtésére gyermekek számára nyújtott információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Az Adatkezelő minden olyan címzettet tájékoztat a törlésről (a személyes adatokra mutató linkek segítségével) 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.

Az Érintett törlési jogának korlátozására csak a GDPR-ban írt alábbi kivételek fennállása esetén kerülhet sor, azaz a fenti indokok fennállása esetén a személyes adatok további megőrzése jogszerűnek tekinthető,

- ha a véleménynyilvánítás és a tájékozódás szabadságához való jog gyakorlása, vagy
- ha valamely jogi kötelezettségnek való megfelelés (azaz az Adatkezelési Nyilvántartásban jogi kötelezettség jogalappal rögzített tevékenység esetén az adatkezelés céljának megfelelő időtartam alatt), vagy
- ha közérdekből végzett feladat végrehajtása, vagy
- ha az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása miatt, vagy
- ha népegészségügy területén érintő közérdekből,
- ha közérdekű archiválás céljából, vagy
- ha tudományos és történelmi kutatás céljából vagy statisztikai célból, vagy
- ha jogi igények előterjesztéséhez, érvényesítéséhez illetve védelméhez szükséges.

5.3.5. ***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

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;
d) az Érintett jogos érdek vagy közérdek jogalap alapján (az Adatkezelési Nyilvántartásban rögzített ezen két jogalap szerinti tevékenységre vonatkozóan) végzett adatkezelés ellen tiltakozott; 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 adatkezelést korlátozásra került.

Az Adatkezelő minden olyan címzettet tájékoztat a korlátozásról (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.

5.3.6. *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).

5.3.7. *A tiltakozáshoz való jog*

5.3.7.1. 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, 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, azaz törlendők.

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 mintája 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 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.

5.3.7.2. *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 visszavonását ugyanolyan egyszerű módon jogosult megtenni, mint annak megadását.

5.3.8. ***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 jogszabály 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 GDPR alkalmazandó.

5.4. Az adatvédelmi tisztviselő (DPO)

5.4.1. *A DPO kijelölése és feladatai*

A DrM-Professional Consulting Kft. adatkezelési célokkal és eszközökkel összefüggésben adatkezelési tevékenységeket végző adatvédelmi tisztviselőt jelölhet ki (DPO).

A DPO feladatai:

a) tájékoztatást és szakmai tanácsot ad a jelen Szabályzat hatálya alá tartozó alkalmazottai részére a GDPR valamint egyéb uniós vagy hazai adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
b) ellenőrzi a GDPR-nak, egyéb uniós vagy hazai rendelkezéseknek való megfelelést, a jelen Szabályzatnak és az adatvédelemmel összefüggő egyéb csoportszintű vagy belső szabályzatnak történő megfelelést, ennek keretében felelős a jelen Szabályzat és a Szabályzat részét képező formanyomtatványok és mellékletek elkészítéséért és naprakészen tartásáért, különös tekintettel felelős az Adatkezelési Nyilvántartásának elkészítéséért és naprakészen tartásáért az 5.5 pont figyelembevételével, illetve támogatja és ellenőrzi a jelen Szabályzat hatálya alá tartozók adatkezelési nyilvántartásának elkészítését és naprakészen tartását az 5.5 pont figyelembe vételével;
c) ellenőrzi az adatkezeléssel kapcsolatos feladatkörök kijelölését, részt vesz a jelen Szabályzat hatálya alá tartozók belső audit tevékenységében, javaslatot tesz a személyes adatvédelemmel kapcsolatos szabályozásra, módosításra, véleményezi a szabályozókat a személyes adatvédelem szempontjából,
d) szervezi és ellenőrzi az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését;
e) szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, nyomon követi az elvégzését;
f) együttműködik és bármely kérdésben konzultációt folytat a Felügyeleti Hatósággal, kapcsolattartási pontként szolgál a Felügyeleti Hatóság felé, ennek keretében részt vesz a jelen Szabályzat hatálya alá tartozó társaságok adatvédelmi incidenskezelési tevékenységében.

5.4.2. *Kapcsolattartás a DPO-val*

A jelen Szabályzat hatálya alá tartozók a DPO-val történő operatív kapcsolattartás, az adatkezelési tevékenységek cégen belüli koordinálása, valamint az Egyedi adatkezelési tevékenységekre vonatkozó feladatok teljesítése céljából egy adatvédelmi felelőst jelölnek ki, akinek nevét és elérhetőségét a jelen Szabályzat hatályba lépésével egyidejűleg megküldik a DPO-nak.

Ha a jelen Szabályzat hatálya alá tartozók 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 társasági adatvédelmi felelőst.
- Ha adatvédelmi incidensre utaló eseményt tapasztal vagy ezzel kapcsolatban bármely más releváns információhoz jut, haladéktalanul köteles értesíteni a SOC-ot, illetőleg a társasági adatvédelmi felelősén keresztül a DPO-t és köteles továbbítani neki a releváns dokumentumokat és információkat.
- Ha a SOC a működési körében személyes adatkezelési tevékenységgel összefüggésbe hozható rendkívüli eseményt észlel, köteles értesíteni a DPO-t és köteles továbbítani neki a releváns információkat. (Lásd a jelen Szabályzat 5.8. pontja).

5.5. 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 DrM-Professional Consulting Kft. nyilvántartásait a DPO vezeti.

5.5.1. ***Az adatkezelési tevékenységekre vonatkozó jogszabályi kötelezettségek***

5.5.1.1. Adatkezelési Nyilvántartás vezetése és felülvizsgálata

Az Adatkezelő (a jelen Szabályzat hatálya alá tartozó minden társaság) az általa végzett adatkezelési tevékenységekről nyilvántartást vezet a GDPR 30. cikk (1) bekezdése alapján, amelynek mintáját a NY-08 formanyomtatvány tartalmazza.

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 (lásd még 5.5.1.3. pont).

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. Az 5.3.1. 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 társasági adatvédelmi felelősének, különösen jogszabályváltozás, új belső folyamatok, fejlesztések vagy szolgáltatások esetén, figyelembe véve az 5.5.1.3. pont rendelkezéseit is.

5.5.1.2. 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 rendszeresen 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 adatvédelmi felelős valamint szükség szerint az adatfeldolgozó bevonásával törlési bizottságot hoz létre az intézkedések meghatározása érdekében. A törlési intézkedések határidőben történő megtételét anonimizált módon dokumentálni szükséges.

5.5.1.3. 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.

5.5.2. ***Az adatfeldolgozói nyilvántartás vezetése és felülvizsgálata***

Az Adatfeldolgozó nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységekről a GDPR 30. cikk (2) bekezdése alapján, amelynek mintáját a [dok_szam]-NY-09 formanyomtatvány tartalmazza. Az adatfeldolgozási nyilvántartást az alapjául szolgáló adatfeldolgozási megállapodások módosulása, megszűnése vagy új adatfeldolgozási megállapodás megkötésével egyidejűleg folyamatosan kell frissíteni az 5.7. pontban írtak szerint.

5.5.3. ***Nyilvántartás az adatvédelmi incidensekről***

A DrM-Professional Consulting Kft. nyilvántartást vezet az adatkezelési tevékenységekkel összefüggő adatvédelmi incidensekről a GDPR 33. cikk (5) bekezdés alapján, az 5.8. pontban írtaknak megfelelően, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. Az Egyedi adatkezelési tevékenységet végző Adatkezelő a Cég adatvédelmi felelős útján nyilvántartást vezet az Egyedi adatkezelési tevékenységekkel összefüggő adatvédelmi incidensekről.

Az adatvédelmi incidens nyilvántartás mintáját a NY-10 formanyomtatvány tartalmazza. 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.

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

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

Az Adatkezelő a GDPR jelen Szabályzat 5.1. pontjában írt alapelveinek megfelelően tárolja, használja fel, továbbítja és egyéb módon kezeli a személyes adatokat.

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 személyes adatok informatikai alap adatbázisban történő elektronikus tárolása az adatkezelési tevékenységért felelős szervezeti egység által az informatikai szolgáltatást nyújtó adatfeldolgozó társasággal egyeztetett módon meghatározott és az Adatkezelési Nyilvántartásban (NY-08) rögzített helyen történik (O oszlop).

A papíralapú dokumentumok papíralapú vagy elektronikus másolatainak létrehozását, továbbítását (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 Adatkezelő működési körén belül az informatikai adatbázisban tárolt személyes adatok elektronikus másolatainak létrehozásával kapcsolatos biztonsági előírásokat valamint az adattovábbításra vonatkozó biztonsági előírásokat az Adatkezelő informatikai feladatok ellátásáért illetve az információbiztonsági feladatok ellátásáért felelős szervezeti egysége a lehetőségekhez mérten folyamatosan frissített adatáramlási és adattovábbítási térképet vezet. Az adatáramlási és adattovábbítási térképnek összhangban kell állnia az Adatkezelési Nyilvántartás és az az alapján készülő Tájékoztató címzettekre vonatkozó adataival, amelyet az elszámoltathatóság alapelvére tekintettel a DPO az 5.4.1. b) pont szerinti feladatkörében rendszeresen ellenőriz.

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 az 5.4.1. b) pont szerinti feladatkörében.

5.6.2. *Személyes adatok törlésére vonatkozó lényeges szempontok*

Az Adatkezelő

- az 5.5.1.2. pontban írtak szerint az Adatkezelési Nyilvántartásban az egyes adatkezelési tevékenységek vonatkozásában az adatkezelés célja tekintetében meghatározott időtartam elteltét vagy
- az 5.3.1.2. pontban írtak szerint az Érintett törlésre irányuló kérelmének (törlési jog gyakorlása vagy tiltakozási jog gyakorlása) teljesítéséről szóló döntést követően

törölni köteles a személyes adatot az alap adatbázisból papír alapon és elektronikus tárolási helyén is (lásd Adatkezelési Nyilvántartás I és J oszlop). A törlési kötelezettség vonatkozik a személyes adatok másolataira is.

Az 5.5.1.2. pont szerinti rendszeres felülvizsgálat körében, valamint az 5.3.1.2. 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 az 5.4.1. b) pont szerinti feladatkörében.

5.6.3. *Adatbiztonság*

A GDPR 32. cikke értelmében az Adatkezelő és az Adatfeldolgozó a tudomány és technológia állására, a megvalósítás költségeire figyelemmel, valamint az adatkezelési tevékenységei természetes személyek jogaira és szabadságaira jelenlett 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 a személyes adatokhoz hozzáféréssel rendelkező alkalmazottai kizárólag a jogszabályoknak megfelelően kezelik a személyes adatokat kivéve, ha ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

Fentiek érdekében rögzíteni szükséges az alábbiakat:

- a biztonság megfelelő szintjének meghatározását, figyelembe véve az adatkezelésből eredő olyan kockázatokat, amelyek a személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésekből erednek,
- fizikai vagy műszaki adatvédelmi incidens esetén az arra vonatkozó intézkedéseket, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását a kellő időben vissza lehessen állítani,
- a személyes adatok kezelésére használt informatikai rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének biztosítására vonatkozó előírásokat;
- a személyes adatok lehetőség szerinti és mihamarabbi álnevesítésére vagy titkosítására vonatkozó előírásokat;
- az adatkezelés biztonságának garantálására hozott intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárásokat.

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

A jelen Szabályzat hatálya alá tartozók Adatkezelőként csak olyan Adatfeldolgozókat vesznek igénybe, amelyek megfelelnek a GDPR előírásainak. Az adatfeldolgozási megállapodást írásban kell megkötni az adatfeldolgozó igénybevételére vonatkozó szerződéssel egyidejűleg. A jogszabálynak megfelelő kötelező elemeket tartalmazó adatfeldolgozási megállapodás mintáját a NY-11 Adatfeldolgozási megállapodás minta formanyomtatvány tartalmazza. Amennyiben a Felügyeleti Hatóság általános szerződési feltételeket határoz meg az adatfeldolgozási megállapodásra vonatkozóan, a mintát annak megfelelően módosítani szükséges.

A jelen Szabályzat hatálya alá tartozók az adatfeldolgozással összefüggésbe hozható beszerzéseik tekintetében a szerződéskötéssel egyidejűleg kötelesek adatfeldolgozási megállapodást kötni, amely a beszerzési eljárás során megkötendő szerződés mellékletét képezi.

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 az kapcsolatot az Érintettel. A megállapodást e tekintetben a társaság adatvédelmi felelősének és a DPO-nak is véleményezni kell. A megállapodás lényegéről az Érintetteket tájékoztatni kell. Biztosítani kell az Érintett jogait abban az esetben is, ha azokat a megállapodás feltételeitől függetlenül kívánja gyakorolni.

5.8. Adatvédelmi incidenskezeléssel kapcsolatos általános szabályok és jogszabályi dokumentációs kötelezettség

5.8.1. *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 az 5.5.3. pont rendelkezései vonatkoznak.

5.8.2. *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 órán belül bejelenti a NAIH részére. A bejelentést, amennyiben ilyen létezik, a NAIH által megadott formában és módon kell megtenni, a NAIH előírásai szerint (például a NAIH által megjelölt felületen vagy hot-line vonalon). Amennyiben a NAIH nem hoz létre ilyen felületet, a bejelentést a kötelező tartalmi elemeivel kell megtenni. Az átmeneti időszakra (NAIH által közzétett kötelező minta bevezetéséig) vonatkozó bejelentés mintáját a NY-12 formanyomtatvány tartalmazza. A bejelentéssel egyidejűleg az 5.8.3. pont rendelkezéseinek megfelelő tájékoztatási kötelezettséget is teljesíteni kell.

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

5.8.3. *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 az alábbi esetekben:

a) ha 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) ha 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) ha 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.

Az Érintettek adatvédelmi incidensről szóló tájékoztatásának mintáját a NY-13 formanyomtatvány tartalmazza.

5.8.4. *Az adatvédelmi incidens belső bejelentése, kivizsgálása, közbenső döntések*

Az Adatkezelő bármely munkavállalója a jelen Szabályzat 5.4.2. pontjai értelmében az adatkezeléssel összefüggésben tudomására jutott, intézkedést igénylő rendkívüli eseményre vonatkozó információt haladéktalanul továbbítja a SOC részére.

Az Adatfeldolgozó bármely munkavállalója az adatfeldolgozással összefüggésben tudomására jutott, intézkedést igénylő rendkívüli eseményre vonatkozó információt haladéktalanul továbbítja a SOC részére.

A DPO az esemény SOC általi észlelésétől számított 48 órán belül, de legkésőbb 60 órán belül az eset összes körülményét figyelembe véve az adatvédelmi incidens kockázat értékelési módszertan alapján döntési javaslatot fogalmaz meg arra vonatkozóan, hogy

- az esemény adatkezelési tevékenységet érintő adatvédelmi incidens-e (lásd 5.8.1. pont),
- amennyiben igen, az adatvédelmi incidens jár-e kockázattal a természetes személyek jogaira és szabadságaira nézve (ez esetben lásd Hatósági bejelentés 5.8.2. pont),
- és ha jár, akkor az magas kockázat-e (ez esetben lásd Hatósági bejelentés 5.8.2 és Érintettek tájékoztatása 5.8.3 pont)
- minden esetben figyelembe véve a bűnüldöző hatóságok jogos érdekeit is olyan esetekben, ha az idő előtti közlés szükségtelenül veszélyeztetné az eset körülményeinek kivizsgálását.

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 Adatkezelő illetve Adatfeldolgozó vonatkozásában felelős szakterületek képviselőjét.

A javaslat alapján haladéktalanul döntést kell hozni arról, hogy kötelező-e a NAIH részére a bejelentés az 5.8.2 pontnak megfelelően illetőleg kötelező-e az Érintettek tájékoztatása az 5.8.3. 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.

A döntést követően a DPO az adatvédelmi incidens tudomásra jutásától 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.

5.9. Jogorvoslati lehetőségek

Az Érintett az általa 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 (a törvényszékek felsorolását és elérhetőségét az alábbi linken keresztül tekintheti meg: http://birosag.hu/torvenyszekek).

Bármely Érintett az egyéb közigazgatási vagy bírósági jogorvoslatok sérelme nélkül jogosult arra, hogy panaszt tegyen a 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.

6. Hatályon kívül helyezés

Nincs hatályon kívül helyezendő dokumentum.

7. Mellékletek és formanyomtatványok

- M-01 Adatkezelési célok
- M-02 Adatkezelési eszközök

- M-03 Adatvédelmi incidens kockázatértékelési módszertan

- NY-01 Hozzájárulás minta
- NY-02 Érdekmérlegelési teszt minta
- NY-03 Adatkezelési Tájékoztató minta „alap”
- NY-04 Adatkezelési Tájékoztató minta „carrier”
- NY-05 Adatkezelési Tájékoztató minta „eseti, hozzájárulással”
- NY-06 Adatkezelési Tájékoztató minta „szabályzat”
- NY-07 Adatkezelési Tájékoztató minta „contract”
- NY-08 Az adatkezelési tevékenységek nyilvántartás mintája
- NY-09 Az adatfeldolgozási nyilvántartás mintája
- NY-10 Adatvédelmi Incidensek nyilvántartás mintája
- NY-11 Adatfeldolgozási megállapodás minta
- NY-12 Adatvédelmi incidens hatósági bejelentési minta
- NY-13 Érintettek tájékoztatásának mintája adatvédelmi incidens esetén
- NY-14 Válaszlevél érintetti kérelem esetén
- NY-15 Értesítés minta címzetteknek kérelemről