

Door To Door Express Kft.

székhely: 2890 Tata, Csever u. 2. F. ép.

Adatvédelmi és adatbiztonsági szabályzat

Hatályos: 2023.09.15.



Tartalomjegyzék

1. Bevezető rendelkezések	3
2. Fogalmak	3
3. Az alkalmazandó jogszabályok kijelölése.....	7
4. A szabályzat célja és hatálya.....	7
5. Az adatkezelés elvei	8
6. Az adatkezelések szabályai	9
7. Az adatkezelés lehetséges jogalapjai.....	10
8. Az érintettek jogai	13
9. Érdelmérlegelés és az érdelmérlegelési teszt elvégzése.....	19
10. Az Adatkezelő adatvédelmi rendszere	19
A vezető tisztségviselő	19
Az adatkezelésben érintett munkatársak	20
11. Adatbiztonsági szabályok.....	20
12. Adatvédelmi incidens.....	22
13. Adatvédelmi oktatás	24
14. Adatvédelmi nyilvántartás.....	25
15. Adatfeldolgozókra vonatkozó szabályok	25
16. Adatvédelmi hatásvizsgálat.....	26
17. Általános adatvédelmi alapvetések	27
18. Nyilvántartások	27
19. Záró rendelkezések.....	28
Mellékletek Nyilvántartás minták, adatkezelési folyamatleírások és tájékoztatók a társaság adatvédelmi szabályzatához	29
Titoktartási nyilatkozat.....	30
Adatvédelmi tájékoztató és folyamatleírás a GDPR 13. cikk szerint - Minta.....	31
Adatvédelmi tájékoztató és folyamatleírás a GDPR 14. cikk szerint - Minta.....	35
Az érintett hozzáférési jogának gyakorlása esetén adott válasz - Minta	39
Az érintett tájékoztatása a rá vonatkozó adat helyesbítéséről - Minta	41
Táblázat az érintetti jogok gyakorolhatóságáról	42
Érdelmérlegelési teszt – Minta	43
Adatvédelmi incidens jelentő lap - Minta	47
Adatvédelmi incidens-nyilvántartó lap - Minta	48
Adatfeldolgozói szerződés	49
Adatvédelmi hatásvizsgálat elkészítéséhez használatos segédanyag - Minta	61
Adatmegsemmisítési jegyzőkönyv - Minta.....	65
Munkavállalói nyilatkozat.....	66
Elektronikus megfigyelőrendszerbe történő betekintési joggal rendelkező személyek nyilvántartása	67
Jegyzőkönyv kamerás képekbe történő betekintéshez - Minta	68
Jegyzőkönyv kamerás képek korlátozásáról - Minta	69
Elektronikus megfigyelőrendszerben történő korlátozási joggal rendelkező személyek nyilvántartása	71
Adatfelvételi nyomtatványokon elhelyezendő adatvédelmi kiegészítés.....	72

Adatkezelő megnevezése:	Door To Door Express Fuvarozó és Szállítmányozó Kft.
Adatkezelő cégjegyzékszáma:	11-09-010199
Adatkezelő adószáma:	13312428-2-11
Adatkezelő székhelye:	2890 Tata, Csever u. 2. F. ép.
Adatkezelő telephelye:	2890 Tata, Csever u. 2. F. ép.
Adatkezelő elérhetősége:	https://www.dtdexpress.hu/
Adatkezelő képviselője:	Bognár Gergely ügyvezető

1. BEVEZETŐ RENDELKEZÉSEK

1.1. A Szabályzatban használt rövidítések:

GDPR: az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Infotv.: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Társaság vagy Adatkezelő: Door to Door Express Kft.

NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság

1.2. Bár a GDPR az Adatkezelő számára kifejezetten adatvédelmi szabályzatalkotási kötelezettséget nem ír elő, ám a GDPR 24. cikk (2) bekezdése és (78) preambulumbekkezdése, valamint a NAIH NAIH/2018/1212/2/K és NAIH/2018/1594/2/K ügyszámú adatvédelmi reformmal kapcsolatos állásfoglalásai alapján az Adatkezelő úgy döntött, hogy adatkezelési tevékenysége okán a belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából jelen Adatvédelmi és adatbiztonsági szabályzatban (a továbbiakban: Szabályzat) határozza meg az adatvédelmi és adatbiztonsági szabályait.

1.3. A Szabályzat rendelkezéseit az Adatkezelő többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent e Szabályzat és a bármely más, jelen Szabályzat hatálybalépése előtt hatályba lépett szabályzat, utasítás előírásai között, úgy abban az esetben e Szabályzat rendelkezései az irányadók.

1.4. Amennyiben ellentmondás áll fent e Szabályzat és a bármely más, jelen Szabályzat hatálybalépése utána hatályba lépő szabályzat vagy utasítás előírásai között, úgy csak abban az esetben nem e Szabályzat rendelkezései az irányadók, ha a később hatályba lépő szabályzat vagy utasítás arról kifejezetten rendelkezik.

2. FOGALMAK

A Szabályzatban használt fogalmak megegyeznek a GDPR 4. cikkében meghatározott értelmező fogalommagyarazatokkal.

- **Érintett:** azonosított vagy azonosítható természetes személy (GDPR 4. cikk 1.);
- **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 (GDPR 4. cikk 1.);
- **Személyes adat különleges kategóriái:** a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok (GDPR 9. cikk 1.);
 - **Különleges adat:** a személyes adatok különleges kategóriába tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok (Infotv. 3. §. 3.);
 - **Bűnügyi személyes adat:** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat (Infotv. 3. §. 4.);
 - **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 (GDPR 4. cikk 11.);
 - **Érintett jogai, a Rendelet 12-21. cikkében szabályozott jogok:**
 - tájékoztatás joga,
 - hozzáférési jog,
 - helyesbítéshez való jog,
 - törléshez való jog,
 - adatkezelés korlátozhatóságához való jog,
 - adathordozhatósághoz való jog,
 - tiltakozáshoz való jog;
 - **Tiltakozás:** az érintett jogosult arra, hogy saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a GDPR 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is (GDPR 21. cikk (1) bekezdés);
 - **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; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja (GDPR 4. cikk 7.);
 - **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 (GDPR 4. cikk 2.);
 - **Adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele (Infotv. 3. § 11.);
 - **Nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele (Infotv. 3. § 12.);
 - **Adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges (Infotv. 3. § 13.);
 - **Adatkezelés korlátozásához való jog:**

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

- a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
- b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- d) az érintett a 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben. [GDPR 18. cikk. (1)]

Adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából (GDPR 4. cikk 3.);

- **Adatmegsemmisítés:** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése (Infotv. 3. § 16.);
- **Adatfeldolgozás:** az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége (Infotv. 3. § 17.);
- **Adatfeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel (GDPR 4. cikk 8.);
- **Adatállomány:** az egy nyilvántartásban kezelt adatok összessége (Infotv. 3. § 21.);
- **Harmadik fél:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak (GDPR 4. cikk 10.);
- **EGT-állam:** az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez (Infotv. 3. § 23.);
- **Harmadik ország:** minden olyan állam, amely nem EGT-állam (Infotv. 3. § 24.);
- **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 (GDPR 4. cikk 12.);
- **Álnevesítés:** a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni (GDPR 4. cikk 5.);
- **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 (GDPR 4. cikk 9.);
- **Egészségügyi adat:** egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról (GDPR 4. cikk 15.);
- **Képviselő:** az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a GDPR 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy

- adatfeldolgozóra a rendelet értelmében háruló kötelezettségek vonatkozásában (GDPR 4. cikk 17.);
- **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 (GDPR 4. cikk 20.);
 - **A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása:** 1) adattovábbítás megfelelőségi határozat alapján, 2) adattovábbítás megfelelő garanciák alapján, 3) megfelelőségi határozat, illetve megfelelő garanciák hiányában, a GDPR által biztosított az eltérés lehetősége különös helyzetekben alapján történhet (GDPR 44-50. cikk);
 - **Nyilvántartási rendszer:** a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető (GDPR 4. cikk 6.);
 - **Profilalkotás:** személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják (GDPR 4. cikk 4.);
 - **Releváns és megalapozott kifogás:** a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy a Rendeletet megsértették-e, illetve, hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a Rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét (GDPR 4. cikk 24.);
 - **Tevékenységi központ:**
 - a) az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira, eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;
 - b) az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozó a Rendelet szerint meghatározott kötelezettségek vonatkoznak [GDPR 4. cikk 16.];
 - **Vállalkozás:** gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is (GDPR 4. cikk 18.);
 - **Vállalkozáscsoport:** az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások (GDPR 4. cikk 19.);
 - **Felügyeleti Hatóság:** egy tagállam által a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv (GDPR 4. cikk 21.);
(Az Infotv. 38. § (2a) alapján a GDPR-ban a felügyeleti hatóság részére megállapított feladat- és hatásköröket Magyarország joghatósága alá tartozó jogalanyok tekintetében a GDPR-ban, valamint az Infotv-ben meghatározottak szerint a NAIH gyakorolja.)
 - **Érintett felügyeleti Hatóság:** az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

- a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság területén rendelkezik tevékenységi hellyel,
- b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket, vagy
- c) panaszt nyújtottak be az említett felügyeleti hatósághoz (GDPR 4. cikk 22.);
- **Személyes adatok határokon átnyúló adatkezelése:**
 - a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
 - b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket (GDPR 4. cikk 23.);
- **Az információs társadalommal összefüggő szolgáltatás:** az (EU) 2015/1535 európai parlamenti és tanácsi irányelv 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás (GDPR 4. cikk 25.);
- **Nemzetközi szervezet:** a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre (GDPR 4. cikk 26.).

Amennyiben a mindenkor hatályos adatvédelmi jogszabály (jelen Szabályzat megalkotásakor a GDPR és az Infotv.) fogalommagyarázatai eltérnek jelen Szabályzat fogalommagyarázataitól, akkor a jogszabályok által meghatározott fogalmak az irányadók.

3. AZ ALKALMAZANDÓ JOGSZABÁLYOK KIJELELÉSE

A GDPR az Európai Parlament és a Tanács Rendelete, amely így teljes egészében kötelező és közvetlenül alkalmazandó az Európai Unió valamennyi tagállamban, így Magyarországon is.

Magyarország Alaptörvényének E) cikke kimondja, hogy az Európai Unió joga megállapíthat általánosan kötelező magatartási szabályt, így a Szabályzat megalkotása és alkalmazása során a szabályok elsődlegesen a GDPR-ból fakadnak.

Abban az esetben, ha a GDPR szabályainak megfelelő módon magyar jogszabály – elsősorban az Infotv., de speciális adatkezelések esetében ágazati jogszabályok – részletszabályokat alkot meg, akkor az Adatkezelő ezeket a szabályokat is alkalmazza.

Abban az esetben, amennyiben az adatkezelés nem esik a GDPR hatálya alá, úgy az Infotv. szabályait alkalmazza az Adatkezelő.

4. A SZABÁLYZAT CÉLJA ÉS HATÁLYA

Az Adatkezelő a Szabályzat megalkotásával és elérhetővé tételével biztosítja a GDPR III. fejezetében meghatározott érintetti jogokat azzal, hogy meghatározza az adatvédelmi elvek gyakorlati megvalósulását és az Adatkezelő által folytatott adatvédelmi folyamatokat. A Szabályzat meghatározza az Adatkezelő által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott személyes adatokat, azok forrását, az adatkezelés célját, jogalapját, időtartamát, az adatkezelésbe esetlegesen bevont adatfeldolgozó nevét, címét és az adatkezeléssel összefüggő tevékenységét, továbbá – az érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapját és címzettjét.

A Szabályzat további célja, hogy egységes szerkezetbe foglalja az Adatkezelőnél az adatkezelésben résztvevő munkavállalók és az Adatkezelővel egyéb munkavégzésre irányuló jogviszonyban álló személy számára az Adatkezelő minden adatkezelési folyamatát.

A Szabályzattal az Adatkezelő biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést, azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.

A Szabályzat személyi hatálya kiterjed minden olyan személyre, aki az Adatkezelővel fennálló, így különösen munkavállalói-, munka-, adatfeldolgozó-, megbízási jogviszonya alapján (továbbiakban: az Adatkezelő munkatársa) személyes adatokhoz hozzáfér, vagy azok birtokába jut.

A Szabályzat tárgyi hatálya kiterjed az Adatkezelőnél megvalósuló minden folyamatra, melynek során a GDPR 4. cikk 1. pontjában meghatározott személyes adat kezelése történik.

A Szabályzat időbeli hatálya annak kihirdetésétől visszavonásáig tart.

5. AZ ADATKEZELÉS ELVEI

5.1. Az Adatkezelő az adatkezelés során az alábbi alapelvek alapján szervezi folyamatait

5.1.1. jogszerűség, tisztességes eljárás és átláthatóság elve [GDPR 5. cikk (1) a)]: az Adatkezelő személyes adatot csak jogszerűen és a tisztességesen kezel, az adatkezelést az érintett számára átlátható módon, többek között jelen Szabályzat nyilvánosságra hozatalával, végzi.

5.1.2. célhoz kötöttség elve [GDPR 5. cikk (1) b)]: az Adatkezelő minden esetben, ha személyes adatot kezel, az adat felvétele előtt meghatározza a személyes adat kezelésének célját, amely így előre meghatározott, egyértelmű és jogszerű. Személyes adatot az Adatkezelő az előre meghatározott céllal össze nem egyeztethető módon nem kezel. Amennyiben teljesült az adatkezelés célja és jogszabály nem írja elő kötelezően az adat további kezelését, úgy a személyes adatot az Adatkezelő törli.

5.1.3. adattakarékosság elve [GDPR 5. cikk (1) c)]: az Adatkezelő az adatkezelés során csak olyan személyes adatot kezel, amely a cél eléréséhez megfelelő és releváns, a Társaság az adatkezelést csak a cél eléréséhez szükséges minimum adatmennyiségre korlátozza.

5.1.4. pontosság elve [GDPR 5. cikk (1) d)]: az Adatkezelő törekszik rá, hogy az általa kezelt személyes adatok pontosak és naprakészek legyenek és a jelen Szabályzatba foglalt módon törekszik rá, hogy a pontatlan személyes adatokat haladéktalanul törölje vagy – az érintett kérelmére vagy tudomására jutása esetén az Adatkezelőtől – helyesbítse.

5.1.5. korlátozott tárolhatóság elve [GDPR 5. cikk (1) e)]: az Adatkezelő személyes adatot csak úgy tárol, hogy a személyes adat érintettje csak az adatkezelés céljának eléréséig azonosítható az adatkezelés során, a személyes adatok ennél hosszabb ideig történő tárolását csak jogszabály kötelező előírása alapján végzi az Adatkezelő.

5.1.6. integritás és bizalmasság elve [GDPR 5. cikk (1) f)]: az Adatkezelő az adatkezelési folyamatait úgy tervezi és hajtja végre, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítja a személyes adatok megfelelő biztonságát, így különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet.

5.1.7. elszámoltathatóság elve [GDPR 5. cikk (2)]: az Adatkezelő az adatkezelési folyamatait úgy tervezi és hajtja végre, hogy az adatkezelés bármely pillanatában képes legyen a jelen pontba foglalt elveknek való megfelelést igazolni.

6. AZ ADATKEZELÉSEK SZABÁLYAI

6.1. Alapvetések

6.1.1. Az Adatkezelő kizárólag a hatályos jogszabályok rendelkezései alapján végez adatkezelést.

6.1.2. Az Adatkezelő személyes adatot csak és kizárólag a GDPR 6. cikkében foglalt jogalapokkal, személyes adatok különleges kategóriába tartozó személyes adatot csak és kizárólag a GDPR 9. cikk (2) bekezdésében rögzített feltétel fennállása mellett kezel.

6.1.3. A konkrét adatkezelési folyamattal érintett jogosultság vagy kötelezettség keletkezhet az Adatkezelő, az érintett vagy harmadik fél oldalán is.

6.1.4. Az Adatkezelő kezelésében lévő személyes adat az adatkezelés során mindaddig megőrzi személyes adat minőségét, amíg belőle az érintett azonosított vagy azonosítható. Az Adatkezelő akkor tekint egy adatot személyes adatnak, amennyiben rendelkezik azzal a technikai feltétellel, amely segítségével képes az adatból azonosítani az érintettet.

6.1.5. Az Adatkezelő csak úgy folytat adatkezelést, hogy az minden szakaszában megfelel az adatkezelési célnak.

6.1.6. Az Adatkezelő jelen Szabályzat vagy a konkrét adatkezelési folyamatleírás nyilvánosságra hozatalával minden esetben közli az érintettel az adatkezelés célját, az adatkezelés jogalapját, valamint az adatkezeléssel kapcsolatos, a GDPR 13-14. cikkében meghatározott tényeket.

6.1.7. Az Adatkezelő munkaszervezési, fizikai, informatikai és jogosultságkezelési eszközökkel gondoskodik arról, hogy illetéktelen személyek a személyes adatokat ne ismerhessék meg.

6.1.8. Az Adatkezelő munkatársai és az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek munkatársai és megbízottjai (alvállalkozói) kötelesek az adatkezelés során megismert személyes adatokat titokként megőrizni.

6.2. A személyes adatokkal kapcsolatos titoktartási szabályok

6.2.1. A személyes adatok egyetlen része vagy töredéke sem tehető közzé, nem bocsátható rendelkezésre vagy nem tárható fel semmilyen módon harmadik személy előtt, kivéve, ha a személyes adat közérdekből nyilvános adatként történő nyilvánosságra hozatalát jogszabály írja elő.

6.2.2. Az Adatkezelő munkatársai kötelesek megtenni azokat az intézkedéseket, amelyek kizárják, hogy a szóban elhangzott, papíralapon vagy elektronikus formátumban rögzített személyes adatot bármely harmadik személy jogosulatlanul megismerje.

6.2.3. Személyes adatról papíralapú vagy elektronikus másolat csak abban az esetben készíthető, ha azt az adatkezelés folyamata szükségessé teszi vagy jogszabály előírja.

6.2.4. Ha az Adatkezelő valamely munkatársa a Szabályzatot megszegi, az Adatkezelő és közte lévő jogviszony jellegétől függően felelősséggel tartozik.

6.2.5. Ha a Szabályzatot az Adatkezelővel munkaviszonyban álló személy szegi meg és ezzel kárt okoz, úgy a munkaviszony ellátásra vonatkozó általános (a Szabályzat kiadásakor a munka

törvénykönyvről szóló 2012. évi I. törvény) vagy speciális jogszabály munkaviszonyból származó kötelezettségének megszegésével okozott kárra vonatkozó szabályok szerint felel.

6.2.6. Ha a Szabályzatot az Adatkezelővel egyéb jogviszonyban álló személy szegi meg és ezzel kárt okoz, úgy a mindenkori Polgári törvénykönyv (a Szabályzat kiadásakor a Polgári Törvénykönyvről szóló 2013. évi V. törvény) károkozásért való felelősségre vonatkozó szabályok szerint felel.

6.2.7. A személyes adatokkal kapcsolatos titoktartási nyilatkozat a Szabályzat **1. sz. melléklete**.

7. AZ ADATKEZELÉS LEHETSÉGES JOGALAPJAI

7.1. Általános szabályok

7.1.1. Az adatkezelés jogalapját az Adatkezelő minden adatkezelési folyamatnál meghatározza. Az adatkezelésre jogalapot csak a GDPR 6. cikk (1) bekezdésekben rögzítettek szerint határoz meg az Adatkezelő.

7.1.2. Az Adatkezelő az adatkezelési rendszerét úgy alakítja ki, hogy minden személyes adatra vonatkozóan bizonyítani tudja, hogy mikor, milyen formában történt a személyes adat felvétele és milyen tájékoztatást kapott az érintett a személyes adat felvételekor.

7.1.3. A személyes adatok különleges kategóriába tartozó személyes adatot főszabály szerint az Adatkezelő nem kezel, kivéve abban az esetben, amennyiben bizonyítani tudja a GDPR 9. cikk (2) bekezdésében foglalt valamely körülmény fennállását.

7.2. Az adatkezelés lehetséges jogalapjai személyes adatok esetében

7.2.1. Az **érintett hozzájárulását adta** személyes adatainak egy vagy több konkrét célból történő kezeléséhez. [GDPR 6. cikk (1) a)]

7.2.2. Az adatkezelés olyan **szerződés teljesítéséhez szükséges**, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. [GDPR 6. cikk (1) b)]

7.2.3. Az adatkezelés a Társaságra vonatkozó **jogi kötelezettség** teljesítéséhez szükséges. [GDPR 6. cikk (1) c)]

7.2.4. Az adatkezelés az érintett vagy egy másik természetes személy **létfontosságú érdekeinek¹ védelme** miatt szükséges. [GDPR 6. cikk (1) d)]

7.2.5. Az adatkezelés **közérdekű vagy közhatalmi jogosítvány gyakorlásának** keretében végzett feladat végrehajtásához szükséges. [GDPR 6. cikk (1) e)]

7.2.6. Az adatkezelés a Társaság vagy egy harmadik fél **jogos érdekeinek érvényesítéséhez** szükséges. [GDPR 6. cikk (1) f)]

7.2.7. A Társaság a GDPR 6. cikk (1) e) pontban nevesített, az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásával kapcsolatos jogalappal adatkezelést nem végezhet, mert a Társaság nem közhatalmi szerv, így közhatalmi jogosítvánnyal sem rendelkezik.

7.3. Körülmények, amelyek esetén az Adatkezelő személyes adatok különleges kategóriába tartozó adatokat kezelhet

¹ Létfontosságú érdek például, de nem kizárólagosan: járvány, katasztrófa, szükséghelyzet.

7.3.1. Az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy a hatályos magyar jog úgy rendelkezik, hogy 7.1.3. pontban foglalt tilalom az érintett hozzájárulásával sem oldható fel.

7.3.2. Az adatkezelés az Adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy hatályos magyar jog lehetővé teszi.

7.3.3. Az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni.

7.3.4. Az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott.

7.3.5. Az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

7.3.6. Az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy a hatályos magyar jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

7.3.7. Az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy hatályos magyar jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, amennyiben az adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, akire szakmai titoktartási kötelezettség hatálya alatt áll.

7.3.8. Az adatkezelés a népegészségügy területét érintő közérdekből szükséges.

7.3.9. Az adatkezelés közérdekű archiválás, tudományos és történelmi kutatási vagy statisztikai célból szükséges olyan uniós vagy hatályos magyar jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

7.4. Hozzájárulás, mint jogalapra vonatkozó különleges szabályok

7.4.1. Amennyiben az adatkezelés az érintett hozzájárulásán alapszik, úgy az érintett a hozzájárulását bármilyen bizonyítható módon megadhatja, így írásban (nyilatkozaton, dokumentumon), szóban és ráutaló magatartással is.

7.4.2. Az Adatkezelő fenntartja magának a jogot, hogy egyes adatkezelések esetén a hozzájárulás egyes formáit kizárja.

7.4.3. Az Adatkezelő minden adatkezelési folyamatát úgy határozza meg, hogy amennyiben annak jogalapja az érintett hozzájárulása, úgy képes legyen annak bizonyítására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Ennek elsősorban úgy tesz eleget az Adatkezelő, hogy elsődlegesen írásban szerzi be az érintett hozzájárulását, amelyet így az írásbeliséggel tud igazolni.

7.4.4. Amennyiben az Adatkezelő a ráutaló magatartást vagy a szóbeliséget is elfogadja a hozzájárulás jogalapjául, úgy az adatkezelés minden körülményét megvizsgálja és dokumentálja, hogy utóbb is igazolni tudja a hozzájárulást.

7.4.5. Az Adatkezelő biztosítja a jogot arra is, hogy az érintett ugyanúgy, ahogy a hozzájárulást megadta, a hozzájárulását visszavonja. A ráutaló magatartással megtett hozzájárulás visszavonását csak írásban fogadja el a Társaság.

7.4.6. Az Adatkezelő a visszavonás tényét az adatkezelés során rögzíti, az adatot a továbbiakban nem kezeli, de az adat helyét „a hozzájárulás visszavonva” jelzéssel jelöli meg.

7.5. Szerződéses jogviszonyra, mint jogalapra vonatkozó különleges szabályok

7.5.1. Ha az adatkezelés jogalapja a Társasággal írásban kötött szerződés megkötését megelőzően lépések tétele vagy teljesítése, úgy a szerződésnek minimálisan tartalmaznia kell az arra való utalást, hogy az adatkezelés a jelen Szabályzat szerint történik.

7.5.2. Ezen jogalap csak akkor használható, ha az szerződés egyik szerződő fele az érintett.

7.6. Jogi kötelezettségre, mint jogalapra vonatkozó különleges szabályok

7.6.1. Amennyiben az adatkezelés jogalapja az adatkezelőre vonatkozó jogi kötelezettség, úgy e jogi kötelezettséget csak és kizárólag az Európai Unió vagy Magyarország hatályos és alkalmazandó jogszabályának kell megállapítania.

7.6.2. Jogi kötelezettséget az Infotv. 5. § (3) alapján csak törvény vagy önkormányzati rendelet állapíthat meg. A gyakorlatban jogi kötelezettség, mint jogalap azonban alkalmazható egyéb jogszabályi szinten való szabályozás alapján is.

7.6.3. Amennyiben a jogi kötelezettség adja az adatkezelés jogalapját, úgy a jogszabálynak az Infotv. 5. § (3) előírása alapján, nem csak az adatkezelés kötelezettségét kell meghatároznia, hanem a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát is.

7.6.4. Amennyiben a Társaság az adatkezelése során jogalként a jogi kötelezettséget határozza meg, úgy a Társaság megnevezi a jogi kötelezettséget előíró jogszabályt annak nevével és a kötelezettséget előíró pontos jogszabályi helyet.

7.7. Létfontosságú érdekre, mint jogalapra vonatkozó különleges szabályok

7.7.1. A Társaság természetes személy létfontosságú érdeke jogalappal akkor végez adatkezelést, ha az adott adatkezelés egyéb jogalappal nem végezhető.

7.7.2. Az elszámoltathatóság elve miatt a Társaság az adatkezelés megkezdése előtt köteles megvizsgálni, hogy a személyes adat kezelése megvalósítható-e bármely más jogalappal és tudnia kell bizonyítania a létfontosságú érdek fennálltát.

7.8. Közérdekű feladatra, mint jogalapra vonatkozó különleges szabályok

7.8.1. Ezen jogalappal csak akkor végezhet a Társaság adatkezelést, ha az közérdekű feladatellátás vagy közhatalmi jogosítvány gyakorlásához szükséges.

7.9. Jogos érdekre, mint jogalapra vonatkozó különleges szabályok

7.9.1. Amennyiben a Társaság jogos érdek jogalappal kezel adatok, az adatkezelés megkezdése előtt az érintettek magánszférájának, érdekeinek és alapvető jogainak biztosítása érdekében érdekmérlegelési tesztet végez el.

7.9.2. A jogos érdek jogalapot a szükségesség-arányosság elve alapján alkalmazza a Társaság, ha az adatkezeléssel elérendő cél más jogalappal nem megvalósítható és az érintett magánszférájának korlátozása arányban áll az elérendő céllal.

7.9.3. Az érdekmérlegelési tesztet az érintett – kérelmére – bármikor megismerheti.

8. AZ ÉRINTETTEK JOGAI

8.1. Az érintett tájékoztatása az adat felvételéhez kapcsolódóan a GDPR 13. és 14. cikk szerint

8.1.1. Abban az esetben, **amennyiben az adatkezelés során a személyes adatokat az Adatkezelő közvetlenül az érintettől szerzi meg**, úgy a személyes adatok megszerzésének időpontjában - a jelen Szabályzat **2. sz. mellékletében** foglalt minta segítségével - az alábbiakról tájékoztatja az érintettet:

- az Adatkezelőnek és az Adatkezelő képviselőjének pontos megnevezése, elérhetőségei,
- az Adatkezelő adatvédelmi tisztviselőjének elérhetőségei,
- az adatkezelés célja,
- az adatkezelés jogalapja,
- amennyiben az adatkezelés célja az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítése, úgy az Adatkezelő vagy a harmadik fél jogos érdekének megnevezése,
- amennyiben az Adatkezelő a személyes adatokat az adatkezelés során harmadik fél számára átadja, a személyes adatok címzettjei, illetve a címzettek kategóriái.
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatóságához való jogáról,
- a hozzájárulás visszavonására irányuló jog gyakorlásának szabályai, amennyiben az adatkezelés jogalapja az érintett hozzájárulása [GDPR. 6. cikk 1) a)] vagy a [GDPR. 9. cikk 2) a)] pontba foglalt jogalap,
- a Nemzeti Adatvédelmi és Információszabadság Hatósághoz címzett panasz benyújtásának jogáról;
- annak ténye, hogy a személyes adat kezelése szolgáltatása jogszabályon, szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele és az érintett köteles-e a személyes adatokat megadni, valamint a lehetséges következmények, amennyiben az érintett személyes adatait nem adja meg,
- az automatizált döntéshozatal ténye, valamint legalább az ennek során alkalmazott logika és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

8.1.2. Amennyiben az Adatkezelő **a személyes adatot nem közvetlenül az érintettől szerzi meg** - a jelen Szabályzat **3. sz. mellékletében** foglalt minta segítségével - az alábbiakról tájékoztatja az érintettet:

- az Adatkezelőnek és az Adatkezelő képviselőjének pontos megnevezése, elérhetőségei,
- az Adatkezelő adatvédelmi tisztviselőjének elérhetőségei,
- az adatkezelés célja,
- az adatkezelés jogalapja,
- *a kezelt személyes adatok kategóriái,*

- amennyiben az Adatkezelő a személyes adatokat az adatkezelés során harmadik fél számára átadja, a személyes adatok címzettjei, illetve a címzettek kategóriái.
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- amennyiben az adatkezelés célja az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítése, úgy az Adatkezelő vagy a harmadik fél jogos érdekének megnevezése,
- az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatóságához való jogáról,
- a hozzájárulás visszavonására irányuló jog gyakorlásának szabályai, amennyiben az adatkezelés jogalapja az érintett hozzájárulása [GDPR. 6. cikk 1.) a.)] vagy a [GDPR. 9. cikk 2.) a.)] pontba foglalt jogalap,
- a Nemzeti Adatvédelmi és Információszabadság Hatósághoz címzett panasz benyújtásának jogáról;
- *a személyes adat forrása,*
- *amennyiben az adatok harmadik forrásból való gyűjtését jogszabály írja elő, úgy a konkrét jogszabályi hely megjelölése,*
- *a személyes adat Adatkezelő általi megszerzésének időpontja,*
- *amennyiben az Adatkezelő által folytatott ügyben van szükség a személyes adatokra, úgy a konkrét ügy ügyszámmal vagy egyéb módon történő megjelölése,*
- *annak ténye, hogy a személyes adat nyilvánosan hozzáférhető forrásból származik-e,*
- az automatizált döntéshozatal ténye, valamint legalább az ennek során alkalmazott logika és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

8.1.3. Amennyiben az Adatkezelő az adatkezelése során az adatot nem közvetlenül az érintettől szerzi meg, az érintettet az alábbi időpontban tájékoztatja:

- a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül,
- ha az Adatkezelő a személyes adatokat az érintettel való kapcsolattartás céljára használja, az érintettel való első kapcsolatfelvétel alkalmával vagy
- ha az Adatkezelő az adatokat várhatóan más címmel is közli, legkésőbb a személyes adatok első alkalommal való közlésekor.

8.1.4. Ha az Adatkezelő a személyes adatot nem közvetlenül az érintettől szerzi meg nem kell tájékoztatni, amennyiben:

- az érintett már rendelkezik az ezen pontokba foglalt információkkal,
- a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényelne,
- az adat megszerzését vagy közlését kifejezetten előírja az Adatkezelőre alkalmazandó uniós vagy a hatályos magyar jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről is rendelkezik, vagy
- a személyes adatoknak valamely uniós vagy a hatályos magyar jogban előírt szakmai titoktartási kötelezettség alapján bizalmasnak kell maradnia.

8.1.5. A tájékoztatást az Adatkezelő elsősorban a jelen Szabályzathoz tartozó adatkezelési tájékoztatókkal, folyamatleírásokkal valósítja meg. Ezen tájékoztatókat, folyamatleírásokat az Adatkezelő minden olyan esetben elkészíti, amikor az érintettet tájékoztatnia kell az adatkezelésről. A tájékoztató, folyamatleírás nyilvánosságra hozatalának szabályai:

- a folyamatleírások a jelen Szabályzat szerint elkészített adatkezelési nyilvántartás elválaszthatatlan részét képezi,

- a folyamatleírás minden esetben az adatkezelés megkezdése előtt az érintett számára megismerhető kell, hogy legyen,
- minden olyan folyamat során, amikor az adat felvétele papíralapon történik, az adat felvételének helyén elérhetőnek kell lennie az adott folyamatleírásnak,
- minden olyan folyamat során, amikor az adat felvétele technikai eszköz útján történik, a technikai eszköz segítségével elérhetőnek kell lennie a folyamatleírásnak,
- minden olyan esetben, amikor az érintett ráutaló magatartással járul hozzá az adatkezeléshez, a folyamatleírásnak a ráutaló magatartás megtételéül szolgáló helyen kell elérhetőnek lennie, hogy az érintett ennek tudatában járulhasson hozzá az adatkezeléshez,
- amennyiben feltételezhető, hogy az érintett maga fogja kezdeményezni az adatkezelést, ezen adatkezelések folyamatleírásai elérhetőek kell legyenek az Adatkezelő honlapján az érintett előzetes tájékoztatása érdekében,
- a folyamatleírásokat úgy kell nyilvánosságra hozni, hogy az Adatkezelő minden esetben bizonyítani tudja, hogy az érintett azokat az adatkezelés megkezdése előtt megismerhette, így különösen online felületen történő adatfelvétel esetén egy ún. „check box” segítségével nyilatkoztatja az Adatkezelő, hogy az adatkezelés szabályait megismerte, elolvasta és azokat elfogadta.

Amennyiben az Adatkezelő az adatkezeléssel kapcsolatos tájékoztatót /folyamatleírást az érintettel megismerteti, úgy vélelmezi, hogy az érintett azt megismerte és elfogadta.

8.2. Az érintett tájékoztatása a rá vonatkozó folyamatban lévő adatkezelésről („hozzáférési jog”)

8.2.1. Amennyiben az érintett a GDPR 15. cikke szerinti hozzáférési jogával kíván élni, úgy az Adatkezelő az alábbiakról tájékoztatja:

- az adatkezelés célja vagy céljai,
- az érintett személyes adatok kategóriái,
- azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat az Adatkezelő már közölte vagy a jövőben közölni fogja,
- a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- a helyesbítési jog gyakorlásának szabályai,
- a törlési jog gyakorlásának szabályai,
- az adatkezelés korlátozására irányuló jog gyakorlásának szabályai,
- a tiltakozási jog gyakorlásának szabályai,
- a Nemzeti Adatvédelmi és Információszabadság Hatósághoz való panasz benyújtásának joga,
- ha a személyes adatok forrás nem az érintett, a forrásra vonatkozó minden elérhető információ,
- amennyiben az adatkezelés automatizált döntéshozatalon alapszik, úgy ennek ténye, valamint az alkalmazott logikára és arra vonatkozó érthető információk.

8.2.2. Az Adatkezelő ezen tájékoztatás során az adatkezelés tárgyát képező személyes adatok másolatát az érintett kérelmére az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az Adatkezelő ésszerű mértékű díjat számíthat fel.

8.2.3. Ha az érintett elektronikus úton nyújtotta be a kérelmét, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett máshogy kéri.

8.3. Az érintett helyesbítéshez való joga

8.3.1. Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat, vagy kérje azok kiegészítését.

8.3.2. Amennyiben az érintett személyes adatának helyesbítését kéri és nem áll rendelkezésre a személyes adat, amelyre a már kezelt adatot helyesbíteni kell, hiánypótlásra hívja fel az Adatkezelő az érintettet.

8.3.2. Amennyiben az érintett személyes adatának helyesbítését kéri és a személyes adat rendelkezésre áll, az Adatkezelő a személyes adatot helyesbíti és azzal egyidőben írásban tájékoztatja az érintettet a helyesbítés tényéről és időpontjáról az **5. sz. melléklet** felhasználásával.

8.4. Az érintett törléshez való joga („az elfeledtetéshez való jog”)

8.4.1. Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, ha az alábbi indokok valamelyike fennáll:

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- a személyes adatokat jogellenesen kezelték;
- a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- a személyes adatok gyűjtésére a 16 éven aluli gyermekek részére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor;

8.4.2. Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és az 8.4.1. pontban írtak szerint törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

8.4.3. A személyes adat az érintett kérelmére sem törölhető a GDPR 17. cikk (3) bekezdésében foglalt adatkezelések esetében.

8.4.4. A személyes adatot az Adatkezelő olyan módon törli, hogy helyreállítása többé ne legyen lehetséges.

8.4.5. Amennyiben a személyes adat a személyes adatot hordozó adathordozóról nem törölhető, az Adatkezelő a személyes adat adathordozóját köteles megsemmisíteni.

8.4.6. Amennyiben az érintett olyan személyes adatot kíván töröltetni, amely hiányában az érintett az Adatkezelő közötti jogviszony nem tartható fenn, a jogviszony megszűnik. Erről azonban a törlés előtt az Adatkezelő tájékoztatja az érintettet és amennyiben törlési kérelmét fenntartja, a törlés megtörténik. A törlési kérelem fenntartásának minősül, ha a tájékoztatás kézbesítésétől számított 3 napon belül az érintett törlési kérelmét nem vonja vissza.

8.4.7. A személyes adat törlésére vagy az adathordozó megsemmisítésére az alábbi szabályok közül a felsorolásban előbb szereplő szabályt kell alkalmazni. Amennyiben az alkalmazandó szabály az adott személyes adatra nézve nem értelmezhető, a felsorolásban soron következő szabályt kell alkalmazni:

- a személyes adat kezelésének megszüntetésére vonatkozó kötelező jogszabályi előírás;
- a Szabályzat konkrét adatkezelésre vonatkozó, adattörlési vagy adatmegsemmisítési GDPR szerinti adattörlési, vagy adatmegsemmisítési szabálya.

8.5. Az adatkezelés korlátozásához fűződő érintetti jog

8.5.1. Az érintett kérelmezheti az Adatkezelőnél a rá vonatkozóan az Adatkezelő által tárolt személyes adatok megjelölését jövőbeli kezelésük korlátozása céljából.

8.5.2. Az Adatkezelő az érintett kérelmére akkor korlátozza az adatkezelést, amennyiben az alábbi feltételek egyike fennáll:

- az érintett kérelmében vitatja a rá vonatkozó személyes adatok pontosságát, ebben az esetben a korlátozás arra az időtartamra vonatkozik, ameddig az Adatkezelő ellenőrzi a személyes adatok pontosságát,
- az adatkezelés jogellenes, de az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,
- bár az Adatkezelőnek az adatkezelés megkezdése előtt meghatározott cél eléréséhez már nincs szüksége a személyes adat kezelésére, de az érintett kérelmében igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett a 8.6. pont alapján az tiltakozott az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

8.5.3. Amennyiben a személyes adat kezelését korlátozza az Adatkezelő, úgy a korlátozás időtartama során csak az érintett hozzájárulásával vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve a valamely tagállam fontos közérdekéből lehet kezelni.

8.5.4. A 8.5.3. pont nem vonatkozik az adat tárolására, mint adatkezelési műveletre, azt a korlátozás alatt is köteles megtenni az Adatkezelő.

8.5.5. Amennyiben az adatkezelés korlátozását az Adatkezelő feloldja, a korlátozás feloldása előtt legkésőbb három (3) munkanappal korábban a korlátozás feloldásának tényéről írásban tájékoztatja azt az érintettet, akinek a kérésére a korlátozás megtörtént.

8.6. Tiltakozás a személyes adat kezelése ellen

8.6.1. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladattal kapcsolatos kezelése, vagy az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítése kapcsán végzett kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is.

8.6.2. Az Adatkezelő tiltakozás esetén megvizsgálja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják-e, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

8.6.3. Amennyiben az Adatkezelő megállapítja, hogy a 8.6.2. pontba foglalt feltételek egyike sem érvényesül, a tiltakozással érintett személyes adatot nem kezeli tovább.

8.7. Az adathordozhatósághoz való érintetti jog gyakorlása

8.7.1. Amennyiben az adatkezelés jogalapja az érintetti hozzájárulás, vagy az adatkezelés szerződés teljesítéséhez, vagy előkészítéséhez szüksége, úgy az érintett jogosult arra, hogy az általa az Adatkezelő részére átadott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja. Ezt az Adatkezelő elsősorban .xml, .csv vagy .doc formátumban teljesíti a kérelemmel érintett személyes adatok jellegétől függően.

8.7.3. Az érintett kérelmezheti továbbá az Adatkezelőtől, hogy az általa kezelt személyes adatokat egy másik, az érintett által egyértelműen megjelölt adatkezelőnek továbbítsa.

8.7.4. E pontba foglalt jog nem illeti meg az érintettet, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges, valamint, ha ez a jog hátrányosan érintené mások jogait és szabadságait.

8.8. Jogorvoslat

8.8.1. Az érintett a GDPR 77. cikk (1) bekezdése alapján az Adatkezelő **adatkezelési eljárásával kapcsolatos panasszal a NAIH-hoz fordulhat.**

8.8.2. Az érintett a GDPR 79. cikk (1) bekezdése szerint az **Adatkezelő adatkezelési eljárásával kapcsolatos jogsértés miatt a lakóhelye vagy tartózkodási helye szerint illetékes törvényszékhez fordulhat.**

8.9. Az érintett jogainak érvényesítése az Adatkezelő adatkezelései során

8.9.1. Az Adatkezelő annak érdekében, hogy az érintettek érintetti jogaikkal élhessenek, jelen pontban rögzíti az érintetti joggyakorlással kapcsolatos jogokat, kötelezettségeket és eljárási szabályokat.

8.9.2. Az Adatkezelő minden esetben törekszik arra, hogy az érintettnek adott tájékoztatása minden esetben a GDPR által meghatározott szabályok teljesítése mellett is a lehetőségekhez mérten tömör, átlátható, érthető, könnyen hozzáférhető, világos és közérthető legyen.

8.9.3. Az Adatkezelő az érintettnek adott minden tájékoztatást főszabály szerint írásban tesz meg, ideértve az elektronikus utat is.

8.9.4. Amennyiben az érintett kéri a szóbeli tájékoztatást, úgy személyazonossága igazolását követően az Adatkezelő erre felhatalmazott munkatársa a tájékoztatást szóban is megadhatja.

8.9.5. Az Adatkezelő az érintett számára tájékoztatást csak és kizárólag abban az esetben nyújt, ha az Adatkezelő erre felhatalmazott munkatársa meggyőződött az érintett személyazonosságáról.

8.9.6. Az érintett személyazonosságáról való meggyőződésnek számít, ha az Adatkezelő erre felhatalmazott munkatársa előtt:

- az érintett személyazonosságát a hatályos magyar jog szerinti személyazonosság igazolására alkalmas okmány bemutatásával (így különösen, de nem kizárólagosan személyazonosító igazolvánnyal, útlevéllel, vezetői engedéllyel) igazolja,
- az érintett személyazonosságát az Európai Unió joga szerint személyazonosság igazolására alkalmas okmány bemutatásával igazolja,
- az érintett kérelme az Adatkezelő előtt már korábbi ügyből ismert, az érintetthez köthető e-mail címről érkezik,
- az érintett kérelme az Adatkezelő által biztosított, zárt, a megfelelő személyazonosítás megtörténte után használható csatornán érkezik.

8.9.8. Amennyiben a személyazonosság igazolása nem történik meg, az Adatkezelő az érintetti joggyakorlási kérelmet elutasítja és egyben tájékoztatja az érintettet, hogy a Szabályzatban írtak szerint miként gyakorolhatja érintetti jogait.

8.9.9. Az Adatkezelő az érintettet a kérelem beérkezésétől számított **egy hónapon belül tájékoztatja az érintetti joggyakorlásra vonatkozó kérelme kapcsán tett intézkedésről.**

8.9.10. Beérkezésnek az számít, ha az igényt az érintett:

- szóban személyesen az Adatkezelőnek személyazonosítást követően megteszi,
- az írásba foglalt igény az Adatkezelő elérhetőségére megérkezik.

8.9.11. **Az egy hónapos határidőt az Adatkezelő maximum további két hónappal meghosszabbítja, ha a kérelem összetettsége vagy az aktuálisan kezelt kérelmek száma azt indokolja.**

8.9.12. A határidő meghosszabbításáról a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül az Adatkezelő tájékoztatja az érintettet.

8.9.13. Amennyiben az Adatkezelő nem intézkedik az érintett kérelmére, úgy az érintett jogorvoslati jogával élhet az Adatkezelő ellen.

8.9.14. Az Adatkezelő a tájékoztatást és intézkedéseket díjmentesen végzi.

8.9.15. A tájékoztatás és intézkedés megtételéért az Adatkezelő képviselője vagy az általa kijelölt személy felelős.

9. ÉRDEKMÉRLEGELÉS ÉS AZ ÉRDEKMÉRLEGELÉSI TESZT ELVÉGZÉSE

9.1. A jogos érdekre, mint jogalapra való hivatkozás esetén a **7. sz. melléklet** felhasználásával érdekmérlegelési tesztet kell elvégezni.

9.2. Amennyiben az érdekmérlegelési teszt eredményeként a Társaság megállapítja, hogy az adatkezeléssel érintett jogos érdekekkel szemben elsőbbséget élveznek az érintett érdekei és alapvető jogai, a jogos érdek adatkezelési jogalapot nem alkalmazza.

9.4. Nem végez érdekmérlegelési tesztet a Társaság, amennyiben az adatkezelés során a személyes adatok különleges kategóriába tartozó személyes adatot kezel a Társaság, lévén ebben az esetben ez nem lehet az adatkezelés jogalapja.

10. AZ ADATKEZELŐ ADATVÉDELMI RENDSZERE

10.1. Általános rendelkezések

10.1.1. A Társaság vezető tisztségviselője a Társaság sajátosságainak figyelembevételével e Szabályzatban határozza meg az adatvédelmi előírások megvalósításához szükséges feladat- és hatásköröket.

10.1.2. A Társaság minden adatkezelése felett a felügyeletet a vezető tisztségviselő látja el.

10.1.3. A Szabályzatban előírtak betartatásáért a Társaság minden munkatársa felelős.

10.1.5. Mindenki köteles gondoskodni arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

10.2. Hatáskörök az adatvédelemmel kapcsolatosan

A vezető tisztségviselő

- felelős az érintettek 8.2. pontba foglalt jogainak gyakorlásához szükséges feltételek biztosításáért,

- felelős az Adatkezelő által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért,
- felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért,
- felügyeli az adatvédelmi tisztviselő tevékenységét,
- belső adatvédelmi vizsgálatot rendelhet el,
- kiadja az Adatkezelő adatvédelemmel kapcsolatos belső szabályzatait,
- különösen súlyos törvénytörés esetén a munkajogi szabályok alapján fegyelmi eljárást indít a személyes adatot jogszabálysértő módon kezelő személy ellen.

Az adatkezelésben érintett munkatársak

- kötelesek a Szabályzat előírásai szerint kezelni a személyes adatokat;
- felelősek feladatkörükben eljárva a személyes adatok a Szabályzat szerinti feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos és követhető dokumentálásáért;
- amennyiben szükséges, előzetesen egyeztetnek a felettesükkel és az adatvédelmi tisztviselővel a személyes adatok kezelését érintő ügyekben;
- a tudomásukra jutott adatkezeléssel kapcsolatos jogsértésekről haladéktalanul tájékoztatják a felettesüket.

11. ADATBIZTONSÁGI SZABÁLYOK

11.1. Az Adatkezelő, illetőleg tevékenységi körében az Adatkezelő által megbízott adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a GDPR, valamint a Szabályzat érvényre juttatásához szükségesek.

11.2. Az Adatkezelő az adatbiztonsági folyamatait úgy alakítja ki, hogy azok a személyes adatokat megvédjék a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

11.3. Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit a GDPR, valamint az adatkezelésre vonatkozó külön törvények keretei között az Adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az Adatkezelő felel.

11.4. Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az Adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az Adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

11.5. A papíralapon kezelt személyes adatok biztonsága érdekében az Adatkezelő az alábbi intézkedéseket alkalmazza:

- az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatók;
- a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el;
- a személyes adatokat tartalmazó iratokhoz csak az illetékesek férhetnek hozzá;
- az Adatkezelő adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;
- az Adatkezelő adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;

- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza az Adatkezelő.

11.6. A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében az Adatkezelő az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- az adatkezelés során használt számítógépek az Adatkezelő tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír;
- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal – legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről az Adatkezelő rendszeresen, illetve indokolt esetben gondoskodik;
- az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
- a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez, a mentés az összes számítógép teljes adatállományára vonatkozik és mágneses adathordozóra történik;
- a napi rendszerességgel lementett adatokat tároló mágneses adathordozó az erre a célra kialakított páncéldobozban, tűzbiztos helyen és módon tárolt;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;
- a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését (pl.: A vendégek és a mobiltelefonok nem érik el a belső hálózatot, vendég WiFi hálózatra csatlakoznak.)

11.7. Jogosultságkezelés

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetők legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészsége nagymértékben hozzásegíti az Adatkezelőt a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.

A személyes adatok biztonsága érdekében az Adatkezelő az alábbi jogosultságkezelési előírásokat alkalmazza:

o Alapelvek

- Új jogosultság beállítását, illetve jogosultság megváltoztatását a jogosultság birtokosának felhatalmazása alapján az informatikus végzi.
- A jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani.
- El kell kerülni, hogy teljes hozzáférést, illetve adminisztrátori jogosultságokat kapjanak más munkát végző, illetve a jogosultság birtoklására igényt nem tartó személyek.
- Adminisztrátori jogosultsággal rendelkező, nevesített felhasználót kell alkalmazni a rendszer adminisztrálása érdekében minden esetben, ahol ez lehetséges. A nem nevesített rendszergazdai jelszavakat zárt borítékban, felbontást gátló módon, aláírva kell tárolni. Ezek használatát az Adatkezelő vezető tisztviselője vagy akadályoztatása esetén a helyettesítési rend szerinti helyettese engedélyezheti. A nem nevesített felhasználói jogosultságok használatát indokolni és dokumentálni kell.
- Külső – karbantartó vagy fejlesztő – cég alkalmazottja folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet.

11.7.1. Jogosultságkezelési folyamat

A jogosultság birtokosának munka- vagy egyéb jogviszonya megszűnése esetén a közvetlen felettesének igazolható módon intézkednie kell a jogosultságainak törlése érdekében.

Az informatikai rendszerben a kilépő felhasználók profiljait fel kell függeszteni, használaton kívül kell helyezni. A felhasználói fiókok törlése a rendszerek ellenőrzését követően történhet meg, ha a törlés nem okoz adatvesztést.

11.8. Oktatás és tréningrendszer

Kiemelt területként kell kezelni a munkatársak kapcsán az adatvédelmi és adatbiztonsági tudatosság növelését, melyet rendszeres időközönként tartott oktatásokkal lehet elősegíteni.

A Társaság dolgozóinak általános adatvédelmi-információbiztonsági tréningje évente (kapcsolható más rendszeres képzésekhez, tréningekhez, mint pl.: tűz- és munkavédelem) egy óra időtartamban történik.

12. ADATVÉDELMI INCIDENS

12.1. Adatvédelmi incidens észlelése és jelentése

12.1.1. A Társaság minden munkatársa köteles a tudomására jutott adatvédelmi incidenst haladéktalanul jelenteni a vezető tisztségviselőnek vagy az általa kijelölt személynek.

12.1.2. Az adatvédelmi incidenst írásban kell jelenteni a mellékletben található formanyomtatvány kitöltésével (**8. sz. melléklet**). Amennyiben az írásbeli jelentés akadályba ütközik, akkor szóban kell ezt megtennie. A vezető tisztségviselő vagy általa kijelölt személy ezen szóbeli jelentést írásban rögzíti. Az akadály megszűnését követően az adatvédelmi incidenst észlelő vagy jelentő személy köteles a bejelentést haladéktalanul írásban is megerősíteni.

12.1.3. Amennyiben az adatvédelmi incidens érinti a Társaság informatikai rendszerét is, akkor a kivizsgálásába be kell vonni az informatikai feladatok ellátásáért felelős személyt is.

12.1.4. A bejelentés érkezését követően a vezető tisztségviselő haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését, melyben külön hangsúlyt fektet az adatvédelmi incidens várható hatásainak vizsgálatára és a következményeinek enyhítése érdekében szükséges intézkedések kidolgozására/megtételére.

12.2.5. A vizsgálatot úgy kell befejezni, hogy amennyiben az incidens valószínűsíthetően kockázattal jár az érintettekre nézve, a Hatósági bejelentést az incidens tudomásra jutásától számított 72 órán belül meg kell tenni.

12.2. Adatvédelmi incidens kivizsgálása

12.2.1. Az adatvédelemért felelős személy megvizsgálja a jelentést és amennyiben szükséges, a bejelentőtől, illetve az érintett szervezeti egységek vezetőitől, munkatársaitól további adatokat kér az incidensre vonatkozóan.

12.2.2. Az adatvédelemért felelős személy az alábbi információkat (amennyiben azok a jelentésből nem derülnek ki) lehetőségéhez mérten köteles felderíteni:

- az adatvédelmi incidens bekövetkezésének időpontja és helye,
- az adatvédelmi incidens által érintett adatok köre,
- az adatvédelmi incidenssel érintett személyek köre és száma.

12.2.3. Ezen adatokból az adatvédelemért felelős személy összegzést készít az adatvédelmi incidens várható hatásairól és cselekvési tervet készít a következményeinek enyhítése érdekében, az érintett szakterületek szakmai véleményei és javaslatai figyelembevételével.

12.2.4. A vizsgálatot legkésőbb az adatvédelemért felelős személyhez történő érkezésétől számított 48 órán belül be kell fejezni. A vizsgálat eredményéről és a tervezett további feladatokról az adatvédelemért felelős személy tájékoztatja a vezető tisztségviselőt.

12.3. Adatvédelmi incidens értékelése

12.3.1. A Társaság az adatvédelmi incidenseket három kategóriába sorolja:

- 1. kategória: valószínűsíthetően kockázattal nem járó incidens (nem kell NAIH-nak jelenteni)
- 2. kategória: valószínűsíthetően alacsony kockázattal járó incidens (NAIH-nak be kell jelenteni)
- 3. kategória: valószínűsíthetően magas kockázattal járó incidens.(az érintettet is tájékoztatni kell)

12.3.2. A Társaság az adatvédelmi incidenst az alábbi szempontok szerint értékeli:

- az incidens típusa (bizalmassági, integritási vagy elérhetőségi),
- a személyes adatok jellege (személyes adat / különleges kategória),
- a személyes adatok száma,
- az érintett személyek száma,
- az érintett természetes személyek kategóriái,
- az érintett természetes személyek azonosíthatósága,
- a természetes személyre nézve fennálló következmények valószínűsége és súlyossága;
- az érintett adatkezelés jogalapja.

12.3.3. A Társaság az incidens értékelése során az alábbi konkrét szempontok alapján értékeli:

- az incidensben érintett adatok között találhatóak a személyes adatok különleges kategóriáiba eső adatok,
- az incidensben érintett személyes adatok száma
- az incidensben érintett természetes személyek között találhatóak 16. életévüket be nem töltött természetes személyek,
- az incidensben érintett természetes személyek száma....
- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre (így különösen lakcím, telefonszám, e-mail cím)
- az incidensben érintett adatkezelés jogalapja 7.2.4. szerinti jogalap,
- az incidensben érintett adatkezelés jogalapja 7.2.5. szerinti jogalap,
- az incidensben érintett adatkezelés jogalapja 7.2.6. szerinti jogalap,
- a személyes adatok alkalmasak az érintett természetes személy személyazonosságának ellopására vagy a személyazonosságával való visszaélésre,
- az incidensben érintett személyes adatok alkalmasak arra, hogy pénzügyi veszteséget illetve nem vagyoni kárt okozzanak az érintettjüknek.

12.3.4. Az incidenst a Társaság „1. kategória: valószínűsíthetően kockázattal nem járó incidens”-nek minősíti, ha:

- a 12.3.3. pontban felsorolt feltételek közül legfeljebb kettő áll fenn és
- a Társaság képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

12.3.5. Az incidenst a Társaság „2. kategória: valószínűsíthetően alacsony kockázattal járó incidens”-nek minősíti, ha:

- a 12.3.3. pontban felsorolt feltételek közül egy áll fenn és

- a Társaság nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

12.3.6. Az incidens a Társaság „3. kategória: valószínűsíthetően magas kockázattal járó incidens”-nek minősíti, ha:

- a 12.3.3. pontban felsorolt feltételek közül legalább kettő áll fenn és
- a Társaság nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

12.4. Adatvédelmi incidens bejelentése a NAIH-nak

12.4.1. Amennyiben a Társaság az incidenst a 2. kategóriába vagy a 3. kategóriába tartozónak minősíti, a vezető tisztségviselő legkésőbb 72 órával azután, hogy az adatvédelmi incidens a Társaság tudomására jutott, az incidenst bejelenti a NAIH-nak, a www.naih.hu oldalon elérhető elektronikus bejelentő rendszer vagy a szintén ezen oldalról letölthető formanyomtatvány segítségével.

12.5. Az érintettek tájékoztatása az adatvédelmi incidensről

12.5.1. Amennyiben az adatvédelmi incidens veszélyességének súlyossága valószínűsíthetően magas kockázattal jár az érintett személyek jogaira nézve, az Adatkezelő a kockázati értékelés elvégzését követően azonnal tájékoztatja az adatvédelmi incidensben érintetteket.

12.5.2. Az érintettek írásban elektronikus vagy postai úton kell tájékoztatni, amely kizárólag akkor mellőzhető, ha az érintett elérhetősége ismeretlen.

12.5.3. Az érintetteket úgy kell tájékoztatni minden esetben, hogy annak ténye, tartalma és a tájékoztatott érintetti kör bizonyítható legyen.

12.6. Helyesbítő-megelőző intézkedések bevezetése

12.6.1. A 12.2. pont szerinti vizsgálat eredménye alapján a Társaság szükség szerint helyesbítő és/vagy megelőző intézkedések bevezetéséről gondoskodik.

12.7. Az adatvédelmi incidens nyilvántartása

12.7.1. Az adatvédelmi incidensről a Társaság nyilvántartást vezet a Szabályzat 9. sz. *melléklete* szerinti nyilvántartó-minta alkalmazásával.

13. ADATVÉDELMI OKTATÁS

13.1. Az Adatkezelő évente legalább egy alkalommal oktatást szervez az adatvédelmi tudatosság emelése érdekében, amelyen kötelesek részt venni az Adatkezelő kijelölt munkatársai. Az adatvédelmi oktatásnak legalább az alábbi témákra kiterjed:

- az előző oktatás óta eltelt időszak tapasztalatai az adatvédelem területén
- amennyiben az előző oktatás óta módosult a Szabályzat, a módosítással kapcsolatos legfontosabb tudnivalók,
- az esetlegesen megtörtént adatvédelmi incidens bemutatása, értékelése, a helyesbítő-megelőző intézkedések ismertetése,
- az adatvédelem területén történt általános változások, jogszabály módosítások, Magyarországon és az Európai Unióban, különös tekintettel a hatóságok bírságolási gyakorlatára.

13.2. Az Adatkezelőnél rendkívüli oktatást kell tartani – amennyiben az indokolt – az alábbi esetekben:

- adatvédelmi incidens megtörténte,
- marasztalással záruló NAIH-eljárás lefolytatása az Adatkezelővel szemben,
- adatvédelmi bírság kiszabása bármely, hasonló vagy azonos feladatot ellátó jogi személy ellen, ha eltérő gyakorlatot igényel az Adatkezelő adatvédelmi rendszerében.

14. ADATVÉDELMI NYILVÁNTARTÁS

14.1. Az Adatkezelő minden általa végzett adatkezelési tevékenységről nyilvántartást vezet.

14.2. A 14.1. szerinti nyilvántartást az Adatkezelő elektronikusan vezeti.

14.3. A 14.1. szerinti nyilvántartás a következő információkat tartalmazza:

- az Adatkezelő neve és elérhetősége,
- az Adatkezelő adatvédelmi tisztviselőjének a neve és elérhetősége;
- az adatbiztonságra vonatkozó technikai és szervezési intézkedések általános leírása jelen Szabályzat vagy egyéb, technikai és szervezési intézkedéseket tartalmazó egyéb belső szabályzat vonatkozó pontjára való utalással;
- adatkezelésként:
 - o adatkezelés céljai;
 - o az érintettek kategóriái
 - o a személyes adatok kategóriái
 - o olyan címzettek kategóriái, akikkel a személyes adatokat az Adatkezelő közli vagy várhatóan közölni fogja,
 - o a különböző adatkategóriák törlésére előírányzott határidők, ha lehetséges,
 - o az adatvédelmi folyamatleírás.

14.4. Az adatkezelési nyilvántartást az adatvédelemért felelős személy tartja naprakészen és módosítja szükség esetén.

14.5. Az adatkezelési nyilvántartás naprakészsége biztosítása érdekében a munkatársak, az általuk végzett adatkezelési folyamatban bekövetkező változásokat (módosítás, megszűnés stb.) vagy általuk tervezett új adatkezelési műveletet a tervezett változás vagy a bevezetés előtt legkésőbb 5 munkanappal kötelesek írásban bejelenteni az adatvédelemért felelős személynek.

14.6. Az adatvédelmi tisztviselő a 14.5. szerinti bejelentés alapján gondoskodik:

- az adatkezelés 14. pont szerinti nyilvántartásban való átvezetéséről,
- szükség esetén a 16. pontban foglalt hatásvizsgálat lefolytatásáról.

15. ADATFELDOLGOZÓKRA VONATKOZÓ SZABÁLYOK

15.1. Az Adatkezelő csak és kizárólag olyan adatfeldolgozót vesz igénybe bármely adatkezelési folyamata során, aki vagy amely megfelelő garanciákat nyújt az adatkezelés GDPR követelményeinek való megfeleléséről és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtásáról.

15.2. Az Adatkezelő minden adatfeldolgozójával adatfeldolgozói írásbeli szerződést köt, amely legalább az alábbi kérdéseket tisztázza:

- az adatkezelés, amelybe az Adatkezelő az adatfeldolgozót bevonta,
- az adatfeldolgozó által ellátott adatkezelői tevékenység
- az adatfeldolgozás időtartamát, jellegét és célját,
- az adatfeldolgozásra átadott adatok típusa,
- az adatfeldolgozással érintettek kategóriái,

- az adatkezelő jogai és kötelezettségei,
- az adatfeldolgozó jogai és kötelezettségei.

15.3. Az Adatkezelő csak olyan adatfeldolgozóval köt szerződést adatfeldolgozói feladatra, aki a 15.2. pont szerinti szerződésben vállalja, hogy:

- a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli,
- az általa személyes adatok feldolgozásában résztvevő személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak,
- biztosítja a GDPR 32. cikk szerinti adatbiztonsági szabályokat,
- adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vesz igénybe,
- az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az Adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett 8. pontban foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében,
- adatvédelmi incidens esetén az incidens tudomására jutása pillanatában azonnal értesíti az Adatkezelőt és együttműködik az adatvédelmi incidens 12. pont szerinti kezelésében,
- az adatfeldolgozási szolgáltatásának nyújtásának befejezését követően az Adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az Adatkezelőnek, valamint a személyes adatokról készült másolatokat ezzel egyidőben megsemmisíti vagy törli,
- lehetővé teszi és elősegíti, hogy az Adatkezelő ellenőrizhesse az adatvédelmi szabályok megvalósulását,
- vezeti a GDPR 30. cikk (2) bekezdése szerinti adatfeldolgozói nyilvántartást.

15.4. Az adatfeldolgozói szerződés minta a Szabályzat **10. sz. melléklete**.

16. ADATVÉDELMI HATÁSVIZSGÁLAT

16.1. Az adatvédelmi hatásvizsgálat-köteles adatkezelések

16.1.1. Ha a Társaság új adatkezelést kíván rendszerébe bevezetni adatvédelmi hatásvizsgálatot kell lefolytatni, különösen, ha az alábbi feltételek legalább egyike fennáll:

- az adatkezelés természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek,
- személyes adatok különleges kategóriái, vagy bűnügyi személyes adatok nagy számban történő kezelése történik,
- az adatkezelés nyilvános helyek nagymértékű, módszeres megfigyelését valósítja meg,
- a 16.1.2. pontba sorolt feltételek közül az adatkezelésre legalább három szempont igaz.

16.1.2. A Társaság a bevezetendő új adatkezelés hatásvizsgálat-kötelességét az alábbi szempontok alapján ítéli meg:

- az adatkezelésben érintett személyes adatok nagy száma,
- az adatkezelésben érintett természetes személyek között találhatók 16. életévüket be nem töltött természetes személyek,
- az adatkezelésben érintett természetes személyek nagy száma,
- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre (így különösen lakcím, telefonszám, e-mail cím)
- az adatkezelés jogalapja a 7.2.4. szerinti jogalap,
- az adatkezelés jogalapja a 7.2.5. szerinti jogalap,
- az adatkezelés jogalapja a 7.2.6. szerinti jogalap,
- az adatkezelésben érintett személyes adatok alkalmasak az érintett természetes személy személyazonosságának ellopására vagy a személyazonosságával való visszaélésre,

- az adatkezelésben érintett személyes adatok alkalmasak arra, hogy pénzügyi veszteséget vagy nem vagyoni kárt okozzanak az érintettjüknek.

16.2.4. Az adatvédelmi hatásvizsgálat elvégzéséhez használatos segédanyag jelen szabályzat **11. sz. melléklete**.

17. ÁLTALÁNOS ADATVÉDELMI ALAPVETÉSEK

17.1. Személyazonosító igazolványok kezelése

17.1.1. Az adatkezelés alapelvei, a szükségesség és a célhoz kötöttség elvének való megfelelés érdekében az Adatkezelő nem készít fénymásolatot személyazonosító igazolványokról. Az arcképes hatósági igazolvány értelemszerűen csak akkor rendelkezik bizonyító erővel, ha annak alapján az Adatkezelő megbizonyosodhat arról, hogy az igazolványon szereplő személy képmása és az igazolványt felmutató személy megegyeznek.

17.1.2. Az Adatkezelő fenntartja magának a jogot, hogy az okmány érvényességét a <https://www.nyilvantarto.hu/ugyseged/OkmanyErvenyessegLekerdezes.xhtml> oldalon ellenőrizze.

17.2. Az érintettek értesítése elektronikus kapcsolattartás során

17.2.1. Abban az esetben, ha az Adatkezelő bármely munkatársa az érintett számára elektronikus levelet küld, az érintett elektronikus levélcímét köteles a küldés során úgy megjelölni, hogy az az elektronikus levél egyetlen címzettje számára se legyen látható. Ezt az Adatkezelő munkatársai elsősorban „titkos másolat”-tal történő címezéssel kötelesek megtenni, de az Adatkezelő kidolgozhat olyan üzenetküldő rendszert, amely alapvető beállításként, további emberi beavatkozás nélkül automatikusan így küldi meg az információt az érintettek számára.

17.2.2. A 17.2.1. pontban foglalt szabály érvényes többek között, de nem kizárólagosan az ügyintézés során használt elektronikus kapcsolattartásra.

17.3. A személyes adatok megsemmisítése

17.3.1. Abban az esetben, ha az Adatkezelő az általa kezelt személyes adatokat az adatkezelés szabályai alapján a továbbiakban nem kezelheti, köteles a személyes adatokat tartalmazó adathordozót megsemmisíteni, a megsemmisítés tényéről pedig jelen Szabályzat **12. sz. melléklete** szerinti megsemmisítési jegyzőkönyvet felvenni.

17.3.2. A megsemmisítési jegyzőkönyv tartalmazza az alábbiakat:

- az adatmegsemmisítésért felelős munkavállaló azonosító adatait,
- a megsemmisítést engedélyező személyazonosító adatait,
- a megsemmisítés tárgya,
- az adathordozók száma legalább megközelítőlegesen,
- a megsemmisítéssel érintett adatkezelési folyamat megnevezése,
- az adatmegsemmisítés módja,
- a megsemmisítés időpont, helyszíne,
- a megsemmisítést ténylegesen lefolytató, illetve azon jelenlévők neve és aláírása (minimum három fő).

17.3.3. Az Adatkezelő az Adatmegsemmisítési jegyzőkönyvet iratkezelési szabályzata szerint tárolja.

18. NYILVÁNTARTÁSOK

18.1. Az Adatkezelő az adatkezelési folyamataihoz az alábbi nyilvántartásokat, jegyzőkönyveket, nyilatkozatokat, köteles vezetni:

- Adatkezelési folyamatok nyilvántartása.

19. ZÁRÓ RENDELKEZÉSEK

A Szabályzat személyi, tárgyi és időbeli hatályára a 4. pontban írt rendelkezések az irányadók.