Személyes adatok kezelésére és közérdekű adatok nyilvánosságára vonatkozó szabályzat

Változat: 3.1.

Készítette: Számol és Társai
Szolgáltató és Tanácsadó Bt.

Hatályba léptette:

Lanku Ildikó
ügyvezető igazgató

Érd, 2020. január 1.

Tartalomjegyzék

Technikai oldal

A dokumentum jellemzői

Dokumentum címe:	Személyes adatok kezelésére és közérdekű adatok nyilvánosságára vonatkozó szabályzat
Dokumentum célja:	Megfelelés az információs önrendelkezési jogról és az információszabadságról szóló törvény, valamint az Európai Unió Általános Adatvédelmi Rendelete (GDPR) előírásainak.
Kiadás száma:	3.1.
Kiadás kelte:	2020. január 1.
Azonosító:	TSZ-5
Állapot:	jóváhagyott
Fájlnév:	5-2020 Személyes adatok kezelésére és közérdekű adatok nyilvánosságára vonatkozó szabályzat 20200101.docx

Jóváhagyások

Készítette:	Számol és Társai Szolgáltató és Tanácsadó Bt.		
Módosította:	Számol és Társai Szolgáltató és Tanácsadó Bt.		
Jóváhagyta:	Varga Emília		
Hatályba helyező:	Lanku Ildikó		

Módosítások jegyzéke

Kiadás	Dátum	Változtatás rövid leírása
1.0.	2016.08.01.	Első kiadás.
2.0.	2018.05.25.	Szabályzat teljes átdolgozása jogszabályváltozás miatt.
3.0.	2019.02.01.	A szabályzat teljes átdolgozása.
3.1.	2020.01.01.	3. sz. függelék módosítása.

I.

Általános rendelkezések

1. A szabályzat célja, fogalmi meghatározások

1.1 A szabályzat célja

Az Adatkezelési szabályzat (a továbbiakban Szabályzat) célja, hogy az Érd és Térsége Csatorna-szolgáltató Kft. (a továbbiakban: „**Társaság**") által kezelt személyes adatok tekintetében biztosítsa az adatkezelésre, az adatok védelmére, az adatbiztonságra vonatkozó követelmények betartását a hatályos adatvédelmi és adatkezelési jogszabályoknak megfelelően.

Főbb adatvédelmi jogszabályok:

- A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)" szóló Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelet (a továbbiakban: GDPR).
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.).

A további, a személyes adatkezelés szempontjából releváns szabályok jegyzékét az Adatkezelési Nyilvántartás tartalmazza.

Amennyiben a jelen Szabályzatban nem kerül külön meghatározásra a Társaság kötelezettségi körébe tartozó, végrehajtandó feladatokat a Társaság nevében ellátó, végrehajtó szervezet, abban az esetben azokat mindig az Adatkezelési Nyilvántartás alapján, az adott adatkezelési cél vonatkozásában, az adatkezelésért felelős szervezet köteles ellátni.

1.2 Fogalmi meghatározások

a. Társaság: a társaságon az Érd és Térsége Csatorna-szolgáltató Kft -t. kell érteni.

b. „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;

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

d. „adatkezelés”: a 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;

e. „Adatkezelési Nyilvántartás”: A Társaság adatkezelési tevékenységeiről vezetett nyilvántartása az adatkezelés céljáról, az érintettek és a személyes adatok kategóriáról, a címzettek kategóriáról, adatok őrzési idejéről, az adatkezelés jogalapjáról, az adatok forrásáról;

f. „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

g. „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. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

h. „az érintett hozzájárulása”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

i. „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;

j. „kötelező erejű vállalati szabályok”: a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ.

2. A szabályzat hatálya

2.1 Személyi hatály

A Szabályzat szervezeti hatálya kiterjed:

a. a Társaság minden szervezeti egységre,
b. a Társaság minden munkatársára, vezető tisztviselőire, és az egyéb munkavégzésre irányuló jogviszonyban álló személyekre (a továbbiakban Munkavállaló), akik vonatkozásában a személyes adatok kezelése előfordulhat,
c. a Társaság adatkezelő és/vagy adatfeldolgozó tevékenységi körében adatkezelési tevékenységeket végző személyekre,
d. azon természetes személyekre, akikkel kapcsolatban a Társaság személyes adatokat kezel vagy feldolgoz (Érintett).

A jelen szabályozásban foglaltak érvényre juttatása érdekében a Szabályzatban foglaltak betartását a külső partnerekkel kötött és védett adatok kezelését érintő szerződésekben és megállapodásokban kötelezően elő kell írni. Ennek végrehajtásáért a Társaság Ügyvezető Igazgatója a felelős.

2.2. Tárgyi hatály

A jelen Szabályzat tárgyi hatálya kiterjed:

a. a Szabályzat személyi hatálya alá tartozók által a fenti adatkezelési célokkal és eszközökkel összefüggésben az adatkezelési tevékenységek során kezelt vagy feldolgozott, illetve bármely adathordozón tárolt személyes adatokra, beleértve a munkatársak és az ügyfelek, egyéb szerződéses partnerek munkavállalóinak adatait is, valamint

b. minden adatkezelési tevékenységre, beleértve
   - a nyilvántartást,
   - a hozzáférést,
   - a hozzáférési jogosultságok kezelését,
   - a feldolgozást (beleértve a rögzítést, módosítást),
   - az adattárolást,
   - az adattovábbítást,
   - a nyilvánosságra hozatalt és
   - az archiválást, az adattörlést, megsemmisítést.

II.

A Társaság adatvédelmi szervezete

1. Ügyvezető Igazgató

Az adatvédelem első számú felelőse a Társaságnál az Ügyvezető Igazgató.

Feladatai:

- gondoskodik a személyes adatok kezelésére vonatkozó jogelvek érvényesüléséről;
- gondoskodik az adatkezelési műveletekre vonatkozó utasítások jogszerűségéről;
- gondoskodik az adatok biztonságáról, az ehhez szükséges szervezési és technikai intézkedések meghozataláról, eljárási szabályok kialakításáról;
- gondoskodik az adatvédelemmel összefüggő tevékenységek és felelősségek körültekintő és egyértelmű elhatárolásáról;
- biztosítja a Szabályzatban meghatározott feladatokhoz a szükséges erőforrásokat;
- kinevezi az adatvédelmi tisztségviselőt és ellenőrzi a munkáját.

2. Adatvédelmi tisztviselő (DPO)

Kijelölés

A GDPR alapján a Társaság köteles adatvédelmi tisztviselőt (Data Protection Officer - a továbbiakban DPO) kijelölni. A DPO-t a szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a DPO feladatkörök ellátására való alkalmasság alapján kell kijelölni.

A DPO nevét és elérhetőségét az 1. sz függelék tartalmazza.

Jogállása

A Társaság biztosítja, hogy a DPO a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon. A Társaság a DPO-t a feladatai ellátásával kapcsolatban nem bocsáthatja el, szankcióval nem sújthatja. A DPO a feladatai ellátásával kapcsolatban közvetlenül a Társaság Ügyvezető Igazgatójának tartozik felelősséggel.

A DPO feladatai:

- tájékoztatást és szakmai tanácsot ad a Társaság alkalmazottai részére a GDPR valamint egyéb uniós vagy hazai adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
- ellenőrzi a GDPR-nak, egyéb uniós vagy hazai rendelkezéseknek való megfelelést, a jelen Szabályzatnak és az adatvédelemmel összefüggő egyéb 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 a Társaság Adatkezelési nyilvántartásának elkészítéséért és naprakészen tartásáért;
- ellenőrzi az adatkezeléssel kapcsolatos társasági feladatkörök kijelölését, részt vesz a Társaság adatkezeléssel kapcsolatos belső audit tevékenységében, javaslatot tesz a személyes adatvédelemmel kapcsolatos szabályozásra, módosításra, véleményezi a szabályozókat a személyes adatvédelem szempontjából;
- szervezi és ellenőrzi az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését;
- szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, nyomon követi az elvégzését;
- 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.

3. Szervezeti egységek vezetői

Feladataik:

- ellenőrzik az irányításuk alatt álló szervezeti egységek adatkezelését;
- szervezeti egységükben biztosítják az adatvédelmi előírások betartását;
- kijelölik az adatgazdákat azon szervezeti egységekben, ahol személyes adatkezelési tevékenység folyik;
- fogadják, kivizsgálják a bejelentéseket, és intézkedést kezdeményeznek a DPO-nál vagy Ügyvezető Igazgatónál.

4. Információbiztonsági felelős (IBF)

Az IBF feladatai:

- munkája során szorosan együttműködik a fejlesztési felelősökkel, valamint a rendszergazdákkal, adatgazdákkal, és kapcsolatot tart valamennyi védelmi feladatot ellátó személlyel;
- együttműködik az informatikai rendszerek üzemeltetőivel az informatikai működés folytonosságát biztosító terv elkészítésének érdekében;
- tárolja és őrzi valamennyi, a társaság informatikai biztonságára vonatkozó dokumentumot és adatbázist, beleértve az informatikai biztonsági politikát. valamint a biztonsági eseményekről készült adatbázist is;
- kockázatelemzést végez az informatikai biztonságot érintő kérdésekben, és erről tájékoztatja az informatikai vezetőt;
- az informatikai biztonságot érintő gyakorlati kérdésekben tájékoztatja és irányítja az érintetteket annak érdekében, hogy elősegítse a megfelelő informatikai biztonsági szint elérését.

5. Adatgazdák

Minden olyan szervezeti egység, amely személyes adatot kezel, adatgazdákat jelöl, akik feladatkörükben a következő feladatokat látják el:

- meghatározzák az adott szervezeti egységen belül kezelt személyes adatok körét;
- a kezelt személyes adatok körét bejelentik a DPO által vezetett Adatkezelési Nyilvántartásba, a szükséges egyéb információk megjelölése mellett;
- gondoskodnak az Adatkezelési Nyilvántartásban szereplő személyes adatok körének naprakész nyilvántartásáról, bármilyen változás esetén soron kívül jelzik a módosítás szükségességét a DPO-nál;
- ha az adatkezelés jogos érdek miatt kerül kezelésre, elvégzik a DPO szakmai iránymutatása mellett az érdekmérlegelési tesztet.

6. Munkavállalók

Feladataik:

- felelős az általuk végzett adatkezelés vagy adatfeldolgozás szabályszerűségéért;
- a tudomására jutott személyes adatokat kizárólag a Társaság mindenkor hatályos ügyvezető igazgatói utasításainak rendelkezései szerint dolgozhatják fel, saját célra adatfeldolgozást nem végezhetnek, továbbá a személyes adatokat az Társaság rendelkezései szerint kötelesek tárolni és megőrizni;

- az adatkezelést érintő érdemi döntést nem hozhatnak, a hozzájuk beérkező bejelentéseket, kérelmeket és az érintettek személyes adatuk kezelésével kapcsolatban benyújtott tiltakozásait a DPO-nak továbbítják;
- kötelesek jelenteni a DPO-nal késedelem nélkül, teljes körűen lehetőleg írásban, ha adatvédelmi eseményt, incidenst, annak következményeit tapasztalják, vagy bekövetkezését valószínűsítik, vagy ha a Szabályzat rendelkezéseinek érvényesülése bármilyen módon ellehetetlenül.

III.

Személyes adatok védelme az adatkezelés során

1. Személyes adatkezelésre vonatkozó alapelvek

Az Érintettek személyes adataihoz való jogának érvényesítése érdekében a Társaság működése során tiszteletben tartja az adatvédelmi jog 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 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 törölje vagy helyesbítse;
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.

A Szabályzat a fenti alapelvek körében a következőkről rendelkezik:

- adattárolással és adattörléssel kapcsolatos 1. e) pont szerinti szervezési és technikai intézkedésekről vagy az azokra való utalásról,
- az adat- és információbiztonsággal kapcsolatos 1. f) pont szerinti szervezési és technikai intézkedésekről vagy az azokra való utalásról valamint,
- az elszámoltathatóság alapelvének történő megfelelés érdekében a jogszabályi dokumentációs kötelezettségekről.

2. A személyes adatok kezelésének jogszerűsége

2.1. Jogalapok

Személyes adatot a Társaság kizárólag az alábbi esetekben kezel:

a) ha az Érintett **hozzájárulás**át 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 Társaságra vonatkozó **jogi kötelezettség** teljesítéséhez szükséges, vagy
d) ha az adatkezelés az Érintett vagy egy másik természetes személy **létfontosságú érdekeinek védelme** miatt szükséges, vagy
e) ha az adatkezelés az Társaság vagy egy harmadik fél **jogos érdek**einek 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.

Az egyes adatkezelési tevékenységek jogalapjait az Adatkezelési nyilvántartás és az annak alapján készített Adatkezelési Tájékoztató tartalmazza.

2.2 Dokumentáció

2.2.1. Hozzájárulás

Ha az Adatkezelési nyilvántartás a hozzájárulást jelöli meg az adatkezelés jogalapjaként, akkor az elszámoltathatóság alapelvére tekintettel az Adatkezelési nyilvántartás szerint az adott adatkezelési cél vonatkozásában felelős szervezetnek igazolnia kell, hogy az Érintett a személyes adatainak kezeléséhez önkéntes, konkrét és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánításával hozzájárult. Tehát igazolni kell azt, hogy az Érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelezte, hogy beleegyezését adta az őt érintő személyes adatok kezeléséhez.

Hozzájárulás jogalap esetén személyes adat csak az Érintett nyilatkozatát követően kezelhető. A hozzájárulás mintáját a 2. sz. függelék szerinti formanyomtatvány tartalmazza.

2.2.2.Érdekmérlegelési teszt

Amennyiben az Adatkezelési nyilvántartás jogos érdeket jelöl meg az adatkezelés jogalapjaként, úgy ez esetben érdekmérlegelési teszt lefolytatására van szükség. Ennek keretében meg kell határozni, hogy mi a Társaság vagy a harmadik fél jogszerű érdeke, meg kell vizsgálni, hogy mi az Érintett olyan érdeke vagy alapvető joga és szabadsága, amely 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 az 1. sz. melléklet szerinti formanyomtatvány tartalmazza.

Az érdekmérlegelési teszteket az adatkezelés megkezdését megelőzően az Adatkezelési nyilvántartás szerint az adott adatkezelési cél vonatkozásában felelős szervezeti egység által kijelölt adatgazdának kell elkészíteni a DPO bevonásával. Az elvégzett érdekmérlegelési tesztek írásbeli dokumentációját a DPO őrzi.

2.3 Az Érintett jogainak védelme

2.3.1 Átlátható tájékoztatáshoz és kommunikációhoz való jog

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

A tájékoztatás jogának gyakorlása az alábbi esetekben tagadható meg:

a) az Érintett már rendelkezik az előírt információval;
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 a Társaság 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).

A Tájékoztatót az Adatkezelési nyilvántartás alapján készíti el a DPO. A jogszabálynak megfelelő, kötelező elemeket tartalmazó Tájékoztatók (munkaügyi adatokra, belépésre, kamarahasználatra, gépjárműhasználtra, informatikai eszközökre stb.) a munkavállalók számára a Társaság belső intranetes portálján érhetőek el, míg az ügyfelek számára pedig az a Társaság internetes oldalán kerül kihelyezésre. Az Adatkezelési Tájékoztatókat a 3. sz. függelék tartalmazza.

Az egyéb speciális adatkezelés esetében lehetőség szerint az online elérést kell biztosítani az Érintett számára, s amennyiben ez a Társaság részéről nem megoldható, e-mailben vagy papír alapon igazolható módon kell megküldeni, átadni az Adatkezelési Tájékoztatót.

Ha a Felügyeleti Hatóság további formai vagy tartalmi előírásokat határoz meg a Tájékoztatóra vonatkozóan, a mintát annak megfelelően módosítani szükséges.

Az Érintett a jogainak gyakorlása érdekében jogosult bármely formában kérelmet benyújtani a Társaság részére, amely kérelem teljesítését a Társaság nem tagadhatja meg, kivéve, ha bizonyítja, hogy az Érintettet nem áll módjában azonosítani.

A kérelem benyújtását és dokumentált érkeztetését követően az adatkezelési tevékenységért felelős szervezeti egység kijelölt munkavállalója szükség esetén a DPO 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 Társaság jogszabály szerint kötelezett-e.

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 az 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. 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 Társaság bizonyítani tudja, hogy a kérelem egyértelműen megalapozatlan (különösen például ismétlődő) vagy túlzó.

A II. 2.3.2.-II. 2.3.7. pontokra vonatkozó visszajelzés (válaszlevél az érintett személyes adatkezeléssel összefüggő kérelmére) mintáját a 4. sz. függelék szerinti formanyomtatvány tartalmazza, az ugyanott említett címzetti értesítések mintáját az 5. sz. függelék szerinti formanyomtatvány tartalmazza.

2.3.2. Az Érintett hozzáférési joga

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 Tájékoztatóban egyébként kötelezően rögzítendő információhoz.

Az Érintett jogosult arra, hogy a személyes adatok másolatát kérje a Társaságtól. Az Érintett által kért további másolatokért a Társaság 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

2.3.3. Helyesbítéshez való jog

Az Érintett erre vonatkozó kérelme esetén a Társaság 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.

A Társaság 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 a Társaság tájékoztatja e címzettekről.

2.3.4.Törléshez való jog

Az Érintett jogosult arra, hogy a Társaságtól a rá vonatkozó személyes adatok törlését kérje, a Társaság 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 a Társaságra 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 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 Társaságre ruházott közhatalmi jogosítvány gyakorlása miatt, vagy
- ha népegészségügy területén érintő közérdekből, vagy
- ha közérdekű archiválás céljából, vagy
- ha tudományos és történelmi kutatás céljából vagy statisztikai célból, vagy
- ha jogi igények előterjesztéséhez, érvényesítéséhez illetve védelméhez szükséges.

2.3.5. Az adatkezelés korlátozásához való jog

A korlátozás általában egy átmeneti intézkedés egy érintetti igény elbírálásáig vagy egy intézkedés megtételéig. Az Érintett kérelmére a Társaság korlátozza az adatkezelést, ha

a) az Érintett vitatja a személyes adatok pontosságát, amely esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a Társaság ellenőrizze a személyes adatok pontosságát;
b) az adatkezelés jogellenes, és az Érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
c) a Társaságnak 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 a Társaság 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.

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

2.3.6. Az adathordozhatósághoz való jog

Az Érintett jogosult arra, hogy a rá vonatkozó, általa a Társaság 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 a Társaság, 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).

2.3.7. A tiltakozáshoz való jog

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 a Társaság a személyes adatokat nem kezelheti tovább, azaz törölni köteles, kivéve, ha a Társaság 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.

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.

2.3.8. Automatizált döntéshozatal, profilalkotás

A Társaság 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:

- a Társaság és az Érintett közötti szerződés megkötése vagy teljesítése érdekében szükséges;
- meghozatalát a Társaságra 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.

3. A személyes adatok védelmének biztosítása

A személyes adatokat kezelő szervezeti egységek vezetőinek gondoskodniuk kell az általuk kezelt adatok védelméről. Az adatokat és az adatok kezeléséhez használt eszközöket védeni kell különösen:

- a jogosulatlan adathozzáféréstől, felhasználástól
- az adatok indokolatlan megváltoztatásától,
- a nyilvánosságra kerüléstől,
- nem kívánt törlés, sérülés vagy megsemmisülés ellen.

Amennyiben a szervezeti egység vezetője az előírtaknak bármilyen okból nem tud eleget tenni, kezdeményeznie kell a Társaság Ügyvezető Igazgatójánál a védelem személyi, tárgyi és anyagi feltételeinek biztosítását.

IV.

Adatvédelem és adatbiztonság

A Társaság nevében az Informatikai Csoport gondoskodik az adatok védelméről. Ennek érdekében megteszi a szükséges technikai és szervezési intézkedéseket mind az informatikai eszközök útján tárolt, mind a hagyományos, papíralapú adathordozókon tárolt adatállományok tekintetében. Gondoskodik arról, hogy a vonatkozó jogszabályokban előírt adatbiztonsági szabályok érvényesüljenek. Ugyancsak gondoskodik az adatok biztonságáról, megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az irányadó jogszabályok, adatvédelmi szabályok, valamint a véletlen érvényre juttatásához szükségesek.

A Társaság az adatokat megfelelő intézkedésekkel védi a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Az adatbiztonság szabályainak érvényesüléséről a Társaság külön szabályzatok, utasítások, eljárási rendek útján gondoskodik. Az adatbiztonság feltételeinek érvényesítése érdekében gondoskodik az érintett munkatársak megfelelő felkészítéséről.

A Társaság az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel van a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt választja, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

A nem elektronikus formában tárolt adatok biztonsága vonatkozásában az Iratkezelési szabályzatának rendelkezései az irányadóak.

Minden Munkavállaló köteles késedelem nélkül, lehetőleg írásban a közvetlen felettesének valamint a DPO-nak jelenteni, amennyiben a fenti szabályzatokban a szabályozás hiánya folytán az adatvédelmet és adatbiztonságot veszélyeztető esemény bekövetkezése, vagy bekövetkezésének lehetősége tudomására jut. A bejelentésekről a DPO feljegyzést készít, és kivizsgálást kezdeményez. A feljegyzés megőrzési ideje az adott adatkezelési célhoz kapcsolódó adatok megőrzésére előírt időtartam.

V.

Személyes adatok kezelésével összefüggő tevékenységek

1. Nyilvántartási kötelezettség

1.1. Az adatkezelési tevékenység nyilvántartása, Adatkezelési nyilvántartás

A Társaság az általa végzett adatkezelési tevékenységekről nyilvántartást vezet. A nyilvántartást a DPO vezeti az adatkezelési tevékenységért felelős szervezeti egységek adatgazdáinak adatszolgáltatása alapján a 7. sz. függelék szerinti adattartalommal.

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. Az Adatkezelési nyilvántartás alapján kerül elkészítésre a 2.3.1. pont szerinti Tájékoztató, ezért 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.

A Társaság 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 DPO valamint szükség szerint az adatfeldolgozó bevonásával törlési bizottságot hoz létre az intézkedések meghatározása érdekében. Személyes adat törlése és/vagy megsemmisítése esetén úgy kell eljárni, hogy a törölt vagy megsemmisített dokumentum tartalma ne legyen visszaállítható.

Papír alapú dokumentumok esetén iratmegsemmisítőt kell használni, míg számítógépes adatbázisok esetén a programnyelv fizikai törlés utasítását és/vagy a tárterület többszörös felülírását kell alkalmazni a mindenkori informatikai biztonsági szabályoknak megfelelően.

A törlési intézkedések határidőben történő megtételét anonimizált módon dokumentálni szükséges, amely jegyzőkönyvet a törlést végző személyek és az érintett szervezeti egység vezetője ír alá. A törlési jegyzőkönyv mintáját a személyes adat törléséről, hozzáférhetetlenné tételéről az 6. sz. függelék tartalmazza.

Adatvédelmi hatásvizsgálat

A Társaságnak az adatkezelést megelőzően hatásvizsgálatot kell végeznie, 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.

1.2. Az adatfeldolgozói tevékenység nyilvántartása

A Társaság adatfeldolgozó nyilvántartást vezet az Társaság nevében végzett adatkezelési tevékenységekről, amelynek mintáját a 7. sz. függelék tartalmazza. Az adatfeldolgozási nyilvántartást az alapjául szolgáló adatfeldolgozási megállapodások módosulása, megszűnése vagy új adatfeldolgozási megállapodás megkötésével egyidejűleg folyamatosan kell frissíteni az alábbi II.2.3. pontban írtak szerint.

1.3. Adatvédelmi incidens nyilvántartás

A Társaság nyilvántartást vezet az adatkezelési tevékenységekkel összefüggő adatvédelmi incidensekről a IV.1 pontban foglaltak szerint, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. Az Egyedi adatkezelési tevékenységet végző Társaság nyilvántartást vezet az Egyedi adatkezelési tevékenységekkel összefüggő adatvédelmi incidensekről.

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.

VI.

Személyes adatok tárolása, felhasználása, adatbiztonság

1. A személyes adatok tárolásának, felhasználásának, továbbításának lényeges szempontjai

A Társaság a GDPR jelen Szabályzat III.1. pontjában írt alapelveinek megfelelően tárolja, használja fel, és továbbítja a személyes adatokat. A szervezési és technikai intézkedéseket az Adatkezelési nyilvántartás összegzi.

Az egyes adatkezelési tevékenységekre irányadó belső szabályzatok „Adatkezelés és adatvédelem" címszó alatt részletezhetik a feladatkörükbe tartozó adatkezeléssel összefüggő tevékenységek releváns eljárásait.

A személyes adatok (alap adatbázis) papíralapú tárolása fizikailag az adatkezelési tevékenységért felelős szervezeti egység által meghatározott és az Adatkezelési nyilvántartásban rögzített helyen történik.

A személyes adatok informatikai alap adatbázisban történő elektronikus tárolása az adatkezelési tevékenységért felelős szervezeti egység által meghatározott és az Adatkezelési nyilvántartásban rögzített helyen történik.

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 a Társaság működési körén belül a feladat elvégzéséhez szükséges mértékben a minimálisra kell szorítani összhangban az Ügyviteli és iratkezelési szabályzatban meghatározottakkal.

A Társaság működési körén belül az informatikai adatbázisban tárolt személyes adatok elektronikus másolatainak létrehozásával kapcsolatos biztonsági előírásokat valamint az adattovábbításra vonatkozó biztonsági előírásokat az Informatikai biztonsági szabályzat tartalmazza. A DPO a feladatkörében rendszeresen ellenőrzi az adatkezelési és adatvédelmi rendelkezéseket tartalmazó szabályzatokat annak érdekében, hogy a GDPR rendelkezésekkel összhangban kerüljenek kialakításra.

A munkavégzést követően a személyes adatokat tartalmazó adathordozó csak olyan zárható helyen tárolható, amelynek kulcskezelése egyértelműen meghatározza azon személyek körét, akik az adathordozókhoz hozzáférhetnek.

Személyes adatokat tartalmazó adatbázisok off-line adathordozóinak tárolására zárható szekrényt kell alkalmazni.

Az Társaság 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 Társaság és az Adatfeldolgozó egyúttal biztosítja, hogy a személyes adatokhoz hozzáféréssel rendelkező alkalmazottai kizárólag a jogszabályoknak meghatározottaknak megfelelően kezelik a személyes adatokat kivéve, ha ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

2. A személyes adatok törlésének lényeges szempontjai

A Társaság

- az Adatkezelési nyilvántartásban az egyes adatkezelési tevékenységek vonatkozásában az adatkezelés célja tekintetében meghatározott időtartam elteltét, vagy
- az Érintett törlésre irányuló kérelmének (törlési jog gyakorlása vagy tiltakozási jog gyakorlása lásd III.2.3. pont) teljesítéséről szóló döntést követően törölni köteles a személyes adatot az alap adatbázisból (lásd Adatkezelési nyilvántartás). A törlési kötelezettség vonatkozik a személyes adatok másolataira is, kivéve, ha azok az iratkezelési szabályzat hatálya alá tartozó iraton jelennek meg, amely esetben az irat tárgyára vonatkozóan meghatározott megőrzési és selejtezési idő az irányadó.

A rendszeres felülvizsgálat körében, valamint a 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 időközönként, de legalább évente jelentést készít a feladatkörében eljárva.

Informatikai rendszerekből és különösen a biztonsági mentésekből történő törlésekkel kapcsolatban az informatikai rendszerekre vonatkozó külön szabályozások tartalmaznak előírásokat.

3. Adatfeldolgozó igénybevétele, közös adatkezelés

Az Társaság csak olyan Adatfeldolgozókat vesz 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 8. sz. függelék szerinti Adatfeldolgozási megállapodás minta tartalmazza. Amennyiben a Felügyeleti Hatóság általános szerződési feltételeket határoz meg az adatfeldolgozási megállapodásra vonatkozóan, a mintát annak megfelelően módosítani szükséges.

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

Az adatfeldolgozással összefüggő szerződéskötések tényét a beszerzésért felelős terület kijelölt munkavállalója köteles bejelenteni a DPO-nak annak érdekében, hogy az Adatkezelési nyilvántartás és ezzel egyidejűleg a Tájékoztató 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 a Társaság 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. Kapcsolattartó, cégképviselők személyes adatainak kezelése

Azon szerződések esetében, ahol kapcsolattartói és/vagy cégképviselői adatként a Társaság vagy külső partner munkavállalóinak, megbízottjainak stb. neve, elérhetőségi adatai szerepelnek, ezen adatok is személyes adatnak minősülnek, ezért a 2. sz. melléklet szerinti szerződéses rendelkezésekkel szükséges az adott szerződést módosítani, kiegészíteni.

Minden, a szerződésért felelős szervezet köteles a megkötött, fentiek szerinti adatokat tartalmazó szerződéseket felülvizsgálni, s amennyiben a vonatkozó adatvédelmi rendelkezések hiányoznak a szerződésből, úgy a szerződést a 3. sz. melléklet szerinti tartalommal kell kiegészíteni.

A szerződés módosítására, kiegészítésére minden ésszerű intézkedést meg kell tenni, de mindenképpen fel kell hívni a szerződéses partner figyelmét ezen adatok jogszerű kezelésének fontosságára.

Az új szerződések esetében pedig a 8. sz. függelék szerinti tartalmat kötelező elemként kötelesek a szerződésgazda szervezetek a szerződésben szerepeltetni.

VII.

Az adatvédelmi incidens szabályozása

1. Incidens nyilvántartás

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 V.1.1.3. pont rendelkezései vonatkoznak, a nyilvántartás mintát pedig a 9. sz. függelék tartalmazza.

2. Hatósági bejelentés

Az adatvédelmi incidenst az Társaság a tudomására jutását követően indokolatlan késedelem nélkül, ha lehetséges, legkésőbb 72 (hetvenkettő) órával 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, amelynek mintáját a 10. sz. függelék tartalmazza. A bejelentéssel egyidejűleg az érintetett is tájékoztatni kell..

Ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, az elszámoltathatóság elvével összhangban bejelentést nem kell megtenni. Ezt a döntést a Társaság Ügyvezető Igazgatója hozza meg, mérlegelve az eset összes körülményeit.

3. Az Érintett tájékoztatása

Az Társaság indokolatlan késedelem nélkül tájékoztatja (11. sz. függelék) az Érintettet az adatvédelmi incidensről, **ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve**.

Ezt a döntést az eset összes körülményeire tekintettel kell meghozni, amelyről feljegyzés készül.

Nem kell értesíteni az Érintettet az alábbi esetekben:

- ha az Társaság 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
- ha az Társaság 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
- 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.

4. Az adatvédelmi incidens belső vizsgálata

Az Társaság és az Adatfeldolgozó bármely munkavállalója a jelen Szabályzat értelmében az adatkezeléssel/adatfeldolgozással összefüggésben tudomására jutott, intézkedést igénylő rendkívüli eseményre vonatkozó információt haladéktalanul továbbítja a DPO részére.

Az adatkezelési eszközöket üzemeltető szervezeti egység elektronikus úton naponta riportot küld a DPO részére előző 72 órában előforduló adatvédelmi incidens lehetőségét rejtő hibaelhárításokról.

DPO az esemény észlelésétől számított 96 órán belül, az eset összes körülményét figyelembe véve az adatvédelmi incidens kockázat értékelési módszertan alapján döntési javaslatot fogalmaz meg arra vonatkozóan, hogy

- az esemény adatvédelmi incidens-e ,
- amennyiben igen, az adatvédelmi incidens jár-e kockázattal a természetes személyek jogaira és szabadságaira nézve,
- és ha jár, akkor az magas kockázat-e ,
- 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 Társaság illetve Adatfeldolgozó vonatkozásában felelős szakterületek képviselőjét, az információbiztonsági felelős vezetőt. A javaslat alapján haladéktalanul döntést kell hozni arról, hogy kötelező-e a NAIH részére a bejelentés a 2. pontnak megfelelően illetőleg kötelező-e az Érintettek tájékoztatása a 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 észlelésétől számított lehetőleg legkésőbb 72 (hetvenkettő) 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 (hetvenkettő) órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

5. Jogorvoslati lehetőségek

Az Érintett által tapasztalt jogellenes adatkezelés esetén polgári pert kezdeményezhet az Társaság 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 a következő linken keresztül tekintheti meg: http://birosag.hu/torvenyszekek).

Az egyéb közigazgatási vagy bírósági jogorvoslatok sérelme nélkül, minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti e rendeletet.

Magyarországon az illetékes Felügyeleti Hatóság:

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
postacím: 1530 Budapest, Pf.: 5
e-mail: ugyfelszolgalat@naih.hu
telefon: +36 (1) 391-1400
fax.: +36 (1) 391-1410
honlap: www.naih.hu

VIII.

Záró rendelkezések

1. Tájékoztatási tevékenység

A Társaság adatvédelemmel kapcsolatos belső tájékoztatási tevékenység a vállalati intranet oldalon keresztül történik, míg a küldő partnerek, ügyfelek tájékoztatására a Társaság honlapján keresztül, vagy közvetlenül levélben, elektronikus levélben történik.

2. Szabályzat felülvizsgálata

A Szabályzatot a személyes adatkezelésre vonatkozó jogszabályok módosulása során felül kell vizsgálni, de legalább évente egyszer szükséges ellenőrizni, hogy megfelel-e a hatályos rendelkezéseknek. A Szabályzat felülvizsgálatáért a DPO a felelős.

Mellékletek:

1. sz. melléklet: Érdekmérlegelési teszt minta
2. sz. melléklet: Kapcsolattartók, cégképviselők személyes adatainak kezelése

Függelékek:

1. sz. függelék: DPO neve és elérhetősége
2. sz. függelék: Hozzájárulás minta
3. sz. függelék: Adatvédelmi Tájékoztatók
4. sz. függelék: Válaszlevél érintetti kérelem esetén
5. sz. függelék: Értesítés minta címzetteknek kérelemről
6. sz. függelék: Törlési jegyzőkönyv minta
7. sz. függelék: Adatkezelési nyilvántartás minta
8. sz. függelék: Az adatfeldolgozási nyilvántartás mintája
9. sz. függelék: Adatvédelmi incidensek nyilvántartás mintája
10. sz. függelék: Adatvédelmi incidens bejelentése felügyeleti hatóságnak minta
11. sz. függelék: Érintettek tájékoztatásának mintája adatvédelmi incidens esetén