A PORT-FAKTOR ZRT.
ADATVÉDELMI SZABÁLYZATA

Kibocsátó: Port-FAKTOR Zrt. Igazgatósága

Hatályos: 2022. szeptember 5. napjától

TARTALOMJEGYZÉK

CÍM ***OLDALSZÁM***

1. BEVEZETÉS 4

1.1 A SZABÁLYZAT CÉLJA 4

ADATKEZELÉSI ELVEK 4

1.2 A SZABÁLYZAT KEZELÉSE 5

2. A SZABÁLYZAT HATÁLYA 5

2.1 SZERVEZETI ÉS SZEMÉLYI HATÁLY 5

2.2 TÁRGYI HATÁLY 5

3. AJÁNLÁSOK, JOGSZABÁLYOK 6

4. FOGALOM MEGHATÁROZÁSOK ÉS RÖVIDÍTÉSEK 7

5. A TÁRSASÁG ÉS KÖRNYEZETE 10

A TÁRSASÁG ADATKEZELÉSI TEVÉKENYSÉGE 10

6. VEZETÉS 10

6.1 VEZETŐI ELKÖTELEZETTSÉG ÉS ADATVÉDELMI POLITIKA 10

6.2 SZERVEZETI SZEREPEK, FELELŐSSÉGEK ÉS HATÁSKÖRÖK 10

7. TERVEZÉS 12

7.1 ELŐZETES ADATGYŰJTÉS 12

7.2 ADATKEZELÉSI TERVEK 12

7.3 ADATVÉDELMI HATÁSVIZSGÁLAT 13

7.4 ÉRDEKMÉRLEGELÉSI TESZT 13

7.5 BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM 14

8. TÁMOGATÁS 16

8.1. FELKÉSZÜLTSÉG 16

8.2. TUDATOSSÁG 16

8.3. DOKUMENTÁLT INFORMÁCIÓK KEZELÉSE 16

9. MŰKÖDÉS 17

9.1. VÁLTOZÁSKEZELÉS 17

9.2. ADATVÉDELMI KÉPZÉS 17

9.3. AZ ADATKEZELÉS JOGSZERŰSÉGE 18

9.4. ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA 20

9.5. ÉRINTETTI JOGOK ÉRVÉNYESÍTÉSE 21

9.6. CÉLHOZ KÖTÖTTSÉG ÉS ADATTAKARÉKOSSÁG 21

9.7. PONTOSSÁG ÉS KORLÁTOZOTT TÁROLHATÓSÁG 21

9.8. INTEGRITÁS ÉS BIZALMAS JELLEG 22

9.9. SZERZŐDÉSEK KEZELÉSE 22

9.10. ADATTOVÁBBÍTÁS HARMADIK ORSZÁGOKBA 24

10. TELJESÍTMÉNYÉRTÉKELÉS 24

10.1. BELSŐ AUDIT 24

10.2. TESZTELÉS 24
11. FEJLESZTÉS 25
11.1. NEMMEGFELELŐSÉGEK, LEHETŐSÉGEK, JAVÍTÓ INTÉZKEDÉSEK 25

1. BEVEZETÉS

1.1 A Szabályzat célja

A Társaság jelen Szabályzat megalkotásával és hatályba léptetésével a **személyes adatok** törvényi követelményeknek és a Társaság üzleti stratégiájának megfelelő **kezelését biztosító szabályrendszert** hoz létre.
A Társaság a Szabályzat által meghatározott rendszer működtetésével a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.

A Szabályzat célja, hogy alkalmazásával a Társaság megfeleljen az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló általános adatvédelmi rendeletének (a továbbiakban: „**GDPR”**), és a személyes adatok kezelését érintő magyar jogszabályoknak.

Adatkezelési elvek

A Társaság a személyes adatok kezelésénél és az adatvédelmi intézkedéseinek megválasztásánál figyelembe veszi a **GDPR 5. cikk** szerinti adatkezelési elveket:

- **Jogszerűség, tisztességes eljárás és átláthatóság**
  - A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
- **Célhoz kötöttség**
  - A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon;
- **Adattakarékosság**
  - A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.
- **Pontosság**
  - A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék
- **Korlátozott tárolhatóság**
  - A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.
- **Integritás és bizalmas jelleg**
  - 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 adatkezelő elszámoltathatósága**
  - Az adatkezelő felelős a fenti hat elvnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

1.2 A Szabályzat kezelése

A Szabályzat gazdája

Jelen Szabályzat és mellékleteinek elkészítéséért, érvényes állapotban tartásáért és fejlesztéséért felelős a Társaság adatvédelmi tisztviselője.

A Szabályzat karbantartása

Jelen Szabályzatot **legalább évente**, vagy jogszabályi változásokat, illetve jelentős szervezeti változásokat követően át kell vizsgálni és aktualizálni kell.
A GDPR változása és/vagy a magyarországi vonatkozó jogszabályok változása esetén a Szabályzat aktualizálását teljes körűen és késedelem nélkül el kell végezni.

Végrehajtási felelősség

Jelen Szabályzatban meghatározott feladatok elvégzéséért, a folyamatok működtetéséért felelős személy a Társaság adatvédelmi tisztviselője.
A feladatok végrehajtása a legtöbb esetben az érintett **üzleti terület**en (beleértve a támogató folyamatokat is) felül a **jogi** és az **informatikai** (beleértve IT biztonság) területek szakemberinek bevonását is igényli. A szükséges kompetenciák bevonása a feladat végrehajtásáért felelős személy feladata.

2. A SZABÁLYZAT HATÁLYA

2.1 Szervezeti és személyi hatály

Jelen Szabályzat szervezeti hatálya kiterjed a Társaság minden szervezeti egységére.
Jelen szabályzat személyi hatálya kiterjed a Társaság által foglalkoztatott munkavállalókra, valamint olyan természetes vagy jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre, amelyek a Társaság informatikai rendszereivel, üzleti szolgáltatásaival jogviszonyba kerülnek, beleértve a vállalkozási/szolgáltatási/megbízási szerződéssel, vagy egyéb szerződéssel rendelkező szerződő partnereket.

2.2 Tárgyi hatály

Ezt a Szabályzatot kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik vagy a későbbiekben részévé kívánják tenni.

3. AJÁNLÁSOK, JOGSZABÁLYOK

A személyes adatok kezelésére vonatkozó törvényi előírások

GDPR

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (**EU) 2016/679 RENDELETE** (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

Info tv.

- **2011. évi CXII. törvény** az információs önrendelkezési jogról és az információszabadságról.

További törvények

- **2001. évi CVIII. törvény** az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- **2005. évi CXXXIII. törvény** a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
- **2013. évi CLXV. törvény** a panaszokról és a közérdekű bejelentésekről

A személyes adatok kezelésére vonatkozó ajánlások

EU Bizottsági iránymutatások a GDPR alkalmazásához, ARTICLE 29 WORKING PARTY

- **WP242** – Iránymutatás az adatok hordozhatóságáról;
- **WP243** – Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban;
- **WP244** – Iránymutatás az adatkezelő vagy az adatfeldolgozó fő felügyeleti hatóságának meghatározásához;
- **WP248** – Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e;
- **WP250** – Guidelines on Personal data breach notification under Regulation 2016/679;
- **WP251** –Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679;
- **WP253** – Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679;
- **WP259** – Guidelines on Consent under Regulation 2016/679;
- **WP260** - Guidelines on transparency under Regulation 2016/679.

Szabványok:

- **BS 10012:2017** Data protection – Specification for a personal information management system;
- **MSZ ISO/IEC 27001: 2014** Információbiztonság-irányítási rendszerek;
- **MSZ EN ISO/IEC 27002: 2017** Gyakorlati útmutató az információbiztonsági kontrollokhoz;
- **ISO/IEC 29134:2017** Guidelines for privacy impact assessment.

4. FOGALOM MEGHATÁROZÁSOK ÉS RÖVIDÍTÉSEK

A Szabályzat a GDPR-ban meghatározott fogalmakat használja a következők szerint:
„személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

„adatkezelés”: 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;

„az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

„profilalkotás”: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

„álnevesítés”: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

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

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

„címzett”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon

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

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

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

„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;

„genetikai adat”: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;

„biometrikus adat”: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;

„egészségügyi adat”: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

„képviselő”: az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

„vállalkozás”: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;

„felügyeleti hatóság”: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv;

„érintett felügyeleti hatóság”: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
c) panaszt nyújtottak be az említett felügyeleti hatósághoz;

„személyes adatok határokon átnyúló adatkezelése”:

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

„releváns és megalapozott kifogás”: a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve, hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;

„az információs társadalommal összefüggő szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv (1) 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás;

„nemzetközi szervezet”: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre.

5. A TÁRSASÁG ÉS KÖRNYEZETE

A Társaság adatkezelési tevékenysége

A Társaság az adatkezelési tevékenységet **önállóan** végzi.
A Társaság a GDPR meghatározása alapján **Adatkezelőnek** minősül, ugyanakkor bizonyos adatfeldolgozási tevékenységek kapcsán **Adatfeldolgozó**ként működik.

6. VEZETÉS

6.1 Vezetői elkötelezettség és adatvédelmi politika

A Társaság vezetése elkötelezett abban, hogy megfelelő intézkedéseket tegyen a természetes személyek személyes adatainak védelmében.
Ezen elkötelezettség jegyében a Társaság vezetése stratégiájával összhangban **adatvédelmi szabályrendszert** alakít ki, vezet be és működtet a mindenkor hatályos, az Európai Unió és Magyarország területén hatályos, irányadó jogszabályoknak és iránymutatásoknak megfelelően.
Az adatvédelmi szabályrendszer kialakításának és a Társaság adatvédelmi működésének legfontosabb elveit a szervezet **ügyvezetője** által kiadott adatvédelmi politika határozza meg. A Társaság gondoskodik arról, hogy az adatvédelmi politikát a Társaság minden jelenlegi és leendő munkatársa megismerje, részükre hozzáférhető legyen.
A Társaság vezetése biztosítja az adatvédelmi szabályrendszer céljainak megvalósulásához szükséges erőforrásokat, közvetlenül támogatja az adatvédelmi szabályrendszer működését biztosító személyek munkáját és a szabályrendszer folyamatos fejlesztését.

6.2 Szervezeti szerepek, felelősségek és hatáskörök

A Társaság igazgatósága közvetlen és szamon kérhető felelősséggel tartozik azért, hogy a személyes adatok kezelése megfeleljen a jogszabályi előírásoknak és a jelen Szabályzatban meghatározott vállalati elvárásoknak.
Ezt a felelősséget a **munkaköri leírásban** szükséges meghatározni.

A Társaság **adatvédelmi tisztviselőt** jelöl ki.
Az adatvédelmi tisztviselő hatáskörét, felelősségét és feladatait a munkaköri leírása vagy megbízási szerződése tartalmazza.
A Társaság biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.
A Társaság támogatja az adatvédelmi tisztviselőt feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.
A Társaság biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható.
Az adatvédelmi tisztviselő közvetlenül a Társaság igazgatóságának tartozik felelősséggel.

Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban a személyes adatok kezelésére vonatkozó titoktartási kötelezettség köti.
Amennyiben az adatvédelmi tisztviselő más feladatokat is ellát, a Társaság biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

A Társaság adatvédelmi tisztviselőjének neve és elérhetősége:
Neve: Marton Adorján
E-mail címe: info@portfaktor.hu
Telefonszáma: +36 20 330 3308

Adatgazdák

Az adatkezelési tevékenységek felelőseit adatgazdáknak nevezzük.
Az adatgazdák azok az üzleti/szakterületi vezetők, aki üzleti folyamataik működtetése során személyes adatokat kezelnek és az adatkezelési tevékenységek nyilvántartásában meghatározott **konkrét adatkezelési tevékenységekhez vannak rendelve, mint felelősök**.
Az adatgazdák hatáskörét, felelősségét és feladatait a munkaköri leírásuk tartalmazza.

Adatkezelésre feljogosított személyek:
A Társaság azonosítja azokat a személyeket, akik munkájuk során **nagy mennyiségben, szisztematikusan** dolgoznak személyes adatokkal.
A Társaság gondoskodik arról, hogy ezek az adatkezelésére feljogosított személyek kifejezetten a személyes adatok kezelésére vonatkozó titoktartási kötelezettséget vállaljanak.

Információbiztonsági felelős:
A Társaság az információbiztonsági intézkedések megfelelő menedzselése érdekében információbiztonsági felelőst neveznek ki.
Az információbiztonsági felelős hatáskörét felelősségét és feladatait a munkaköri leírása vagy megbízási szerződése tartalmazza.

7. TERVEZÉS

7.1 Előzetes adatgyűjtés

Az üzleti folyamatok és adatok nyilvántartásba vétele

A Társaság célja, hogy egyértelműen beazonosítsa és nyilvántartsa az üzleti folyamatai kapcsán kezelendő (kapott, küldött, feldolgozott, továbbított stb.) adatokat.
Ez a nyilvántartás szorosan és logikusan kapcsolódik az informatikai vagyonleltárhoz, ezért is tartalmazza a **személyes adatok**on felül a **Bizalmas minősítésű** (de nem személyes) **adatok**at is.
A kiindulás a szervezeti felépítés és az üzleti folyamatok. Ezek alapján határozzuk meg a felelősöket, ők az adatgazdák, akik a saját területükön kezelt adatokat azonosítják, és kitöltik a táblázatot.
Az adatok nyilvántartásba vételénél adat-csoportokat képzünk a funkcionálisan és logikusan összekapcsolható adatokból.
A Társaság a személyes adatokról nyilvántartást vezet. A Társaság törekszik arra, hogy a nyilvántartásba vett vagyonelemek ne legyenek túl nagyok (általánosítás veszélye) vagy túl kicsik (elaprózás, nehéz nyomon követhetőség).

Adattovábbítás címzettjeinek nyilvántartása

A Társaság az adattovábbítás címzettjeiről nyilvántartást vezet, itt tartja nyilván azokat a címzetteket, akinek személyes adatokat ad át.
A címzettek három fő csoportba sorolandóak:

- adatfeldolgozók – akik a Társaság személyes adatait kizárólag a Társaság írásos utasítása alapján kezelik;
- közös adatkezelők – akik a Társasággal közösen döntenek az adatkezelés céljáról és eszközeiről;
- harmadik felek – mindenki más, akinek a Társaság személyes adatokat ad át és nem tartozik az előző két csoportba, és nem azonos az érintettel.

Adatkezelési tevékenyégek azonosítása

Az üzleti folyamatokhoz kapcsolódóan az adatgazdák azonosítják az adatkezelési tevékenységeket, oly módon, hogy meghatározzák azok célját és azonosítóját, és ezeket az adatokat a Társaság az adatkezelési tevékenységek nyilvántartásában rögzíti.
Az adatkezelési tevékenység azon adatkezelési műveletek összessége, amelyeknek egy adott célja van. A célok ne legyenek se elnagyoltak, se túlzottan lebontottak.

Felelős:	adatgazda
Végrehajtásban részt vesz:	adatvédelmi tisztviselő

7.2 Adatkezelési tervek

Az előző pontban azonosított adatkezelési tevékenységek adatkezelési folyamatait részletesen meg kell tervezni, ennek érdekében a Társaság adatkezelési terveket készít:

- annyi önálló adatkezelési terv készül, ahány adatgazdája van a Társaságnak,
- az adatkezelési tervek elkészítéséért az adatgazdák felelősek (mindenki a sajátjáért),
- az adatvédelmi tisztviselő részvétele a tervezésben kötelező,

- az Adatkezelési terveket a felső vezetésnek jóvá kell hagynia.

Az adatkezelési terv célja:

- egyrészről, hogy a Társaság pontos, részletes és ellenőrzött nyilvántartással rendelkezzen az egyes adatkezelési tevékenységek során kezelt személyes adatokról,
- másrészről, hogy a terv pontosan meghatározza az adatkezelés kereteit.

A fentiekben foglaltaknak megfelelően a Társaságnál **a személyes adatok kezelése csak a jóváhagyott adatkezelési tervekben meghatározottak szerint történhet**.
Amennyiben új adatkezelésre van szükség (pl. üzletfejlesztés okán) vagy a meglévő adatkezelési folyamatot módosítani szükséges, a tervezési és jóváhagyási folyamatot minden esetben ismételten végre kell hajtani.
Az adatkezelési tervek készítése szorosan kapcsolódik a következő fejezetekben tárgyalt **adatvédelmi hatásvizsgálat**hoz és **érdekmérlegelési teszt**hez, amelyek megállapításait, a feltárt kockázatokat figyelembe kell venni az adatkezelési tervek elkészítésekor.

Felelős:	adatgazda
Végrehajtásban részt vesz:	adatvédelmi tisztviselő

7.3 Adatvédelmi hatásvizsgálat

A személyes adatok kezelése kockázatokkal járhat a természetes személyek alapvető jogaira és szabadságaira és különösen a személyes adatok védelméhez való jogukra nézve, ezért a Társaság az **adatkezelés megkezdése előtt**, az adott adatkezelés vonatkozásában **mérlegeli a kockázatokat** és ennek megfelelően hoz döntést az adatkezelési tevékenységről.
Az adatkezelési tevékenységek kockázatértékelése a Társaság adatvédelmi hatásvizsgálat szabályzata alapján történik.
Az adatkezelési tevékenységek esetében a kockázatértékelést az adatkezelés megkezdése előtt el kell végezni és az adatkezelést csak a kockázatértékelésből következő kockázatcsökkentő intézkedések bevezetését követően szabad megkezdeni.

Felelős:	adatvédelmi tisztviselő
Végrehajtásban részt vesz:	adatgazda

7.4 Érdekmérlegelési teszt

Az érdekmérlegelési teszt annak írásbeli dokumentálása, hogy a Társaság által „jogos érdek” jogalapra (GDPR 6. cikk (1) bekezdésének f) pontja) hivatkozással tervezett adatkezelésre miért van szükség, hogyan is végezné azt, és milyen – az érintettek érdekeit védő – garanciákat épített be az adatkezelés folyamatába.
Az érdekmérlegelési tesztet **minden olyan esetben el kell végezni, amikor az adatkezelés jogalapja** az adatkezelő vagy egy harmadik fél **jogos érdek**e érvényesítéséhez szükséges. Annyi érdekmérlegelési tesztet kell elvégezni, ahány jogos érdek jogalapú adatkezelési tevékenység van a Társaságnál.
Az érdekmérlegelés tesztet a Társaság által készített érdekmérlegelési teszt elnevezésű dokumentum kitöltésével kell elvégezni. A tárgyi dokumentumban megadottakat kell részletesen kifejteni és az

összes feltárt szempont, érv és ellenérv mérlegelésével döntést hozni az adatkezelés alkalmazhatóságáról.
Amennyiben az érdekmérlegelési teszttel nem bizonyítható, hogy az adatkezelő (illetve a harmadik fél) jogos érdeke elsőbbséget élvez az érintett érdekeivel és jogaival szemben, az adatkezelési tevékenység nem végezhető el.
Pótlólagos szervezési és technikai intézkedésekkel adott esetben csökkenthető az érintett alapvető jogait és szabadságait érintő kockázat, ezáltal az érintett érdeke és a Társaság érdeke egyensúlyba hozható, és az adatkezelés alkalmazható.

7.5 Beépített és alapértelmezett adatvédelem

A Társaság végrehajtja a megfelelő **technikai és szervezési intézkedések**et annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek (GDPR 25. cikk).

7.5.1. Szervezési intézkedések

A szervezési intézkedések keretét jelen Szabályzat és a hozzá kapcsolódó szabályzatok alkotják.
Az adatkezelési tevékenységhez kapcsolódó adatkezelési folyamatlépések tervezése, működtetése és folyamatos fejlesztése során a következőket kell figyelembe venni:

- jelen adatvédelmi szabályrendszer
- az adatvédelmi hatásvizsgálatból következő intézkedések
- az incidensek elemzéséből következő incidensek
- a nemmegfelelőségek és lehetőségek elemzéséből származó javító intézkedések.

Az adatkezelési folyamatok:

- egy része az adatkezelési tevékenységre feljogosított **személyek által végzett munka**,
- a másik része az **informatikai rendszer**ben megvalósított automatizált, vagy kezelői beavatkozással megvalósuló **folyamatok**.

Az adatkezelési folyamatok megtervezése során meghatározásra kerülnek a következő szervezési intézkedések:

- **munkaköri leírások**, amelyek a személyes adatok kezeléséhez kapcsolódó jogosultságok és felelősségeket pontosítják,
- a **munkautasítások**, amelyek az emberi tevékenységeket határozzák meg és
- az **informatika rendszerrel szembeni elvárások.**

Felelős:	adatgazda
Végrehajtásban részt vesz:	adatvédelmi tisztviselő informatikai vezető

7.5.2. Technikai intézkedések

Az informatikai rendszerre vonatkozó technikai intézkedések megtervezésének kiindulópontja az szervezési intézkedések tervezése során meghatározott „informatika rendszerrel szembeni elvárások”.

Ezen elvárások alapján kell első lépésben az elvárt informatikai fejlesztések megvalósíthatóságát megvizsgálni. Az elvárások megvalósíthatóságának értékelése alapján a Társaság döntést hoz, hogy

- mely informatikai fejlesztések valósíthatók meg az adatkezelési tevékenység megkezdéséig,
- és melyek csak később,
- vagy esetleg egyáltalán nem.

A kiértékelési, döntési folyamatba az adatgazdákat be kell vonni, mert a késedelmesen vagy egyáltalán nem megvalósuló informatikai fejlesztések az adatkezelésre vonatkozó emberi tevékenységek (munkautasítások) módosításának szükségességét vonhatják maguk után.

A szervezési és a technikai intézkedéseknek együttesen le kell fedniük az adatkezelés teljes folyamatát és meg kell felelniük az adatvédelmi követelményeknek.
A kisebb erőforrást igénylő, és rövid időn belül megvalósítható fejlesztéseket el kell végezni az adott adatkezelési tevékenység megkezdése előtt.
Azok a fejlesztések, amelyek nem elvégezhetők az adatkezelési folyamat megkezdéséig, de jövőbeli megvalósításuk tervezett, bekerülnek a Társaság által vezetett javító intézkedések nyilvántartásába, mint tervezett intézkedések.

Felelős:	informatikai vezető
Végrehajtásban részt vesz:	adatgazda, adatvédelmi tisztviselő

7.5.3. Információbiztonsági intézkedések

Az információbiztonsági intézkedések azok a technikai és szervezési intézkedések, amelyek a Társaság információs vagyonának, és ezen belül kiemelten a személyes adatoknak a **bizalmas jellegét**, az **integritását** és a **rendelkezésre állását** biztosítják.
A Társaság információbiztonsági intézkedéseit az Informatikai biztonsági szabályzat tartalmazza.

Felelős:	információbiztonsági felelős
Végrehajtásban részt vesz:	adatgazda, adatvédelmi tisztviselő

8. TÁMOGATÁS

8.1. Felkészültség

Az adatvédelmi tisztviselő és az adatgazdák esetében a szükséges szakmai felkészültséget a munkatársak munkaköri leírásában vagy a megbízási szerződésükben kell meghatározni.

Elvárás az adatvédelmi tisztviselő és az adatgazdák esetében:

- évente egy alkalommal a Társaság által biztosított adatvédelmi oktatáson való részvétel;
- a tárgyi Szabályzat ismerete.

Felelős:	Ügyvezető
Végrehajtásban részt vesz:	HR vezető

8.2. Tudatosság

A Társaság felügyelete alatt munkát végző személyeknek tudatában kell lenniük a következőknek:

- a Társaság adatvédelmi politikájával és adatvédelmi elvárásaival,
- szerepükkel az adatvédelmi rendszer működtetésében,
- az adatkezelésre vonatkozó szabályok megszegésének lehetséges következményeivel.

A Társaság irányítása alatt munkát végző személyeknek rendszeres adatvédelmi tudatossági képzésben kell részesülniük a jelen Szabályzatban foglaltak szerint.

8.3. Dokumentált információk kezelése

A Társaság az adatvédelmi szabályzási rendszer támogatása céljából dokumentált információkat hoz létre és tart fenn. A dokumentált információk lehetnek papíralapúak, illetve elektronikus dokumentumok.

A dokumentált információk karbantartása, megőrzése biztosítja a Társaság számára, hogy teljesítse az „elszámoltathatóság” követelményét (GDPR 5. cikk (2) bekezdése).

A dokumentumoknak egyértelmű azonosíthatósága érdekében minden dokumentumnak legyen:

- azonosító kódja, elnevezése (címe),
- jóváhagyója, felelőse (gazdája),
- verziókövetése.

A dokumentumokkal kapcsolatosan (ahol relevánsak) meghatározásra kerülnek a következők:

- hozzáférők köre
- átvizsgálásra vonatkozó utasítás
- tárolási követelmények, megőrzési idő

Az adatvédelmi szabályozáshoz kapcsolódó dokumentumok kapcsán a Társaság nyilvántartást vezet.

Felelős:	adatgazda
Végrehajtásban részt vesz:	adatvédelmi tisztviselő

9. MŰKÖDÉS

9.1. Változáskezelés

A Társaság folyamatosan figyelemmel kíséri az adatkezelési tevékenységeket érintő változásokat:

- Az **adatvédelmi tisztviselő** feladata, hogy beazonosítsa azokat a **jogszabályi változások**at, amelyek hatással lehetnek az adatkezelési tevékenységnek a természetes személyek jogait és szabadságait érintő kockázataira.
- Az adatkezelési tevékenységért felelős **adatgazdák** feladata, hogy beazonosítsák azokat a **szervezési és technikai változások**at, amelyek hatással lehetnek az adatkezelési tevékenységnek a természetes személyek jogait és szabadságait érintő kockázataira.
- Az **információbiztonsági felelős** feladata, hogy beazonosítsa azokat az **információbiztonságot érintő** szervezési és technológiai **változások**at, amelyek hatással lehetnek az adatkezelési tevékenységnek a természetes személyek jogait és szabadságait érintő kockázataira.

9.2. Adatvédelmi képzés

A Társaság irányítása alatt munkát végző személyek rendszeres, differenciált adatvédelmi képzésben részesülnek az adatkezeléssel való kapcsolatuk és az ebben rejlő kockázatok alapján.

9.2.1. Képzési tematikák:

Adatvédelmi tisztviselő képzés

Több napos, személyes oktatás, amely a felkészíti az adatvédelmi tisztviselőt munkája elvégzésére.

Adatvédelmi oktatás adatgazdáknak

Egy napos személyes oktatás, amely a felkészíti az adatvédelmi felelőst és az adatgazdákat a személyes adatok kezelésével kapcsolatos feladataikra.

Általános adatvédelmi tudatossági képzés

GDPR alapok – elektronikus oktatási anyag.

9.2.2. Képzési program

A képzéseket rendszeres kell végezni a következők szerint:

- új belépők: a munkába állást követően a lehető legrövidebb időn belül
- minden érintett: évente megismételve
- adatvédelmi tisztviselő és adatgazdák: a tárgyi Szabályzat változtatását követően 4 (négy) héten belül.

Minden lehetséges esetben az elért tudásszintet ellenőrző kérdésekkel és/ vagy vizsgával ellenőrizni kell.

Az oktatások szervezettségének és megvalósíthatóságának biztosítása érdekében a Társaság legalább egy éves előre tartással adatvédelmi képzési programot készít, melyről nyilvántartást vezet. A fentiekben foglalt képzési program nyilvántartás egyben a megvalósult képzések nyilvántartása is.

Felelős:	HR vezető
Végrehajtásban részt vesz:	adatvédelmi tisztviselő

9.3. Az adatkezelés jogszerűsége

A Társaság a személyes adatok kezelését csak akkor végzi, ha a GDPR 6. cikk (1) bekezdésében megadott hat jogalap közül, legalább az egyik alkalmazható, illetve különleges adatok kezelése esetében, amennyiben a GDPR 9. cikk (2), (3) és (4) bekezdésében foglalt feltételek teljesülnek.
A jogalapok meghatározásának felelőssége:

Felelős:	adatgazda
Végrehajtásban részt vesz:	adatvédelmi tisztviselő

Gyermekek személyes adatainak kezelése (GDPR 8. cikk):
A 16. életévét be nem töltött gyermek esetén, a **gyermekek személyes adatainak kezelése** csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte. A Társaság – figyelembe véve az elérhető technológiát – észszerű erőfeszítéseket tesz, hogy ilyen esetekben ellenőrizze, hogy a hozzájárulást a gyermek feletti szülői felügyeleti jog gyakorlója adta meg, illetve engedélyezte.
A személyes adatok különleges kategóriái (GDPR 9. cikk (1) bekezdés):
Különleges adatok a következők: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
A Társaság a **személyes adatok különleges kategóriáit** csak a legszükségesebb, elkerülhetetlen esetekben kezeli.
A személyes adatok különleges kategóriáinak kezelése esetén biztosítani kell, hogy a jogalap ki legyen egészítve a GDPR 9. cikk (2), (3) és (4) bekezdésében meghatározott releváns adatokkal.

9.3.1. Hozzájárulás jogalap alkalmazása

GDPR 6. cikk (1) bekezdés a) pontja: *„az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;"*
Az érintetti hozzájáruláson alapuló adatkezelést megelőzően az érintettet tájékoztatni kell a releváns adatkezelési tájékoztató rendelkezésre bocsátásával. A tájékoztatásnak ugyanazon a csatornán, a hozzájárulás kérésével egyidőben kell megtörténnie.

Hozzájárulási nyilatkozat
A hozzájárulási nyilatkozatnak – függetlenül annak megjelenési formájától – teljesítenie kell a következő feltételeket:

- legyen egyértelmű,
- más ügyektől elkülöníthető,
- érhető, világos, egyszerű nyelvezetű.

A hozzájárulás érvényességének feltétele az önkéntesség, ezért

- az „*érintett hozzájárulása jogalap*” **munkavállalók esetében nem alkalmazható** (a jogi függőség miatt az önkéntesség nem biztosítható) és
- annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, hogy a szerződés teljesítésének feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

Hozzájárulás visszavonása

Az érintett az adatkezeléshez való hozzájárulását bármikor visszavonhatja, erről a jogáról, illetve a visszavonás módjáról a hozzájárulási nyilatkozatban vagy az ezzel egyidőben átadott adatkezelési tájékoztatóban kell tájékoztatni.

A hozzájárulás visszavonásának olyan egyszerűnek kell lenni, mint amilyen a hozzájárulás megadása.

A hozzájárulás visszavonásához alternatív csatornát is kell biztosítani, és erről az érintettet tájékoztatni kell.

A hozzájárulások meglétét és a visszavonást követő intézkedéseket a Társaságnak igazolni kell tudni, ennek megfelelően a szükséges szervezési és technikai intézkedéseket a Társaság megteszi.

9.3.2. Szerződéses jogalap alkalmazása

GDPR 6. cikk (1) bekezdés b) pontja: *„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;”*

Jogi személyekkel (vállalkozások, céges ügyfelek) kötött szerződések esetében ez a jogalap **nem használható**.

Szerződéskötésre irányuló közvetlen cselekmények esetében (ajánlatkérés, ajánlatadás, szerződéses feltételek egyeztetése) ez a jogalap alkalmazandó.

9.3.3. Jogi kötelezettség jogalap alkalmazása

GDPR 6. cikk (1) bekezdés c) pontja: *„az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;”*

Tipikus jogszabályi kötelezettségek: a számvitelről szóló 2000. évi C. törvényben, az adózás rendjéről szóló 2017. évi CL. törvényben, és a munka törvénykönyvről szóló 2012. évi I. törvényben stb. foglalt jogszabályi kötelezettségek. A jogi kötelezettségre hivatkozva csak azokat a személyes adat kategóriákat szabad tárolni, amelyeket az adott jogszabály előír, azokat viszont kötelező.

A jogi kötelezettség jogalap alkalmazása estében kötelező a Társaság adatvédelmi tisztviselőjének egyetértését megszerezni.

9.3.4. Létfontosságú érdek jogalap alkalmazása

GDPR 6. cikk (1) bekezdés d) pontja: *„az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;”*

A Társaság a létfontosságú érdek jogalapot **nem alkalmazza** a személyes adatkezelési tevékenységei során.

9.3.5. Közhatalmi jogosítvány jogalap alkalmazása

GDPR 6. cikk (1) bekezdés e) pontja: *„az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;"*

A Társaság a közhatalmi jogosítvány jogalapot **nem alkalmazza** a személyes adatkezelési tevékenységei során.

9.3.6. Jogos érdek jogalap alkalmazása

GDPR 6. cikk (1) bekezdés f) pontja: *„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, különösen, ha az érintett gyermek;"*

Jogos érdek jogalap alkalmazását megelőzően a Társaság mérlegeli, hogy az adott adatkezelés esetében az érintett alapvető jogai és szabadságai és különösen a személyes adatok védelméhez való joga milyen mértékben sérülhet, és ezt összeveti saját érdekével, amely az adatkezelést szükségessé teszi.

Közvetlen üzletszerzés

A GDPR preambulum (47) alapján a személyes adatok közvetlen üzletszerzési célú kezelése jogos érdeken alapulónak tekinthető, tehát a Társaság adott esetben **érdekmérlegelési teszt elvégzése nélkül** alkalmazza az *„adatkezelő jogos érdeke"* adatkezelési jogalapot a **közvetlen üzletszerzés**t szolgáló marketing tevékenységeihez (hírlevelek, rendezvények stb.).

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett számára biztosítani kell a jogot arra, hogy bármikor díjmentesen tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen. Az érintett figyelmét e jogra kifejezetten fel kell hívni, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Más adatkezelési célok

Más adatkezelési célok esetében, különösen a munkavállalók (vagy más érintettek) megfigyelése esetében, az „*adatkezelő jogos érdeke*" adatkezelési jogalap alkalmazhatóságáról a Társaság az adatkezelési tevékenység megkezdése előtt elvégzett érdekmérlegelési teszt eredménye alapján dönt.

9.4. Adatkezelési tevékenységek nyilvántartása

A Társaság a GDPR 30. cikk (1) bekezdése alapján elkészíti az adatkezelőként végzett adatkezelési tevékenységek nyilvántartását.

Az adatkezelési tevékenységek azonosítása a tervezési fázisban történik.

A Társaság a GDPR 30. cikk (2) bekezdése alapján elkészíti az adatfeldolgozóként végzett adatkezelési tevékenységek nyilvántartását.

A nyilvántartást a releváns adatfeldolgozási szerződésekben megadott szerződéses rendelkezések alapján kell elkészíteni.

Az adatkezelési tevékenységek nyilvántartása csak azokat az adatokat tartalmazza, amelyek a GDPR 30. cikke alapján szükségesek, minden további nyilvántartást a Társaság ettől elkülönítve kezel.

Az adatkezelési tevékenységek nyilvántartását a Társaság naprakészen vezeti, és megkeresés alapján a felügyeleti hatóság (Nemzeti Adatvédelmi és Információszabadság Hatóság) rendelkezésére bocsátja.

Felelős:	adatgazdák
Végrehajtásban részt vesz:	adatvédelmi tisztviselő

9.5. Érintetti jogok érvényesítése

A Társaság fokozott figyelmet fordít arra, hogy a GDPR 12. - 23. cikkeiben meghatározott érintetti jogok érvényesítése megfeleljen a jogszabályi követelmények és az érintettek elvárásinak. A Társaság az érintetti jogok érvényesítésére vonatkozó szabályokról belső eljárásrendet készít.

9.6. Célhoz kötöttség és adattakarékosság

GDPR 5. cikk (1) bekezdés b) pontja: *„A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhoz kötöttség”);”*

GDPR 5. cikk (1) bekezdés c) pontja: *„A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”);”*

A Társaság személyes adatokat csak tisztességes, jól meghatározott, egyértelmű és jogszerű célból kezel.

A Társaság az adatkezelési tevékenységek megtervezése során gondoskodik arról, hogy a kezelt személyes adatok terjedelme (adatkategóriák számossága és típusa) csak a cél szempontjából releváns és szükséges mértékű legyen.

9.7. Pontosság és korlátozott tárolhatóság

9.7.1. Intézkedések a pontosság érdekében

GDPR 5. cikk (1) bekezdés d) pontja: „A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („pontosság”);”

A Társaság az adatkezelési tevékenysége során folyamatba épített ellenőrzéseket végez a kezelt személyes adatok pontosságának biztosítása érdekében.

Ahol, ez lehetséges az informatika rendszer a személyes adatok szintaktikai ellenőrzésével is támogatja a pontosságot.

A személyes adatokhoz való hozzáférés korlátozása és a hozzáférés ellenőrzése csökkenti az adatok véletlen vagy szándékos megváltoztatásának kockázatát.

9.7.2. Adatmegőrzés és adateltávolítás

GDPR 5. cikk (1) bekezdés e) pontja: *„A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási*

célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („korlátozott tárolhatóság”);

Az adatkezelési tevékenységek tervezése során részletesen és konkrétan meghatározásra kerülnek az adatkezelés jogalapjai. Az adatbázisokban, illetve az adatfájlokban tárolt személyes adatok megőrzési idejét a jogalapok határozzák meg. Ennek megfelelően a személyes adatokat **a jogalap által meghatározott ideig kötelezően meg kell őrizni**, **azt követően** – amennyiben nincs más jogalapja az adatkezelésnek – a személyes adatot, illetve az adatrekordot **törölni kell**.

Az adatkezelés céljának megszűnése esetén – amennyiben nincs jogszabályi kötelezettség jogalapja az adatkezelésnek – törölni kell az adott céllal kezelt adatokat.
Az adatkezelési cél megváltozását vagy megszűnését az adatgazdának kell figyelemmel kísérni és adott esetben ennek megfelelően intézkedni az adatok törléséről.

A jogalapok változási lehetőségei:
- jogszabályi változások,
- érintetti jogok gyakorlása (hozzájárulás visszavonása, tiltakozás, törlési kérelem),
- az idő múlása (letelik a jogalap által meghatározott idő).

A megőrzési idő leteltének jelzésére lehetőség szerint jelezze az informatikai rendszer, de automatizált törlést nem szabad alkalmazni.

Az adatkezelési cél és/vagy az adatkezelés jogalapjának megszűnése esetén szükséges törléseket a Társaság **negyedévente egy alkalommal** végzi, kivéve az érintettek kérése alapján szükséges adattörléseket.
A törlést minden esetben **az adatgazdának jóvá kell hagynia**, miután megvizsgálta nem áll-e fenn olyan körülmény, ami elsőbbséget élvező jogszerű ok az adat további tárolására.
A személyes adatokat tartalmazó adathordozók selejtezésekor különös gondossággal kell eljárni, és minden esetben az Informatikai biztonsági szabályzatban meghatározott az adathordozók megsemmisítésre vonatkozó eljárást kell alkalmazni.

9.8. Integritás és bizalmas jelleg

9.8.1. Biztonsági intézkedések

A Társaság által megtervezett és megvalósított információbiztonsági intézkedések biztosítják a személyes adatok **bizalmas jellegét**, **integritását** és **rendelkezésre állását.** Ezeket az intézkedéseket a Társaság Informatikai biztonsági szabályzata tartalmazza.

9.8.2. Adatvédelmi incidensek kezelése

A Társaság az adatvédelmi incidensek kezelését, beleértve a felügyeleti hatósághoz való bejelentést és szükség esetén az érintettek tájékoztatását a Társaság az incidenskezelési szabályzata alapján végzi.

9.9. Szerződések kezelése

A Társaság a partnereivel kötött szerződéseket adatkezelési szempontból felülvizsgálja és úgy módosítja, hogy azok feleljenek meg mind a GDPR követelményeknek, mind más adatok kezelésre vonatkozó jogszabályoknak.

9.9.1. Adatfeldolgozók szerződéseinek kezelése

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

Az **adatfeldolgozó** az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag technikai feladatként a Társaság rendelkezései szerint dolgozhatja fel, saját céljára a Társaság adatain adatfeldolgozást nem végezhet, a személyes adatokat a Társaság rendelkezései szerint köteles tárolni és megőrizni.

A Társaság csak olyan adatfeldolgozókat vesz igénybe, akik szervezési és technikai intézkedésekkel biztosítani tudják, hogy a Társaság adatvédelmi követelményei teljesüljenek.

Az **adatfeldolgozásra vonatkozó szerződést írásba kell foglalni**.

Az adatfeldolgozókkal kötött szerződésnek rendelkeznie kell az alábbiakról:

- az adatfeldolgozó a személyes adatokat kizárólag a Társaság írásbeli utasításai alapján kezeli – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is.
- az adatfeldolgozó biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
- az adatfeldolgozó meghozza az adatkezelés biztonságát szavatoló megfelelő technikai és szervezési intézkedéseket (GDPR 32. cikk);
- az adatfeldolgozó tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan a feltételeket, azaz
  - csak a Társaság előzetesen írásban tett eseti vagy általános felhatalmazásnak birtokában vesz igénybe további adatfeldolgozót,
  - biztosítja, hogy a további adatfeldolgozó megfelelő garanciákat nyújtson a megfelelő technikai és szervezési intézkedések végrehajtására,
  - ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik a Társaság felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért;
- az adatfeldolgozó megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti a Társaságot abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;
- az adatfeldolgozó segíti a Társaságot az adatvédelmi incidensek kezelésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
- az adatfeldolgozó az adatkezelési szolgáltatás nyújtásának befejezését követően a Társaság döntése alapján minden személyes adatot töröl vagy visszajuttat a Társaságnak, és törli a meglévő másolatokat;
- az adatfeldolgozó a Társaság rendelkezésére bocsát minden olyan információt, amely lehetővé teszi és elősegíti a Társaság által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.
-

Felelős:	adatgazdák
Végrehajtásban részt vesz:	adatvédelmi tisztviselő, IT vezető

9.9.2. Más partneri szerződések kezelése

A vevőkkel, szállítókkal (legyenek azok magánemberek vagy jogi személyek) kapcsolatos üzleti folyamatok kapcsán szükséges adatkezelési tevékenységeket a Társaság átvizsgálta és kialakította a követelményeknek megfelelő adatkezelési tevékenységeket.

Felelős:	adatgazdák
Végrehajtásban részt vesz:	adatvédelmi tisztviselő, IT vezető

9.10. Adattovábbítás harmadik országokba

Harmadik országnak tekintendő minden olyan ország, ami az **EGT tagállamain** kívül van.
Amennyiben a címzett harmadik országban van, az EU-n belüli adattovábbítás feltételein felül további feltételek biztosítása szükséges.

10. TELJESÍTMÉNYÉRTÉKELÉS

10.1. Belső audit

A Társaság tervezett módon belső auditokat végez, annak ellenőrzésére, hogy az adatvédelmi irányítási rendszer megfelel-e a jogszabályi elvárásoknak és a Társaság saját követelményeinek.
A Társaság legalább egy éves előre tekintéssel **adatvédelmi audit programot** alakít ki, amely az adatkezelési folyamatok kritikussága alapján tervez meg.
Az auditok elvégezhetők mind külső, mind belső erőforrásokkal.
Az auditokat az auditálásra vonatkozó szakmai ajánlások szerint kell elvégezni, és az eredményeket dokumentált információként meg kell őrizni.

Felelős:	adatvédelmi tisztviselő
Végrehajtásban részt vesz:	adatgazda

10.2. Tesztelés

A Társaság tervezett módon teszteli a kritikus adatkezelési folyamatokat, annak ellenőrzésére, hogy a folyamatok kialakítása és működtetése megfelel-e a jogszabályi elvárásoknak és a Társaság saját követelményeinek.
Az alábbi folyamatok tesztelését évente egy alkalommal, vagy jelentős változásokat követően szükséges elvégezni:

- incidenskezelési folyamat,
- érintetti kérelmek teljesítését támogató folyamatok.

A Társaság legalább egy éves előre tekintéssel **adatvédelmi teszt programot** alakít ki, amely az adatkezelési folyamatok kritikussága alapján tervez meg.
A teszt jegyzőkönyveket dokumentált információként a Társaság megőrzi.

Felelős:	adatvédelmi tisztviselő
Végrehajtásban részt vesz:	tesztelő

11. FEJLESZTÉS

11.1. Nemmegfelelőségek, lehetőségek, javító intézkedések

Az adatvédelmi szabályozási rendszer folyamatos működését és fejlesztését a Társaság oly módon biztosítja, hogy információkat gyűjt az irányítási rendszer állapotáról, a nemmegfelelőségekről, a fejlesztési lehetőségekről, és ezek alapján intézkedéseket tervez, majd azokat megvalósítja.

Az adatvédelmi szabályzási rendszer működtetése során a Társaság elvégzi a következő elemzéseket:

- adatvédelmi kockázatelemzés,
- információbiztonsági kockázatelemzés és
- az incidensek elemzése.

E tevékenységek során feltárt nemmegfelelőségek és a tervezett javító intézkedések az adott elemzéshez kapcsolódó nyilvántartásban találhatók.

Az adatvédelmi szabályzási rendszer állapotáról, a fejlesztési lehetőségekről a következő forrásokból kap információt a Társaság:

- vezetőségi ellenőrzések,
- belső auditok,
- belső ellenőri vizsgálat
- harmadik fél auditja,
- jelentések az adatvédelmi és információbiztonsági gyengeségekről,
- hatósági iránymutatások.

A nemmegfelelőségeket és a fejlesztési lehetőségeket a Társaság megvizsgálja, és meghatározza a szükséges javító intézkedéseket, amelyek végrehajtását nyomon követi.

A nemmegfelelőségeket, a fejlesztési lehetőségeket, a javító intézkedéseket és azok végrehajtását a Társaság dokumentált információként nyilvántartja.

Felelős:	adatvédelmi tisztviselő
Végrehajtásban részt vesz:	adatgazda