VERESEGYHÁZI
VÁROSGAZDA KFT.

ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZAT

Tartalomjegyzék

I. Az adatvédelmi és adatkezelési szabályzat alkalmazása

A szervezet megnevezése:	**Veresegyházi Városgazda Korlátolt Felelősségű Társaság (továbbiakban: Társaság vagy Adatkezelő)**
A szervezet székhelye:	2112 Veresegyház, Sport u. 4.
A szabályzat tartalmáért felelős személy:	Kisák Péter ügyvezető
A szabályzat hatályba lépésének dátuma:	2024. január 1.
A szabályzat felülvizsgálatának időpontja:	2025. szeptember 1.

Ez a szabályzat a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg. A szabályzatban foglaltakat kell alkalmazni a konkrét adatkezelési tevékenységek során, valamint az adatkezelést szabályozó utasítások és tájékoztatások kiadásakor.

Feladatai közé tartozik többek között egyes önkormányzati kötelező és önként vállalt közfeladatok (karbantartási munkálatok, gyermekétkeztetési tevékenység, közterületek és zöld területek fenntartása, egyéb városüzemeltetési feladatok ellátása és egyes városi rendezvények kiszolgálása. .

Adatkezelő alapítója Versegyház Város Önkormányzata. Adatvédelmi tisztviselő kijelölése a GDPR 37. cikk (3) bekezdése szerint az Intézménynél kötelező, mivel az adatkezelő/adatfeldolgozó közfeladatot ellátó szerv.

Adatvédelmi tisztviselő neve: Dr. Csapó Csilla
Elérhetőségei:
Székhelye: 8000 Székesfehérvár, Zsolt u. 51.
E-mail címe: cscsapo@gmail.com
Mobil: 06 (30) 6413314

1. A szabályzat hatálya

E szabályzat visszavonásig érvényes.

A Szabályzat személyi hatálya kiterjed
a) az Adatkezelő valamennyi alkalmazottjára, valamint az eseti vagy tartós jelleggel munkavégzés céljából bármilyen jogviszony alapján foglalkoztatott természetes személyre,
b) az Adatkezelő vezető tisztségviselőire,
c) az Adatkezelő által igénybe vett adatfeldolgozókra, valamint azok alkalmazottaira,
d) valamennyi, az Adatkezelővel üzleti/partneri viszonyban álló személyekre,
e) a fentieken kívül mindazon természetes személyekre, akik a Társasággal (Adatkezelővel) bármilyen jogviszonyban állnak, vagy akiket a Társaság adatkezelése bármilyen módon érint.

A Szabályzat tárgyi hatálya kiterjed az Adatkezelő által kezelt valamennyi személyes adatra.

Az adatkezelési szabályzat az Adatkezelő ügyvezetője által meghatározott időponttal lép hatályba, és határozatlan időre szól.

Az Adatvédelmi és Adatkezelési Szabályzatot a jóváhagyás dátumával fennálló és azt követő dátummal létesített jogviszony esetén a foglalkoztatott köteles tudomásul venni, valamint a Munka

Az Adatvédelmi és Adatkezelési Szabályzatot a jóváhagyás dátumával fennálló és azt követő dátummal létesített jogviszony esetén a foglalkoztatott köteles tudomásul venni, valamint a Munka Törvénykönyve (továbbiakban: Mt.) vagy megbízási jogviszony esetében a Polgári Törvénykönyv szabályai alapján eljárni. A foglalkoztatottak esetében az Mt. 46.§ (1) bekezdése szerint készült írásos tájékoztatóban a foglalkoztatottak figyelmét az adatvédelemmel kapcsolatos kötelezettségeikre fel kell hívni.

2. A szabályzat célja

E szabályzat célja, hogy harmonizálja az adatkezelési tevékenységek tekintetében az Adatkezelő egyéb belső szabályzatainak előírásait a természetes személyek alapvető jogainak és szabadságainak védelme érdekében, valamint biztosítsa a személyes adatok megfelelő kezelését. A szervezet tevékenysége során teljes mértékben meg kíván felelni a személyes adatok kezelésére vonatkozó jogszabályi előírásoknak, különösen az Európai Parlament és a Tanács (EU) 2016/679 rendeletében (továbbiakban: GDPR) foglaltaknak.

A szabályzat kiadásának fontos célja továbbá, hogy megismerésével és betartásával az Adatkezelő által foglalkoztatottak képesek legyenek a természetes személyek adatai kezelését jogszerűen végezni.

3. Lényeges fogalmak, meghatározások

- **GDPR** (General Data Protection Regulation) az Európai Unió új Adatvédelmi Rendelete, Általános Adatvédelmi Rendelet (32016R0679 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 irányelv hatályon kívül helyezéséről)

- **Info tv:** az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

- **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;

- **érintett:** azonosított vagy azonosítható természetes személy, akinek adatát adatkezelő bármilyen okból kezeli; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

- **adatkezelés**: 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;

- **adatfeldolgozó**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

- **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;

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

- **az adatkezelés korlátozása**: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

- **nyilvántartási rendszer**: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

- **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;

4. Az adatkezelés irányelvei

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet.

A személyes adatok kezelésének célja megfelelő és releváns legyen, és csak a szükséges mértékű lehet.

A személyes adatoknak pontosnak és naprakésznek kell lenniük. A pontatlan személyes adatokat haladéktalanul törölni kell.

A személyes adatok tárolásának olyan formában kell történnie, hogy az érintettek azonosítását csak szükséges ideig tegye lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, ha a tárolás közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történik.

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell.

Az adatkezelést végző foglalkoztatottak fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartoznak a személyes adatok jogszerű kezeléséért. Amennyiben a foglalkoztatott tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

Az Adatkezelő ügyvezetője határozza meg a foglalkoztatottak adatkezeléssel kapcsolatos feladatait.

5. Személyes adatok kezelése, az adatkezelés jogszerűsége

Az adatkezelésre Adatkezelőnél az alábbi esetekben kerülhet sor:

- Az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez. Az érintett hozzájárulásának minősül 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. Hozzájárulásnak minősül az is, ha valamely felhasználó az elektronikus szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, vagy olyan nyilatkozatot, illetve cselekedet tesz, amely az adott összefüggésben az érintett személy hozzájárulását személyes adatainak kezeléséhez egyértelműen jelzi. (GDPR 6. cikk (1) bek. a) pont)

- 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) bek. b) pont)

- Az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges; (GDPR 6. cikk (1) bek. c) pont)

- Az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges. (GDPR 6. cikk (1) bek. d) pont)

- Az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé. (GDPR 6. cikk (1) bek. f) pont)

Azon esetekben, amikor az Adatkezelő – kivételesen - a személyes adatok különleges kategóriáit is kezeli (pl. a foglalkoztatottak egészségügyi alkalmasságára vonatkozó adatai, baleset kivizsgálása, szociális juttatások feltételeinek vizsgálata, egészségügyi járványhelyzet kezelése, stb) a fenti jogalapok egyikének a teljesülése esetén az alábbi feltételek valamelyikének teljesülése is szükséges:

- Az érintett kifejezett hozzájárulását adta különleges személyes adatai egy vagy több konkrét célból történő kezeléséhez. (GDPR 9. cikk (2) bek. a) pont)
- 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. (GDPR 9. cikk (2) bek. b) pont)
- 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; (GDPR 9. cikk (2) bek. c) pont)
- Az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett

jogszerű tevékenysége keretében történik a GDPR-ban meghatározott feltételekkel. (GDPR 9. cikk (2) bek. d) pont)
- Az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott; (GDPR 9. cikk (2) bek. e) pont)
- Az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges. (GDPR 9. cikk (2) bek. f) pont)
- Az adatkezelés uniós jog vagy tagállami jog alapján jelentős közérdek miatt szükséges. (GDPR 9. cikk (2) bek. g) pont)
- 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. (GDPR 9. cikk (2) bek. h) pont)
- Az adatkezelés a népegészségügy területét érintő közérdekből szükséges. (GDPR 9. cikk (2) bek. i) pont)
- Az adatkezelés közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges. (GDPR 9. cikk (2) bek. j) pont)

6. Az érintett személy hozzájárulása, a hozzájárulás megadásának feltételei

Amennyiben az adatkezelés hozzájáruláson alapul, az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.
Az érintett hozzájárulását önkéntesen adja, azaz szabad választási lehetőséggel kell rendelkezzen a hozzájárulás megadásakor. Ezért alá- és fölérendeltségi viszonyban (pl. munkaviszony, közszolgálati jogviszonyban) és az ahhoz kapcsolódó adatkezelésekkor, vagy ha az adatkezelés szerződés teljesítéséhez szükséges az adatkezelés jogalapja nem lehet az érintett hozzájárulása.
A tisztességes és átlátható adatkezelés elve megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól az adatkezelést megelőzően.
A hozzájárulásnak kellően konkrétnak kell lennie és megfelelő tájékoztatáson kell alapulnia, ezért az érintettet az adatkezelő köteles megfelelő információkkal ellátni, amely tájékoztatót az Adatkezelő honlapján közzé kell tenni. Az információkat szabványosított ikonokkal is ki lehet egészíteni annak érdekében, hogy az érintett a tervezett adatkezelésről jól látható, könnyen érthető és jól olvasható formában általános tájékoztatást kapjon.

Abban az esetben, ha az adott jogviszonyra az aktuális tájékoztató szövege nem alkalmazható, az adatkezelő az érintettet az alábbiakról tájékoztatja:
- az Adatkezelő kiléte és elérhetőségei;
- a személyes adatok tervezett kezelésének célja, valamint az, hogy az adatkezelés az érintett hozzájárulásán alapul
- azon természetes vagy jogi személyek kilétéről, akivel vagy amellyel a személyes adatot közölni fogják.
- azon jogokat, amelyek az érintettet megilletik, különösen az adatkezeléshez adott hozzájárulásának visszavonására vonatkozó jogait.

Ha az érintett a hozzájárulását olyan nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell közölni.

Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás

megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

7. Az érintett jogai

7.1. Átlátható tájékoztatás

Az érintettnek joga, hogy az őt érintő adatkezelésekről tömör, átlátható, érthető és könnyen hozzáférhető formában világosan és közérthetően megfogalmazva tájékoztatást kapjon. Ezért az Adatkezelő minden adatkezeléssel is foglalkozó dolgozójának kellő információval kell rendelkeznie, hogy – amennyiben írásbeli tájékoztatás nem elérhető, vagy az nem ad az adott kérdésre választ, vagy az érintettnek további kérdései lennének – az adatkezelésről kielégítő információt nyújtson. Amennyiben a kérdés azonnal nem válaszolható meg vagy a kérdés elektronikus úton vagy írásban érkezett, úgy az Adatkezelő 1 hónapon belül tájékoztatja az érintettet olyan formában, ahogy az érintett a kérdést feltette, kivéve, ha ezt az érintett más módon kéri.
A tájékoztatás díjmentes, ezért díj nem számítható fel.
Ha az Adatkezelő az érintettre vonatkozó személyes adatokat az érintettől gyűjti, akkor legkésőbb az adatok megszerzésének időpontjában tájékoztatja a foglalkoztatottat/az ügyfelet (összességében az érintettet) főszabályként a jelen szabályzat mellékletét képező adatkezelési tájékoztató megismerhetővé tételével.
Ha az Adatkezelő az érintettre vonatkozó személyes adatokat nem az érintettől gyűjti, akkor az adatok megszerzését követő 1 hónapon belül tájékoztatja az ügyfelet a fenti módon.

7.2. Hozzáférés joga

Az érintett jogosult arra, hogy az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz hozzáférést kapjon. Az Adatkezelő köteles kérelem esetén az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátani. Az érintett által kért további másolatokért az Adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel, amely magában foglalja a másolás díját, valamint a postaköltséget. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat elektronikus úton (e-mail) kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

7.3. Helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Pl. névváltozás, lakcímváltozás bejelentése esetén.

7.4. Törléshez való jog

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

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat az Adatkezelő kezelte
- az érintett visszavonja az adatok kezelésére vonatkozó hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- igazolható, hogy az Adatkezelő a személyes adatokat jogellenesen kezeli
- a személyes adatok törlését jogszabály előírja

Ha az Adatkezelő bármilyen módon – pl. internetes honlapján - nyilvánosságra hozta a személyes adatot, és azt a fentiek értelmében törölni köteles, az Adatkezelő a lehetőségeihez képest megteszi az észszerűen elvárható lépéseket - ideértve technikai intézkedéseket annak érdekében, hogy tájékoztassa az adatokat kezelő további adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

7.5. Adatkezelés korlátozásához való jog

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

- 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;
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő adatkezelést igazoló jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében vagy fontos közérdekéből lehet kezelni.
Amennyiben az Adatkezelő a korlátozást feloldja, mivel annak okai már nem állnak fenn, az érintettet az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

7.6. Adathordozhatósághoz való jog

Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat közismert módon tagolt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

7.7. Tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak az Adatkezelő jogos érdekén alapuló adatkezelés ellen. Ebben az esetben az Adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha 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.

7.8. Az adatkezeléssel kapcsolatos jogérvényesítési lehetőség

Nemzeti Adatvédelmi és Információszabadság Hatóság
Postacím: 1363 Budapest, Pf.: 9.
Cím: 1055 Budapest, Falk Miksa utca 9-11.
Telefon: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat (kukac) naih.hu

URL https://naih.hu
Koordináták: É 47°30'36.8"; K 19°02'54.2"

Az érintett a jogainak megsértése esetén az Adatkezelővel szemben bírósághoz is fordulhat. A bíróság az ügyben soron kívül jár el. A pert az érintett - választása szerint - a lakóhelye vagy tartózkodási helye szerint illetékes törvényszék előtt is megindíthatja.

Az érintetti jogok gyakorlásának egyes feltételeit és pontosabb szabályait a GDPR részletesen tartalmazza.

8. Az adatkezelő feladatai

Az Adatkezelő megfelelő és hatékony intézkedéseket hajt végre a személyes adatok biztonságos és szabályszerű kezelése érdekében, valamint azért, hogy képes legyen igazolni azt, hogy az adatkezelési tevékenységek a hatályos jogszabályoknak megfelelnek.

Az adatkezelés során alkalmazandó szabályokat az Adatkezelő az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével, a GDPR szabályai szerint alakította ki.

8.1. Jogszerűség, tisztességes eljárás és átláthatóság biztosítása

Az Adatkezelő minden dolgozójának és munkatársának kötelessége az adatvédelem szabályainak, különösen jelen szabályzatnak a megismerése. Ezért az Adatkezelő által foglalkoztatottak évente oktatáson vesznek részt, melynek szervezése az ügyvezető feladata. Az adatkezelést végző foglalkoztatott munkahelyi vezetője az oktatáson való rendszeres részvételt köteles figyelemmel kísérni.
Az Adatkezelő a személyes adatok kezeléséről készített tájékoztatókat minden érintett részére elérhetővé teszi abból a célból, hogy megismertesse az érintetteket személyes adataik kezelésének céljáról, módjáról, körülményeiről, az adatkezelés következményeiről és garanciáiról.
A tájékoztatást minden esetben világosan és közérthetően kell az érintett felé megfogalmazni.
Az adatkezelés folyamán az emberi méltóság tiszteletben tartásával kell eljárni.
Minden adatkezelést és adatkezeléshez fűződő cselekményt úgy kell dokumentálni – függetlenül, hogy az papíralapon, vagy elektronikusan történik -, hogy ezen cselekmények utólag is rekonstruálhatók legyenek az adatok megőrzésének határidején belül.

8.2. Célhoz kötöttség megvalósítása

Minden, az Adatkezelő tevékenységébe tartozó új folyamatot, mely személyes adatok kezelésével is jár, a tevékenység megkezdését megelőzően adatvédelmi szempontból is gondosan meg kell vizsgálni, az adatkezelés folyamatát meg kell tervezni. Ezen feladat az ügyvezető (vagy az általa kijelölt személy) felelőssége. Ezzel összefüggésben az ügyvezető felelőssége, hogy az új tevékenység/feladat ellátását megelőzően a folyamatokba az általa kijelölt felelős személyt is bevonja.
A vizsgálatot oly módon kell végezni, hogy az utólag is dokumentálható módon igazolja, hogy az Adatkezelő az adatkezelés célját figyelembe véve felmérte a feladat ellátáshoz szükséges adatkört és az adatkezelés érintettre gyakorolt hatásait (hatásvizsgálat). A cél nélküli adatkezelés tilos!
Az adatkezelés céljának meghatározása, soha nem lehet általános jellegű vagy valótlan.

8.3. Adattakarékosság hatékony megvalósítása

Az adatkezelés megkezdése előtt az Adatkezelőnek meg kell vizsgálnia, hogy szükséges-e egyáltalán személyes adatokat kezelni az üzleti cél megvalósításához.

Kizárólag annyi és olyan személyes adat kezelhető, ami szükséges és egyben elégséges az adatkezelés céljának eléréséhez. A kezelt adatok szükségszerűségét folyamatosan ellenőrizni kell. Ezt a feladatot is az ügyvezető által kijelölt felelős személy látja el.
Amint az adatkezelés célja megvalósult, főszabályként a személyes adatokat azonnal törölni kell, illetve anonimizálni, feltéve, ha jogszabály nem írja elő a további adattárolást, vagy nem merül fel további adatkezelési cél, amely megfelel a célok közötti összeegyeztethetőségnek. Ennek megállapításához a feladat elvégzéséért felelős vezető megvizsgálja a személyes adatok gyűjtésének korábbi és jövőbeli céljait, körülményeit, az adatok jellegét (az adatok különleges kategóriáiról beszélünk vagy sem), az adatkezelés következményeit és garanciáit.

8.4. Pontosság megvalósítása

A kezelt adatoknak mindig időszerűnek és naprakésznek kell lennie. Az adatok folyamatos frissítése a feladatot végző adatkezelő feladata és felelőssége.
A foglalkoztatottak és az ügyfelek személyes adatainak felvételénél és rögzítésénél kiemelt figyelmet kell fordítani a precíz munkára. Az adatbázisok karbantartását és naprakészségét folyamatosan biztosítani kell.
A személyes adatok pontosítására irányuló kérelem esetén az adatokat haladéktalanul, legkésőbb 1 hónapon belül módosítani kell a valós adatoknak megfelelően. Amennyiben a személyes adatok pontosítására irányuló kérelem nem a valós adatok nyilvántartását célozza, úgy az erre irányuló kérelmet ezen határidőn belül el kell utasítani az elutasítás indokának feltüntetésével. A kérelem elbírálásáig az adatkezelést a helyesbítendő adatok vonatkozásában az Adatkezelő korlátozza, azaz a tárolt személyes adatokat megjelöli és ezen adatokon az adathelyesbítés végrehajtásáig vagy elutasításáig adatkezelési műveleteket nem végez.

8.5. Korlátozott tárolhatóság megvalósítása

Az Adatkezelő mindent megtesz annak érdekében, hogy az érintett személyes adatait csak az adatkezelés céljának eléréséig szükséges ideig tárolja. Azaz, ha megszűnt az adatkezelés célja vagy már nincs szükség arra, hogy az Adatkezelő az érintettet azonosítsa, akkor az adatait törli, kivéve, ha jogszabály máshogy rendelkezik vagy a korábbi adatkezelés céljával összefüggő okból az adatkezelés más cél elérése érdekében szükséges.

8.6. Integritás és bizalmas jelleg megvalósítása

Az Adatkezelő mindent megtesz annak érdekében, hogy az általa kezelt személyes adatokat megóvja minden külső és nem várt hatástól, amely az adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezheti.
Az Adatkezelő a nyilvántartás rendszerének felépítése, a jogosultságok meghatározása, és egyéb szervezeti intézkedések útján gondoskodik arról, hogy a nyilvántartásaiban szereplő adatokat csak azok a munkavállalók, és egyéb az Adatkezelők érdekkörében eljáró személyek ismerhessék meg, akiknek erre munkakörük, feladatuk ellátása érdekében szükségük van.
Ennek érdekében minden dolgozónak kötelessége az informatikai biztonsági szabályzat előírásainak betartása és betartatása. (jelszavak rendszeres cseréje, meghatározott weblapok kerülése, ismeretlen forrású e-mailek megnyitásának tilalma, stb)
Minden dolgozónak kötelessége továbbá a személyes adatokat tartalmazó papír alapú iratok fokozott védelme, zárt szekrényben történő tárolása. Az ügyfélfogadást végző adatkezelők kötelesek gondoskodni arról, hogy az ügyfélfogadás alkalmával arra jogosulatlan személyek személyes adatokat illetéktelenül ne tekinthessenek meg, azokhoz semmilyen módon ne férjenek hozzá.

Az Adatkezelő informatikai feladatokért felelős megbízottja folyamatosan figyelemmel kíséri az egyes feladatokat ellátó munkatársak számítógépes hálózathoz való hozzáférésének jogosultságait, arról naprakész nyilvántartást vezet.
Személyes adatok elektronikus tárolása kizárólag a megfelelő védelemmel ellátott szervereken lehetséges. Azok mobil adattárolókra (CD, DVD, pendrive, külső adattároló, stb.) történő kiírása, mentése szigorúan tilos!

Minden foglalkoztatott kötelessége, hogy a bármilyen módon tudomására jutó valószínűsíthető adatvédelmi incidenst - annak súlyosságától vagy bizonyosságától függetlenül – az ügyvezetőnek haladéktalanul, de legkésőbb a tudomásra jutástól számított 2 órán belül jelezze. Az incidens kivizsgálása és szükség esetén határidőben történő bejelentése, valamint az egyéb szükséges intézkedések megtétele az ügyvezető felelőssége.

E szabályzat alapján az Adatkezelő az egyéb belső szabályzatait felülvizsgálja és szükség esetén naprakésszé teszi.
Az Adatkezelő megfelelő nyilvántartást vezet a hatásköre alapján végzett adatkezelési tevékenységekről. Köteles a felügyeleti hatósággal együttműködni és ezeket a nyilvántartásokat kérésre hozzáférhetővé tenni az érintett adatkezelési műveletek ellenőrzése érdekében.

9. Az érdekmérlegelés

Ha az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, az Adatkezelőnek kell bizonyítania, hogy érdekei elsőbbséget élveznek az érintett érdekeivel vagy alapvető jogaival és szabadságaival szemben.
Az Adatkezelőnek az általa meghatározott jogos érdekhez képest kell megfelelően kiválasztania azt, hogy milyen célból, mennyi ideig, milyen személyes adatokat kezel, és milyen garanciális intézkedéssel biztosítja azt, hogy az adatkezelés csak szükséges mértékben és arányosan korlátozza az érintettek jogait.
Az érdekmérlegelés jogalapjának az alkalmazását az Adatkezelőnek minden esetben írásban kell dokumentálnia. (érdekmérlegelési teszt)
Az érdekmérlegelési teszt annak bemutatására irányul, hogy az Adatkezelő megfelelően azonosította a jogos érdeket, és erre alapozva olyan alapon végzi az adatkezelést, amely nem jelent aránytalan korlátozást az érintett érdekeire, jogaira és szabadságaira nézve.

Az Adatkezelő által alkalmazott érdekmérlegelési teszt vizsgálandó pontjai:

1. Az adatkezelés leírása
2. Az adatkezelő jogszerű érdekeinek értékelése
3. Az adatkezelés érintettre gyakorolt hatásának leírása (személyes adatok jellege, az érintett ésszerű elvárásai, az érintett státusza)
4. Az érintett jogainak védelme érdekében tett intézkedések (biztosítékok) meghatározása
5. Elszámoltathatóság és átláthatóság biztosításának módja

10. A hatásvizsgálat

Ha a tervezett adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira (az Érintett érdekeire) nézve, akkor az Adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.
Az adatvédelmi hatásvizsgálat elvégzéséről az ügyvezető kötelessége intézkedni.

Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

- természetes személyekre vonatkozó egyes személyes jellemzők módszeres és kiterjedt értékelése – különösen automatizált adatkezelés - esetében

- a személyes adatok különleges kategóriáira vonatkozó adatok nagy számban történő kezelése esetében (pl. egészségügyi adatok nagy száma)
- nyilvános helyek nagymértékű, módszeres megfigyelése esetében (pl. kamerarendszer telepítése).

A felügyeleti hatóság által meghatározott esetekben kötelező az adatvédelmi hatásvizsgálatot elvégezni. A kötelező hatásvizsgálatok listája a https://naih.hu/files/GDPR_35_4_lista_HU_mod.pdf lapon elérhető.

A hatásvizsgálat kiterjed legalább az alábbiakra:
- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára
- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

A hatásvizsgálat elvégzését követően szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén gondoskodni kell a hatásvizsgálat felülvizsgálatáról, mely során a kockázatok értékelését újra el kell végezni. A kockázatok felülvizsgálatát legalább 3 évente végre kell hajtani.

Továbbá a személyes adatok kezelésével kapcsolatosan az ügyvezető kötelezettsége a kockázatelemzés, amelynek lépései az alábbiak:
- a személyes adatok kezelésével kapcsolatos kockázatok azonosítása,
- kockázati lista felállítása,
- az egyes kockázatok valószínűsíthető fő okainak és várható negatív hatásainak meghatározása, majd
- ezek alapján a preventív és a korrektív kockázatkezelési folyamatok kidolgozása.

Szükséges a kockázatforrások feltárása, melyen belül meg kell határozni a kockázati preventív és korrektív célkezelés elemeit, az erőforrás-kezelés rendszerét, továbbá el kell különíteni az objektív és szubjektív kockázati elemeket.
Az elemzés során el kell jutni a teljes kockázatértkelési rendszer kialakításáig. Meg kell állapítani a kockázatforrásokat, értékelni kell a lehetséges kockázatokat valószínűség és értékelés szempontjából is. Az elemzés menetét és eredményeit írásba kell foglalni.

Kockázatforrások:
- műszaki hiba
- természeti katasztrófa
- emberi tevékenység: gondatlan, vagy szándékos károkozás

Valószínűség szempontja szerint:
- nagyon kicsi (szinte soha nem fordul elő)
- kicsi (nagyon ritkán fordul elő)
- közepes (többször előfordul)
- nagy (naponta – vagy még gyakrabban) többször előfordul

Érékelés szempontjából:
- elhanyagolható (nem jár anyagi, erkölcsi veszteséggel)

- kicsi (minimális anyagi, erkölcsi vesztességgel jár)
- közepes (elviselhető vesztességgel jár)
- nagy (nagy anyagi veszteséggel jár, szolgálati, hivatali titok)

11. Előzetes konzultáció

Abban az esetben, ha az elvégzett adatvédelmi hatásvizsgálat megállapítja, hogy az adott adatkezelési folyamat valószínűsíthetően magas kockázattal jár, akkor az Adatkezelő az adatkezelési folyamata megkezdését megelőzően konzultációt kezdeményezhet a Hatósággal.
A konzultáció során az Adatkezelő tájékoztatja a Hatóságot az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről, a tervezett adatkezelés céljairól és módjairól, az érintettek jogainak és szabadságainak védelmében hozott intézkedésekről, az adatvédelmi hatásvizsgálat eredményéről.

12. Az adatvédelem szervezete

12.1. Az ügyvezetés

A Társaság ügyvezetése a Társaság sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, és kijelöli az adatkezelés felügyeletét ellátó személy(eke)t.
A Szabályzatban előírtak betartatásáért a feladatkörében minden munkavállaló felelős.
A Társaság munkavállalói és munkatársai a munkájuk során gondoskodnak 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.
A Társaság adatvédelmi szervezetének felügyeletét az ügyvezetés látja el.

Az ügyvezetés adatvédelemmel kapcsolatos feladatai, amelyet részben delegálhat, a következők:
- felelős az érintettek GDPR-ban, Infotv-ben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
- felelős a Társaság 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;
- vizsgálatot rendelhet el;
- kiadja a Társaság adatvédelemmel kapcsolatos belső szabályait;
- szervezi és koordinálja a munkavállalók, és kifejezetten az informatikus munkavállalók adatvédelemmel, információbiztonsággal kapcsolatos munkáját; továbbá
- minden, az adatvédelemmel kapcsolatban felmerült kérdés megoldása.

12.2. Az adatvédelmi tisztviselő

Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai:
- segítséget nyújt az érintettek jogainak biztosításában;
- jogosult a jelen Szabályzat betartását az egyes szervezeti egységeknél ellenőrizni;
- figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi a jelen Szabályzat módosítását;
- közreműködik a NAIH-tól a Társasághoz érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;

- általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg;
- tájékoztatást és szakmai tanácsot ad a Társaság adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban;
- kérésre ellenőrzi az adatvédelmi jogszabályoknak, valamint a Társaság belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosságnövelését és képzését, valamint a kapcsolódó auditokat is;
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
- együttműködik a NAIH-hal;
- az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint bármely egyéb kérdésben konzultációt folytat le a Hatósággal.

12.3. Megbízott Informatikai karbantartó (Informatikai feladatokkal megbízott munkatárs)

A Társaság informatikáért felelős munkavállalójának adatvédelemmel kapcsolatos feladatai, - ezek a feladatok részben vagy egészben kiszervezhetők -, a következők:

- ellátja a munkaköri leírásában meghatározott rendszergazdai feladatokat;
- ellátja az informatikai fejlesztésekkel, beszerzésekkel kapcsolatos feladatokat, ügyelve a beszerzések racionalizálására, kompatibilitására;
- közreműködik az adatkezelők egyéni kódjának, jelszavának, jogosultságának beállításában azon szerverek tekintetében, amelyekre adminisztrátori jogosultsággal rendelkezik;
- használatba állítás előtt ellátja a szoftverek és hardverek rendszerbe állítását (telepítését);
- a szervereken tárolt adatok vonatkozásában gondoskodik a kezelt adatok jogosultak általi hozzáféréséről, módosításáról, illetőleg gondoskodik a tárolt adatok megsemmisülésének megakadályozásáról;
- igény esetén közreműködik a számítógépen/szerveren tárolt adatok esetében a megadott szempontú adatszolgáltatásban;
- elvégzi a szervereken tárolt adatok biztonsági mentését, naplózását;
- vírusfertőzöttség esetén elvégzi a fertőzött informatikai eszköz vírusmentesítését;
- szükség szerint ellátja a számítógépek és a hálózat karbantartását, gondoskodik a szerverek üzemszerű működéséről;
- ellátja az informatikai eszközök szervizelésével kapcsolatos feladatokat, amennyiben megoldható szakszerviz segítsége nélkül;
- üzemzavar esetén elvégzi az informatikai rendszerek újra indítását, a hálózat alkalmazásainak és adatainak a visszatöltését;
- folyamatosan üzemelteti a számítógépes hálózatot;
- igény esetén segítséget nyújt az adatkezelőknek a számítástechnikai alkalmazások használatánál és az adatbázisok kezelésénél;
- hozzájárulását adja valamennyi munkavállaló szerverhozzáférési jogosultságához;
- ellátja az Informatikai Biztonsági Szabályzatban meghatározott feladatokat, biztosítja az abban foglaltak teljesítését.

12.4. Az adatkezelő (alkalmazott)

- Kezeli a feladatkörébe tartozó adatokat, más adatot csak helyettesítés esetén kezelhet, vezeti a nyilvántartásokat.
- A jogszabály által felhatalmazott személynek vagy szervezetnek adatot szolgáltat.
- Vezeti (kezeli) az adat-, valamint az adatszolgáltatási nyilvántartást.
- Megőrzi a tudomására jutott adatot.

- Gondoskodik arról, hogy az általa vezetett nyilvántartás adataihoz illetéktelen személy ne férhessen hozzá, ügyel a nyilvántartás biztonságos tárolására.
- Betartja az adatkezelésre, adatvédelemre és az adatbiztonságra vonatkozó rendelkezéseket.
- Haladéktalanul jelzi az informatikusoknak a számítástechnikai eszközök bárminemű meghibásodását, illetőleg az adatállomány kezelhetőségében bekövetkező problémát.
- Az adatkezelő köteles a közvetlen vezetőjét tájékoztatni minden olyan eseményről, mely esetben őt jogszerűtlen adatkezelésre kérték fel, utasították, illetve a saját rendszerében bármilyen egyéb illetéktelen adathozzáférést, vagy adatkezelést tapasztalt.

13. Adatfeldolgozói tevékenység

Adatfeldolgozónak minősül az a természetes vagy jogi személy, közhatalmi szerv vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni.

Az adatfeldolgozási szerződés legalább az alábbi rendelkezéseket tartalmazza:

(a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;

(b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

(c) meghozza az adatkezelés biztonsága tekintetében előírt intézkedéseket;

(d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozó rendelkezésekben említett feltételeket;

(e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

(f) segíti az adatkezelőt az adatkezelés biztonságára, adatvédelmi incidens bejelentésére, az adatvédelmi hatásvizsgálat és előzetes konzultáció lefolytatására vonatkozó kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;

(g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;

(h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely az adatfeldolgozás tekintetében meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az adatfeldolgozókkal kötendő megállapodás mintapéldányát jelen szabályzat melléklete tartalmazza.

Az igénybe vett adatfeldolgozók felsorolását és adatait a Társaság által naprakészen vezetett adatfeldolgozói nyilvántartás tartalmazza.

A Társaság a tevékenysége során adatfeldolgozóként nem jár el.

14. Az adatkezelési tevékenységek nyilvántartása

Az ügyvezető által az adatvédelmi feladatokkal megbízott munkatárs vezeti az adatkezelési tevékenységek nyilvántartását (Adatkezelési Tevékenységek Nyilvántartása). Az Adatkezelési Tevékenységek Nyilvántartása valamennyi, az Adatkezelő általi adatkezelés esetén tartalmazza:

a/ az adatkezelés célját,
b/ az adatkezelés jogalapját,
c/ az érintettek körét,
d/ az érintettekre vonatkozó személyes adatok kategóriáit,
e/ az adatok kezelésének időtartamát vagy az adattörlés ideje megállapításának szempontjait;
f/ a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat és azok garanciáinak leírását is,
g/ az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
h/ az adatkezelő, valamint közös adatkezelés esetén a közös adatkezelők megnevezését és elérhetőségét,
i/ az adatvédelmi tisztviselő nevét és elérhetőségét, (amennyiben ilyen van Adatkezelőnél)
j/ ha lehetséges, az adatbiztonsági intézkedések általános leírását,

Az Adatkezelési Tevékenységek Nyilvántartásának célja az Adatkezelő, mint adatkezelő adatkezelési tevékenysége átláthatóságának biztosítása, és ezzel az esetleges felesleges, párhuzamos adatkezelések elkerülése.

Az Adatkezelő ügyvezetője az Adatkezelési Tevékenységek Nyilvántartásába való betekintést – a Hatóság képviselőin kívül – az Adatkezelő vezetői és adatkezelést végző foglalkoztatottjai, továbbá a közös adatkezelést érintő rész tekintetében a közös adatkezelő részére biztosítja.
Az Adatkezelési Tevékenységek Nyilvántartásába bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős 5 munkanapon belül köteles jelezni az ügyvezetőnek, aki ennek megfelelően – indokolt esetben - módosíttatja az adatvédelmi feladatokkal megbízott munkatárssal az Adatkezelési Tevékenységek Nyilvántartásának adatait.

15. Adatbiztonság

Az Adatkezelő gondoskodik az adatok biztonságáról. Ennek érdekében megteszi a szükséges technikai és szervezési intézkedéseket mind az informatikai eszközök útján tárolt, mind a hagyományos, papíralapú adathordozókon tárolt adatállományok biztonságos kezelése és tárolása tekintetében.
Az Adatkezelő gondoskodik arról, hogy a vonatkozó jogszabályokban előírt adatbiztonsági szabályok érvényesüljenek. Az Adatkezelő gondoskodik az adatok biztonságáról, megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az irányadó jogszabályok, adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az Adatkezelő az adatokat megfelelő intézkedésekkel védi a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
Az Adatkezelő az adatbiztonság feltételeinek érvényesítése érdekében gondoskodik az érintett munkatársak megfelelő felkészítéséről.
Az Adatkezelő az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel van a technika mindenkori fejlettségére. Az Adatkezelő több lehetséges adatkezelési

megoldás közül azt választja, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

15.1. Informatikai nyilvántartások védelme

Az Adatkezelő az informatikai védelemmel kapcsolatos feladatai körében gondoskodik különösen:

- a jogosulatlan hozzáférés elleni védelmet biztosító intézkedésekről, ezen belül a szoftver és hardver eszközök védelméről, illetve a fizikai védelemről (hozzáférés védelem, hálózati védelem);
- az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről (tükrözés, biztonsági mentés);
- az adatállományok vírusok elleni védelméről (vírusvédelem);
- az adatállományok, illetve az azokat hordozó eszközök fizikai védelméről, ezen belül a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról (archiválás, tűzvédelem).

Az informatikai biztonság feltételeinek kialakítása és betartásának ellenőrzése az informatikai feladatokat ellátó munkatárs feladata.

15.2. Papíralapú nyilvántartások védelme

Az Adatkezelő a papíralapú nyilvántartások védelme érdekében megteszi a szükséges intézkedéseket különösen a fizikai biztonság, illetve tűzvédelem tekintetében.
A munkavállalók, és egyéb, az Adatkezelő érdekében eljáró személyek az általuk használt, vagy birtokukban lévő, személyes adatokat is tartalmazó adathordozókat, függetlenül az adatok rögzítésének módjától, kötelesek biztonságosan őrizni, és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

A papíralapú nyilvántartások és a papíron tárolt adatok biztonsága feltételeinek kialakítása és betartásának ellenőrzése az adatvédelmi feladatokat ellátó munkatárs feladata.

A papíralapon kezelt személyes adatok biztonsága érdekében a Társaság 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 helyiségben helyezi el;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;
- a Társaság 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 a Társaság.

Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, a Társaság intézkedik a papíralapú adathordozó megsemmisítéséről. Ebben az esetben a Társaság kijelöli a megsemmisítésért felelős munkavállalót. A megsemmisítésen legalább háromtagú megsemmisítési bizottság vesz részt. A megsemmisítésről jegyzőkönyvet kell felvenni, ha más, automatizált eljárással nem biztosítható a törlés igazolása.
Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, a fizikai eszköz megsemmisítésére a papíralapú dokumentumokra vonatkozó megsemmisítési szabályok megfelelően irányadók.

15.3. Az informatikai biztonság

Az információbiztonság kiemelt céljai:
1) a bizalmasság (confidentiality),
2) a sérthetetlenség (integrity) és
3) a rendelkezésre állás (availability).

Ez az úgynevezett CIA-háromszög.
Ezen belül szintén három kontrollt különböztetünk meg:
- fizikai,
- logikai, és
- adminisztratív kontroll.

Fizikai kontroll
A számítógépes környezethez való hozzáférés korlátozása, valamint az adatmentés biztosítása.

Logikai kontroll
Olyan intézkedések, mint például a jelszó- és erőforrás-menedzsment, azonosság- és jogosultságkezelés, logikai hozzáférés, információbiztonsági eszközök, illetve hálózati konfiguráció.

Adminisztratív kontroll
A Társaság belső szabályai, rendelkezései, eljárásrendjei tartoznak ezen kontroll alá.

Informatikai védelem
A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Társaság az alábbi intézkedéseket és garanciális elemeket alkalmazza:
- az adatkezelés során használt számítógépek a Társaság 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 a Társaság rendszeresen, illetve indokolt esetben gondoskodik;
- az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
- a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
- a Társaság a hálózaton tárolt adatok biztonsága érdekében a szervereket magas rendelkezésre állású infrastruktúrával védi, az adatvesztést mentésekkel és archiválással kerüli el;
- a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;
- a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését,
- a társaság gondoskodik a számítógépes infrastruktúrájának megfelelő védelméről.

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 a Társaságot a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.

Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell.

A személyes adatok biztonsága érdekében a Társaság az alábbi jogosultságkezelési alapelveket alkalmazza:

- 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 ügyvezetése vagy az általa kijelölt személy 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.

Jogosultságkezelési folyamat

Jogosultságigénylést a társaságnál az adott adatkör adatgazdája hagyja jóvá. Ezen adatgazdák kijelölése az ügyvezetés feladata.
A jogosultság kezelésekről az informatikáért felelős munkavállaló nyilvántartást vezet.
A jóváhagyott jogosultságok beállításáról az informatikai csoport gondoskodik.
A megszületett döntést követően az informatikai csoport kijelölt munkatársa beállítja a jogosultságokat, amiről visszaigazolást küld az igénylő felé.
A jogosultság birtokosa munka- vagy egyéb jogviszonyának megszűnéséről közvetlen felettesének kötelessége értesíteni az informatikust, valamint a munkáltatói jogok gyakorlóját a jogosult eddig birtokolt jogosultságainak törlése érdekében.
A jogosultság megszűnése esetén a jogosult felettese a megszüntetési kérelmet elektronikus úton vagy papíralapon a jogosultságkezelési megrendelőlapon küldi meg az informatikusnak, aki gondoskodik a jogosultság törléséről. Ezt követően az informatikus vagy az általa megbízott munkatárs visszajelzést küld a törlést kezdeményezőnek.
Áthelyezés esetén a korábbi munkakör feletti munkáltatói jogokat gyakorló felettes és az új munkakör feletti munkáltatói jogokat gyakorló felettes együtt kötelesek gondoskodni a régi jogosultságok törlésének, módosításának vagy új jogosultságok felvételének kezdeményezéséről.
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.

Álnevesítés

Az 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, mivel a Társaság az ilyen további információt külön tárolja, technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.
Az álnéven történő adatkezelést a Társaság a nagyobb fokú biztonság érdekében, valamint a statisztikai célra gyűjtendő adatok vagy a fejlesztés, tesztelés, karbantartás alatt álló rendszerek esetében a tesztadatok tekintetében végez, mivel a személyes adatok álnevesítése csökkentheti az érintettek számára a kockázatokat, valamint a Társaság ezáltal könnyebben meg tud felelni az adatvédelmi kötelezettségeinek.
Az álnevesítés személyes adatok kezelése során történő alkalmazásának ösztönzése céljából lehetővé teszi az álnevesítésre irányuló intézkedések és az általános elemzés egyidejű alkalmazását a Társaság szervezetén belül. A Társaság továbbá biztosítja, hogy az ahhoz

szükséges további információkat, amelyek által a személyes adatokat egy adott érintetthez lehessen kapcsolni, elkülönítve tárolják.
A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a Rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Ahhoz, hogy az Adatkezelő igazolni tudja a Rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik, különösen a beépített és az alapértelmezett adatvédelem elveit.
A Társaság törekszik – a GDPR-nak való megfelelés érdekében – a személyes adatok kezelésének minimálisra csökkentésére, a személyes adatok mihamarabbi álnevesítésére, a személyes adatok funkcióinak és kezelésének átláthatóságára, valamint arra, hogy az érintett nyomon követhesse az adatkezelést, a Társaság pedig biztonsági elemeket hozhasson létre és tovább fejleszthesse azokat.

15.4. Oktatás és tréningrendszer

Kiemelt területként kell kezelni a munkavállalók kapcsán a biztonságtudatossági képzést a szervezet informatikai és nem informatikai alkalmazottai részére.
A biztonságtudatos magatartás komoly üzleti károkat okozó hibák és támadások megelőzésében játszhat szerepet.
Nem elegendő a megfelelően kidolgozott információbiztonsági rendelkezések és az adatvédelmi, adatbiztonsági szabályozás megléte a szervezetben, a munkavállalókkal rendszeres képzések, tréningek során kell tudatosítani, hogy a kialakított szabályrendszer és az IT eszközök önmagukban nem képesek garantálni a szervezet számára az adat- és információbiztonságot, ehhez a napi munkatevékenységük során felelős magatartásukkal a munkavállalóknak is hozzá kell járulniuk.
A munkavállalók megfelelő képzése a képzést követően kimutathatóan kevesebb biztonsági incidenst eredményez, ami a közvetlen adatvesztésből és esetleges adatvédelmi bírságból eredő károkon túl a pénzügyi eredményekben is nyilvánvalóan megmutatkozik.
A munkavállalók általános adatvédelmi-információbiztonsági tréning rendje évente (kapcsolható más rendszeres képzésekhez, tréningekhez, mint pl.: tűz- és munkavédelem) egy óra időtartamban javasolt.
Külön tréningrendet kell biztosítani az informatikai, különösen a rendszergazdai feladatokat ellátók részére. Ennek célja, hogy kizökkentse a képzés alatt állókat a megszokott munkamenetükből és feltárja előttük a rosszindulatú támadások, hekkerek által folyamatosan fejlesztett aktuális támadási szemléletet, rámutasson az aktuális trendek szerint jellemzően keresett gyenge pontokra és segítse őket abban, hogy érzékelt behatolási kísérlet esetén milyen megoldásokat preferáljanak a támadások elhárítására és a kockázat alacsony szinten tartásának érdekében.

16. Az adatvédelmi incidensek kezelése

16.1. Az adatvédelmi incidens minősítése

Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések – akár vétlen, akár szándékos – megsértésének következtében bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés:

a/ súlyos incidens: olyan incidens (pl. adatvesztés, adatsérülés), mely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl.: a jogosulatlan hozzáféréssel érintett adatok esete; az olyan adatsérülés, adatvesztés, amelynél az adatok naplózott állományból nem állíthatóak helyre). Magas kockázatúnak minősül az az eset, amely fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, pl. az érintetteknek a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, hátrányos megkülönböztetést, a

személyazonosság-lopást vagy a személyazonossággal való visszaélést, pénzügyi veszteséget, jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését eredményezheti;
b/ enyhe incidens: minden incidens, amely nem tartozik az a) pont alá (pl. átmeneti szolgáltatásleállás, - kiesés az Adatkezelő munkavállalói által használt olyan belső rendszerekben, amely nem jár adatsérüléssel vagy adatvesztéssel).

Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni az Adatkezelő tulajdonát képező adathordozón, mobiltelefonon, laptopon, egyéb számítástechnikai eszközön tárolt adatokra, továbbá az Adatkezelő alkalmazottainak olyan saját tulajdonú eszközein (adathordozó, mobiltelefon, laptop, egyéb számítástechnikai eszköz) tárolt adatokra, amely eszközöket munkavégzéshez, munkaköri feladatok ellátásához, hivatalos célból használhat. Az adatvédelmi incidensre vonatkozó szabályokat az Adatkezelő birtokában lévő papíralapú adathordozón lévő adatokra is alkalmazni kell.

Az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események adatvédelmi incidensnek is minősülnek, amennyiben személyes adatokra nézve következik be. A jelen Szabályzat adatvédelmi incidens kezelésére vonatkozó rendelkezéseinek alkalmazása nem mentesít az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események kezelésére (bejelentésére, kivizsgálására stb.) vonatkozó szabályok betartása alól, azaz az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események kezelésére vonatkozó szabályokat jelen Szabályzat előírásaival párhuzamosan alkalmazni kell.

16.2. Az adatvédelmi incidens bejelentése

Az a munkavállaló vagy megbízott, aki az Adatkezelő által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy az Adatkezelő szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban adatvédelmi incidenst vagy annak gyanúját észleli, köteles azt haladéktalanul – legkésőbb a tudomásszerzéstől számított 2 órán belül - bejelenteni az ügyvezetőnek.

Az adatvédelmi incidensről szóló bejelentésben ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az adatvédelmi incidenssel érintett személyes adatok kategóriáit és hozzávetőleges számát, továbbá a bejelentő nevét és elérhetőségét.

A közös adatkezelésről szóló szerződésben [GDPR 26. cikk], illetve az adatfeldolgozóval kötendő szerződésben [GDPR 28. cikk] egyértelműen rendelkezni kell a másik adatkezelő, illetve az adatfeldolgozó azon kötelezettségéről, hogy az adatvédelmi incidensről az Adatkezelő köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni. A szerződésnek tartalmaznia kell továbbá a közös adatkezelő, illetve az adatfeldolgozó kötelezettségeit adatvédelmi incidens bejelentésében és kivizsgálásában.

16.3. Incidensprotokoll általában

Az informatikai feladatokat ellátó bevonásával a riasztásokban szereplő sérülékenység elhárításakor a következők szerint kell eljárni:
a/ figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó rendelkezéseket;
b/ amennyiben a riasztás személyes adatot tartalmazó alkalmazás sérülékenységével kapcsolatban keletkezett, az ügyvezetőt haladéktalanul tájékoztatni kell;
c/ amennyiben az Adatkezelő rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;

d/ ha az Adatkezelő nem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni;
e/ amennyiben a sérülékenység elhárítása belső erőforrásból nem kivitelezhető, akkor külső szakértőket kell bevonni az elhárítás folyamatába.

A papíralapon kezelt iratokkal kapcsolatban a jelen Szabályzat személyi hatálya alá tartozó személyek kötelesek a személyes adatokat tartalmazó iratokat a munkavégzés befejezését követően, ahol ennek feltételei biztosítottak, zárható szekrényben, zárral ellátott fiókban tárolni. Ahol a tárolás előbb nevesített feltételei nem adottak, az irodahelyiség ajtajának kulcsra zárásával kell a személyes adatok védelmét biztosítani abban az esetben, ha az irodahelyiségben senki sem tartózkodik. A Szabályzat személyi hatálya alá tartozó személyek kötelesek az Adatkezelő egyéb belső szabályzatai, így különösen az iratkezelés rendjéről, illetve a biztonsági előírásokról szóló mindenkor hatályos belső szabályzatnak megfelelően eljárni.

16.4. Az adatvédelmi incidens kivizsgálása

Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóak egyaránt) felmerülése esetén az Adatkezelő informatikai feladatokat ellátó munkatársa az Adatkezelő adatvédelmi feladatokat ellátó munkatársával együtt megvizsgálja, és kategorizálja a bekövetkezett incidenst, és meghatározza az esetleges elhárítás érdekében szükséges további intézkedéseket.

A bejelentés előzetes megvizsgálása során az alábbi szempontokat kell figyelembe venni:
a/ a bejelentés személyes adatot érint-e,
b/ amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,
c/ megállapítható-e az incidensben érintett személyek köre,
d/ a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása (beleértve a törlést/megsemmisítést is) történt,
e/ az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve,
f/ melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,
g/ az Adatkezelő által alkalmazott technikai és szervezési védelmi intézkedések az incidensben érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik-e az adatokat.

16.5. Az érintett tájékoztatása a súlyos adatvédelmi incidensről

Súlyos adatvédelmi incidens esetén az Adatkezelő – az érintettel kapcsolatban rendelkezésére álló elérhetőségeken, ennek hiányában vagy alkalmazásuk lehetetlensége esetén (GDPR 34. cikk) a az Adatkezelő helyi napilapban közzétett közlemény útján – indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat és intézkedéseket:
a/ az Adatkezelő kapcsolattartójának nevét és elérhetőségeit;
b/ az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
c/ az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintettet nem kell tájékoztatni, amennyiben az incidens nem jár magas kockázattal, és a következő feltételek bármelyike teljesül:
a/ az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták,

különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
b/ az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az említett magas kockázat a továbbiakban valószínűsíthetően nem áll fenn;
c/ a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Az Adatkezelő ügyvezetőjének döntése alapján az Adatkezelő az érintetteket az Adatkezelő honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény útján is értesítheti.

16.6. Az adatvédelmi incidens bejelentése a Hatóságnak

Az adatvédelmi incidensről szóló bejelentést a Hatóság mindenkori kapcsolati pontjára kell eljuttatni. A bejelentés összeállításának és beadásának felelőse az ügyvezető.

Az adatvédelmi incidensről szóló bejelentésben legalább:
a/ ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b/ közölni kell a tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c/ ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d/ ismertetni kell az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Ha nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

16.7. Az adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidensekről az ügyvezető által megbízott munkatárs elektronikus nyilvántartást vezet.

A nyilvántartásban rögzíteni kell:
a/ az incidensben érintett személyes adatok körét és számát,
b/ az adatvédelmi incidenssel érintettek körét és számát,
c/ az adatvédelmi incidens észlelésének és tudomásszerzésének időpontját,
d/ az adatvédelmi incidens körülményeit, hatásait,
e/ az adatvédelmi incidens elhárítására megtett intézkedéseket,
f/ az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

Az Adatkezelő az adatvédelmi incidens kivizsgálásával kapcsolatos papíralapú és elektronikus dokumentumokat 10 évig köteles megőrizni. Az adatvédelmi incidensek vizsgálata során keletkezett, iktatott dokumentumokat az Adatkezelő az incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

17. Harmadik országba irányuló adattovábbítás különös szabályai

Amennyiben személyes adatnak harmadik országba történő továbbításának szükségessége merül fel, az adatkezelő köteles adatvédelemmel foglalkozó szakértő véleményét kérni az adattovábbítás megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról.

18. Adatvédelmi audit

Az adatvédelmi audit célja, hogy az ügyvezető meggyőződjön arról, hogy az Adatkezelő az adatvédelemmel kapcsolatos jogszabályoknak és belső szabályzatoknak megfelelően kezelik-e az adatokat.
Az adatvédelmi feladatokkal megbízott munkatárs – az ügyvezető utasításai alapján - éves ellenőrzési tervet készít. Az éves ellenőrzési tervnek az ellenőrzés várható időpontját, továbbá az ellenőrzés tárgykörét kell tartalmaznia.

Az ellenőrzés során az adatvédelmi feladatokkal megbízott munkatárs az ügyvezető utasítása, illetve engedélye alapján az Adatkezelő irodahelységeibe szabadon beléphet, az – ellenőrzés tárgyával összefüggésben kezelt – irataiba betekinthet, a munkatársaktól tájékoztatást kérhet adott üggyel kapcsolatos adatkezelésről.
Az adatvédelmi feladatokkal megbízott munkatárs az ellenőrzés megtörténtéről jegyzőkönyvet készít. A jegyzőkönyv az ellenőrzés lefolytatásának tényét, annak időpontját és időtartamát, továbbá a tevékenység során rögzített tényeket, megállapításokat, információkat tartalmazza.

19. A személyes adatok kezelhetőségének felülvizsgálata

Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg.

A szervezet vezetője által megállapított rendszeres felülvizsgálati határidő: 2 év.

II. A Társaság által kezelt adatok köre és az adatkezelés rendje

1. Munkaviszonnyal és egyéb foglalkoztatásra irányuló jogviszonnyal kapcsolatos adatkezelések

1.1. Foglalkoztatással kapcsolatos adatkezelés

Az adatkezelés célja	Munkaszerződéseknek való megfelelés, munkáltatás dokumentálása, törvényi előírásoknak való megfelelés
Az adatkezelés jogalapja - GDPR 6. cikk (1)	c) pont; Mt. 10. §
A kezelt adatok köre	Név, cím, telefonszám, TAJ szám, adóazonosító jel, lakcímkártya szám, személyigazolvány szám, anyja neve, születési hely, idő, munkaruha méret, éleslátásra vonatkozó adatok, jogviszony kezdete és egyéb jogszabály által előírt személyes adatok, megváltozott munkaképességű foglalkoztatása, beteg családtag ápolása, betegséghez köthető adókedvezmények igénybevétele esetén a megbetegedésre vonatkozó adatok.
Az adatok forrása	Munkavállaló (Érintett)
Az adatok tárolásának ideje	öregségi nyugdíjkorhatár betöltését követő 5 évig

Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	Adott esetben, ha szükséges a továbbítás a jogi képviseletet ellátó ügyvéd, illetékes bíróság, jogszabályban megnevezett hatóságok felé.
Profilalkotás vagy automatikus döntéshozatal	Nincs
Harmadik országba történő adattovábbítás	Nincs

Munkáltató a Munkavállalókról munkaügyi aktát vezet. Az adatkezelés jogalapja a munkaügyi akták esetében az Adatkezelőre vonatkozó jogi kötelezettség teljesítése [GDPR 6. cikk (1) bek. c) pont], ezen belül a jelen pontban megjelölt törvényi előírások, amelyek kötelezővé teszik az adatkezelést Munkáltató részére.

A munkaügyi akta tartalmazza: a Munkavállalók jelentkezése és munkaviszonya fennállása alatt keletkezett dokumentumokat és adatokat.

A munkaügyi akták kezelése papír alapon valósul meg a Munkáltató székhelyén.

A munkaügyi akták fizikai tárolása:

A munkaügyi akták részét képező munkaügyi iratok tárolása alapvetően papír alapon, zárt szekrényben történik. Az adatok elektronikus úton is tárolásra kerülnek az Adatkezelő saját szerverén, melyhez a hozzáférés jogosultság alapján történik.

A munkaügyi aktákban található iratokba kizárólag az alábbi munkaköröket ellátó személyek jogosultak betekinteni:

-ügyvezető

-cégvezető

A tárolt adatokhoz kizárólag azok a Munkavállalók rendelkeznek hozzáférési jogosultsággal, akiknek az adott dokumentumok megismerése a munkavégzésükhöz nélkülözhetetlen: Adatkezelő munkaügyi feladatokat ellátó munkavállalói, valamint az érintett felett munkáltatói jogot gyakorló személy(ek)

Munkavállaló köteles az adataiban bekövetkezett változásokat haladéktalanul bejelenteni Munkáltató felé.

1.2 Önéletrajzokkal kapcsolatos adatkezelés

Az adatkezelés célja	Munkavállaló iskolai végzettségének és korábbi jogviszonyainak kezelése az adott feladatra történő alkalmasság igazolása céljából
Az adatkezelés jogalapja - GDPR 6. cikk (1)	b.) pont
A kezelt adatok köre	iskolai végzettség, korábbi jogviszonyok és a Munkavállaló (Érintett) által megadott egyéb adatok

Az adatok forrása	Munkavállaló
Az adatok tárolásának ideje	Jogviszony megszűnését követő 5 évig
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	Nincs
Profilalkotás vagy automatikus döntéshozatal	Nincs
Harmadik országba történő adattovábbítás	Nincs

1.3 Bérszámfejtéssel kapcsolatos adatkezelés

Az adatkezelés célja	Bérszámfejtés, bérkifizetés, szabadság és táppénz elszámolása
Az adatkezelés jogalapja - GDPR 6. cikk (1)	c) pont; - Mt. 10. §; 155. §; - az adózás rendjéről szóló 2017. évi CL. törvény 34. § (1) bekezdés és 50. §; - a társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fedezetéről szóló 2019. évi CXXII. törvény 66. §; - a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény 43. § (3) bekezdés és 96. §; - a személyi jövedelemadóról szóló 1995. évi CXVII. törvény 2. § (2) bekezdés, 3. § 8. pont; 12/B §, 15. §
A kezelt adatok köre	Név, cím, TAJ szám, adóazonosító jel, állampolgársága, lakcímkártya száma, házastárs neve, adóazonosító jele, házasságkötés ideje, tartós betegség igazolások, anyja neve, születési hely, idő, lakcímkártya szám, személyigazolvány száma, bankszámla száma, törzsszám (nyugdíjas munkav.), munkabér összege, munkaórák száma, jogviszony kezdete, táppénzen töltött napok száma és egyéb, jogszabály által előírt személyes adatok, gyermekek száma, gyermekek adóazonosító jele, TAJ száma, szül. hely, idő, anya-apa neve, neme.
Az adatok forrása	Munkavállaló (Érintett)
Az adatok tárolásának ideje	Az öregségi nyugdíjkorhatár betöltését követő 5 évig
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	Adott esetben, ha szükséges a továbbítás a jogi képviseletet ellátó ügyvéd, illetékes bíróság, jogszabályban megnevezett hatóságok felé.
Profilalkotás vagy automatikus döntéshozatal	Nincs
Harmadik országba történő adattovábbítás	Nincs

1.4 Munkavédelmi és tűzvédelmi oktatással kapcsolatos adatkezelés

Az adatkezelés célja	Munkabalesetek és tűzesetek megelőzése, a Munkavállaló védelme és veszélyhelyzetekre történő figyelemfelhívása érdekében oktatási tevékenység, valamint annak dokumentálása
Az adatkezelés jogalapja - GDPR 6. cikk (1)	c) pont; a munkavédelemről szóló 1993. évi XCIII. törvény 55. §
A kezelt adatok köre	Név, oktatás ideje, aláírás
Az adatok forrása	Oktatási jegyzőkönyv
Az adatok tárolásának ideje	Törvényi előírás szerint, általános elévülési időn belül (5 év)
Adatfeldolgozó	A Munkáltató által megbízott munkavédelmi, munkaügyi szakértő
Adattovábbítás címzettjei	Adott esetben, ha szükséges a továbbítás a jogi képviseletet ellátó ügyvéd, illetékes bíróság, jogszabályban megnevezett hatóságok felé.
Profilalkotás vagy automatikus döntéshozatal	Nincs
Harmadik országba történő adattovábbítás	Nincs

1.5 Munkavállalói alkalmassági orvosi vizsgálattal kapcsolatos adatkezelés

Az adatkezelés célja	Munkavállaló munkavégzésre való alkalmasságának felmérése
Az adatkezelés jogalapja - GDPR 6. cikk (1)	c) pont; a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendelet 15. §
A kezelt adatok köre	Név, beosztás, alkalmasság (igen/nem)
Az adatok forrása	A Munkáltató által megbízott foglalkozás-egészségügyi orvos
Az adatok tárolásának ideje	Az alkalmassági vizsgálat érvényességéig (1 év)
Adatfeldolgozó	Foglalkozás-egészségügyi orvos
Adattovábbítás címzettjei	Adott esetben, ha szükséges a továbbítás a jogi képviseletet ellátó ügyvéd, illetékes bíróság, jogszabályban megnevezett hatóságok felé.
Profilalkotás vagy automatikus döntéshozatal	Nincs
Harmadik országba történő adattovábbítás	Nincs

1.6 Munkahelyi balesethez kapcsolódó adatkezelés

Az adatkezelés célja	Munkahelyi baleset körülményeivel kapcsolatos jogi kötelezettségek teljesítése
Az adatkezelés jogalapja	c) pont; Mt. 10. §; a munkavédelemről szóló 1993. évi XCIII. törvény 64. §, 64/A §, 64/B §

A kezelt adatok köre	A sérült neve, címe, telefonszáma, baleset dátuma, időpontja, érülés és a baleset leírása, elsősegélyt nyújtó neve, tanú neve, elérhetősége, baleset helyszíne
Az adatok forrása	Baleseti jegyzőkönyv
Az adatok tárolásának ideje	A munkabaleseti jegyzőkönyv keletkezését követő 5 évig
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	Adott esetben, ha szükséges a továbbítás a jogi képviseletet ellátó ügyvéd, illetékes bíróság, munkavédelmi hatóság (kormányhivatal), és a NAV.
Profilalkotás vagy automatikus döntéshozatal	Nincs
Harmadik országba történő adattovábbítás	Nincs

1.7 Alkoholos vagy pszihotrop anyagok alatti befolyásoltság vizsgálatával kapcsolatban történő adatkezelés

A Munkavállalónak a munkaideje alatt alkoholos, illetve más pszichotrop anyag befolyásoltságtól mentesen kell munkáját végezni.

A munkáltatói jogkör gyakorlója vagy a képviseletében eljáró személy jogosult minden Munkavállalóját ellenőrizni, hogy alkoholos befolyásoltság hatása alatt áll-e, amennyiben alapos okkal feltehető, hogy a Munkavállaló alkoholos befolyásoltság alatt áll. A Munkáltató az alkoholszint mérését alkoholszondával a munkahelyen a munkavédelemért felelős Munkavállaló, valamint a Munkavállaló felettesének, a felettes akadályoztatása esetén más vezető beosztású Munkavállaló jelenlétében jogosult végrehajtani. Az ellenőrzés megtagadása esetén, amennyiben a Munkavállaló nyilvánvalóan munkavégzésre alkalmatlan állapotban van, úgy Munkáltató jogosult erről kettő tanú jelenléte mellett jegyzőkönyv felvételére, egyidejűleg a Munkavállalót a további munkavégzéstől el kell tiltani.

Az ellenőrzés során történő, az alkohol szonda 0,3%-ot kimutató elszíneződés esetén a Munkavállalót a további munkavégzéstől el kell tiltani, az adott nap igazolatlan hiányzásnak számít, munkabér nem jár, valamint az eset Munkáltatói figyelmeztetést von maga után.

Ismételt figyelmeztetéssel járó eset után Munkáltató jogosult a Munkavállaló munkaviszonyának azonnali hatályú megszüntetésére.

Amennyiben a Munkavállaló az eredményt vitatja, jogosult orvosi vizsgálatot kezdeményezni.

Az orvosi vizsgálatot Munkáltató nem akadályozhatja meg.

A vizsgálatok eredményét Munkáltató rögzíti és a pozitív és negatív eredményeket is a munkaviszony megszűnésekor törli. Munkáltató a vizsgálatok eredményeit nem adja át harmadik személyeknek, kivéve azt az orvost, aki az utólagos ellenőrzést végzi.

A pszihotrop anyagok alatti befolyásoltság alapos gyanúja esetén Munkáltató jogosult orvosi közreműködés igénybevételével ellenőrzést végezni. Az orvosi ellenőrzést Munkáltató kifejezett tiltakozása ellenére nem hajtható végre. Amennyiben a Munkavállaló nyilvánvalóan munkavégzésre alkalmatlan állapotban van, úgy Munkáltató jogosult erről kettő tanú jelenléte mellett jegyzőkönyv felvételére, és egyidejűleg a Munkavállaló munkavégzésének megtiltására. Ezen esetben a

Munkavállaló nem jogosult az aznapi bére megtérítésére. Az eset a Munkavállaló számára figyelmeztetéssel jár. A Munkáltató jogosult a második ismételt figyelmeztetés után Munkavállaló munkaviszonyának azonnali hatályú megszüntetésére. Az ellenőrzést megelőzően a Munkavállalónak lehetőséget kell biztosítani, hogy nyilatkozhasson a befolyásoltságról, amennyiben a befolyásoltságot elismeri, további orvosi vizsgálatot nem lehet elvégezni. A nyilatkozatot bizalmasan kell kezelni.

Amennyiben a Munkavállaló orvosi kezelés alatt áll, és emiatt következik be a pszichotrop anyag alatti befolyásoltság, úgy részére lehetőséget kell biztosítani, hogy hátrányos következmények nélkül felmentsék a munkavégzés alól.

Az adatkezelés célja	A Munkavállaló szabályszerű és biztonságos munkavégzésének ellenőrzése
Az adatkezelés jogalapja - GDPR 6. cikk (1)	c.) pont
A kezelt adatok köre	Munkavállaló neve, beosztása, az ellenőrzés eredményes
Az adatok forrása	Nyilvántartás, vizsgálat
Az adatok tárolásának ideje	A vizsgálati jegyzőkönyv keletkezését követő 5 évig
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	Adott esetben, ha szükséges a továbbítás a jogi képviseletet ellátó ügyvéd, illetékes bíróság, jogszabályban megnevezett hatóságok felé.
Profilalkotás vagy automatikus döntéshozatal	Nincs
Harmadik országba történő adattovábbítás	Nincs

1.8. Céges eszközhasználat ellenőrzése

1.8.1. E-mail fiók használatának ellenőrzésével kapcsolatos adatkezelés

Ha a Társaság e-mail fiókot bocsát a munkavállaló rendelkezésére – ezen e-mail címet és fiókot a munkavállaló kizárólag munkaköri feladatai céljára használhatja, annak érdekében, hogy a munkavállalók ezen keresztül tartsák egymással a kapcsolatot, vagy a munkáltató képviseletében levelezzenek az ügyfelekkel, más személyekkel, szervezetekkel.
A munkavállaló az e-mail fiókot személyes célra nem használhatja, a fiókban személyes leveleket nem tárolhat.
A munkáltató jogosult az e-mail fiók teljes tartalmát és használatát rendszeresen – 3 havonta - ellenőrizni, ennek során az adatkezelés jogalapja a munkáltató jogos érdeke. Az ellenőrzés célja az e-mail fiók használatára vonatkozó munkáltatói rendelkezés betartásának ellenőrzése, továbbá a munkavállalói kötelezettségek (Mt. 8.§, 52. §) ellenőrzése.
Az ellenőrzésre és adatkezelésre a munkáltató vezetője, vagy a munkáltatói jogok gyakorlója jogosult.
Amennyiben az ellenőrzés körülményei nem zárják ki ennek lehetőségét, biztosítani kell, hogy a munkavállaló jelen lehessen az ellenőrzés során.
Az ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre, munkáltató részéről ki végezheti az ellenőrzést, - milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete, - milyen jogai és jogorvoslati lehetőségei vannak az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

Az ellenőrzés során a fokozatosság elvét kell alkalmazni, így elsődlegesen az email címéből és tárgyából kell megállapítani, hogy az a munkavállaló munkaköri feladatával kapcsolatos, és nem személyes célú. Nem személyes célú e-mailek tartalmát a munkáltató korlátozás nélkül vizsgálhatja. Ha jelen szabályzat rendelkezéseivel ellentétben az állapítható meg, hogy a munkavállaló az e-mail fiókot személyes célra használta, fel kell szólítani a munkavállalót, hogy a személyes adatokat haladéktalanul törölje. A munkavállaló távolléte, vagy együttműködésének hiánya esetén a személyes adatokat az ellenőrzéskor a munkáltató törli. Az e-mail fiók jelen szabályzattal ellentétes használata miatt a munkáltató a munkavállalóval szemben munkajogi jogkövetkezményeket alkalmazhat.
A munkavállaló az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban e szabályzatnak az érintett jogairól szóló fejezetében írt jogokkal élhet.

A kezelt adatok köre: Munkavállaló neve, e-mail címe, ellenőrzés eredménye

Az adatkezelés jogalapja: A munka törvénykönyvéről szóló 2012. évi I. tv 8. §., 52. §, tehát jogi kötelezettség teljesítése (Rendelet 6. cikk (1) bek. c) pont)

Az adatkezelés időtartama: Az ellenőrzés tényéből származtatott jogok és kötelességek által megalapozott igények érvényesítési lehetőségeiből fakadó határidő.

1.8.2. Számítógép, laptop, tablet ellenőrzésével kapcsolatos adatkezelés

A Társaság által a munkavállaló részére munkavégzés céljára rendelkezésre bocsátott számítógépet, laptopot, tabletet a munkavállaló kizárólag munkaköri feladata ellátására használhatja, ezek magáncélú használatát a Társaság megtiltja, ezen eszközökön a munkavállaló semmilyen személyes adatot, levelezését nem kezelheti és nem tárolhatja. A munkáltató ezen eszközökön tárolt adatokat ellenőrizheti. Ezen eszközök munkáltató általi ellenőrzésére és jogkövetkezményire egyebekben az előbbi 1.8.1. pont rendelkezései irányadók.

1.8.3. A munkahelyi internethasználat ellenőrzésével kapcsolatos adatkezelés

A munkavállaló csak a munkaköri feladatával kapcsolatos honlapokat tekintheti meg, a személyes célú munkahelyi internethasználatot a munkáltató megtiltja.
A munkaköri feladatként az Adatkezelő nevében elvégzett internetes regisztrációk jogosultja az Adatkezelő, a regisztráció során az Adatkezelőre utaló azonosítót, jelszót kell alkalmazni. Amennyiben a személyes adatok megadása is szükséges a regisztrációhoz, a munkaviszony megszűnésekor azok törlését köteles kezdeményezni az Adatkezelő.
A munkavállaló munkahelyi internethasználat a munkáltató ellenőrizheti, amelyre és jogkövetkezményire az 1.8.1. pont rendelkezései irányadók.

1.8.4. Céges mobiltelefon használatának ellenőrzésével kapcsolatos adatkezelés

A munkáltató engedélyezi a céges mobiltelefon magáncélú használatát meghatározott költségtérítés megfizetése ellenében, így a mobiltelefon a továbbiakban nem csak munkavégzéssel összefüggő célokra használható. A munkáltató a kimenő – üzleti célú - hívások hívószámát és adatait, továbbá a mobiltelefonon üzleti célból tárolt adatokat ellenőrizheti.
A munkavállaló nem köteles külön bejelenteni a munkáltatónak, ha a céges mobiltelefont magáncélra is használta, de az ellenőrzéskor az üzleti és magáncélú használatot el kell különíteni. Az ellenőrzés akként folytatható le, hogy a munkáltató hívásrészletezőt kér a telefonszolgáltatótól és felhívja a munkavállalót arra, hogy a dokumentumon a magáncélú hívások esetében a hívott számokat tegye felismerhetetlenné.
Egyebekben az ellenőrzésre és jogkövetkezményire az 1.8.1. pont rendelkezései irányadóak.

1.9. Megváltozott munkaképességű munkavállalók

A megváltozott munkaképességű munkavállalókra adatkezelési szempontból azonos szabályok vonatkoznak, mint az Adatkezelő saját alkalmazottjaira, rájuk vonatkozóan azonban bővebb a kezelt adatok köre. Az Adatkezelő törvényi előírás alapján kezeli a megváltozott munkaképességű munkavállalók egészségi állapotára vonatkozó adatokat.

2. A Társaság tevékenységével kapcsolatos adatkezelések

2.1.

2.1. Étkeztetés biztosítása

Adatkezelő az Önkormányzattal létrejött szerződése alapján végzett közfeladatok ellátása körében étkeztetési szolgáltatást biztosít, mind kiskorú, mind nagykorú személyek részére.
Az étkeztetés igénybevétele során Adatkezelő az érintettek által kezdeményezett és általuk vagy rájuk tekintettel más személy által jogszerűen megadott információk alapján egyénre szabott diétás étrendnek, speciális étrendnek megfelelően teljesít. Továbbá az intézmények által biztosított étkeztetési szolgáltatás térítési díjait szedi be.

Az adatkezeléshez kapcsolódó közfeladat: A gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény (a továbbiakban: Gyvt.) 21. § (1) bek. e) pontja, valamint 21/A. § (3) bek. a) pontja alapján a települési önkormányzat feladata az iskolai gyermekétkeztetés biztosítása. A Gyvt. 21/B. § (1) bek. b)-d) pontjában, valamint a (2) bek. b) pontjában meghatározott esetben az intézményi gyermekétkeztetést ingyenesen, illetve kedvezményesen kell biztosítani.
Az adatkezeléshez kapcsolódó közfeladat: A Gyvt. 21/C. § (1) bekezdése alapján, valamint a szociális igazgatás és szociális ellátások helyi szabályozásáról szóló 10/2006 (VI: 28.) önkormányzati rendelet (a továbbiakban: Önk. r.) alapján szünidei gyermekétkeztetés biztosítása.

A speciális diétás étrend biztonságos nyújtását és kedvezmények nyújtását Adatkezelő külön orvosi vizsgálat és/vagy megfelelő orvosi igazolás nyújtásához kötheti.
Különleges (jelen esetben egészségügyi) adat esetén a GDPR 6. cikk (1) bekezdés e) pontja alapján, az adatok kezelése az Adatkezelő közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, valamint a GDPR 9. cikk (2) bek. h) pontja alapján az adatkezelés egészségügyi vagy szociális ellátás nyújtása érdekében szükséges.
Az adatkezelés a közétkeztetésre vonatkozó táplálkozás-egészségügyi előírásokról 37/2014. (IV. 30.) EMMI rendelet 15. §-a szerinti diétás étrend biztosítása érdekében szükséges.

Az Adatkezelő bármilyen a kiskorú érintettekkel összefüggő adatkezelést a kizárólag eljárni jogosult törvényes képviselő jóváhagyásának és/vagy utasításának megfelelően végez.

Az adatkezelés célja	étkeztetés biztosítása
Az adatkezelés jogalapja - GDPR 6. cikk (1)	e) pontja - az adatok kezelése az Adatkezelő közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.
GDPR 9. cikk (2)	h) pontja - az adatkezelés egészségügyi vagy szociális ellátás nyújtása érdekében szükséges.

A kezelt adatok köre	Szolgáltatást igénybe vevő neve, születési helye, ideje, anyja neve, lakcíme, látogatott intézmény neve, osztály/csoport elnevezése, az igénybe vevő diétája, igénybe vehető kedvezménye, támogatása, a törvényes képviselő neve, születési neve, születési helye, ideje, anyja neve, lakcíme, e-mail címe és telefonszáma.
Az adatok forrása	az érintett vagy törvényes képviselője
Az adatok tárolásának ideje	5 év – Ptk. szerinti általános elévülési idő
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	Veresegyház Önkormányzata és Polgármesteri Hivatala
Profilalkotás vagy automatikus döntéshozatal	nincs

2.2. Piacüzemeltetés

Adatkezelő az Önkormányzat megbízásából Veresegyház Város Főterén és a Fő utcán, illetve egyes mellékutcákat is érintve piaci napokat szervez. A standokon őstermelők és kereskedők árusítják portékáikat.
A standok bérletére Adatkezelő bérleti szerződést köt magánszemélyekkel és vállalkozásokkal.

2.2.1. Szerződést kötő természetes személy adatainak kezelése

Az adatkezelés célja	A piacon történő árusítás – stand bérlet
Az adatkezelés jogalapja - GDPR 6. cikk (1)	b) pontja - az adatkezelővel létrejött szerződéses jogviszony
A kezelt adatok köre	Név, anyja neve, születési hely és dátum, állampolgárság, telefonszám, e-mail cím, lakcím, levelezési cím, személyi igazolvány szám, adóazonosító jel.
Az adatok forrása	az érintett
Az adatok tárolásának ideje	a szerződés megszűnését követő 5 év – Ptk. szerinti általános elévülési idő
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	nincs
Profilalkotás vagy automatikus döntéshozatal	nincs

A nem magánszemélyként bérelt standokon való árusításhoz vállalkozási, valamint a veresegyházi piacra szóló működési engedély szükséges, a termékre vonatkozó piaci kereskedelmi engedélyek megléte mellett. A működési engedélyben megadott adatok körét a 210/2009. (IX.29.) Korm. rendelet határozza meg.

A nem magánszemély partnerek esetében a természetes személyek adatainak kezelése kizárólag a partner természetes személy kapcsolattartói vonatkozásában valósul meg.

2.2.2. Szerződésben megnevezett kapcsolattartók adatainak kezelése

Az adatkezelés célja	Az érintettel, mint a szerződést kötő alkalmazottjával vagy megbízottjával a kapcsolat tartása a szerződés teljesítése érdekében
Az adatkezelés jogalapja - GDPR 6. cikk (1)	f) pont – az adatkezelő jogos érdeke Az érintett az adatkezelés ellen bármikor tiltakozhat.
A kezelt adatok köre	név, telefonszám, e-mail cím
Az adatok forrása	a szerződést kötő személy
Az adatok tárolásának ideje	Adatkezelő az elérhetőségi adatokat amennyiben a szerződés létrejön a jogviszony megszűnését követő 5 évig – igényérvényesítési határidőig - kezeli
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	nincs
Profilalkotás vagy automatikus döntéshozatal	nincs

2.3. Általános üzemeltetési, karbantartási feladatok során történő adatkezelés

2.6.1. Üzemeltetéshez, karbantartáshoz vállalkozókkal kapcsolattartás

A természetes személy partnerrel az Adatkezelő közvetlenül köt szerződést.

Az adatkezelés célja	Az érintettel a kapcsolat tartása a szerződés teljesítése érdekében
Az adatkezelés jogalapja - GDPR 6. cikk (1)	b) pontja - az adatkezelővel létrejött szerződéses jogviszony
A kezelt adatok köre	Név, anyja neve, születési hely és dátum, állampolgárság, telefonszám, e-mail cím, lakcím, levelezési cím, személyi igazolvány szám, adóazonosító jel.
Az adatok forrása	az érintett
Az adatok tárolásának ideje	a szerződés megszűnését követő 5 év – Ptk. szerinti általános elévülési idő
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	nincs
Profilalkotás vagy automatikus döntéshozatal	nincs

A nem magánszemély partnerek esetében a természetes személyek adatainak kezelése kizárólag a partner természetes személy kapcsolattartói vonatkozásában valósul meg.

Az adatkezelés célja	Az érintettel, mint a szerződést kötő alkalmazottjával vagy megbízottjával a kapcsolat tartása a szerződés teljesítése érdekében
Az adatkezelés jogalapja - GDPR 6. cikk (1)	f) pont – az adatkezelő jogos érdeke Az érintett az adatkezelés ellen bármikor tiltakozhat.
A kezelt adatok köre	név, telefonszám, e-mail cím
Az adatok forrása	a szerződést kötő személy

Az adatok tárolásának ideje	Adatkezelő az elérhetőségi adatokat amennyiben a szerződés létrejön a jogviszony megszűnését követő 5 évig – igényérvényesítési határidőig - kezeli
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	nincs
Profilalkotás vagy automatikus döntéshozatal	nincs

2.4. Egyéb adatkezelések, igényérvényesítés, jogviták, hatósági eljárások

2.4.1. Panaszkezelés

Az adatkezelés célja	Kapcsolatfelvételi lehetőség adatkezelővel, panaszkezelés az adatkezelő szolgáltatásaival kapcsolatosan
Az adatkezelés jogalapja - GDPR 6. cikk (1)	c) pontja jogi kötelezettség alapján történő adatkezelés: a fogyasztóvédelemről szóló 1997. évi CLV. törvény 17/A. § értelmében
A kezelt adatok köre	E-mailben, a honlapon vagy közösségi oldalon keresztüli üzenetben történő megkeresés esetén az érintett azonosítási (név, cím) és kapcsolattartási adatai (e-mailcím, közösségi felhasználó azonosító), valamint az üzenet és a válasz tartalma. Telefonhívás esetén a rögzített telefonhívás, a hívás ténye és az elhangzott információk. Postai megkeresés esetén a panaszlevél és az alapján tett intézkedések, a megküldött válasz.
Az adatok forrása	érintett
Az adatok tárolásának ideje	Írásbeli panasz esetén a panasz felvételétől számított öt (5) év, telefonos szóbeli panaszról felvett jegyzőkönyv esetében a jegyzőkönyv felvételének napjától számított 5 év. A panaszról felvett jegyzőkönyvet és a válasz másolati példányát 3 évig őrizzük meg (Fgytv. 17/A. § (7) bek.)
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	nincs
Profilalkotás vagy automatikus döntéshozatal	nincs

2.4.2. Számlázással kapcsolatos adatkezelés

Az adatkezelés célja	A szerződéses ellenérték megfizetésével kapcsolatos adatkezelés
Az adatkezelés jogalapja - GDPR 6. cikk (1)	b) pontja - az adatkezelővel létrejött szerződéses jogviszony, valamint c) pont - az adatkezelőre vonatkozó jogi kötelezettség teljesítése - Számviteli tv. és Áfa tv. rendelkezései szerint
A kezelt adatok köre	A számlán szerepelő adatok: név és cím, igénybe vett szolgáltatás megnevezése, időpontja, mennyisége, vételára

Az adatok forrása	érintett
Az adatok tárolásának ideje	a számla kiállításának évét követő 8 év
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	nincs
Profilalkotás vagy automatikus döntéshozatal	nincs

2.4.3. Adatkezelés a szerződéses kötelezettség nem teljesítése esetén

Az adatkezelés célja	A szerződéses kötelezettségek nem teljesítése esetén a követelések érvényesítése céljából
Az adatkezelés jogalapja - GDPR 6. cikk (1)	f) pontja – az adatkezelő jogos érdeke Az érintett az adatkezelés ellen bármikor tiltakozhat.
A kezelt adatok köre	Név, születési hely és idő, anyja neve, cím, e-mail cím, telefonszám, a fennálló kötelezettség ténye és összege, illetve a keletkezésének körülményei, valamint a kapcsolattartás alatt váltott üzenetek tartalma és az üzenetre vonatkozó technikai információk
Az adatok forrása	érintett
Az adatok tárolásának ideje	az igény érvényesítés lehetőségének fennállásáig (általános elévülési idő – 5 év)
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	nincs
Profilalkotás vagy automatikus döntéshozatal	nincs

2.4.4. Jogviták rendezése során történő adatkezelés

Az adatkezelés célja	A jogviták, folyamatban lévő perekkel kapcsolatos adatkezelés azon esetekben releváns, ahol az adatkezelés eredeti jogalapja szerinti megőrzési idő lejárt, csak folyamatban lévő jogvita/per miatt szükséges a további adatkezelés
Az adatkezelés jogalapja - GDPR 6. cikk (1)	az adatkezelés eredeti jogalapjával azonos és f) pontja – az adatkezelő jogos érdeke Az érintett az adatkezelés ellen bármikor tiltakozhat.
A kezelt adatok köre	A jogvita vagy a per tárgyától függő adatok
Az adatok forrása	érintett vagy hatóság, hatósági megkeresés alapján
Az adatok tárolásának ideje	A jogvita vagy per végleges lezárását követő 1 évig
Adatfeldolgozó	jogi képviseletet ellátó ügyvéd
Adattovábbítás címzettjei	a jogvita eldöntésére illetékes és hatáskörrel rendelkező bíróság, hatóság
Profilalkotás vagy automatikus döntéshozatal	nincs

2.4.5. Marketingtevékenység során történő adatkezelés

Az adatkezelés célja	Közvetlen üzletszerzés érdekében a saját és partnerek ajánlatainak elküldése azok részére, akik ehhez hozzájárulásukat adják.
Az adatkezelés jogalapja - GDPR 6. cikk (1)	f) pontja – az adatkezelő jogos érdeke Az érintett az adatkezelés ellen bármikor tiltakozhat.
A kezelt adatok köre	Név, telefonszám, e-mail cím, lakcím
Az adatok forrása	érintett
Az adatok tárolásának ideje	az érintett tiltakozásáig
Adatfeldolgozó	a saját szerveren történő tárolás esetén az informatikai feladatokkal megbízott, illetve a Microsoft Corporation a levelező szerver tekintetében.
Adattovábbítás címzettjei	nincs
Profilalkotás vagy automatikus döntéshozatal	nincs

Veresegyház, 2025

VERESEGYHÁZI VÁROSGAZDA KFT.
2112 Veresegyház, Sport utca 4.
Bsz.: 10402991-50527087-51861010
Adószám: 32405741-2-13
15.

Kisák Péter
ügyvezető