Adatvédelmi és adatkezelési szabályzat

A szabályzatot jóváhagyom és annak alkalmazását jelen változat hatálybalépési dátumával elrendelem:

Információbiztonsági besorolás:	
Bizalmas [Restricted]	☐
Belső [Internal]	☒
Nyilvános [Unclassified]	☐

Szarvas Tibor
Ügyvezető igazgató

Szerzői jogi nyilatkozat
A jelen szabályzat (továbbiakban Szabályzat) a Gill &Murry Kft. szellemi tulajdona, mely a Gill & Murry Kft - GDPR Dokumentumsablon Csomag alapján készült. A Gill &Murry Kft. a felek közötti szerződés alapján nem kizárólagos, nem átruházható, Magyarország területére korlátozott felhasználási jogot engedett a Szabályzatra a Szabályzatot megvásárló Felhasználó (továbbiakban Felhasználó) részére. Felhasználó A számlán szereplő szervezet jogosult a Szabályzatot - saját, nem üzleti célú, szakmai felhasználása érdekében - átdolgozni, módosítani, nem jogosult azonban a Szabályzatot terjeszteni, a nyilvánosság számára közvetíteni (ide nem értve a saját honlapján a nem értékesítési célú közzétételt), többszörözni, üzleti célra felhasználni, 3. személy részére megismerhetővé tenni (az érintett hatóságokon kívül) és tovább értékesíteni. Felhasználó a Szabályzatot A számlán szervezet a megvásárolt szabályzatcsomag licenc számának megfelelően 1-3-6 jogi személy adatkezelési tevékenységének dokumentálására használhatja fel.

0. TARTALOMJEGYZÉK

0.1 MÓDOSÍTÁSOK NYOMONKÖVETÉSE

Verzió szám	A módosítás leírása	Készítette	Elfogadta	Dátum
1.0	Alap verzió	Gill & Murry Kft.	Szarvas Tibor	2018.05.24.
2.0	Integrált rendszer bevezetése	”ARIES” Nonprofit Kft.	Szarvas Tibor	2020.01.01.
3.0	Adatvédelmi tisztviselő változás (1. és 3. sz.függelékek)	”ARIES” Nonprofit Kft.	Szarvas Tibor	2020.06.02.
	Adatkezelési tájékoztató Felügyelőbizottsági tagok részére (8. pont)	”ARIES” Nonprofit Kft.	Szarvas Tibor	2020.06.02.

1. BEVEZETÉS

1.1 A szabályzat célja

Az "ARIES" Nonprofit Kft. (a továbbiakban: **Szervezet**) jelen szabályzat megalkotásával és hatályba léptetésével a **személyes adatok** törvényi követelményeknek és a Szervezet üzleti stratégiájának megfelelő **kezelését biztosító szabályrendszert** hoz létre.
A Szervezet 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 Szervezet megfeleljen az **EU 2016/679 számú Általános Adatvédelmi Rendelet**ének (a továbbiakban: **GDPR**), és a személyes adatok kezelését érintő magyar jogszabályoknak.

1.2 A szabályzat kezelése

1.2.1 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. *A szabályzat elkészítéséért és rendszeres felülvizsgálatáért felelős:* ***Adatvédelmi Tisztviselő***

Az ellenőrzést elvégzi: a külső megbízott Szakértő.

2. A SZABÁLYZAT HATÁLYA

2.1 Személyi hatály

Jelen szabályzat a Szervezet irányítása alatt tevékenységet végző természetes személyekre, valamint a Szervezet számára/megbízásából adatfeldolgozói tevékenységet végző természetes személyekre vonatkozik, valamint a Szervezet szolgáltatásait igénybe vevő természetes személyekre vagy jogi személyek nevében eljáró természetes személyekre.

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.

2.3 Ajánlások, jogszabályok

2.3.1 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
- **2008. évi XLVIII. törvény** a gazdasági reklámtevékenység alapvető feltételeiről és egyéb korlátairól
- **2013. évi CLXV. törvény** a panaszokról és a közérdekű bejelentésekről

2.3.2 A személyes adatok kezelésére vonatkozó ajánlások

2.3.2.1 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

2.3.2.2 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

3. 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 előre jelzésére 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;
„tevékenységi központ”:

a) az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;
b) az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak;

„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;

„vállalkozáscsoport”: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;

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

„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.

„Adatvédelmi tisztviselő”: az Szervezet legfelső vezetésének direktben felelősséggel tartozó a Szervezet adatkezelési tevékenységet ellenőrző, az adatkezelés tevékenységhez szaktanácsadással a szervezet számára rendelkezésre álló a szervezet munkavállalója vagy külső szerződött partnere. A szerepkört betöltőt a Szervezet bejelenti az adatvédelmi hatósághoz (NAIH);

„**Adatkezelési folyamatgazda”**: 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.

4. A SZERVEZET ADATKEZELÉSI TEVÉKENYSÉGEI

4.1 A Szervezet adatkezelési tevékenysége

A Szervezet a GDPR meghatározása alapján **Adatkezelő**nek minősül alkalmazottai, vevői, egyéb szerződéses partnerei alkalmazottainak adatainak kezelésének tekintetében, ugyanakkor bizonyos adatfeldolgozási tevékenységek kapcsán **Adatfeldolgozó**ként működik.

4.2 A Szervezet adatfeldolgozói tevékenysége

A Szervezet a GDPR meghatározása alapján **Adatfeldolgozónak** minősül az Önkormányzat, mint megrendelő által a számára átadott vagy az Önkormányzat nevében kezelt adatok tekintetében.

A Szervezet az adatkezelési tevékenységeiben betöltött szerepét az ***ASZ-01-1 Adatkezelési tevékenység nyilvántartás*** dokumentumában határozza meg és rögzíti.

5. VEZETÉS

5.1 Vezetői elkötelezettség

A Szervezet vezetése elkötelezett abban, hogy megfelelő intézkedéseket tegyen a természetes személyek személyes adatainak védelmében.
Ezen elkötelezettség jegyében a Szervezet vezetése a Szervezet stratégiájával összhangban **adatvédelmi szabályrendszert** alakít ki, vezet be és működtet.
A Szervezet vezetése biztosítja az adatvédelmi szabályrendszer céljainak megvalósulásához szükséges erőforrásokat, közvetlenül támogatja az adatvédelmi szabályrendszer működését biztosító személyek munkáját és a szabályrendszer folyamatos fejlesztését.
A Szervezet vezetése ezen felül rendszeresen, de minimálisan évente egy alkalommal ellenőrzi a Szervezetben a személyes adatkezelés folyamatait.

5.2 Szervezeti szerepek, felelősségek és hatáskörök

5.2.1 Ügyvezető igazgató

A Szervezet Ügyvezető igazgatója mindent megtesz annak érdekében, hogy a Szervezet megfeleljen a jogszabályi előírásoknak és a jelen szabályzatban meghatározott vállalati elvárásoknak. A Szervezet Ügyvezető igazgatója biztosítja a Szervezet számára az 1.1 pontban meghatározott cél eléréshez szüksége erőforrásokat.

5.2.1.1 Ügyvezető igazgató feladatai

- Kinevezi az Adatvédelmi Tisztviselőt.
- Rendszeresen ellenőrzi az adatvédelmi folyamatokat a szervezetben.
- Döntést hoz az Adatvédelmi tisztviselő által előkészített Adatvédelemmel kapcsolatos kérdésekben.
- Aktív részese az Adatvédelmi incidens kezelési eljárásnak.
- Biztosítja a szükséges erőforrásokat a Szervezeten belüli személyes adatkezeléshez.
- Bevonja az Adatvédelmi Tisztviselőt a személyes adatkezeléssel kapcsolatos ügyekbe.

5.2.2 Adatvédelmi Tisztviselő

A Szervezet a GDPR 37. cikk (1) bekezdés a) pontja alapján adatvédelmi tisztviselőt jelöl ki.
Az Adatvédelmi Tisztviselő hatáskörét, felelősségét és feladatait a munkaköri leírása vagy megbízási szerződése tartalmazza. A feladat meghatározást az *ASZ-04 Adatvédelmi tisztviselő feladatai és felelősségei minta* alapján kell elkészíteni.

Legfontosabb feladatai:

- Ellenőrzi a Szervezetben a GDPR rendelet elvárásainak és a belső adatvédelemmel kapcsolatos szabályozásoknak való megfelelést, a feladatkörök kijelölését, az adatkezelésben részt vevők képzését és az auditokat,
- Kérésre szakmai tájékozgatást és tanácsot adat adatkezelési kérdésekben, így különösen az adatvédelmi hatásvizsgálatra vonatkozóan, és nyomon követi annak elvégzését,
- Kapcsolatot tart, konzultál és együttműködik az adatvédelmi hatósággal,
- Tájékoztat és szakmai tanácsot a Szervezetben adatkezelést végző alkalmazottak részére a GDPR rendelet és a hatályos magyar jogszabályok szerinti kötelezettségeikkel kapcsolatosan,
- Kezeli az adatvédelmi incidenseket,
- Érintetti igényérvényesítési kéréseket intézi.

5.2.2.1 Az Adatvédelmi Tisztviselő jogállása

A Szervezet biztosítja, hogy az Adatvédelmi Tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.
A Szervezet 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 Szervezet biztosítja, hogy az Adatvédelmi Tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el.

Az Adatvédelmi Tisztviselő feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható.
Az Adatvédelmi Tisztviselő közvetlenül a Szervezet legfelső vezetésének tartozik felelősséggel.

Az Adatvédelmi Tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség (ha van ilyen) vagy a személyes adatok kezelésére vonatkozó titoktartási kötelezettség köti. Ez utóbbit az *ASZ-02 Titoktartási nyilatkozat minta* alapján kell elkészíteni.

Amennyiben az Adatvédelmi Tisztviselő más feladatokat is ellát, a Szervezet biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

- Ez különösen azt jelenti, hogy az Adatvédelmi Tisztviselő nem tölthet be olyan pozíciót a szervezeten belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit, azaz a szervezeten belül nem tölthet be felsővezetői pozíciót (például vezérigazgató, ügyvezető igazgató, pénzügyi igazgató, főorvos, marketing osztályvezető, humán erőforrás vezető vagy informatikai osztályvezetők).

5.2.2.2 Hatósági bejelentés, közzététel

A Szervezet az Adatvédelmi Tisztviselő kinevezését követően késedelem nélkül
- bejelentést teszt a területileg illetékes adatvédelmi hatóságnál a kinevezésről.
- a Szervezet által kiadott adatvédelmi tájékoztatókban közzéteszi az Adatvédelmi Tisztviselő nevét és elérhetőségét.

5.2.2.3 A Szervezet Adatvédelmi Tisztviselőjének elérhetősége:

Az 1.sz. függelékben meghatározva

5.2.3 Adatkezelésre feljogosított személyek

A Szervezet minden alkalmazottja kisebb-nagyobb mértékben kezel a munkája során személyes adatokat.
A Szervezet gondoskodik arról, hogy minden alkalmazottja a személyes adatok kezelésére vonatkozó titoktartási kötelezettséget vállaljon. A titoktartási nyilatkozatokat az *ASZ-02 Titoktartási nyilatkozat minta* alapján kell elkészíteni.

> *A titoktartási nyilatkozatokat a munkavállalókkal a belépéskor a beléptetést végző HR munkatárs végzi.*
> *Az ellenőrzést elvégzi:* ***Adatvédelmi Tisztviselő.***

Jelen szabályzat bevezetése előtt munkába állt kollégák esetében az *ASZ-02 Titoktartási nyilatkozat mintát* a bevezetést követő 30 napon belül alá kell íratni.

6. ADATKEZELÉSI FOLYAMATOK MENEDZSMENTJE

6.1 Beépített és alapértelmezett adatvédelem

A Szervezet az adatkezelés tervezésekor a kockázatokkal arányos technikai és szervezési védelmi intézkedéseket épít az adatkezelés folyamatába, hogy biztosítsa az érintettek személyes adatainak védelmét.
A Szervezet 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.

6.2 Adatkezelési tevékenységek kockázatértékelése

A személyes adatok kezelése kockázatokkal járhat a természetes személyek alapvető jogaira és szabadságaira és különösen a személyes adatok védelméhez való jogukra nézve, ezért a Szervezet az **adatkezelés megkezdése előtt**, az adott adatkezelés vonatkozásában **mérlegeli a kockázatokat** és ennek megfelelően hoz döntést az adatkezelési tevékenységről.

A jelen szabályzat bevezetése előtt megkezdett adatkezelési tevékenységek esetében a kockázatértékelést jelen szabályzat bevezetéséig el kell végezni.
A jelen szabályzat bevezetését követően megkezdendő 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.

A Szervezet a kockázatelemzést követőn hozott **szervezési és a technikai** intézkedésekkel együttesen fedi le az adatkezelés teljes folyamatát és így felel meg az adatvédelmi követelményeknek. *Az adatkezelési folyamatokat megelőző kockázatelemzés és kezelés, valamint a hatásvizsgálat elvégzését a szervezet végzi.*

*Az ellenőrzést elvégzi: **Adatvédelmi Tisztviselő***

6.2.1 Kockázatok mérlegelése az adatkezelés előtt

6.2.1.1 A hatásvizsgálat szükségességének meghatározása

Első lépésként, **még az adatkezelési tevékenység megkezdése** előtt el kell végezni egy előzetes kockázatértékelést, amely alapján a Szervezet eldönti, hogy az adott adatkezelési tevékenység estében az adatkezelés **valószínűsíthetően magas kockázattal jár-e az Érintettek jogaira nézve és** szükséges-e adatvédelmi hatásvizsgálatot végezni vagy nem.

6.2.1.2 Előzetes kockázatértékelés

A Szervezet által az adatvédelmi hatásvizsgálatot megelőző előzetes kockázatértékeléseket az ***ASZ-05-01 Hatásvizsgálatot megelőző kockázatértékelés*** táblázat tartalmazza.

A kockázatértékelő táblázat kitöltése:

1) Az új adatkezelési tevékenységet az ***ASZ-01 Adatvédelmi szabályzat*** alapján kell azonosítani és nyilvántartásba venni. Az itt meghatározott azonosítóval és névvel hivatkozunk az adatkezelési tevékenységre.
2) A kockázatértékelés az értékelő kérdésekre adott válaszok alapján történik. A kérdésekre **igen-nem** válaszokat kell adni.
3) Döntési kritériumok:
    a. Az első kérdésre adott **igen** válasz esetén, azaz, ha a NAIH kötelező adatvédelmi hatásvizsgálatokat tartalmazó jegyzéken szerepel az adatkezelési tevékenység, **kötelező adatvédelmi hatásvizsgálatot** végezni. Ebben az esetben a többi kérdésre nem szükséges válaszolni.
    b. Ha érvényesíthető valamilyen felmentés (2. kérdés), akkor **nem kell adatvédelmi hatásvizsgálatot** végezni. Ebben az esetben a többi kérdésre nem szükséges válaszolni.
    c. Amennyiben az első két kérdés alapján nem lehet egyértelműen eldönteni az adatvédelmi hatásvizsgálat szükségességét **a további kérdésekre is válaszolni kell**. hogy Ha a további kérdések bármelyikére **igen** a válasz, abban az esetben **szükséges adatvédelmi hatásvizsgálatot** végezni.
    d. A válaszok alapján a táblázat automatikusan meghatározza, hogy szükséges-e az adatvédelmi hatásvizsgálat.

Az előzetes kockázatértékelést az adatkezelés megkezdése előtt a szervezet minden alkalommal elvégzi.
Az előzetes kockázatértékeléseket **felül kell vizsgálni**, minden esetben, ha az adatkezelési tevékenység, illetve a jogszabályi és/vagy a belső szabályzási környezet változik. Az előzetes kockázatértékelés elvégzését a szervezet végzi.

Az ellenőrzést elvégzi: ***Adatvédelmi Tisztviselő***

A hatásvizsgálat az *1.sz. mellékletben rögzített hatáselemzési folyamat alapján történik***.**

6.2.2 Szervezési intézkedések

A szervezési intézkedések keretét jelen Adatvédelmi 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 szabályrendszert,
- Az adatvédelmi hatásvizsgálatból következő intézkedéseket,
- Az adatvédelmi incidensek elemzéséből következő intézkedéseket,
- A belső ellenőrzések során feltárt vagy az adatkezelésben résztvevő által jelentett gyengeségek elemzéséből származó javító intézkedéseket.

Az adatkezelési folyamatok alatt az alábbi tevékenységeket azonosítjuk:

- Az adatkezelési tevékenységre feljogosított **személyek által végzett munka**,
- Az **informatikai rendszerek**ben megvalósított automatizált vagy kezelői beavatkozással megvalósuló **folyamatok**.

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

- Az **Adatkezelési szerepkörök** meghatározása,
- Az **Adatvédelemi tisztviselő** kinevezése és a munkaköri feladatainak meghatározása,
- A személyes adatok kezelés kapcsolódó jogosultságok és felelősségeket kerülnek pontosítása,
- A **munkautasítások**, amelyek az adatkezelési tevékenységek pontos lépéseit határozzák meg és
- Az informatika rendszerrel szembeni elvárások.

A szervezési intézkedéseket részét képző dokumentumok felsorolását a jelen szabályzat 2. függeléke tartalmazza. *Az adatkezelési dokumentumlista napra készen tartását a szervezet végzi.*

Az ellenőrzést elvégzi: ***Adatvédelmi Tisztviselő***

6.2.3 Technikai intézkedések

A Szervezet a személyes adatok védelmével kapcsolatos technikai intézkedéseket megvalósítás érdekében bevezette, üzemelteti és rendszeresen felülvizsgálja a Szervezet Információbiztonsági szabályzatát.

6.2.3.1 Informatikai rendszerrel szembeni elvárások

Az informatikai rendszerre vonatkozó technikai intézkedések megtervezésének kiindulópontjaként a szervezési intézkedések tervezése során figyelembe kell venni minimálisan az alábbiakat:
Az informatikai rendszer képes legyen:

- Biztosítani a benne kezelt személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását,
- A kockázatokkal arányos titkosítási eljárások alkalmazására,
- Teljesíteni az üzletmenet folytonossági eljárásokat és incidens esetén az adatok hozzáférését képes legyen a megfelelő időn belül visszaállítani.

További elvárás az informatikai rendszer üzemeltetőjétől a technikai és szervezési intézkedések rendszeres, de minimum évente egy alkalommal történő tesztelése.

6.2.4 Információbiztonsági intézkedések

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

6.3 Adatkezelési tevékenységek azonosítása és nyilvántartása

A Szervezet a már megkezdett és a későbbiekben bevezetésre kerülő adatkezelési tevékenységekről teljes körű nyilvántartást vezet.
Az „adatkezelési tevékenység" azon adatkezelési műveletek összessége, **amelyeknek egy adott célja van**. Az Adatvédelmi Tisztviselő az adatkezelés megkezdéses előtt ellenőrzi, hogy az adatkezelés megfelelő a GDPR rendelet és jelen szabályzat elvárásainak.
Folyamat:

1. Azonosítja az adatkezelési tevékenységeket a szervezeten belül.
2. Csoportosítja az azonos cél érdekében történő adatkezelési tevékenységeket.
3. Minden adatkezelési célhoz az 6.4 pontban megfogalmazott jogalapok közül társít egyet. Amennyiben nem társítható jogalap az adatkezelési célhoz úgy az adatkezelési tevékenységet nem szabad elkezdeni vagy azonnal meg kell szakítani.
4. Meghatározza a 6.3.1 és 6.3.2 pontban meghatározott paramétereket.
5. Adatkezelési folyamatgazdát jelöl ki minden azonos céllal megjelölt adatkezelési tevékenységcsoporthoz.
6. Megvizsgálja, hogy az adatkezelési cél megszűnése estén vagy a hozzá kapcsolódó határidő lejáratakor a Szervezet befejezi-e az adatkezelési tevékenységet vagy másik adatkezelési cél mentén kezeli tovább az adatokat.

6.3.1 Adatkezelési tevékenységek azonosítása

A Szervezet azonosítja az adatkezelőként vagy adatfeldolgozóként végzett adatkezelési tevékenységeit. Az adatkezelési tevékenységek azonosításának célja, hogy a szervezet tisztában legyen a személyes adatok kezelési folyamatainak Szervezeten belüli megvalósításával annak érdekében, hogy megfelelő kontroll alatt tarthassa azokat. Az adatkezelési tevékenységek azonosítását a szervezet végzi.

Az ellenőrzést elvégzi: ***Adatvédelmi Tisztviselő***

A Szervezet adatkezelési tevékenységek azonosításánál az alábbi paramétereket határozza meg a Szervezet:

Adatkezelési folyamat	A Szervezet által végzett adatkezelési tevékenységek csoportba foglalva, azonos adatkezelési cél mentén.
Adatkezelési folyamatgazda	Az a szervezeti egység vezető, akinek a szervezeti egységében kezelik az azonosított adatkezelési tevékenységeket.
Adatkezelői szerep	Azonosítani kell, hogy adatkezelő vagy adatfeldolgozói szerepkörben kezeli az adatokat a Szervezet.
Adatkezelési Cél	Az adatkezelési tevékenységek összefoglaló célja.
Jogalap	A 6.4.3- 6.4.9 pontokban definiált jogalapok közül egy.
Érintettek kategóriái	Azon természetes személyek összefoglaló csoportjai, akik adatait az adatkezelési folyamatban kezeli a Szervezet
Kezelt személyes adatok kategóriái	A kezelt személyes adatok összefoglaló megnevezése

Adatfeldolgozók kategóriái	Azon szervezetek összefoglaló megnevezése, melyeknek adatfeldolgozásra továbbítják, vagy hozzáférési lehetőséget biztosít az Adatkezelő
Címzettek kategóriái	Azon szervezetek összefoglaló megnevezése, melyeknek továbbítják, vagy hozzáférési lehetőséget biztosít a Szervezet az adatkezelési tevékenység során.
3. Országba továbbítás címzettje	Az EGT tagállamain kívüli szervezetbe vagy címzettjének történő adattovábbítás esetén a címzett megnevezése.
Továbbítás garanciái	A 3. Országba történő adattovábbítás biztonsági garanciának dokumentálása.
Tervezett adattárolási határidő	Az adatok kezelésének tárolásának tervezett határideje, vagy annak kiszámítási módja vagy definíciója. (pld: visszavonásig)
Adatbiztonság leírása	Az adatkezelés során alkalmazott információbiztonsági megoldások.
Elfogadás /tudomásul vétel bizonyítása	Hozzájárulásos jogalap esetén az adatkezelő milyen módon bizonyítja a hozzájárulást/tudomásul vételt.
Az adatkezelés folyamatában betöltött szerep	A Szervezet adatkezelő vagy adatfeldolgozói szerepet tölt be.

A Szervezet a GDPR 30. cikk (1) pontja alapján elkészíti adatkezelési tevékenységek nyilvántartását, amelyet az ***ASZ01-1 Adatkezelési tevékenységek nyilvántartása*** táblázatban rögzíti. Az adatkezelési tevekénységek dokumentálását a szervezet végzi.

Az ellenőrzést elvégzi: ***Adatvédelmi Tisztviselő***

6.3.2 Adatfeldolgozói tevékenységek nyilvántartása

A Szervezet a GDPR 30. cikk (2) pontja alapján elkészíti az **adatfeldolgozóként** végzett adatkezelési tevékenységek nyilvántartását, az ***ASZ-01-2 Adatfeldolgozói adatkezelések nyilvántartása*** táblázatban rögzíti.

Az adatkezelési tevékenységek nyilvántartása csak azokat az adatokat tartalmazza, amelyek a GDPR 30. cikke szerint szükséges, minden a további nyilvántartást a Szervezet ettől elkülönítve kezel. Az adatkezelési dokumentumlista nyilvántartását és napra készen tartását a szervezet végzi.

Az ellenőrzést elvégzi: ***Adatvédelmi Tisztviselő***

A Szervezet **adatfeldolgozóként** végzett adatkezelési tevékenységek nyilvántartásánál az alábbi paramétereket rögzíti a Szervezet:

ASZ-01-2 Adatfeldolgozói adatkezelések nyilvántartásban tárolt adatok

Adatkezelő neve	Az a szervezet, akinek megbízása alapján, akinek vagy amelynek a nevében történik az adatkezelés.
Az adatkezelő elérhetősége	Az előző sorban meghatározott adatkezelő elérhetősége.
Adatkezelési tevékenységek kategóriái	Az adatkezelési tevékenységek összefoglaló csoportosítása. Pl. IT üzemeltetés, bérszámfejtés, könyvelés, adattisztítás stb.

További adatfeldolgozók	Azon adatfeldolgozók megnevezése akiket a Szervezet, mint alvállalkozó adatfeldolgozó bevon az adatkezelési tevékenységbe, vagy akik/amelyek hozzáférnek, tárolják vagy kezelik az adatkezelő adatait.
3. országba továbbítás címzettje	Az EGT tagállamai kívüli szervezetbe vagy címzettének történő adattovábbítás esetén a címzett megnevezése.
A 3. országba továbbítás garanciái	Azok a biztonsági garanciák megnevezése melyek mentén a Szervezet az adatokat a 3. Országba továbbítja. pl.: EU Bizottsági megfelelőségi határozat, Kötelező érvényű vállalati szabályok, az érintett kifejezett hozzájárulása stb.

6.4 Az adatkezelés jogszerűsége

A Szervezet a személyes adatok kezelését csak akkor végzi, ha a GDPR 6. cikk (1) pontjában megadott hat jogalap közül, legalább az egyik alkalmazható. *A jogala*pok meghatározását a szervezet végzi.

Az ellenőrzést elvégzi: ***Adatvédelmi Tisztviselő***

6.4.1 Gyermekek személyes adatainak kezelése

A Szervezet alaptevékenységét és szolgáltatásait kifejezetten NEM gyermek (16. életévét be nem töltött) korúak számára nyújtja. A Szervezet ennek megfelelően beépített védelem formájában nem vizsgálja az általa kezelt adatok személyes adatok esetében a természetes személy korát.
Amennyiben az adatkezelés során a Szervezet számára egyértelművé válik, hogy természetes személy még nem töltötte be a 16. életévét késelem nélkül beszerzi a szülői felügyeleti jog gyakorlójától az adatkezeléshez a hozzájárulást az ***ASZ-23 Szülői hozzájárulás minta*** alapján vagy megszünteti az adatok kezelését.

Ha a Szervezet felügyelete alatt adatkezelést végzők számára egyértelművé válik, hogy egy kezelt adat 16 éven aluli természetes személyé, késedelem nélkül jelenti az incidens kezelési szabályozásnak megfelelően.

6.4.2 A személyes adatok különleges kategóriái kezelése

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 Szervezet a **személyes adatok különleges kategóriáit** alapértelmezetten nem kezeli, kivéve a GDPR rendelet 9.cikk 2 pontjában megfogalmazott kivételek alapján, de legfőképpen:

a) Az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy az (1) bekezdésben említett tilalom nem oldható fel az érintett hozzájárulásával;

b) Az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;

c) Szakszervezeti tagságra vonatkozó információkat kezel és tárol Szervezet, valamint a szakszervezeti tagdíjat levonja a bérszámfejtés során a tagok munkabéréből. A szakszervezeti tagsággal rendelkező munkavállalók az adatkezeléshez az **ASZ-42 Szakszervezeti adatkezelés hozzájárulás** aláírásával járulnak hozzá, amely eredeti példányát a hozzájárulás bizonyítása érdekében a munkáltató tárol.

d) Az adatkezelést megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá a (3) bekezdésben említett feltételekre és garanciákra figyelemmel;

6.4.3 Hozzájárulás jogalap alkalmazása

GDPR 6. cikk (1) a): 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 egy időben kell megtörténnie.
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.

6.4.3.1 Hozzájáruló nyilatkozat

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

- Legyen egyértelmű,
- Más ügyektől elkülöníthető,
- Érhető, világos, egyszerű nyelvezetű.

6.4.3.2 Hozzájárulás munkavállalók esetében

A hozzájárulás érvényességének feltétele az önkéntesség, ezért munkavállalók esetében a Szervezet különös körültekintéssel alkalmazza. A hozzájárulás munkavállalók esetében csak olyan adatkezelési tevékenységre vonatkozzon, ami nincs összefüggésben a munkaviszonnyal és a munkáltatói jogok gyakorlásával nem áll kapcsolatban.
A Szervezet kifejezetten figyelmet fordít arra, hogy a munkavállalók esetében a hozzájárulásos jogalap mentén kezelt adatok esetében a hozzájárulás megtagadása esetén munkaviszonyával kapcsolatosan semmilyen hatás ne érje a munkavállalót.

6.4.3.3 Hozzájárulás visszavonása

Az érintettet az adatkezeléshez való hozzájárulását bármikor visszavonhatja, erről a jogáról, illetve a visszavonás módjáról a hozzájárulási nyilatkozatban vagy az ezzel egy időben átadott adatkezelési tájékoztatóban kell tájékoztatni.
A hozzájárulás visszavonásának olyan egyszerűnek kell lenni, mint amilyen a hozzájárulás megadása.
A Szervezet a hozzájárulás visszavonásához alternatív csatornát is biztosít. Az Adatvédelmi tisztviselő elérhetőségén írásban bejelentett hozzájárulás visszavonási igényeket is elfogadja.
A hozzájárulások meglétét és a visszavonást követő intézkedéseket a Szervezet az *ASZ-01-1* ***Adatkezelési tevékenységek nyilvántartása*** adatkezelési tevékenységenként megadott módon igazolja és ennek megfelelően a szükséges szervezési és technikai intézkedéseket a Szervezet megteszi.

6.4.4 Szerződéses jogalap alkalmazása

GDPR 6. cikk (1) b): „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;”
Szerződéskötésre irányuló közvetlen cselekmények esetében (ajánlatkérés, ajánlatadás, szerződéses feltételek egyeztetése) ez a jogalap alkalmazandó.

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

6.4.5 Jogi kötelezettség jogalap alkalmazása

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

Tipikus jogszabályi kötelezettségek: számviteli tv., adó tv, munkajog stb. 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 Szervezet **jogászának egyetértését** megszerezni.
A jogi kötelezettség jogalap esetén az ASZ-01-1 ***Adatkezelési tevékenységek nyilvántartása*** táblázatban (Excel munkafüzet külön munkalapján) nyilván kell tartani a jogszabályban megfogalmazott határidőket.

6.4.6 Létfontosságú érdek jogalap alkalmazása

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

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

6.4.7 Közhatalmi jogosítvány jogalap alkalmazása

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

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

6.4.8 Jogos érdek jogalap alkalmazása

GDPR 6. cikk (1) f): „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 Szervezet **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 érdekéve, amely az adatkezelést szükségessé teszi.

6.4.8.1 Közvetlen üzletszerzés

A GDPR preambulum (47) alapján a személyes adatok közvetlen üzletszerzési célú kezelése jogos érdeken alapulónak tekinthető, tehát a Szervezet adott esetben **érdekmérlegelés 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.

6.4.8.2 Más adatkezelési célok esetében

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

6.5 Célhoz kötöttség és adattakarékosság

A Szervezet személyes adatokat csak tisztességes, jól meghatározott, egyértelmű és jogszerű célból kezel.
A Szervezet 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. Ezt többek között az adatkezelés előtt elvégzett kockázatelemzéssel és hatásvizsgálattal éri el a szervezet.

6.6 Pontosság és korlátozott tárolhatóság

6.6.1 Intézkedések a pontosság érdekében

A Szervezet az adatkezelési tevékenysége során folyamatba épített ellenőrzéseket végez a kezelt személyes adatok pontosságának biztosítása érdekében.
Ahol, ez lehetséges az informatikai 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.

6.6.2 Adatmegőrzés és adateltávolítás

Amíg az adatkezelésnek van **célja és** érvényes **jogalapja**, addig az adatot meg kell őrizni, ezt az időpontot követően az adatot törölni kell.
Az adatkezelési cél megváltozását vagy megszűnését az Adatkezelési folyamatgazdának 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.
A törlést minden esetben az Adatkezelési folyamatgazdának **jóvá kell hagynia**, miután megvizsgálta nem áll-e fenn olyan körülmény, ami elsőbbséget élvező jogszerű ok az adat további tárolására.

A melegviz@arieskft.hu és a lomtalanitas@arieskft.hu e-mail fiókok esetében a felügyelet és a selejtezés az előírt időközönként a felhasználók felelőssége.
A titkarsag@arieskft.hu e-mail fiók felügyelete és selejtezése az IT üzemeltető felelőssége.

6.7 Integritás és bizalmas jelleg

6.7.1 Biztonsági intézkedések

A Szervezet által megtervezett és megvalósított információbiztonsági intézkedések biztosítják a személyes adatok **bizalmas jellegét**, **integritását** és **rendelkezésre állását.** Ezeket az intézkedéseket az Szervezet ***Információ Biztonsági Szabályzata*** tartalmazza.

7. ADATVÉDELMI INCIDENSEK KEZELÉSE

7.1.1 Az incidenskezelés Szerepkörei

Az adatvédelmi Incidensek menedzseléséért felelős az: **Adatvédelmi Tisztviselő,**

- akinek felelőssége és feladata a teljes incidenskezelési folyamat menedzselése, az incidenskezelésben résztvevő munkatársak és szakértők munkájának irányítása.

Az **Adatvédelmi Tisztviselő** – amennyiben ennek szükségét látja – kérheti a Szervezet más munkatársainak segítségét az incidenskezelési folyamat során.

7.1.2 Incidenskezelési folyamat

A Szervezet az adatvédelmi incidensek kezelésére a következő folyamatot vezeti be.

7.1.3 Incidensek észlelése

Adatvédelmi incidensekkel, illetve az Információbiztonsági és adatvédelmi kontrollok gyengeségeivel, potenciális veszélyforrásokkal a Szervezet valamennyi alkalmazottja, szerződött partnere, ügyfele, illetve az informatikai rendszereit fejlesztő, működtető és üzemeltető munkatársa szembesülhet, illetve észlelhet incidensre utaló jeleket.
Az incidensek korai felismerése érdekében a Szervezet információbiztonsági rendszereket és eljárásokat működtet, melynek segítségével észlelésre kerülnek információbiztonsági és/vagy adatvédelmi események, amelyek adott esetben incidensnek minősülhetnek.
Incidens észlelésekor minden lényeges részletet azonnal fel kell jegyezni, a számítógép képernyőről másolatot kell készíteni (amennyiben releváns).
Általában az incidensek bekövetkezése előtt vagy bekövetkezése során különleges emberi viselkedés és/vagy az informatikai rendszer helytelen, szokatlan működése lép fel. Az esemény későbbi nyomon-követhetősége érdekében fontos, hogy szakmai kompetencia hiányában az incidenst észlelő ne avatkozzon be, saját hatáskörben ne kezdje meg az esemény kivizsgálását. (Kivételt képez ez alól a vagyoni kárelhárítás, illetve az emberi élet védelmében tett intézkedések.)

7.1.4 Incidensek bejelentése

A Szervezet adatkezelési tevékenysége kapcsán felmerülő minden személyes adatokra vonatkozó adatvédelmi incidenst indokolatlan késedelem nélkül az **Adatvédelmi Tisztviselő** felé kell jelenteni.

Folyamat:

1. Az incidenst észlelő késedelem nélkül (azonnal) értesíti az **Adatvédelmi Tisztviselőt** telefonon az 3. számú függelékben megjelölt kapcsolattartási telefonszámon vagy személyesen.

7.1.5 Az incidensek nyilvántartása

A bejelentést követően az Adatvédelmi Tisztviselő az incidens adatait rögzíti az *ASZ08-1 Adatvédelmi incidensek nyilvántartása* táblázatban
Az **Adatvédelmi Tisztviselő** kötelessége, hogy az incidenskezelési folyamat minden lépése – a bejelentéstől az incidens lezárásáig – dokumentált legyen.
A nyilvántartás naprakész vezetése egyben lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze vonatkozó törvényi követelményeinek való megfelelést.

7.1.6 Gyorselemzés, kárenyhítés

A bejelentés követően az **Adatvédelmi Tisztviselő** azonnal megkezdi az incidensek elemzését. Már ebben a fázisában is szükséges lehet – az **Adatvédelmi Tisztviselő** döntése alapján – további szakértők (**jogász, informatikus, információbiztonsági elemző**) bevonására.

Az **Adatvédelmi Tisztviselő** információt gyűjt az incidensről. Az incidens körülményeinek vizsgálata és a kezdeti diagnosztikai lépések célja, hogy minél hamarabb, minél részletesebb információ álljon rendelkezésre az incidensről. Cél, hogy meghatározásra kerüljön:

- Az incidens jellege,
- Az érintettek kategóriái és száma,
- Az érintett személyes adatok kategóriái és száma,
- A valószínűsíthető következmények,
- Az érintett IT infrastruktúra, alkalmazói rendszer környezet, felhasználói kör,
- Ki vagy mi okozta az esemény bekövetkezését,
- Milyen sérülékenység, gyengeség került kihasználásra.

Ebben a szakaszban elsősorban az incidens **káros hatásának a minimalizálásához** szükséges ismereteket kell összegyűjteni, feltárni, hogy **meghatározható legyen az incidens súlyossági** szintje, kiterjedtsége, annak érdekében, hogy a fellépő káreseményt minimalizálni lehessen.
Az elemzés során kiemelt figyelmet kell fordítani az incidenshez kapcsolódó **bizonyítékok** szakszerű gyűjtésére és **megőrzésé**re.
Az összegyűjtött releváns információkat a kapcsolódó nyilvántartásban rögzíteni kell.
Amennyiben indokolt az incidens természetéhez illeszkedően **azonnali válaszlépés**ként meg kell tenni a szükséges és lehetséges intézkedéseket az incidens **elhatárolására**. Cél, hogy a fellépő károk minimalizálása érdekében az incidens kiterjedését, a további károkat megakadályozzuk.
Az elhatárolási módszer kiválasztásánál figyelembe kell venni a bizonyítékgyűjtési elvárásokat és az üzleti alkalmazások és egyéb szolgáltatások által támasztott rendelkezésre állási követelményeket.

7.1.7 Az incidens egyértelműen nem jár kockázattal Érintettek számára

Amennyiben a gyorselemzés során egyértelműen bebizonyosodik, hogy a bejelentés téves volt vagy a korábban megtett biztonsági intézkedések (pl.: titkosítás) következtében az Érintettek személyes adatai nincsenek veszélyben az incidens vizsgálata a Adatvédelmi Tisztviselő döntését követően lezárható.
Az Adatvédelmi Tisztviselő az incidenst és a hozzá kapcsolódó összes bizonyítékot jelen utasítás rendelkezéseinek megfelelően az *ASZ-08-1 Adatvédelmi incidensek nyilvántartásban* dokumentálja.
A bejelentett incidens lezárható például a következő esetekben:

1. Titkosított notebook vagy USB adathordozó elvesztése/ eltulajdonítása esetén.
2. Személyes adatok rendelkezésre állásának sérülése esetén abban azt esetben, ha az informatikai mentési rendszerből az adatok hiánytalanul visszaállításra kerültek.
3. Személyes adatok integritásának sérülése esetén, ha az informatikai mentési rendszerből az adatok az eredeti állapotban visszaállításra kerültek.

7.1.8 Döntés az Incidensről

Az azonnali kárenyhítő intézkedések megtételét követően, vagy ha lehetséges azzal egy időben az **Adatvédelmi Tisztviselő** kiértékeli az incidens a következő szempontok alapján:

- Érintettek száma, köre,
- Érintett személyes adatok kategóriái,
- Az érintett adatrekordok száma, köre,
- Érint-e különleges adatot,
- Könnyen/nehezen azonosíthatók az érintett természetes személyek,
- Érint-e gyermekeket vagy hátrányos helyzetű/ sérült embereket,
- Sérült-e a személyes adatok bizalmassága,
- Sérült-e a személyes adatok integritása,
- Sérült-e a személyes adatok rendelkezésre állása,
- Szándékos károkozás történt-e,
- A jogsértés (lehetséges) következményei, annak súlyossága.

Minden egyes szempont értékelését rögzíteni kell az adatvédelmi incidensek nyilvántartásában.
Az egyes szempontok áttekintését követően amennyiben az incidens nem zárható le az 7.1.7 pontban megfogalmazott szempontok alapján az **Adatvédelmi Tisztviselő** döntést hoz az incidens eszkalálásáról.

7.1.9 Az incidens eszkalálása

Az Adatvédelmi Tisztviselő 7.1.8. pontban meghozott döntése alapján **az incidens eszkalálásra kerül,** azaz az incidenskezelés további folyamatába bevonásra kerül a Szervezet **Ügyvezető igazgatója.**
Az eszkalációt követően, a kibővített csoport **újraértékeli** az adatvédelmi incidens kockázatait és **döntést hoz** az incidens kezeléséről, amely a következő lehet:

1) az incidens **valószínűsíthetően nem jár kockázattal** a természetes személyek jogaira és szabadságaira nézve és 7.1.7 pontban meghatározottak mentén lezárásra kerül. (Az Adatvédelmi Tisztviselő rosszul ítélte meg a helyzetet vagy újabb korábban nem ismert körülmény került a vizsgálat fókuszába)
2) az incidens **valószínűsíthetően kockázattal jár** a természetes személyek jogaira és szabadságaira nézve.
   Az **incidenskezelést folytatni kell** és **az incidenst be kell jelenti az** illetékes **adatvédelmi hatóságnak** az 7.1.11 pontban meghatározottak alapján.
3) az incidens **valószínűsíthetően magas kockázattal jár** a természetes személyek jogaira és szabadságaira nézve.
   Az **incidenskezelést folytatni kell** és **az incidenst be kell jelenti az** illetékes **adatvédelmi hatóságnak** az 7.1.11 pontban meghatározottak alapján és az incidensről **tájékoztatni kell az érintetteket** az 7.1.12 pontban meghatározottak alapján.

   Az incidens magas kockázatúnak kell tekinteni minimálisan a következő esetekben:

   a) Ha az incidens különleges adatokat, kiemelten gyermekek különleges adatait érinti.
   b) Ha az incidens az adatkezelési folyamatban kezelt összes adatot érinti.
   c) Ha az incidens az érintett pénzügyi adatainak integritását érintette.

7.1.10 Kommunikáció

Az incidenskezelésbe bevontak körén túl bármilyen kommunikáció csak a Szervezet **ügyvezető igazgató** jóváhagyásával lehetséges.
Az incidens természetétől és súlyosságától függően a Szervezet tájékoztatja a következő érdekelti köröket:

- Az illetékes felügyeleti hatóságot (lásd: 7.1.11 pont),
- Az érintetteket (lásd: 7.1.12 pont),
- A Szervezet munkatársait, illetve azok adott csoportjait,
- Azokat az adatkezelőket, akik személyes adatokat adtak át a Szervezet részre további adatkezelésre vagy adatfeldolgozásra, és az átadott személyes adatok érintettek az incidensben.

A média, illetve a fenti felsorolásban nem szereplő személyek és szervezetek részére tájékoztatás adására **csak a Szervezet Ügyvezető igazgatója jogosult**.

7.1.11 Bejelentés a felügyeleti hatóságnak

Azt az adatvédelmi incidenst, amely valószínűsíthetően kockázattal jár az **Adatvédelmi Tisztviselő** indokolatlan késedelem nélkül, és ha lehetséges, **legkésőbb 72 órával azután**, hogy az adatvédelmi incidens a Szervezet tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak (**NAIH - https://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html**).
Ha a bejelentés nem történik meg 72 órán belül, a bejelentéshez mellékelni szükséges a késedelem igazolására szolgáló indokokat is.
A bejelentésnek legalább a következőket kell tartalmaznia (összhangban a hatóság által elvártakkal):

- Ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- Közölni kell a bejelentő Adatvédelmi Tisztviselő nevét és elérhetőségeit;
- Ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- 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, azokat további indokolatlan késedelem nélkül később részletekben kell közölni.
A bejelentéseket minden esetben írásos formában, a hatóság által biztosított felületen / formában kell megtenni.
A bejelentések kapcsán a szervezet **Adatvédelmi Tisztviselője**

- Nyilvántartást vezet a bejelentésektől,
- Köteles meggyőződni a bejelentések hatósághoz történő megérkezéséről,
- További kommunikációt folytat az bejelentett incidensek hatósági megítéléséről és a teendőkről.

7.1.12 Érintettek tájékoztatása

Arról az adatvédelmi incidensről, amely valószínűsíthetően magas kockázattal jár, a Szervezet indokolatlan késedelem nélkül tájékoztatja az érintetteket.
Az érintettek részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a következőket:

- A Szervezet Adatvédelmi Tisztviselőjének nevét, elérhetőségét,
- Az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- Az Szervezet által az adatvédelmi incidens javítására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az értesítés összeállítását a szervezet **Adatvédelmi Tisztviselője** végzi és a szervezet **ügyvezető igazgató** hagyja jóvá.
Az értesítéstől el lehet tekinteni, korlátozni lehet, illetve halasztani lehet a következők mérlegelésével:

- A Szervezet 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;
- A Szervezet az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy a „magas kockázat” a továbbiakban valószínűsíthetően nem valósul meg;
- A tájékoztatás aránytalan erőfeszítést tenne szükségessé, ilyen esetekben az érintetteket nyilvánosan közzétett információk (pl. honlap, média stb.) útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Ha a Szervezet még nem értesítette az érintetteket az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett(ek) tájékoztatását, vagy megállapíthatja a fenti bekezdésben említett feltételek valamelyikének teljesülését.
Az érintettek felé megvalósult tájékoztatásról a Szervezet **Adatvédelmi Tisztviselője** nyilvántartást vezet.

7.1.13 Javító intézkedések tervezése és végrehajtása

A károk enyhítését és az incidens lokalizálását követően az **Adatvédelmi Tisztviselő** az incidenst kiváltó ok megtalálásával, meghatározásával foglalkozik. Az javító intézkedések kidolgozásakor a meglévő intézkedéseket mind a **szervezési**, a **technikai** és az **információbiztonsági** területeken át kell tekinteni.
A Szervezet **Ügyvezető igazgatója** felelős a javító intézkedések végrehajtásához szükséges erőforrások biztosításáért és a javító intézkedések jóváhagyásáért.
A kidolgozott és jóváhagyott javító intézkedéseket az adatvédelmi incidensek nyilvántartásába be kell vezetni. A Javító intézkedések végrehajtását a szervezet végzi.

Az ellenőrzést elvégzi: ***Adatvédelmi Tisztviselő***

7.1.14 Incidenskezelési megállapodások más szervezettekkel

A Szervezet incidenskezelési megállapodásokat ír alá minden partnerével, amely

- számára adatfeldolgozást végez vagy
- akinek a Szervezet adatfeldolgozást végez.

A megállapodásban részletezni kell az átadott adatkategóriák és az adatfeldolgozási folyamat ismeretében, hogy milyen eseményeket tekintenek adatvédelmi incidensnek. Az ismerté vált adatvédelmi incidensekről minden félnek nyilvántartást kell vezetnie.
Az Szervezet az adatfeldolgozókkal kötött szerződés alapján elvárja minden adatfeldolgozójától, hogy a náluk bekövetkezett adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül jelentsék.
A jelentés tartalmának legalább azokat az információkat kell tartalmaznia, amelyek az adatfeldolgozónak is szükségesek lehetnek az incidens hatásainak megfelelő felméréséhez. A bejelentéseket minden esetben a Szervezet kijelölt **Adatvédelmi Tisztviselője** felé kell megtenni írásos (e-mail) formában, és meg kell győződni annak tudomásulvételéről.

8. ÉRINTETTI JOGOK ÉRVÉNYESÍTÉSE

A Szervezet fokozott figyelmet fordít arra, hogy a GDPR rendeletben meghatározott érintetti jogok érvényesítése megfeleljen a jogszabályi követelmények és az érintettek elvárásinak.

8.1 Az érintettek tájékoztatása

8.1.1 Adatkezelési tájékoztató

A Szervezet a tevékenységéhez kapcsolódóan az érintetti csoportok figyelembe vételével több különböző adatkezelési tájékoztatót készít, ezáltal biztosítva, hogy azok tömörek, könnyen áttekinthetők és közérthetők legyenek.
A Szervezet a következő adatkezelési tájékoztató típusokat alkalmazza:

- Adatkezelési tájékoztató - Ügyfél
- Adatkezelési tájékoztató – Munkavállaló
- Adatkezelési tájékoztató – Toborzás
- Adatkezelési tájékoztató – Rendezvény
- Adatkezelési tájékoztató – Üdülő
- Adatkezelési tájékoztató – FB tag

Az adatkezelési tájékoztatóknak a következő információkat kell tartalmazniuk az adott érintetti csoportra és adatkezelésekre:

- A Szervezetnek, mint adatkezelőnek megnevezése és elérhetőségei;
- A szervezet képviselője és elérhetősége;
- Az Adatvédelmi Tisztviselő (ha van) és elérhetőségei;
- Az érintettek köre;
- A személyes adatok forrása, ha nem az érintettől szerezték;
- A személyes adatok kezelésének célja, jogalapja és kategóriái
    - jogos érdek jogalap esetén a jogos érdek meghatározása
    - szerződéskötés esetén az adatszolgáltatás a szerződéskötés előfeltétele-e;
    - az adat szolgáltatása jogszabályon alapul-e
    - érintett köteles-e az adatszolgáltatásra, az adatszolgáltatás következményeinek elmaradása

- A személyes adatok címzettjei, vagy a címzettek kategóriái;
- Adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat;
- Személyes adatok tárolásának időtartama (vagy ezen időtartam meghatározásának szempontjai);
- Az érintett joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az adathordozhatósághoz való jog;
- Az érintett hozzájárulásán alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog;
- Adott esetben az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelésnek mi a jelentősége és következménye az érintettre nézve;
- A felügyeleti hatósághoz címzett panasz benyújtásának joga.

A konkrét adatkezelési tájékoztatókat az adatkezelési tevékenységek nyilvántartásában megadott adatkezelési paraméterekkel összhangban kell elkészíteni.

8.2 Tájékoztatási szabályok

8.2.1 Általános rész

A tájékoztatást átadásának módjai:

- **írásban** (személyesen vagy postai úton)
- **elektronikusan** (web, e-mail)

A tájékoztatások legyenek:

- tömörek,
- könnyen áttekinthetők,
- érthetőek,
- könnyen hozzáférhetőek,
- megfogalmazásuk legyen világos és közérthető.

A tájékoztatás nyújtása az érintett részére:

- ha az Érintettre vonatkozó személyes adatokat az Érintettől gyűjtik, a Szervezet a személyes **adatok megszerzésének időpontjában** az érintett rendelkezésére bocsátja az adatkezelési tájékoztatót
- ha az Érintettre vonatkozó személyes adatokat nem az Érintettől szerezték meg, a Szervezet az Érintett rendelkezésére bocsátja az adatkezelési tájékoztatót
    - a személyes adatok megszerzésének időpontjától számított ésszerű határidőn belül, de legkésőbb **egy hónapon belül** vagy
    - legalább az Érintettel való első kapcsolatfelvétel alkalmával (ha az adatok kapcsolattartás céljára használják) vagy
    - ha más címzettel is közlik az adatokat, legkésőbb a személyes adatok **első alkalommal való közlésekor**.

8.2.2 A Szervezethez álláspályázat útján jelentkező természetes személyek tájékoztatása

A Szervezet a www.arieskft.hu weblapon elérhetővé teszi az ASZ-07-04 Adatkezelési tájékoztató - Toborzás dokumentumot.
A tájékoztatás megadásának igazolása:

- A weboldalon elhelyezett jelölőnégyzet logolásával.

vagy

- A jelentkező a ***ASZ-07-04*** **Adatkezelési tájékoztató - Toborzás.pdf** fájlt letölti és az önéletrajzával együtt beküldi a Szervezet számára

vagy

- Az internetes toborzási portál által nyújtott adatkezelés igazolásával

8.2.3 Munkavállalók, Felügyelőbizottsági tagok tájékoztatása

A Szervezet munkavállalói esetében az ***ASZ-07-03 Adatkezelési*** **tájékoztató - Munkavállaló** a munkaszerződés melléklete.
A Szervezetnél megbízási szerződés alapján dolgozók esetében az ***ASZ-07-03*** **Adatkezelési tájékoztató - Munkavállaló** a megbízási szerződés mellékletét kell képezze, akként, hogy a meglévő szerződések kiegészítésre kerülnek, az újonnan megkötésre kerülő szerződésekhez pedig mellékletként csatolásra kerül.
A Szervezetnél megválasztott vezető tisztségviselők,Felügyelőbizottsági tagok esetében az ***ASZ-07-03*** **Adatkezelési tájékoztató – FB tag** a megválasztásról szóló határozat mellé kell elhelyezni, amennyiben megbízási szerztődés megkötésére is sor kerül,úgy annak mellékletét kell,hogy képezze.
A tájékoztatás megadásának igazolása:

- A hozzájárulás jogalap mentén kezelt adatkezelési tevékenységek esetében az aláírt munkaszerződés, illetve szerződés kiegészítő mellékletek,
- Kifejezett hozzájárulás esetén az egyedi adatkezeléshez aláírt nyilatkozat.

8.2.4 Ügyfelek tájékoztatása

Az **ügyfelek** kifejezés az alábbi weboldalakon vagy a Szervezet által nyújtott szolgáltatást igénybe vevő természetes személyeket és a cégek képviseltében eljáró **magánszemélyeket** jelenti.
A Szervezet a következő weboldalakon elérhetővé teszi az ***ASZ07-05*** **Adatkezelési tájékoztató—Ügyfél**

http://www.arieskft.hu

A Szervezet az ***ASZ-07-05*** **Adatkezelési tájékoztató—Ügyfél** dokumentumot papíralapon is megjeleníti és a telephelyen kifüggeszti.

A tájékoztatás megadásának igazolása:

- A hozzájárulás jogalap mentén kezelt adatkezelési tevékenységek esetében a Szervezet weboldalán rögzített naplófájl vagy az Érintett hozzájárulását igazoló papír alapú dokumentum.

8.2.5 Üdülő vendégek tájékoztatása

Az Önkormányzati feladat-átruházás keretén belül a Szervezet üdülőt üzemeltet. Jogszabályi kötelezettség a vendégeket bejelenteni a hatóságnak az Idegenforgalmi adó elszámolása miatt, ezért az Üdülőgondnok nyilvántartást vezet a vendégek törvény szerint előírt személyes adatiról. Az üdülőben megszálló személyek részére az ***ASZ-07-06 Adatkezelési* tájékoztató - Üdülő** a vonatkozó tájékoztató.
A tájékoztatás megadásának igazolása:

- Személyesen, az üdülőben elérhető minden vendég számára a tájékoztató és a Gondnok ismerteti a tartalmát és elérhetőségét a vendégekkel.

8.2.6 Partner tájékoztatása

Itt a **Partnerek** kifejezés a más cégekkel kötött (szolgáltatási, kereskedelmi, szállítói) szerződésekhez kapcsolódóan kezelt személyes adatok érintettjeit jelenti.

A Szervezet olyan szerződéseket köt üzleti partnereivel, amely rendelkezik arról, hogy a szerződő felek a szerződés során egymás számára átadott alkalmazotti személyes adatokat illetve teljesítési segédjük érintettjei személyes adatait (kapcsolattartói adatok) a jogos érdek mentén - a Szervezet és a partnere között a szerződés teljesítése és kapcsolattartás érdekében – a Szervezet és a partnere közötti szerződés megszűnésétől az általános elévülési idő leteltéig kezelik és őrzik meg a későbbi esetleges jogviták rendezése céljából a vonatkozó jogszabályi előírások betartásával.
A tájékoztatás megadásának igazolása:
A Szervezet az üzleti partnereivel megállapodik továbbá, hogy jogvita vagy érintetti adatkezeléssel kapcsolatos igénybejelentés esetén késedelem nélkül a egymás rendelkezésére bocsátják a tájékoztatással kapcsolatos bizonyítékokat.
Az adatkezelési elvárásokat az ***ASZ-24 Partneri szerződés Adatkezelési melléklet*** dokumentum alapján kell elkészíteni.

8.3 Az érintetti kérelmek teljesítésének támogatása

8.3.1 A kapcsolattartás csatornái

A Szervezet a következő kapcsolattartási csatornákat működteti:

- e-mail
- telefonon
- személyesen
- webformon keresztül.

Amennyiben az érintett kérdés, kérés vagy panasz okán a Szervezethez fordul, ezeket a bejelentkezéseket és az ezek nyomán született intézkedéseket a Szervezet nyilvántartja.
A nyilvántartást az ASZ-***07-01 Érintetti kérelmek nyilvántartása*** *dokumentumban* kell nyilvántartani.

8.3.2 Az érintett azonosítása

Az érintetti jogok teljesítésénél fontos szempont, hogy a kérelmet benyújtó érintett azonosítása megfelelő legyen.

8.3.3 E-mailen érkező kérelem

Csak azok a kérelmek teljesíthetők, melyekben a kezelt e-mail cím megegyezik a kérelem feladójának e-mail címével.
Az Érintett a kérelmét a titkarsag@arieskft.hu e-mail címre küldheti.

8.3.4 Telefonos ügyfélszolgálaton érkező kérelem

Az ügyintéző kolléga tájékoztatja az Érintettet, hogy a Szervezet csak írásban fogad el kérelmet az Érintettek azonosítása és védelme érdekében.

8.3.5 Személyesen bejelentett kérelem

Az ügyintéző kolléga személyazonosításra alkalmas fényképes igazolvány bemutatását kéri az Érintettől majd az ***ASZ-07-02 Érintetti adatkezelési igény bejelentés űrlap*** kitöltését követően átveszi az érintett kérelmét.
Amennyiben a természetes személy kilétével kapcsolatban kételyek merülnek fel a Szervezet további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.
Például:

- Korábbi szolgáltatás igénybevételének / vásárlásnak a részleteit,
- Az adatkezelő által kezelt további bármely adat vagy adatrészlet.

Az Érintettek azonosítását az Érintetti igényt felvevő kolléga végzi el. Kétség esetén késedelem nélkül bevonja az azonosításba az Adatvédelmi Tisztviselőt.

8.4 Kommunikáció és eszkaláció

Az 8.3.1 pontokban meghatározott csatornákon érkező Érintetti kérelmeket az Adatvédelmi Tisztviselő kezeli. Saját hatáskörben válaszol a kérelmekre.

8.4.1 Eszkaláció

Az Adatvédelmi Tisztviselő nem elutasítható adatkezelési korlátozási kérelem és tiltakozási kérelem esetén jelenti a Szervezet ügyvezetőjének az esetet és a GDPR-ban, illetve a jelen szabályzatban foglaltak szerint jár el.

8.4.2 Incidens gyanú

Amennyiben az Adatvédelmi Tisztviselő egy Érintetti kérelem kapcsán adatkezelési incidens gyanúját tárja fel, akkor az incidenskezelési szabályozásnak megfelelően kivizsgálja az esetet.

8.5 Tájékoztatás az érintetti jogok gyakorlása során

Az érintetti jogok érvényesítése kapcsán **az egyes folyamatok részeként** az érintetteket **tájékoztatni** szükséges.
A tájékoztatások ütemezése:
A Szervezet a kérelem nyomán hozott intézkedésekről tájékoztatja az érintettet:

- indokolatlan késedelem nélkül, de
- legkésőbb a kérelem beérkezésétől számított **egy hónapon belül**.

Amennyiben a kérelem egy hónapon belül nem teljesíthető, a Szervezet

- a kérelem kézhezvételétől számított **egy hónapon belül** a késedelem okainak megjelölésével **tájékoztatja az érintettet, és**
- **tájékoztatja** az intézkedések végrehajtásának új határidejéről, amely a kérelem kézhezvételétől számított **három hónapon belül** kell legyen.

Amennyiben a Szervezet **nem tesz intézkedéseket** az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított **egy hónapon belül tájékoztatja** az érintettet

- az intézkedés **elmaradásának okairól**, valamint
- arról, hogy az érintett **panaszt nyújthat** be valamely felügyeleti hatóságnál, és
- élhet bírósági jogorvoslati jogával.

8.5.1 Tájékoztatás költsége

A Szervezet az intézkedéseket, illetve a szükséges tájékoztatásokat első alkalommal **díjmentesen** biztosítja.
Amennyiben az Érintett egy hónapon belül 2. alkalommal is kikéri ugyan azon adatokat, melyek ez idő alatt nem változtak az Adatkezelő adminisztratív költséget számít fel.

- Az adminisztratív költség elszámolás alapja a mindenkori minimálbér órára vetített költsége, mint óradíj.
- A tájékoztatáshoz felhasznált munkaórák száma az előbbi óradíjon elszámolva.
- Továbbá a papír alapú tájékoztatási igény esetén a válasz nyomtatási költsége önköltségi áron és postázási költsége.

8.5.2 Tájékoztatás megtagadása

Ha az érintett kérelme egyértelműen **megalapozatlan**, nem jogosult a tájékoztatásra vagy az Szervezet, mint adatkezelő bizonyítani tudja, hogy az Érintett rendelkezik a kért információkkal az adatkezelő elutasítja a tájékoztatási kérelmet.
Például:

- Három hónapon belül megismételt tájékoztatási kérelem.
- Nem gondviselő szülő adatszolgáltatási igénye esetén.
- 16 évnél fiatalabb adatszolgáltatási kérelme esetén.

Ha az érintett kérelme különösen ismétlődő jellege miatt – **túlzó**, a Szervezet megtagadhatja a kérelem alapján történő intézkedést, ha

- Egy hónapon belül harmadik alkalommal él az Érintett ugyanazon tárgyú a 15-22. cikk szerinti jogai gyakorlására irányuló kérelemmel.

8.6 Az érintett hozzáférési joga

Az érintett jogosult arra, hogy a Szervezettől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és az adatkezeléssel kapcsolatos információkhoz hozzáférést kapjon.
A következő adatkezeléssel kapcsolatos információkat kell megadni:

- Az adatkezelés céljai;
- Az érintett személyes adatok kategóriái;
- Azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
- Adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- Az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- A valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- Ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- Az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.
- Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a GDPR 46. cikk szerinti megfelelő garanciákról.

A Szervezet az érintett kérésére az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. A személyes adatok összegyűjtését a szervezet végzi el.

Az Érintett felé kommunikálja az összegyűjtött adatokat: ***Adatvédelmi Tisztviselő***

8.7 Helyesbítéshez való jog

Az érintettek kérésére a Szervezet biztosítja a rájuk vonatkozó **pontatlan személyes adatok** indokolatlan késedelem nélküli **helyesbítését**.
Az adatkezelés célját figyelembe véve, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – kiegészítő nyilatkozat útján történő – kiegészítését.
Az adatok módosítását a kapcsolattartásra kijelölt személy végzi

- A központi kapcsolattartásra szolgáló adatbázisban.
- Minden olyan szigetszerű alkalmazásban, ahol a központi adatbázis nem szinkronizálódik automatikusan.

Az Adatvédelmi Tisztviselő rendszeresen ellenőrzi az Érintettek adatmódosítási kérelmeinek pontos végrehajtását.

Amennyiben az Érintett olyan adatot szeretne módosítani, amelyet valamely Európai Uniós vagy magyar jogszabályi előírás alapján az adatkezelő nem módosíthat, a Szervezet késedelem nélkül, de maximum egy hónapon belül tájékozgatja az Érintettet, hogy a változtatási igényt nem hajtja végre.
Például:

- A számvitelről szóló 2000. évi C. törvényben meghatározott bizonylatokat módosíthatatlan formában kell 8 évig megőrizni. Ezt az Érintett kérésére módosítani tilos.

8.8 Törléshez való jog

Amennyiben az érintett személyes adatainak törlését kéri, a Szervezet azt indokolatlan késedelem nélkül elvégzi, ha fennáll a következő indokok valamelyike:

- Az érintett **visszavonja** az adatkezelés alapját képező **hozzájárulását**, és az adatkezelésnek nincs más jogalapja,
- Az érintett a **8.11.1 pont** alapján **tiltakozik** az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
- Az érintett a **8.11.2 pont** alapján **tiltakozik** az adatkezelés ellen,
- A személyes adatokat kezelése jogellenesen történik,
  a személyes adatokat uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell.

Amennyiben az Érintett olyan adatot szeretne törölni, amely valamely Európai Uniós vagy magyar jogszabályi előírás alapján az adatkezelő nem törölhet, a Szervezet késedelem nélkül, de maximum egy hónapon belül tájékoztatja az Érintettet, hogy a törlési igényt nem hajtja végre.
Például:

- A számvitelről szóló 2000. évi C. törvényben meghatározott bizonylatokat módosíthatatlan formában kell 8 évig megőrizni. Ezt az Érintett kérésére törölni tilos.

Az Szervezet továbbá törli a kezelt személyes adatokat, ha a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték és az adatkezelést a Szervezet nem minősítette át más adatkezelési célra és jogalapra.

8.9 Korlátozáshoz való jog

Az érintett kérésére a Szervezet **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 a Szervezet 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 a **8.11.1 pont** szerint tiltakozott az adatkezelés ellen, mely esetben a korlátozás arra az időtartamra vonatkozik, amíg a megállapításra nem kerül, hogy a Szervezet jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben. A korlátozás következő lehetőségek egyikével zárulhat:
    - a Szervezet elfogadja a tiltakozást és a befejezi a tiltakozás szempontjából releváns adatkezelést
    - az érintett elfogadja a Szervezet indoklását az adatkezelés jogszerűségére vonatkozóan, az adatkezelést nem kell korlátozni
    - jogorvoslati eljárás keretében döntés születik a tiltakozás elfogadásáról vagy elutasításáról.

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 az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.
A korlátozásra vonatkozó követelmények teljesítése érdekében a Szervezet a korlátozással érintett adatokat **megjelöli**.
Az adatkezelés korlátozásának feloldásáról előzetesen a Szervezet értesíti az érintettet.

8.10 Adathordozhatósághoz való jog

Az érintett jogosult arra, hogy a rá vonatkozó, általa a Szervezet rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, ha:

- az adatkezelés az érintett hozzájárulásán alapul **vagy**
- az adatkezelés az érintettel kötött szerződésen alapul, **és**
- az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

A hordozható adatok átadásáért felelős az: ***Adatvédelmi Tisztviselő***

8.11 Tiltakozáshoz való jog

8.11.1 Tiltakozás jogos érdek vagy közérdek, közhatalmi jogosítvány gyakorlása jogalapú adatkezelés ellen

Az érintett jogosult arra, hogy bármikor tiltakozzon személyes adatainak a jogos érdek vagy közhatalmi jogosítvány jogalapon alapuló kezelése ellen.
Ebben az esetben a Szervezet 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.

8.11.2 Tiltakozás közvetlen üzletszerzés célú adatkezelés ellen

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ebben az esetben a Szervezet a személyes adatokat e célból **nem kezelheti tovább**.
A 8.11.1. és a 8.11.2 pontban foglalt tiltakozási jogról legkésőbb az első kapcsolatfelvétel során kifejezetten, egyértelműen és minden más információtól elkülönítve kell az érdekeltet tájékoztatni.

8.12 Automatikus döntéshozatal, profilalkotás

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag **automatizált adatkezelésen alapuló döntés,** illetve a **profilalkotás**t hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené, ezért a Szervezet az ilyen tevékenységet csak a következő esetekben végez:

- Az érintett kifejezett hozzájárulása vagy
- Uniós vagy tagállami jog teszi lehetővé vagy
- Az érintett és a Szervezet közötti szerződés megkötése vagy teljesítése érdekében szükséges.

Amennyiben a Szervezet az érintettre joghatással bíró automatizált adatkezelésen alapuló döntéseket hoz, illetve a profilalkotást végez köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, biztosítva, hogy az érintett

- Emberi beavatkozást kérjen a döntési folyamatba,
- Álláspontját kifejezze, és
- A döntéssel szemben kifogást nyújtson be.

9. AZ ÉRINTETTI KÉRELMEK TELJESÍTÉSE

9.1 Az igény jogosságának vizsgálata

A szabályzatnak megfelelő csatornán érkező igény kezelhető csak. A nem megfelelő csatornán érkező igényét át kell irányítani a megfelelő csatornára.

- E-mailek esetében át kell küldeni a titkarsag@arieskft.hu e-mail címre. A fogadó levelező fiók beérkező és a kimenő levelei közül is el kell távolítana az igényt tartalmazó levelet.

A szervezet csak írásban fogad el érintetti igényt, telefonon érkező igényeket el kell utasítani.

9.2 Az érintetti igény rögzítése

Az igényt az ***ASZ-07-01 Érintetti kérelmek nyilvántartása*** dokumentumban az Adatvédelmi Tisztviselő rögzíti és az igény teljesítésének lezárásáig folyamosan kezeli.

Kivételt képez, ha az érintett a törlési, tiltakozás vagy hozzájárulás követően megvalósuló törlési igényét a Szervezet által üzemeltetett hírlevél küldő rendszer leiratkozás funkcionalitásával hajtja végre.

A titkarsag@arieskft.hu-ra érkező igények esetében az igény egyedi azonosítót kap.

9.3 Az érintetti igény rögzítése

1. Az Adatvédelmi Tisztviselő ellenőrzi a következőket:

a. Kezeli-e a szervezet az Érintett adatait törvényi kötelezettség mentén. (Számviteli, munkaügyi, egészségügyi stb.) Ha igen lejárt-e a törvényben előírt adatkezelési határidő. Amennyiben nem kezeli törvényi szabályozás mentén az adatokat vagy már lejárt a törvényben meghatározott határidő az adatok törölhetők.
b. Kezeli-e a Szervezet az Érintett adatait Szerződéses jogalap mentén, és a megkötött szerződés (melyben az érintett az egyik fél) érvényben van-e?
c. Amennyiben érvényben van akkor azok az adatok melyeket e jogalap mentén kezel a Szervezet nem törölhetők, csak a szerződés felmondásával együtt.
d. Amennyiben nincs szerződés vagy már nincs érvényben, az adatok törölhetők.
e. Ha a szervezet az érintett érdeke jogalap mentén kezeli az adatokat az adatok nem törölhetők.
f. Ha a szervezet jogos érdek mentén kezeli az adatokat akkor érdekmérlegelést kell végezni. Amennyiben az érdekmérlegelés eredményeképpen igazolhatóan a Szervezetnek erősebb az érdeke az adatkezelésre akkor elutasítható a törlési igény. Ebben az esetben tájékoztatni kell az érdekmérlegelés eredményéről az érintettet. Ezt az érvelést az érintett vitathatja és bírósághoz fordulhat. Ha a szervezet közvetlen üzletszerzés céljából jogos érdekre hivatkozva kezeli az adatokat, az adatkezelést meg kell szakítani, az adatokat törölni kell és nem kell érdekmérlegelést végezni.

2. Az Adatvédelmi Tisztviselő ellenőrzi, hogy az érintett adatát a Szervezet átadta-e adatfeldolgozónak, vagy további adatkezelőnek.
   Amennyiben igen, akkor értesíteni kell az adatfeldolgozót vagy a további adatkezelőt az alábbiak szerint:
   a. Amennyiben az érintett már rendelkezik adatvédelmi azonosítóval, melyet az adatfeldolgozó is nyilván tart, abban az esetben a korábbiakban kiadott adatvédelmi azonosítóra hivatkozva kéri az érintett törlését.
   b. Amennyiben az érintett még nem kapott az adatátadáshoz egyedi azonosítót, az adatkezelő tájékoztatja az adatfeldolgozót, vagy további adatkezelőt hogy Érkezett egy érintetti igény erre a felhasználóra, és ezt az alábbi adatvédelmi azonosítóval láttuk el. Egy következő levélben már csak az adatvédelmi azonosítóra hivatkozva küldjük a teendőket. Az első e-mailt, amelyben még a személyes adatok benne voltak, az e-mailt majd törölje le az adatfeldolgozó.

3. Amennyiben nincs adatfeldolgozói adattovábbítás, akkor az Adatvédelmi Tisztviselő a Szervezet minden aktív rendszeréből törli az érintett adatait és kizárólag az ***ASZ-07-01 Érintetti kérelmek nyilvántartásban*** szerepelhet az érintett neve és az egyértelmű azonosításhoz szükséges további kiegészítő adat (cím, anyja neve, egyedi azonosító)

   Az 2. sz. melléklet tartalmazza az aktív rendszerek listáját, amelyekben ellenőrizni kell, hogy szerepel-e az érintett.

   Az ***ASZ-07-01 Érintetti kérelmek nyilvántartás*** hozzáférésre jogosultak: Ügyvezető igazgató és az Adatvédelmi Tisztviselő.

   A szervezet az ASZ***-07-01 Érintetti kérelmek nyilvántartás*** minden érintetti igény esetén, de negyed évente egy alkalommal mindenképpen mentést végez egy titkosított USB pendrive-ra. Az ASZ***-07-01 Érintetti kérelmek nyilvántartás*** biztonsági mentésének tárolási helye (USB pendrive fizikai elérhetősége: ügyvezető igazgató

A biztonsági mentést tartalmazó USB pendrive-hoz ugyan azok a személyek férhetnek hozzá, mint akik az ***ASZ-07-01 Érintetti kérelmek nyilvántartóhoz.***

4. Az érintetti igény végrehajtásáról az Adatvédelmi Tisztviselő emailben tájékoztatja az érintettet. Az email törölni kell az levelező rendszerből, az elküldést követően.

10.ADATFELDOLGOZÓK MENEDZSELÉSE

A Szervezet által megbízott **adatfeldolgozó** az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag technikai feladatként a Szervezet rendelkezései szerint dolgozhatja fel, saját céljára a Szervezet adatain adatfeldolgozást nem végezhet, a személyes adatokat a Szervezet rendelkezései szerint köteles tárolni és megőrizni vagy az adatkezelési folyamat végeztével a Szervezet döntése alapján törölni.

10.1 Adatfeldolgozók az EU-n belül

Itt EU-n belülinek az **EGT tagállamai** tekintendők, ezen országok vonatkozásában nincs semmilyen korlátozás, azaz olyan mintha Magyarország területén belüli adattovábbításra kerülne sor.
A Szervezet csak olyan adatfeldolgozókat vesz igénybe, akik szervezési és technikai intézkedésekkel biztosítani tudják, hogy a Szervezet adatvédelmi követelményei teljesüljenek. Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni. Az adatfeldolgozókkal kötött szerződésnek rendelkeznie kell a következőkről:

- Az adatfeldolgozó a személyes adatokat kizárólag a Szervezet 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 Szervezet 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 Szervezet felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért;
- Az adatfeldolgozó megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti a Szervezetet abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak kapcsolódó kérelmek megválaszolása tekintetében;

- Az adatfeldolgozó segíti a Szervezetet az adatvédelmi incidensek kezelésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
- Az adatfeldolgozó az adatkezelési szolgáltatás nyújtásának befejezését követően a Szervezet döntése alapján minden személyes adatot töröl vagy visszajuttat a Szervezetnek, és törli a meglévő másolatokat;
- Az adatfeldolgozó a Szervezet rendelkezésére bocsát minden olyan információt, amely lehetővé teszi és elősegíti a Szervezet által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az adatfeldolgozók adatvédelmi szempontok menedzselésének a felelőse: ***A partner kapcsolattartója***

10.1.1 Adatfeldolgozói szerződés alvállalkozóval

A Szervezet az adatfeldolgozókkal az ***ASZ-30 Adatfeldolgozói szerződés*** minta alapján a fennálló szerződés mellett az adatkezelésre külön szerződést köt. Új szerződés esetén a szerződő felek döntése alapján az adatkezelési elvárások az ***ASZ-30 Adatfeldolgozói szerződés*** minta tartalma a szerződés részeként vagy mellékleteként is kezelhető.

10.1.2 Adatfeldolgozói szerződés, amennyiben a Szervezet az adatfeldolgozó

Amennyiben egy adatkezelési tevékenységben a Szervezet az adatfeldolgozó a Szervezet feltétlen érdeke, hogy az adatfeldolgozás során az adatkezelő utasítása alapján járjon el. Ilyen estekben ***ASZ-31 Adatfeldolgozói szerződés*** minta alapján a fennálló szerződés mellett az adatkezelésre külön szerződést köt. Új szerződés esetén a szerződő felek döntése alapján az adatkezelési elvárások az ***ASZ-31 Adatfeldolgozói szerződés*** minta tartalma a szerződés részeként vagy mellékleteként is kezelhető.

10.1.3 Al-Adatfeldolgozói szerződés

Amennyiben egy adatkezelési tevékenységben a Szervezet az adatfeldolgozó és az adatfeldolgozási tevékenységéhez alvállalkozót, azaz al-adatfeldolgozót vesz igénybe ezt csak az adatkezelő írásos engedélyével teheti.
Az AL- Adatfeldolgozóval a Szervezet a fennálló szerződése mellett az ***ASZ-32 Adatfeldolgozói szerződés*** minta alapján az adatfeldolgozásra külön szerződést köt. Új szerződés esetén a szerződő felek döntése alapján az adatkezelési elvárások az ***ASZ-32 Adatfeldolgozói szerződés*** minta tartalma a szerződés részeként vagy mellékleteként is kezelhető.

11.ADATÁTADÁS 3. FÉL SZÁMÁRA

A Szervezet az általa kezelt adatokat különböző céllal alvállalkozóknak, azaz adatfeldolgozóknak adja át.
A Szervezet adatátadási nyilvántartást vezet az *ASZ-09-1 Adatátadási nyilvántartásban* dokumentumban.

A nyilvántartásban a következő adatokat tartja nyilván a Szervezet:

Adatvédelmi azonosító	Egyedi folyamatosan növekedő sorszám
Teljes Név	Az Érintett vezeték és keresztneve
Vezetéknév	Az Érintett vezetékneve
Keresztnév	Az Érintett keresztneve
Átadás dátuma	Az Adatátadás dátuma
Adatfeldolgozó neve	Az az Adatfeldolgozó, akinek az adatot átadta a Szervezet
Egyéb	A szervezet által meghatározott egyéb adat

11.1 Adatvédelmi Azonosító használata

A Szervezet Adatvédelmi Azonosítót alkalmaz olyan esetben, ahol az Érintett élhet az GDPR rendeletben megfogalmazott törlés, elfeledtetés vagy korlátozás jogával. Az alkalmazás módja az adatkezelés automatizálási szintjétől, az adatok mennyiségétől, a reklamációk számától, valamint az adatkezelés jogalapjától függően különböző.

11.1.1 Adatvédelmi Azonosító használata adatátadáskor regisztrálva

Amikor a Szervezet adatfeldolgozónak átadja az Érintett személyes adatait az alábbiak szerint alkalmazza az Adatvédelmi Azonosító számot.

1. Az Érintett megadja a személyes adatait a Szervezetnek egy olyan adatkezelési folyamatban, ahol a Szervezet alapértelmezetten bevezette az Adatvédelmi Azonosítót. Jelen szabályzat bevezetésekor a Szervezet egy adatkezelési folyamatban sem alkalmaz adatvédelmi azonosítót.
2. A Szervezet egyedi Adatvédelmi Azonosítóval látja el az Érintettet az ASZ-09-01 Adatátadási nyilvántartásban legkésőbb az első adatátadás előtt
3. A Szervezet az Adatvédelmi Azonosítóval együtt emailben átadja az Érintett adatait az Adatfeldolgozónak
    a. A szervezet törli a levelező rendszerből az elküldött adatokat (még a napi mentés lefutása előtt)
4. Az Adatfeldolgozó az emailből az átadott adatokat saját nyilvántartásába átmásolja, majd törli az e-mailt.

11.1.2 Adatvédelmi Azonosító használata Érintetti bejelentéskor alkalmazva

Olyan esetben alkalmazandó, ha a Szervezet az adatátadáskor nem látta el az Érintettet Adatvédelmi Azonosítóval. Az adatkezelés ebben az esetben már folyamatban van és a Szervezet az adatokat már átadta egy adatfeldolgozónak. Mindkét fél kezeli az adatokat a megadott adatkezelési folyamat mentén.

Alkalmazási példa:

a) Ha az adatátadás tömeges, és az adatfeldolgozó alapértelmezetten nem fér hozzá az átadott adatokhoz
   - Felhő alapú automatizált hírlevél küldő rendszer, ahol az Érintett akár közvetlenül is élhet az hozzájárulás visszavonásának jogával.

11.2 Adatkezelési jogalapok szerint kategorizálása

Az egyes adatkezeléshez kapcsolódó jogalapok esetén az adatvédelmi azonosító használata különböző vagy akár szükségtelen az elvégzendő nagymennyiségű, csoportos vagy azonos adatkezelési tevékenység következtében.

11.2.1 Hozzájáruláson alapuló adatkezelés esetében

A Szervezet alkalmazza az Adatvédelmi Azonosító annak érdekében, hogy az Érintett bármikor visszavonhassa hozzájárulását és a Szervezet biztosítsa számára az törléshez, korlátozáshoz, visszavonáshoz, tiltakozáshoz való jogát.

11.2.2 Szerződésen alapuló adatkezelés esetében

A Szervezetnek nem kell alkalmaznia Adatvédelmi Azonosítót, mert a szerződés ideje alatt az érintett nem élhet a törléshez, korlátozáshoz, visszavonáshoz, tiltakozáshoz való jogával. A szerződés lejárata után vagy át kell minősíteni az adatkezelési célt vagy törölni kell az adatot.

11.2.3 Jogi kötelezettségen alapuló adatkezelés esetében

A Szervezetnek nem kell alkalmaznia Adatvédelmi Azonosítót, mert a jogi kötelezettség mentén kezelt adatkezelés ideje alatt az érintett nem élhet a törléshez, korlátozáshoz, visszavonáshoz, tiltakozáshoz való jogával. A határidő lejárata után vagy át kell minősíteni az adatkezelési célt vagy törölni kell az adatot.

11.2.4 Az Érintett érdekeinek védelme

A szervezet ezt a jogalapot nem alkalmazza.

11.2.5 Közérdekű vagy közhatalmi jogosítvány gyakorlása

A Szervezet alkalmazza az Adatvédelmi Azonosítót annak érdekében, hogy az Érintett bármikor tiltakozhasson a személyes adatainak kezelési ellen és amennyiben a Szervezet az érdekmérlegelést követően jogosnak látja biztosítja az Érintett számára a törléshez, korlátozáshoz, visszavonáshoz, tiltakozáshoz való jogát.

11.2.6 Jogos érdek

A Szervezet alkalmazza az Adatvédelmi Azonosítót annak érdekében, hogy az Érintett bármikor tiltakozhasson a személyes adatainak kezelési ellen és amennyiben a Szervezet az érdekmérlegelést követően jogosnak látja biztosítja az Érintett számára a törléshez, korlátozáshoz, visszavonáshoz, tiltakozáshoz való jogát.

12.ADATÁTADÁS – ADATTÖRLÉS FOLYAMATA

12.1 Adatvédelmi Azonosító használata Adatvédelmi Azonosítóval rendelkező Érintettek esetében

1. Az Érintett visszavonja hozzájárulását vagy él a tiltakozási jogával, melyet a Szervezet, mint adatkezelő jogosnak ítél. Az adatkezelő meggyőződik az Érintett személyazonosságáról és mindkét esetben törli az Érintett személyes adatait.
2. A Szervezet értesíti az adatfeldolgozó(ka)t az Érintett igényéről. Az értesítésben csak az Adatvédelmi Azonosító és a kapcsolódó igény szerepelhet. Bármely más személyes adatot kifejezetten Tilos a levélben közölni.
3. A Szervezet értesíti az Érintettet az adattörlésről, amennyiben emailben történt az informálás, úgy törli az emailt is a levelezési rendszeréből.

   A Szervezet törli az Érintett személyes adatait, de megőrzi az Adatvédelmi azonosítót és ezt az Adatvédelmi Azonosítót sem ugyan ennek a Természetes személynek sem másnak nem adja ki még egyszer. Amennyiben az Érintett még egyszer megadja az adatait a Szervezetnek úgy egy új adatvédelmi azonosítót kell a számára kiadni.

12.2 Adatvédelmi Azonosító használata az Érintetti igény bejelentését követően

1. Az Érintett visszavonja hozzájárulását vagy él a tiltakozási jogával, melyet az Adatkezelő jogosnak ítél. Az adatkezelő meggyőződik az Érintett személyazonosságáról.
   A **bejelentést követően az Érintettet felveszi az *ASZ-09-01 Adatátadási nyilvántartásba*** és ellátja egy Adatkezelési Azonosítóval, majd erről informálja az Érintettet. Ezt követelően a hozzájárulás visszavonása és a tiltakozás esetében is törli az Érintett személyes adatait.
2. A Szervezet értesíti az adatfeldolgozó(ka)t, hogy az egyik Érintetett adatvédelmi azonosítóval látta el, emailben közli az azonosításhoz szükséges összes adatot és az Adatvédelmi Azonosítót.
3. Az adatfeldolgozó **rögzíti az adatátadási nyilvántartásban** az Érintettet és a kapcsolódó Adatvédelmi Azonosítót, majd törli az emailt.
4. A Szervezet egy következő emailben értesíti az adatfeldolgozó(ka)t az Érintett igényéről. Az értesítésben **csak az Adatvédelmi Azonosító** és a kapcsolódó igény szerepelhet. Bármely más személyes adatot kifejezetten Tilos a levélben közölni.
5. A Szervezet értesíti az Érintettet az adattörlésről, amennyiben emailben történt az informálás **törli az emailt** a levelezési rendszeréből.

   A Szervezet törli az Érintett személyes adatait, de **megőrzi az Adatvédelmi Azonosítót** és ezt az Adatvédelmi Azonosítót sem ugyan ennek a Természetes személynek sem másnak nem adja ki még egyszer. Amennyiben az Érintett még egyszer megadja az adatait a Szervezetnek úgy egy új adatvédelmi azonosítót kell a számára kiadni.

12.3 Adatvédelmi Azonosító használata Adatkezelés korlátozásának bejelentését követően

1. Az Érintett él azzal a jogával, hogy az általa rendelkezésre bocsátott személyes adatok kezelését korlátozhatja az alábbi indokokkal:
    - Vitatja az adatainak pontosságát,
    - Vitatja az adatkezelés jogosságát,
    - Igényelheti az adatkezelő által törlésre szánt adatok további tárolását jogi igények előterjesztéséhez,
    - Az érintett tiltakozása esetén, míg megállapításra nem kerülnek, hogy mely fél jogos indokai élveznek az ügyben elsőbbséget. Ez esetben a korlátozás csak az tiltakozási ügy lezárásáig áll fent.
2. A Szervezet az Érintett személyes adatait a korlátozás indokaként megjelölt ügy lezárásáig, kizárólag az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez használhatja.
3. Amennyiben a Szervezet a megadott Adatvédelmi Azonosítóval ellátott adatsort kiadta Adatfeldolgozónak, akkor haladéktalanul köteles azt értesíteni az Adatvédelmi azonosítóhoz rendelt adatok korlátozásáról.
4. A korlátozás feloldásáról az Adatkezelő előzetesen értesíti az Érintettet.

13.ÉRINTETTI JOGOK ALKALMAZÁSA ADATVISSZAÁLLÍTÁST KÖVETŐEN

A Szervezet adatmentési és **adat visszaállítási folyamataiba beépíti**, hogy az informatikai rendszer mentéséből vagy archiválásából történő adat visszaállítás esetén az az adat visszaállítást követően, de még az éles használat megkezdése előtt az Adatvédelmi Tisztviselő ellenőrzi a következőket:

1. Az adat visszaállítás időpontja és az adatmentés időpontja között volt-e olyan Érintett, aki leiratkozott a hírlevélről vagy egyéb módon az adatainak törlését, korlátozását kérte a Szervezettől.
2. Az Adatvédelmi Tisztviselő ellenőrzi, hogy az ***ASZ-07-01 Érintetti kérelmek nyilvántartása biztonsági mentése*** tartalmaz-e az előző pontban megadott feltételeknek megfelelő adatokat.
3. Az Adatvédelmi Tisztviselő a visszaállított adatokban az ***ASZ-07-01 Érintetti kérelmek nyilvántartása mentése*** alapján elvégzi a szükséges műveleteket törlés (deperszonalizálja), korlátozza az érintetti adatokat az Érintettek igényének megfelelően.

Az adat visszaállítást követően az Érintettek adatainak ellenőrzését a szervezet végzi.

14.ADATTOVÁBBÍTÁS HARMADIK ORSZÁGOKBA

EU-n kívülinek, azaz 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:

1) Az adattovábbításhoz nem szükséges külön engedély azon országok esetében, ahol a Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, **megfelelő védelmi szintet** biztosít

   Ezen országok aktuális listája: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
2) A felügyeleti hatóság által jóváhagyott megállapodás a Szervezet és a címzett között (GDPR 46. cikk (3)).
3) Kötelező erejű vállalati szabályok vannak érvényben az adatfeldolgozó és a Szervezet között.

   Ezen országok aktuális listája:
   http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

4) Amennyiben az 1-3 pontban megfogalmazott határozat és megfelelő garanciák nem állnak rendelkezésre az adattovábbításhoz a Szervezet tájékoztatja az Érintettet a 3. Országba történő adattovábbítás veszélyeiről és kifejezett hozzájárulását kéri az adatok továbbításához. *ASZ-22 3. Ország adattovábbítási nyilatkozat* alapján.

5) A Szervezet által nyújtott szolgáltatás igénybevételéhez és a szerződés teljesítéséhez szükséges az 3. Országba történő személyes adatok továbbítása. Erről a szervezet az Adatvédelmi tájékoztatóban az Érintettet értesíti ezért ezekhez a tevékenységekhez az 1-4 pontban meghatározott feltételeket nem kell teljesíteni.

Az 3. Országba történő adattovábbítási folyamat előtt a Megfelelő biztonsági garanciák ellenőrzését elvégzi: ***Adatvédelmi Tisztviselő***

15.OKTATÁS ÉS KÉPZETTSÉGI ELVÁRÁSOK

15.1 Felkészültség

Az Adatvédelmi Tisztviselő és az Adatkezelési folyamatgazdák esetében a szükséges szakmai felkészültséget a munkatársak munkaköri leírásában vagy a megbízási szerződésükben kell meghatározni az alábbiak szerint:
Elvárás:

Adatvédelmi Tisztviselő esetében

- A Jogi diploma, adatvédelmi szakjogász, információbiztonsági adatvédelmi szakirányú végzettség vagy releváns munkakörben szerzett szakmai tapasztalat.
    - pld: ISO 27001, BS 10012, CISSP, CISA végzettség
- Rendszeres képzés/önképzés.

Adatkezelési folyamatgazdák estében:

- Évente egy alkalommal a Szervezet által biztosított Adatvédelmi oktatáson való részvétel,
- Jelen adatvédelmi szabályzat vonatkozó részeinek ismerete.

A feladatkört ellátó a felkészültséget igazoló dokumentumokat a Szervezet képviselője számára bemutatja

> *A megfelelő szakirányú végzettség vagy szakmai tapasztalat ellenőrzését elvégzi a:* ***HR vezető***

15.2 Tudatosság fenntartása a szervezetben

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

a) A Szervezet jelen szabályzatban rögzített adatvédelmi elvárásaival,
b) Szerepükkel az adatvédelmi rendszer működtetésében,
c) Az adatkezelésre vonatkozó szabályok megszegésének lehetséges következményeivel,
d) Egy adatvédelmi incidens esetében a riasztási protokollal.

A szervezet irányítása alatt munkát végző személyeknek rendszeres adatvédelmi tudatossági képzésben kell részesülniük a jelen szabályzat 8.2 pontjában részletezettek szerint. A tudatosító képzések megszervezéséért felelős az ***Adatvédelmi tisztviselő***

16.VÁLTOZÁSKEZELÉS

A Szervezet folyamatosan figyelemmel kíséri az adatkezelési tevékenységeket érintő változásokat:

- Az **Adatvédelmi Tisztviselő** feladata, hogy beazonosítsa azokat a **jogszabályi változások**at, illetve az **érdekelt felek elvárásaina**k azon **változásai**t, amelyek hatással lehetnek az adatkezelési tevékenységnek a természetes személyek jogait és szabadságait érintő kockázataira.
- Az adott adatkezelési tevékenységért felelős Adatkezelési folyamatgazda és az Adatvédelmi Tisztviselő feladata, hogy beazonosítsa azokat a **szervezési és technikai változások**at, amelyek hatással lehetnek az adatkezelési tevékenységnek a természetes személyek jogait és szabadságait érintő kockázataira.
- Az **ügyvezető igazgató** 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.

A Szervezetnek felügyelet alatt kell tartania a tervezett változásokat.

17.ADATVÉDELMI KÉPZÉS

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

17.1.1 Képzési tematikák:

Adatvédelmi Tisztviselő képzés

Több napos, személyes oktatás, amely a felkészíti az Adatvédelmi Tisztviselőt munkája elvégzésére.

- GDPR rendelet ismeret
- Kötelező adminisztráció elvárások
- Adatkezelési elvek
- Adatkezelés jogalapjai
- Érintett jogai
- Érintett jogainak teljesítési lehetőségei
- Adatvédelemi incidens bejelentése
- Kommunikációs képzés
- Hatósági kommunikáció
- Ellenőrzés, auditálási ismeretek

Adatvédelmi oktatás az Adatkezelési folyamatgazdáknak

Fél napos személyes oktatás, amely a felkészíti Adatkezelési folyamatgazdákat a személyes adatok kezelésével kapcsolatos feladataikra.

- Adatkezelési elvek
- Adatkezelés jogalapjai
- Érintett jogai
- Érintett jogainak teljesítési lehetőségei
- Adatvédelemi incidens szervezeten belüli eszkalációs rendje

Általános adatvédelmi tudatosító képzés

GDPR alapok – elektronikus oktatási anyag
Adatkezelési elvek

- Adatkezelési elvek, jogalapok
- Érintett jogainak teljesítési lehetőségei
- Adatvédelemi incidens szervezeten belüli eszkalációs rendje

18.AZ ADATKEZELÉSI FOLYAMATOK ÉRTÉKELÉSE

18.1 Folyamatos megfigyelés

A Szervezet tervezett módon belső auditokat végez, annak ellenőrzésére, hogy az adatkezelési folyamatai.

Az Adatvédelmi Tisztviselő folyamatosan ellenőrzi az alábbi teljesítmény mutatókat:

- Az Adatkezelési folyamatgazda kollégák 1 hónapja nem fordultak kérdéssel az Adatvédelmi Tisztviselőhöz
- A szervezet vezető beosztású kollégái 1 hónapja nem jelentettek adatkezelési folyamat változtatást
- Fél éve nem volt Érintetti panaszkezelési igény
- Service desk rendszerben 1 hónapja nem volt adatvédelmi incidens bejelentés (Notebook, USB eszköz elvesztése)

18.2 Időszakos ellenőrzés

Az **Adatvédelmi Tisztviselő** tervezett módon ellenőrzéseket hajt végre az Adatvédelmi szabályozási rendszer működésének megfelelősége érdekében.
Amennyiben a 17.1 pontban megfogalmazott valamely teljesítmény mutató megfigyelésekor eléri a küszöbértéket az Adatvédelmi Tisztviselő késedelem nélkül ellenőrzi az érintett területen a jelen szabályzatban megfogalmazott elvárások teljesülését.

Ezen felül időszakos véletlenszerű mintavételezés alapján ellenőrzést végez negyedévente az alábbi területeken

- Ügyfél / vevőtől átvett adok kezelése
- Vendég beléptetés, video megfigyelés és nyilvántartás
- Marketing célú megkeresések, hírlevél
- Kereskedelmi kommunikáció, ügyfél kezelés
- Adatfeldolgozók menedzsmentje

18.3 A Szervezet adatkezelési folyamatainak éves felülvizsgálata

A Szervezet éves rendszerességgel előre meghatározott időpontban felülvizsgálja a teljes adatkezelési és adatfeldolgozási folyamatait.

A Szervezet az éves felülvizsgálatot minden év június hónap első péntekén végzi el.

Az Adatkezelési folyamatok felülvizsgálatáért a felelős: ***Adatvédelmi Tisztviselő***

A Szervezet a felülvizsgálat során minimálisan az alábbi tevékenységeket elvégzi:

- A Szervezet által vezetett nyilvántartások felülvizsgálata, (ASZ-01-1, ASZ-01-2, stb.)
- Az ASZ-01-1 nyilvántartásban meghatározott adatkezelési folyamatokban meghatározott adatkezelési határidőt elért adatok törlése
- A HR folyamatokban rögzített folyamatokban rögzített adatok törlésének ellenőrzése
- A rögzített incidensek következmények kivizsgálása és szükség esetén a folyamatok módosítása
- Az adatfeldolgozók által végzett tevékenységek minimálisan véletlenszerű ellenőrzése.

18.4 Belső audit

A Szervezet tervezett módon belső auditokat végez, annak ellenőrzésére, hogy az adatkezelési folyamatai megfelelnek-e a jogszabályi elvárásoknak és a Szervezet saját követelményeinek.
Az adatkezelési folyamatok ellenőrzését a belső auditot a Szervezet jelentős átalakítását követően, a külső tényezők kockázatai a szabályozási környezet változása esetén, de minimálisan évente egy alakalommal el kell végezni.
Az auditok elvégezhetők mind külső, mind belső erőforrásokkal. Az audit lebonyolítását vagy a külső erőforrás bevonásával való megvalósítását az Adatvédelmi Tisztviselő végzi el.
A Szervezet a belső auditok során feltárt hiányosságokat jegyzőkönyvben rögzíti.
Az auditokat az auditálásra vonatkozó szakmai ajánlások szerint kell elvégezni, és az eredményeket dokumentált információként meg kell őrizni.

19. AZ ADATKEZELÉSI FOLYAMATOK BIZTONSÁGÁNAK FEJLESZTÉSE

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

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

E tevékenységek során feltárt nem megfelelő működések kijavításra a Szervezet intézkedések hoz.
Az adatvédelmi szabályzási rendszer állapotáról, a fejlesztési lehetőségekről a következő forrásokból kap információt a Szervezet:

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

A megszerzett információkat és a fejlesztési lehetőségeket a Szervezet évente minimum egy alkalommal egy vezetőségi vizsgálat keretében felülvizsgálja, és meghatározza a szükséges javító intézkedéseket, amelyek végrehajtását nyomon követi.

Az évenkénti vezetőségi felülvizsgálatra az Adatvédelmi Tisztviselő a fenti információk alapján előterjesztést készít.

A vezetőségi felülvizsgálat évenként megszervezéséért a felelős az: ***Adatvédelmi Tisztviselő***

20.MELLÉKLETEK / FÜGGELÉKEK

1. sz. Függelék Kapcsolattartók

Az Adatvédelmi Tisztviselő elérhetőségei:

Neve: Csanádi Viktória Gabriella
E-mail címe: dpocsanadi@gmail.com
Telefonszáma: 06-70-334-8703

2. sz. Függelék – Kapcsolódó dokumentumok listája

Azonosító	Megnevezés	Forma	Elérhetőség

3.számú függelék- Az incidenskezelésért felelős személyek

Az adatvédelmi incidensek kezelésében **közvetlenül részt vevő személyek**. A helyettesek csak akkor, ha a szerepkört betöltő személy nem elérhető.

Szerepkör	Név	Mobil telefon	E-mail
Adatvédelmi tisztviselő	Csanádi Viktória Gabriella	06-70-334-8703	dpocsanadi@gmail.com
IT üzemeltetési vezető	Rohacsek Márton	06-24-365-163	titkarsag@arieskft.hu
Szervezet jogásza	dr. Uri József	06-24-365-163	titkarsag@arieskft.hu
Ügyvezető igazgató	Szarvas Tibor	06-24-365-163	titkarsag@arieskft.hu

1.SZ MELLÉKLET - HATÁSVIZSGÁLAT

1. AZ ADATVÉDELMI HATÁSVIZSGÁLAT LEFOLYTATÁSA

Amennyiben az előzetes kockázatértékelés alapján szükséges a Szervezet elvégzi az adatvédelmi hatásvizsgálatot.

1.1 Általános szempontok

Az adatvédelmi hatásvizsgálatot az adatkezelést megelőzően kell elvégezni.
Egymáshoz hasonló típusú adatkezelések, amelyek hasonló kockázatokat hordoznak, egy hatásvizsgálatba összevonva is vizsgálhatók.
Az adatvédelmi hatásvizsgálat az érintettek jogait érintő kockázatok kezelésére szolgál, így az ő szemszögükből kell készülnie.

1.2 A tervezett adatkezelés leírása

A Szervezet elkészíti a tervezett adatkezelési műveletek módszeres leírását, beleértve az adatkezelés céljainak ismertetésére, és adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket.
A leírás határozza meg, hogy az adott adatkezelés megtervezése során:

1) Figyelembe vették-e az adatkezelés jellegét, hatókörét, körülményeit és céljait;
2) A személyes adatokat, a címzetteket, valamint a személyes adatok tárolásának időtartamát rögzítették-e;
3) Készült-e funkcionális leírás az adatkezelési műveletről;
4) Azonosították-e a személyes adatokhoz használt eszközöket (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák);
5) Figyelembe vették-e olyan jóváhagyott magatartási kódex előírásait melyhez a szervezet csatlakozott.

1.3 Szükségesség - arányosság vizsgálat

A szervezet elvégzi az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatát.
A szükségesség – arányosság vizsgálat során tételesen ellenőrizni kell a következőket:

1) Célhoz kötöttség: meghatározott, kifejezett és jogos cél(ok),
2) Az adatkezelés jogszerűsége,
3) Adattakarékosság: a kezelt adatok megfelelőek, relevánsak, és a szükséges adatokra korlátozódnak,
4) Korlátozott tárolási időtartam.

Az adatkezelési műveletek szükségességi - arányossági vizsgálatot az ***ASZ-05-02 Adatvédelmi hatásvizsgálat és kockázat nyilvántartás*** alapján kell elkészíteni. A táblázat kitöltése:

1) A szükségességi – arányossági vizsgálat az értékelő kérdésekre adott válaszok alapján történik. A kérdésekre **igen-nem** válaszokat kell adni.
2) Döntési kritériumok:
    a. Ha a kérdések bármelyikére **nem** a válasz, abban az esetben **a Szervezet nem kezdheti meg az adatkezelés a feltárt elégtelenségek, kockázatok kezelése nélkül.**

Az szükségességi-arányossági vizsgálatot **felül kell vizsgálni**, minden esetben, ha az adatkezelési tevékenység, illetve a jogszabályi és/vagy a belső szabályzási környezet változik. Az szükségességi-arányossági vizsgálatot az Adatvédelmi Tisztviselő végzi el az adatkezelés megkezdése előtt.

Az ellenőrzést elvégzi: ***Adatvédelmi Tisztviselő***

1.4 Kockázatok meghatározása

Az adatvédelmi hatásvizsgálat az adatvédelmi kockázatok feltárását célozza. Ha egyáltalán nem vagy nem megfelelően van megvalósítva egy követelmény, akkor fennáll a veszélye, hogy az érintettek személyes adataik kezeléshez fűződő jogai sérülnek.
A hatásvizsgálatot az ***A ASZ-05-02 Adatvédelmi hatásvizsgálat és kockázat nyilvántartás*** alapján kell elkészíteni.
Az előre meghatározott, illetve az adott adtakezeléshez specifikusan kapcsolódó vizsgálati területeket kell elemezni, és ennek keretében meghatározni a gyengeségeket, az ehhez kapcsolódó fenyegetéseket, amelyek alapján megbecsülhető az incidens bekövetkezési valószínűsége
Ezt követően meghatározzuk (leírjuk) az incidens bekövetkezésekor lehetséges kárt, azaz a személyes adatok bizalmassága, integritása és/vagy rendelkezésre állása sérülésének mértékét. Az adatvédelmi hatás mértékét szakértői becsléssel határozzuk meg

1.4.1 A kockázatmenedzsment folyamat lépései

1. Az Adatvédelmi Tisztviselő az előzetes kockázatelemzés során adatvédelmi hatásvizsgálatra kijelölt Adatkezelési folyamatokat csoportosítja. Az azonos tevékenységek csoportosíthatók és közös hatásvizsgálat készíthető.
2. Minden egymástól elkülönülő adatkezelési csoportra külön hatásvizsgálatot kell készíteni.
3. A rögzített kockázatelemzési módszertan alapján a kockázati kitettség meghatározása.
4. Kockázatkezelés, menedzselés - javaslatok a kockázat elfogadási kritériumok Közepes vagy az azt meghaladó kockázatokat csökkentő intézkedésire.
5. Kockázat kezelési tervet készítése.

1.4.2 Valószínűség

Az adatvédelmi incidens bekövetkezési valószínűségét a **fenyegetések** és az adatkezelési folyamat szervezési, technológiai és információbiztonsági **gyengeségei** együttesen határozzák meg. A fenyegetések a gyengeségeket kihasználva okozhatnak incidenseket.
Az adatvédelmi incidensek bekövetkezési valószínűségének meghatározásához a kockázatfelmérést végzőknek fel kell mérniük:

1) Az **aktuális fenyegetések**et, amelyek lehetnek:
   a. hagyományos fenyegetések (fizikai, természeti kár, technikai meghibásodás, szolgáltatások kiesése stb.)
   b. emberi tevékenységek (szándékos károkozás, figyelmetlenség, tájékozatlanság stb.)
   c. informatikai fenyegetések (hacker támadás, kártékony kódok stb.)
2) Az adatkezelést végző rendszer gyengeségeit:
   a. szervezési intézkedések gyengeségei (nincs felelős, nem megfelelő képzés, GDPR követelmények figyelmen kívül hagyása stb.)
   b. informatikai intézkedések gyengeségei (az adatkezelés nem megfelelő támogatása, nem ellenőrzött folyamatok: duplikálás, ellenőrizetlen adattovábbítás stb.)
   c. információbiztonsági intézkedések gyengeségei.

A kockázatfelmérés során a valószínűséget a következő kategóriákba soroljuk:

Valószínűség		
Mérték		Leírás
1	alacsony	incidens bekövetkezés 3 évnél ritkább
2	közepes	incidens bekövetkezés 1 - 3 évente
3	magas	incidens bekövetkezés 1 éven belül

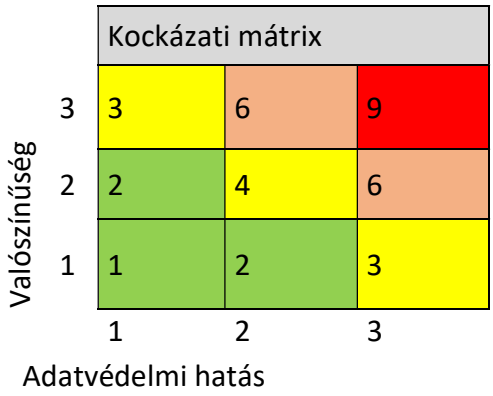
1.4.3 Hatás

Adatvédelmi hatás alatt azt a negatív hatást értjük, amelyet az érintett elszenved egy esetleges adatvédelmi incidens hatására.
Az adatvédelmi incidensek hatásainak meghatározásához a kockázatfelmérést végzőknek figyelembe kell venniük, hogy az adatvédelmi hatásvizsgálat az érintettek jogait érintő kockázatok kezelésére szolgál, így az ő szemszögükből kell mérlegelni a hatásokat.
A kockázatfelmérés során az adatvédelmi hatást a következő kategóriákba soroljuk:

Adatvédelmi hatás		
Mérték		Leírás
1	alacsony	kevés számú érintettre terjed ki, kevés személyes adatot érint, nem érint különleges adatot
2	közepes	közepes számú érintettre terjed ki, közepes mennyiségű személyes adatot érint, minimálisan érint különleges adatot
3	magas	nagyobb létszámú érintettre terjed ki, nagyobb mennyiségű személyes adatot érint, különleges adatokat is érint

1.4.4 Kockázat meghatározása

A kockázat általános meghatározása: **Kockázat = hatás X valószínűség**, amelyet az adatvédelmi kockázatok meghatározásánál is használunk.
Az előzőekben meghatározott valószínűségi és hatás értékek alapján a Szervezet a következő kockázati mátrix alapján értékeli az adatvédelmi kockázatokat.



Az egyes kockázati értékekhez a következők alapján rendelünk kockázati szinteket:

Kockázati érték	Kockázati szint
9	magas
6	közepes
3 - 4	alacsony
1 - 2	elhanyagolható

1.5 Kockázatkezelés

1.5.1 Kockázatelfogadási kritériumok

A hatáselemzés során feltárt kockázatok elfogadására, illetve kezelésére vonatkozó feltételeket a Szervezet a következők szerint határozza meg:
Feltételek új adatkezelések esetén:

Kockázati szint	Kockázatkezelés ÚJ adatkezelési tevékenységek esetén
magas	**Kezelendő kockázat** az adatkezelés megkezdése előtt a kockázatcsökkentő intézkedéseket végre kell hajtani. Amennyiben az ésszerűen megtehető intézkedések nem csökkentik megfelelően a kockázatot a Szervezet a hatóságtól előzetes konzultációt kér
közepes	**Kezelendő kockázat** az adatkezelés megkezdése előtt a kockázatcsökkentő intézkedéseket végre kell hajtani.
alacsony	**Feltételesen kezelendő kockázat** az adatkezelés megkezdhető, de a kockázatcsökkentő intézkedéseket 6 hónapon belül meg kell valósítani.
elhanyagolható	Elfogadott, nem kezelendő kockázat, az adatkezelés megkezdhető.

Feltételek már meglévő adatkezelések esetén:

Kockázati szint	Kockázatkezelés MEGLÉVŐ adatkezelési tevékenységek esetén
magas	**Kezelendő kockázat** az adatkezelést a lehető legnagyobb mértékben korlátozni szükséges, és a kockázatcsökkentő intézkedéseket a legrövidebb időn belül végre kell hajtani. Amennyiben az ésszerűen megtehető intézkedések nem csökkentik megfelelően a kockázatot a Szervezet a hatóságtól előzetes konzultációt kér
közepes	**Kezelendő kockázat** az adatkezelés folytatható, de a kockázatcsökkentő intézkedéseket 6 hónapon belül meg kell valósítani.
alacsony	**Elfogadott, nem kezelendő kockázat** az adatkezelés változatlan formában folytatható.
elhanyagolható	**Elfogadott, nem kezelendő kockázat** az adatkezelés változatlan formában folytatható.

1.5.2 Kockázatkezelési intézkedési terv

A kockázatkezelési döntések eredményeképpen meghatározásra kerülnek azok a kockázatok, amelyek kezelése, azaz a kockázatok csökkentése szükséges.
Ezen kockázatok csökkentése érdekében a Szervezet kockázatkezelési intézkedéseket tervez meg és hajt végre. Az kockázatkezelési intézkedéseket az ***ASZ-05-02 Adatvédelmi hatásvizsgálat és kockázat nyilvántartás táblázatban*** tartjuk nyilván, annak a kockázatnak a sorában, amelyre az intézkedés vonatkozik.
Minden intézkedés estében meg kell határozni:

- A végrehajtás felelősét,
- A végrehajtásban résztvevőket,
- A szükséges erőforrásokat,
- A végrehajtás határidejét,
- A kezelt kockázat értékét ezzel bizonyítva a kockázatkezelés hatékonyságát.

Az adatvédelmi kockázatkezelési intézkedési terv jóváhagyásáért felelős az: ***Adatvédelmi Tisztviselő***
Az ellenőrzést elvégzi: ***Adatvédelmi Tisztviselő***

1.6 Dokumentáció

Az adatvédelmi hatáselemzés folyamatlépéseit, illetve azok eredményeit dokumentált információként kell megőrizni.

1.7 Nyomon követés és felülvizsgálat

Az adatvédelmi hatásvizsgálatot a Szervezet az Adatvédelmi Tisztviselő megismétli, ha:

a) Az adatkezelési folyamat megváltozik,
b) Az adatkezelési folyamatban résztvevő adatfeldolgozó megváltozik,
c) A szabályozási környezet megváltozik,
d) Amennyiben az adatkezelési folyamatgazdák és az **Ügyvezető igazgató** közül bármelyikük is valószínűsíti, hogy az adatkezelési folyamatot érintő változás jelentős befolyással lehet a természetes személyek jogait és szabadságait érintő kockázatokra,
e) Amennyiben egy adott adatkezelésre vonatkozó utolsó hatásvizsgálat 2 évnél régebbi.

2.SZ MELLÉKLET

Aktív rendszerek listája:

Apolló integrált rendszer,
APS posta program,
gmail,
hMailserver,
NHKV Zrt. tömeges számlázó rendszer,
TERC költségvetéskészítő program
Magyar Közlöny kezelő