UP RENDEZVÉNY ÉS PROGRAM KFT.

Adatvédelmi és adatkezelési szabályzat

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

Információbiztonsági besorolás:	
Titkos	☐
Korlátozottan terjeszthető	☒
Nyilvános	☐

_____

Ungi Veronika
ügyvezető

0. TARTALOMJEGYZÉK

0.1 MÓDOSÍTÁSOK NYOMONKÖVETÉSE

Verzió szám	A módosítás leírása	Készítette	Elfogadta	Dátum
1.0	Alap verzió	Gill & Murry Zrt.	Sándor Zsolt András	2025. …
2.0	Felülvizsgálat		xxx	xxx

1. BEVEZETÉS

1.1 A szabályzat célja

Az UP Rendezvény és Program 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 teljeskörűen és késedelem nélkül el kell végezni.

> *A szabályzat elkészítéséért és rendszeres felülvizsgálatáért felelős: az **Adatvédelmi manager***
> *Az ellenőrzést elvégzi az: **Adatvédelmi Tisztviselő***

2. A SZABÁLYZAT HATÁLYA

2.1 Személyi hatály

Jelen szabályzat a Szervezethez munkaviszony létrehozása érdekében önéletrajzot benyújtó természetes személyekre, a Szervezet irányítása alatt tevékenységet végző természetes személyekre, valamint a Szervezet számára/megbízásából adatfeldolgozói tevékenységet végző jogi és természetes személyekre, valamint a Szervezet termékeit megvásárló vagy szolgáltatásait igénybe vevő természetes személyekre vagy jogi személyek nevében eljáró természetes személyekre vonatkozik.

2.2 Időbeli hatály

Jelen Szabályzat a kiadás napján lép hatályba, és visszavonásig/módosításig marad hatályban. Jelen Szabályzatot a hatálybalépéskor már folyamatban lévő adatkezelésekre is alkalmazni kell.

2.3 Tárgyi hatály

Ezt a szabályzatot kell alkalmazni az Adatkezelő által megvalósított 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.

2.4 Ajánlások, jogszabályok

2.4.1 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

2.4.2 A személyes adatok kezelésére vonatkozó ajánlások

2.4.2.1 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

2.4.2.2 Szabványok:

- **BS 10012:2017** Data protection – Specification for a personal information management system
- **MSZ ISO/IEC 27001: 2022** Információbiztonság-irányítási rendszerek
- **MSZ EN ISO/IEC 27002: 2021** 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 tevékenységét ellenőrző, az adatkezelési tevékenységhez szaktanácsadással a Szervezet számára rendelkezésre álló, munkavállaló vagy külső szerződött partner. A szerepkört betöltőt a Szervezet bejelenti az adatvédelmi hatósághoz (NAIH).

„Adatvédelmi manager”: a Szervezeten belül az az operatív személy, aki az adatkezelési tevékenységeket nyilvántartja, szervezi, kezeli, a hatásvizsgálatot elvégzi, az adatkezelési tevekénységhez szakértőként kikérhető a véleménye. Amennyiben a Szervezet nem rendelkezik adatvédelmi tisztviselővel az Adatvédelmi manager látja le a kapcsolattartási szerepet az adatvédelmi hatósággal (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 munkavállalói, a rendezvények résztvevői, szerződéses partnerei, szerződéses partnerei kapcsolattartói adatainak kezelése tekintetében, ugyanakkor bizonyos adatfeldolgozási tevékenységek kapcsán **Adatfeldolgozó**ként működik.

4.1.1 Az adatkezelői tevekénység nyilvántartása

A Szervezetnek a GDPR elvárásai alapján az ***ASZ-01-1 Adatkezelési tevékenység nyilvántartás***ban kell rögzítenie az összes személyes adatkezelést is érintő tevekénységet. Az ***ASZ-01-1 Adatkezelési tevékenység nyilvántartás-t*** egyértelmű verziókövetéssel kell ellátni.

4.1.2 Az adatkezelői tevékenység változáskezelése és dokumentálása

Amennyiben egy adatkezelési folyamatban az adatkezelési tevékenység maga vagy a tevékenységről nyilvántartott bármely adat megváltozik az késedelem nélkül frissíteni kell az az ***ASZ-01-1 Adatkezelési tevékenység nyilvántartás*** -ban . Amennyiben Szervezet nem stilisztikai változtatást hajt végre a nyilvántartáson, úgy annak adattartalmát a jelen szabályzat 8.2 pontjában részletezett adatkezelési tájékoztatók valamelyikében közzé kell tegye.

A Hatósági elvárások teljesítése érdekében a nyilvántartást és a tájékoztatókat egyértelmű verziószámmal kell ellátni, és minden nem stilisztikai változtatást követően a verziószámot egyel növeli kell.
A korábbi verziókat és azok érvényességi idejét nyilván kell tartani és tárolni kell annak érdekében, hogy egy esetleges hatósági vizsgálat során a Szervezet meg tudja állapítani, hogy egy korábbi időpontban melyik verziójú nyilvántartás és melyik verziójú adatkezelési tájékoztató volt érvényben.

4.2 A Szervezet adatfeldolgozói tevékenysége

A Szervezet a GDPR meghatározása alapján **Adatfeldolgozónak** minősül a megrendelői, megbízói – különösen a Budapest Főváros IV. kerület Újpest Önkormányzata - által a számára átadott vagy a nevükben 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, felülvizsgálja a Szervezetben az 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

- Rendszeresen ellenőrzi az adatvédelmi folyamatokat a Szervezetben
- Döntést hoz az Adatvédelmi tisztviselő és az Adatvédelmi manager által előkészített adatvédelemmel kapcsolatos kérdésekben
- Aktív részese az adatvédelmi incidenskezelési eljárásnak
- Biztosítja a szükséges erőforrásokat a Szervezeten belüli személyes adatok kezeléséhez
- Kinevezi az Adatvédelmi managert
- Megbízza az Adatvédelmi tisztviselőt
- Bevonja az Adatvédelmi managert és/vagy az Adatvédelmi tisztviselőt a személyes adatok kezelésével kapcsolatos ügyekbe

5.2.2. Adatvédelmi tisztviselő

A Szervezet a GDPR 37. cikk (1) bekezdés b) pontja alapján adatvédelmi tisztviselőt jelöl ki.
Az adatvédelmi tisztviselő hatáskörét, felelősségét és feladatait a munkaköri leírása vagy megbízási szerződése tartalmazza. A feladatmeghatározást az ***ASZ-03-1 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 adhat adatkezelési kérdésekben, így különösen az adatvédelmi hatásvizsgálatra vonatkozóan, és nyomon követi annak elvégzését
- Kapocslatot tart, konzultál és együttműködik az adatvédelmi hatósággal
- Tájékoztat és szakmai tanácsot ad 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.

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, és
- 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. Adatvédelmi manager

A Szervezet tekintettel az adatvédelmi feladatok menedzselésének fontosságára és az operatív feladatok ellátására **Adatvédelmi managert** nevez ki.
Az Adatvédelmi manager jogállása és feladatköre **nem** azonos a GDPR 38. és 39. cikkében és a jelen szabályzat 5.2.2 pontjában definiált Adatvédelmi tisztviselő jogállásával.
Az Adatvédelmi manager hatáskörét, felelősségét és feladatait a munkaköri leírása vagy megbízási szerződése tartalmazza. A feladatmeghatározást az ***ASZ-03-2 Adatvédelmi manager feladatai és felelősségei minta*** alapján kell elkészíteni.

Legfontosabb feladatai:

- Végrehajtja a jelen szabályzatban megfogalmazott adatkezelési feladatokat
- Adatvédelmi hatásvizsgálat elkészítése, kockázatértékelés, érdekmérlegelés elkészítése,
- Tanácsot ad adatkezelési kérdésekben
- Részt vesz az adatvédelmi oktatásban
- Incidensek esetén megteszi a javító intézkedéseket
- Adatkezelési dokumentumlista kezelése
- Adatkezelési folyamatok azonosítása

5.2.3.1.Az Adatvédelmi manager jogállása

A Szervezet biztosítja, hogy az Adatvédelmi manager a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

A Szervezet támogatja az Adatvédelmi managert 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 manager szakértői szintű ismereteinek fenntartásához szükségesek.
Az Adatvédelmi manager az Ügyvezető igazgatónak tartozik felelősséggel.

Az Adatvédelmi manager kifejezetten a személyes adatok kezelésére vonatkozó titoktartási kötelezettséget vállal az ***ASZ-02 Titoktartási nyilatkozat mintá-ban*** *meghatározottak* alapján.
Amennyiben az Adatvédelmi manager más feladatokat is ellát, a Szervezet biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

5.2.3.2. A Szervezet Adatvédelmi managerének elérhetősége:

Az Adatvédelmi Manager elérhetőségei az 1. Függelékben találhatóak.

5.2.4. Adatkezelésre feljogosított személyek

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

> *A titoktartási nyilatkozatokat a munkavállalókkal a belépéskor a beléptetést végző HR munkatárs íratja alá.*

Jelen szabályzat bevezetése előtt már foglalkoztatott munkavállalók esetében az ***ASZ-02 Titoktartási nyilatkozat mintá****-t* a jelen szabályzat bevezetését 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 esetlegesen szükséges 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 felelős: az* ***Adatvédelmi manager***
> *Az ellenőrzést elvégzi: az* ***Adatvédelmi Tisztviselő***

6.2.2. Kockázatok mérlegelése az adatkezelés előtt

6.2.2.2. Előzetes kockázatértékelés

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.

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 kell hivatkozni a kockázatértékelő táblázatban 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.** Amennyiben 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 szabályozási környezet változik.

*Az előzetes kockázatértékelés elvégzésért felelős: az **Adatvédelmi manager***
*Az ellenőrzést elvégzi: az **Adatvédelmi Tisztviselő***

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

6.2.2.3. Kötelező hatásvizsgálat azonosítása a Hatósági (NAIH) lista alapján.

Az Adatvédelmi Hatóság az alábbi linken tartja nyilván azokat az adatkezelési folyamatokat, melyek alkalmazása esetén az Adatkezelőnek kötelező elvégezni a hatásvizsgálatot az adatkezelés megkezdése előtt.

https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf

Az Adatkezelő minden új adatkezelési tevékenység bevezetése vagy a jelenleg azonosított és nyilvántartott adatkezelési folyamatok változtatása előtt az ***ASZ-05-01_Hatasvizsgalatot_megelozo_kockazatertekeles*** alapján ellenőrzést végez. Az ellenőrzés célja, hogy az Adatkezelő megállapítsa, hogy a bevezetni tervezett adatkezelési folyamat szerepel-e az Adatvédelmi Hatóság kötelező hatásvizsgálati listájában.

*Az adatkezelési tevékenységek azonosításáért felelős: az **Adatvédelmi manager***

Az Adatkezelő a ***Hatásvizsgálati lista ellenőrzésére*** az alábbi paramétereket határozza meg:

Paraméter	Magyarázat
Sorszám	A hatásvizsgálati listában szereplő meghatározások sorszáma.
Adatkezelési tevékenység	Az Adatvédelmi nyilvántartásban szereplő definíciók.
Hatásvizsgálati lista elemzés eredménye	Amennyiben bármelyik kérdésre a válasz IGEN, az Excel automatikusan IGEN -re vált, a háttér színét megváltoztatja színesre.
Ha egy természetes személy egyedi azonosítását célzó biometrikus adatának kezelése módszeres megfigyelésre irányul.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz -e a meghatározásnak megfelelő adatkezelési tevékenységet.
Ha kiszolgáltatott helyzetben lévő érintettekkel – különös tekintettel a gyermekekre, munkavállalókra, idős, mentális betegségben szenvedőkre – kapcsolatos egyedi azonosítását célzó biometrikus adat kezelése történik.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Ha az adatkezelés egy természetes személy genetikai adatainak, egyéb, különleges adatokhoz vagy fokozottan személyes jellegű adatokhoz történő hozzákapcsolásával jár.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Ha egy természetes személy genetikai adatai kezelésének célja a természetes személy értékelése vagy pontozása.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Pontozás. Az adatkezelés célja, hogy az érintett bizonyos tulajdonságait felmérje, és annak eredménye kihatással van az érintett részére nyújtott, illetve nyújtandó szolgáltatás létrejöttére vagy minőségére.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Hitelképesség értékelése. Az adatkezelés célja, hogy az érintett hitelképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Fizetőképesség értékelése. Az adatkezelés célja, hogy az érintett fizetőképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Harmadik személytől gyűjtött adatok további felhasználása. Az adatkezelés célja, hogy a harmadik személytől begyűjtött személyes adatokat felhasználják az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalánál.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Diákok, hallgatók személyes adatainak értékelésre való felhasználása. Az adatkezelés célja a diákok, hallgatók felkészültségének, teljesítményének, alkalmasságának, illetve mentális állapotának rögzítése, valamint vizsgálata és az adatkezelés nem jogszabályon alapul, függetlenül attól, hogy az oktatás alap-, közép- vagy felsőfokú.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Profilozás. Az adatkezelés célja személyes adatok nagy számú, illetve módszeres értékelése révén	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a

végzett profilozás, különösen, ha az az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján történik.	meghatározásnak megfelelő adatkezelési tevékenységet.
Csalás elleni fellépés. Az adatkezelés célja hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázis felhasználása ügyfelek szűrésére.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Okosmérők. Az adatkezelés célja közműszolgáltatók által telepített „okosmérők” alkalmazása (fogyasztási szokások nyomon követése).	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal. Az adatkezelés célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala, amely adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Módszeres megfigyelés. Érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok felhasználásával, illetve bármely más új technológia használatával (Wi-Fi tracking, Bluetooth tracking, testkamera).	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Helymeghatározási adatok kezelése, ha az módszeres megfigyelésre vagy profilalkotásra utal.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Munkavállaló munkájának megfigyelése. . Az adatkezelés célja a munkavállaló munkájának megfigyelése során a munkavállaló személyes adatainak nagy számú és módszeres feldolgozása, illetve értékelése. Például: GPS megfigyelő autóban történő elhelyezése, kamerás megfigyelés lopás vagy csalás elleni fellépés céljából.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Különleges adatok nagy számban való kezelése. A GDPR preambulum (91) bekezdése alapján a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Nagyszámú személyes adatok kezelése bűnüldözési célból	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a

céltól eltérő kezelése: pl. gyermekek, idősek, mentális betegségben szenvedők esetében.	meghatározásnak megfelelő adatkezelési tevékenységet.
Gyermekek személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy marketing céljából, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Új technológiai megoldások használata az adatkezelés során. Ideértve az érzékelővel ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelése (pl.: okos televízió, okos háztartási eszközök, okos játékok stb.), és amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére és amelyek alapján profilalkotás történik.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Egészségügyi adatokra vonatkozó adatkezelések. Nagy számban kezelt adatok tekintetében a kórházak, egészségügyi ellátó intézmények, magán-egészségügyi szolgáltatók vagy nagyszámú páciensi körrel rendelkező természetgyógyászok által kezelt különleges adatok vonatkozásában. Ideértve a nagyobb sportlétesítmények, edzőtermek által a tagoktól felvett egészségügyi adatok kezelése.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Amikor több adatkezelő egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot tervez létrehozni, amelyben különleges adatokat is kezelnek.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.
Az adatkezelés célja a különböző forrásokból származó adatok összevonása, egymással való megfeleltetése vagy összehasonlítása.	Igen / Nem választás annak megfelelően, hogy a bevezetni kívánt adatkezelési folyamat tartalmaz-e a meghatározásnak megfelelő adatkezelési tevékenységet.

6.2.3. Kockázatértékelést követően hozott 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:

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

A szervezési intézkedések részét képző dokumentumok felsorolását a jelen szabályzat 2. függeléke tartalmazza.

*Az adatkezelési dokumentumlista napra készen tartásáért felelős: az **Adatvédelmi manager***
*Az ellenőrzést elvégzi: az **Adatvédelmi Tisztviselő***

6.2.4. Kockázatértékelést követően hozott technikai intézkedések

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

6.2.4.1. 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 biztosítani incidens esetén az adatokhoz való hozzáférést,
- Az adatokat a megfelelő időn belül visszaállítani.

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

6.2.5. 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 (IBSZ).

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 manager az adatkezelés megkezdése előtt ellenőrzi, hogy az adatkezelés megfelel-e a GDPR rendelet és jelen szabályzat elvárásainak.
Folyamat:

1. Azonosítja az adatkezelési tevekénységeket a Szervezeten belül.
2. Csoportosítja az azonos cél érdekében történő adatkezelési tevekénységeket.
3. Minden adatkezelési célhoz az 6.4 pontban megfogalmazott jogalapok közül társít egyet. Amennyiben nem társítható jogalap az adatkezelési célhoz, úgy az adatkezelési tevekénységet 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 tevekénységet vagy másik adatkezelési cél mentén kezeli tovább az adatokat.

6.3.1. Adatkezelési tevékenységek azonosítása és nyilvántartása

A Szervezet azonosítja az adatkezelőként vagy adatfeldolgozóként végzett adatkezelési tevékenységeit. Az adatkezelési tevekénységek 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 tevekénységek azonosításáért felelős: az **Adatvédelmi manager***
*Az ellenőrzést elvégzi: az **Adatvédelmi Tisztviselő***

Az Adatkezelő az adatkezelési tevékenységek azonosításánál az alábbi paramétereket határozza meg:

Paraméter	Magyarázat
Adatkezelési folyamat	A Szervezet által végzett adatkezelési tevekénységek csoportba foglalva, azonos adatkezelési cél mentén.
Adatkezelési folyamatgazda	Az a szervezeti egység vezető, akinek a szervezeti egységében kezelik az azonosított adatkezelési tevekénységeket.
Adatkezelői szerep	Azonosítani kell, hogy adatkezelői vagy adatfeldolgozói szerepkörben kezeli az adatokat a Szervezet.
Adatkezelési Cél	Az adatkezelési tevékenységek összefoglaló célja. A saját vagy más nevében végzett tevékenységeket is fel kell venni.
Jogalap	A 6.5.4-- 6.5.9 pontokban definiált jogalapok közül egy, amelyik alapján a Szervezet kezeli az adott tevékenységgel kapcsolatos adatokat.
Szerződéses jogalap esetén az adatszolgáltatás a szerződéskötés előfeltétele-e	Igen / Nem értéket vehet fel a mező annak függvényében, hogy az adott adatkezelési célon kezelt adatok szükségesek-e a szerződés megkötéséhez. A szerződés folyamán kezelt adatok esetében “nem választ” szükséges rögzíteni.

Érintettek kategóriái	Azon természetes személyek összefoglaló csoportjai, akik adatait az adatkezelési folyamatban kezeli a Szervezet.
Kezelt személyes adatok kategóriái	A kezelt személyes adatok összefoglaló megnevezései.
Címzettek kategóriái	Azon partnerek összefoglaló megnevezése melyeknek, mint önálló adatkezelőknek továbbítja, vagy hozzáférési lehetőséget biztosít a Szervezet az adatkezelési tevékenység során.
Adatfeldolgozó	Azon partnerek összefoglaló megnevezése melyeknek a Szervezet nevében végzendő adatfeldolgozási (adatkezelési) tevékenység elvégzése érdekében továbbítja a Szervezet az általa gyűjtött személyes adatokat.
3. országba továbbítás címzettje	Az EGT tagállamain kívüli szervezetbe vagy címzettnek 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.
Adatok forrása	Amennyiben az adatkezelő az adatokat azérintettől gyűjti, akkor ezt kell rögzíteni, amennyiben nem az érintettől, hanem pld. publikus web gyűjtés vagy saját más adatkezelési célról történik átminősítés, akkor azt kell megjelölni a nyilvántartásban.

A Szervezet a GDPR 30. cikk (1) pontja alapján elkészíti adatkezelési tevékenységek nyilvántartását, amelyet az ***ASZ01-1 Adatkezelési tevékenységek nyilvántartása*** táblázatban rögzít.

Az adatkezelési tevekénységek dokumentálásáért felelős: az ***Adatvédelmi manager***
Az ellenőrzést elvégzi: az ***Adatvédelmi Tisztviselő***

6.3.2. Adatfeldolgozói tevékenységek nyilvántartása

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

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

Az adatkezelési dokumentumlista nyilvántartásáért és napra készen tartásáért felelős: az ***Adatvédelmi manager***
Az ellenőrzést elvégzi: az ***Adatvédelmi Tisztviselő***

A Szervezet **adatfeldolgozóként** végzett adatkezelési tevékenységek nyilvántartásánál (***ASZ-01-2 Adatfeldolgozói adatkezelések nyilvántartása***) az alábbi paramétereket rögzíti:

Paraméter	Magyarázat

Adatkezelő neve	Az a szervezet, akinek megbízása alapján, akinek vagy amelynek a nevében történik az adatkezelés.
Az adatkezelő elérhetősége	Az előző sorban meghatározott adatkezelő adatkezelési helyének megnevezése (székhely vagy telephely).
Értesítendő (adatvédelmi felelős, Adatvédelmi tisztviselő neve)	Az a természetes személy, akit az Adatfeldolgozónak egy esetleges incidens esetén késedelem nélkül értesíteni kell.
E-mail	Az Adatvédelmi Tisztviselő vagy Adatvédelmi manager e-mail címe.
Telefon	Az Adatvédelmi Tisztviselő vagy Adatvédelmi manager telefonszáma.
Adatkezelési tevékenységek kategóriái	Az adatkezelési tevékenységek összefoglaló csoportosítása. Pl. IT üzemeltetés, bérszámfejtés, könyvelés, adattisztítás stb.
További adatfeldolgozók	Azon adatfeldolgozók megnevezése, akiket a Szervezet, mint aladatfeldolgozó bevon az adatkezelési tevékenységbe, vagy akik/amelyek hozzáférnek, tárolják vagy kezelik az adatkezelő adatait az adatfeldolgozó megbízásából. Több Al-adatfeldolgozó használata esetén az összes adatfeldolgozót fel kell sorolni a cellában. Az al-adatfeldolgozók egyéb adatait az Al-adatfeldolgozó nyilvántartási munkalapon kell nyilvántartani.
3. országba továbbítás címzettje	Az EGT tagállamain kívüli szervezetbe vagy címzettnek történő adattovábbítás esetén a címzett megnevezése.
A 3. országba továbbítás garanciái	Azon 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.

A Szervezet minden a 'További adatfeldolgozók' oszlopban szereplő Al-adatfeldolgozóról nyilvántartást vezet (***ASZ-01-2 Adatfeldolgozói adatkezelések nyilvántartása***) melyben az alábbi paramétereket rögzíti:

No.	Folyamatos sorszám
Al-adatfeldolgozó neve	Minden megjelöltet fel kell sorolni, melyet megjelölt az Szervezet valamely adatfeldolgozási tevékenységben, mint teljesítési segéd vagy alvállalkozó
Al-adatfeldolgozó címe	A teljesítési segéd/alvállalkozó székelyének címe
Adatvédelmi kapcsoltató neve	Az a személy, akit az adatfeldolgozási szerződésében, mint adatkezelési kapcsolatartót megjelölt az al-feldolgozó
E-mail	A kapcsolattartó elektronikus elérhetősége
Telefon	A kapcsolattartó telefonos elérhetősége
Adatfeldolgozási szerződés dátuma	Az a dátum amikor a szervezet a teljesítési segéddel/ alvállalkozóval az adatfeldolgozási szerződést megkötötte.
Adatfeldolgozási szerződés elérhetősége	A Szervezeten belül az adatfeldolgozási szerződés tárolási helye.
Bejelentési dátuma	Az a dátum amikor a Szervezet a teljesítési segédet/alvállalkozót az Adatkezelő számára bejelentette.

6.4. Személyes adatokon a gyűjtésük céljától eltérő célból végzendő további adatkezeléshez kapcsolódó eljárásrend

Amennyiben az Adatkezelő személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelés megkezdése előtt az alábbi átminősítés előtti vizsgálatot szükséges elvégezni.

6.4.1. Az új adatkezelési cél jogalapjának megállapítása

Az Adatkezelő megvizsgálja, hogy az eredeti adatkezelési célt milyen jogalap mentén kezeli. Az átminősítési eljárás jogalaponként az alábbi feltételekkel végezhető el:

6.4.1.1. Hozzájárulásos jogalap (6. cikk a))

Az átminősítési vizsgálatot a Szervezet nem értelmezi hozzájárulás jogalap esetében. Az új adatkezelési célhoz tartozó hozzájárulást be kell szerezni az érintettől.

6.4.1.2. A fentiektől eltérő jogalapok esetében

Az alábbi jogalapok esetében a 6.4.2 pontban meghatározott átminősítési eljárás lefolytatása szükséges.

- Jogi kötelezettség (6. cikk b))
- Szerződéses jogalap (6. cikk c))
- Érintett létfontosságú érdeke jogalap (6. cikk d))
- Közhatalmi, közérdek jogalap (6. cikk e))
- Jogos érdek jogalap (6. cikk f))

6.4.2. Az új adatkezelési cél alkalmazása előtti átminősítés vizsgálata

Az Adatkezelő a Rendelet 6. cikk (4). pontjának megfelelően megvizsgálja, hogy az új adatkezelési cél összeegyeztethető-e azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték. Ezen vizsgálat lefolytatására és dokumentálásra az ***ASZ-06-04 Adatkezelési cél átminősítés nyilvántartás*** dokumentum szolgál, melyben az alábbi paramétereket rögzíti a Szervezet:

Paraméter	Magyarázat
Adatkezelés eredeti célja	Az Adatkezelő ***ASZ01-1 Adatkezelési tevékenységek nyilvántartásá***-ban szereplő azon adatkezelési cél, mely célból a személyes adatot gyűjtötték.
Adatkezelés eredeti jogalapja	Az Adatkezelő ***ASZ01-1 Adatkezelési tevékenységek nyilvántartásá***-ban szereplő azon jogalap, mely mentén a személyes adatot jelenleg az Adatkezelő kezeli.
Adatkezelés új célja	Azon új adatkezelési cél, mely mentén a jövőben kezelni kívánja az Adatkezelő a korábban gyűjtött személyes adatokat.
Az eredeti és az új adatkezelési cél közötti kapcsolat	Csak akkor kezelhető az új adatkezelési cél mentén a személyes adat, ha igazolható a kapcsolat a két adatkezelési cél között. Pld. Korábban vásárolt a webáruházban, majd ugyan azokról a termékekről kíván információt küldeni a webáruház.

Az adatok gyűjtésének eredeti körülményei, különös tekintettel az érintettek és az adatkezelő közötti kapcsolatra	Csak akkor kezelhető az új adatkezelési cél mentén a személyes adat, ha bizonyítható az adatgyűjtés jogossága. Dokumentálandó, hogy milyen formában, mikor (nem kell pontos dátum csak meghatározás pld. szerződéskötéskor, regisztrációkor) szerezte meg az Adatkezelő az adatokat.
Személyes adatok jellege és kategóriái	A kezelt adatok kategóriái, Pl: név, cím, kapcsolattartási adatok, telefonszám stb.
A kezelt személyes adatok között van-e a GDPR 9. cikk (1) pontban meghatározott kategóriákba tartozó adat	Igen / nem válasz szükséges. Ha az adatok a kivételek között szerepelnek a 9. cikkben akkor a nem választ kell megadni.
A kezelt személyes adatok között van-e a GDPR 10. cikk szerint meghatározott kategóriákba tartozó adat	Igen / nem válasz szükséges. Ha a hozzájáruló nyilatkozattal vagy törvényi kötelezettség mentén kezeli az adatokat az Adatkezelő, akkor is igen válasz megadása szükséges.
Az érintettekre nézve milyen következményekkel járna az adatok új cél szerinti kezelése	Pozitív és negatív hatást is be kell mutatni szövegesen. Pld. Pozitív: Információkat kap a felhasználó az új termékekről. Negatív: Olyan termékcsoportokról is kap információt, mely esetleg nem érdekli és így zaklató levélként értékelheti az információkat.
Az új célból történő adatkezeléshez kapcsolódó garanciák meglétének vizsgálata	Vizsgálandó, hogy az új adatkezelési cél kezelése során is megvalósulnak-e a 32. cikk elvárásai, valamint a 15- 22. és 34. cikkben megfogalmazott érintetti jogok érvényesíthetők leszenek-e az új adatkezelési folyamat során is.
Az új adatkezelési cél összeegyeztethető-e azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték	Szövegesen igazolandó, hogy a fenti vizsgálat elvégzését követően a régi és az új cél kapcsolata miatt az adatkezelés összeegyeztethető.

6.4.3. Sikeres átminősítést követő adminisztratív feladatok

Amennyiben az átminősítési vizsgálat eredménye pozitív, tehát az új adatkezelési cél összeegyeztethető azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték, akkor az Adatkezelő az adatkezelés megkezdése előtt az alábbi tevékenységeket végzi el:

- Felveszi az új adatkezelési folyamatot az ***ASZ01-1 Adatkezelési tevékenységek nyilvántartás-*** ba.
- Megállapítja az adatkezelés jogalapját, ha az jogos érdek, akkor elvégzi az Érdekmérlegelési tesztet.
- Frissíti és közzéteszi az Adatkezelési tájékoztatót.
- Tájékoztatja az érintetteket legalább az alábbiakról:
    - a Szervezetnek, mint adatkezelőnek megnevezése és elérhetőségei;
    - a Szervezet képviselője és elérhetősége;
    - az adatvédelmi tisztviselő (ha van) és elérhetőségei;
    - az érintettek köre;

- a kezelt személyes adatok kategóriái;
- **a személyes adatok kezelésének eredeti célja, jogalapja és a megállapított új cél és jogalap;**
- jogos érdek jogalap esetén a jogos érdek meghatározása;
- 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;
- 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 fentiek elvégzését követelően az Adatkezelő megkezdheti az átminősített adatkezelést.

*Az adminisztratív tevékenységek elvégzéséért felelős: az **Adatvédelmi manager***
*Az ellenőrzést elvégzi: az **Adatvédelmi Tisztviselő***

6.5. 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 jogalapok meghatározásának felelőse: az **Adatvédelmi manager***
*Az ellenőrzést elvégzi: az **Adatvédelmi Tisztviselő***

6.5.1. Gyermekek személyes adatainak kezelése

A Szervezet alaptevékenységét és szolgáltatásait kifejezetten NEM gyermek (18. életévét be nem töltött) korúak számára nyújtja. A Szervezet ennek megfelelően beépített védelem formájában nem vizsgálja az általa kezelt személyes adatok esetében a természetes személy korát.
Amennyiben az adatkezelés során a Szervezet számára egyértelművé válik, hogy természetes személy még nem töltötte be a 18. életévét késedelem 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 az egy kezelt adat 18 éven aluli természetes személyé, késedelem nélkül jelenti és dokumentálja az incidens kezelési szabályozásnak megfelelően.

6.5.1.1. A Gyermekek személyes adatainak kezelése információs társadalommal összefüggő szolgáltatások esetében

Amennyiben a Szervezet egyes adatkezelési tevékenységeit az információs társadalommal összefüggésben végzi, kizárólag ezen adatkezelési tevekénységek tekintetében a 16. évet betöltött gyermekek esetében lehetőséget biztosíthat az adatkezelés tekintetében a jognyilatkozatok megtételére.
Ezen adatkezelési tevekénységek esetében a 16. életévét betöltött természetes személytől el kell fogadni pld. hozzájáruló nyilatkozatát és teljesíteni kell minden érintetti igényét az Adatkezelő által kezelt adatokkal kapcsolatosan.

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

6.5.3. A büntetőjogi felelősség megállapítására alkalmas személyes adatok kezelése

A Szervezet alapértelmezetten nem kezel büntetőjogi felelősség megállapítására alkalmas adatokat. Ez alól kivételt jelent a pályázati kiírásban szereplő indulási elvárásként megfogalmazott adatkezelési kötelezettsége. A Szervezet ilyen esetekben kizárólag a pályázat elbírálásának időpontjáig vagy a pályázat sikeres megnyerése esetén a szerződésben meghatározott egyéb ideig kezeli a munkavállalói és a projektben részt vevő teljesítési segédeinek büntetőjogi felelősség megállapítására alkalmas adatait (pld. erkölcsi bizonyítvány).

6.5.4. 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 egyidőben 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.

6.5.4.1. Hozzájáruló nyilatkozat

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

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

6.5.4.2. 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 vonatkozik, 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.

6.5.4.3. Hozzájárulás visszavonása

Az érintettet az adatkezeléshez való hozzájárulását bármikor visszavonhatja, erről a jogáról, illetve a visszavonás módjáról a hozzájárulási nyilatkozatban vagy az ezzel egyidőben átadott adatkezelési tájékoztatóban kell tájékoztatni.
A hozzájárulás visszavonásának olyan egyszerűnek kell lenni, mint amilyen a hozzájárulás megadása.
A Szervezet a hozzájárulás visszavonásához alternatív csatornát is biztosít. Az Adatvédelmi manager az 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.

6.5.5. 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 kötött szerződések esetében ez a jogalap **nem használható**!

6.5.6. Jogi kötelezettség jogalap alkalmazása

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

Tipikus jogszabályi kötelezettségek: számviteli tv., adójogszabályok, 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 nyilván kell tartani a vonatkozó jogszabályt.

6.5.7. 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.**

6.5.8. 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 közérdek jogalapot a Budapest Főváros IV. kerület Újpest Önkormányzatával kötött közszolgáltatási szerződésben meghatározott feladatok tekintetében alkalmazza.

6.5.9. 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 érdekével, amely az adatkezelést szükségessé teszi.
Az „adatkezelő jogos érdeke” adatkezelési jogalap alkalmazhatóságáról a Szervezet az adatkezelési tevékenység megkezdése előtt elvégzett **érdekmérlegelés** eredménye alapján dönt.

6.5.10. Érdekmérlegelés folyamata

Az Adatkezelő az ***ASZ01-1 Adatkezelési tevékenységek nyilvántartás-*** ban szereplő és jogos érdek jogalapon kezelt adatkezelési tevékenységekhez az adatkezelés megkezdése előtt vagy az adatkezelési tevékenység változtatásának bevezetése előtt érdekmérlegelést hajt végre az alábbi táblázatban megfogalmazott kérdésekre adott válaszokkal.
Amennyiben az érdekmérlegelés eredményeképpen nem állapítható meg, hogy az Adatkezelő jogos érdeke erősebb, mint az érintetté, az adatkezelési tevékenységet késedelem nélkül fel kell függeszteni vagy a vizsgálat során feltételezett adatkezelési folyamat mentén nem kezdhető meg.
Az adatkezelési folyamat átalakítását követően az érdekmérlegelést ismételten el kell végezni.

Az érdekmérlegelések elvégzéséért felelős: az ***Adatvédelmi manager***
Az ellenőrzést elvégzi: az ***Adatvédelmi Tisztviselő***

Az érdekmérlegelést az ***ASZ-06-01 Érdekmérlegelés nyilvántartás*** alapján kell elkészíteni.
Az Adatkezelő az érdekmérlegelésnél az alábbi paramétereket határozza meg:

Paraméter	Magyarázat
AKT	Az adatkezelési nyilvántartásban az adatkezelési folyamat sorszáma.
Sorszám	Az érdekmérlegelés sorszáma.
Adatkezelés célja	Az adatkezelési folyamat célja – azonos, mint az adatkezelési nyilvántartásban.
Jogalap	Az adatkezelés jogalapja – azonos, mint az adatkezelési nyilvántartásban.
Jogos érdek meghatározása	Az adatkezelési nyilvántartásban szereplő szövegezés további értelmező kiegészítéssel.
Kezelt Adatok	Az adatkezelési nyilvántartásban megadott adatok.
Érintettek	Az adatkezelési nyilvántartásban megadott érintettek köre.
Jogos érdek igazolása	Hivatkozás az Adatkezelő környezetének valós veszélyeire vagy konkrét statisztikára, mely alátámasztja az Adatkezelő jogos érdekét.
Jogos érdek időbeli korlátozottsága	Jogszabályi korlátok vagy bármely egyéb külső vagy szervezeten belüli időbeli korlát.
Adatkezelés tárgyi szükségessége	Meghatározandók és dokumentálandók a tárgyi szükségességet igazoló tényezők. Felsorolás, mely annak a tényét igazolja, hogy az Adatkezelőnek valóban szüksége van a személyes adatok kezelésére.
Adatkezelés időbeli szükségessége	Meghatározandó és dokumentálandó az a határidő, mely ideig az Adatkezelőnek szüksége enne a kezelt személyes adatokra. Az időbeli korlát és a szükséges határidő közül a rövidebb időintervallumig szabad kezelni az adatokat az adott adatkezelési folyamatban.
Van-e alternatív adatkezelési lehetőség?	Az Adatkezelőnek vizsgálnia kell, hogy van-e bármely más mód az adatkezelés jelenleg bevezetni tervezett módján kívül, amely alkalmazása esetén az adatkezelés célja megvalósítható.
Érintett érdekei pozitív	A vizsgált adatkezelési tevékenyég következtében az érintett milyen, számára pozitív eredményre számíthat.
Érintett érdekei negatív	A vizsgált adatkezelési tevékenyég következtében az érintett milyen, számára negatív eredményre számíthat.

Érintett tartozik-e valamilyen sérülékeny, érzékeny csoporthoz (hátrányos helyzetű, gyermek stb.)	Az Adatkezelőnek vizsgálnia szükséges, hogy az érintettek tartoznak-e valamilyen sérülékeny csoporthoz, beleértve a munkavállalókat, gyermekeket, fogyatékkal élőket stb.
Adatkezelés módja (biztonsági intézkedések)	Az adatkezelés technikai megoldásának rövid bemutatása, pld. informatikai rendszerben, papír alapon, az ügyviteli rendszerben stb.
Megfelelő tájékoztatás vizsgálata. Mennyire számíthat az Érintett az adatkezelésre?	Azt kell vizsgálni, hogy mennyire elterjedt az Adatkezelő által választott adatkezelési megoldás és az Érintett mennyire számíthat arra, hogy a vizsgált folyamatban a személyes adatait kezelni fogja az Adatkezelő.
Van-e lehetősége az Érintettnek ellenőrizni az adatkezelést vagy tiltakozni ellene?	Bizonyítandó, hogy az Érintett élhet a GDPR rendelet 15-22. és 33-34. pontban megfogalmazott valamennyi jogával.
Adatbiztonsági intézkedések	Bemutatandó, hogy milyen technikai és szervezési, védelmi megoldásokat alkalmaz az Adatkezelő az adatkezelési folyamat során.
Hozzáférés korlátozása	Azonosítandó, hogy kik férhetnek hozzá az Érinett adataihoz és, hogy az Adatkezelő milyen megoldást alkalmaz a hozzáférés kontrollálására.
Érdekmérlegelés eredménye	Az érdekmérlegelés eredményének rögzítése.

6.6. 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.

6.7. Pontosság és korlátozott tárolhatóság

6.7.1. 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.

6.7.2. Adatmegőrzés és adateltávolítás

Amíg az adatkezelésnek van **célja és** érvényes **jogalapja**, addig az adatot meg lehet őrizni, ezt az időpontot követően az adatot törölni kell. A kötelezettség attól függ, hogy a Szervezet az adatkezelési nyilvántartásban a tervezett adatkezelési időintervallumnál maximális vagy fix időintervallumot adott meg. Amennyiben egy Európai Uniós vagy magyar jogszabály írja elő az adatok tárolási idejét, akkor jogszabályi kötelezettség jogalapon csak a jogszabályban megadott ideig tárolható az adott személyes adat.
A megőrzési idő leteltét lehetőség szerint jelezze az informatikai rendszer, automatizált törlést csak abban az esetben lehet alkalmazni, ha az adatkezelési időtartam elérte a tárolási határidőt.
Az egyéb esetekben pld. érintetti igény teljesítése, a törlést minden esetben **jóvá kell hagyni.**

*Az adattörlések jóváhagyásáért felelős: az **Adatvédelmi Manager***
*Az ellenőrzést elvégzi: az **Adatvédelmi Tisztviselő***

6.7.3. Adatkezelési tevékenységek változása

Az adatkezelési cél során alkalmazott adatkezelési tevékenységek megváltozását vagy megszűnését az Adatkezelési folyamatgazdának kell figyelemmel kísérnie. Minden tervezett változás előtt jelezni kell az Adatvédelmi manager számára a tervezett változtatást. Az Adatvédelmi manager a megváltozott adatkezelési folyamat ismeretében az alábbi tevékenységeket végzi el:

- Frissíti az adatkezelési nyilvántartást,
- Frissíti az adatfeldolgozói nyilvántartást,
- Elvégzi az adatkezelést megelőző kockázatelemzést,
- Frissíti az adatkezelési tájékoztató(ka)t,
- Szükség esetén oktatást tart az adatkezelési folyamatban résztvevők számára.

6.8. Integritás és bizalmas jelleg

6.8.1. Biztonsági intézkedések

A Szervezet által megtervezett és megvalósított információbiztonsági intézkedések biztosítják a személyes adatok **bizalmas jellegét**, **integritását** és **rendelkezésre állását.** Ezeket az intézkedéseket a 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 az információbiztonsági és/vagy adatvédelmi események, amelyek adott esetben incidensnek minősülhetnek.
Incidens észlelésekor minden lényeges részletet azonnal fel kell jegyezni, a számítógép képernyőről másolatot (képernyőképet) 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.) A Szervezet az adatvédelmi incidensek azonosításának megkönnyítése érdekénem egy incidens példatárat készített (***ASZ-29 Incidens Példatár).*** A példatár segítségével a Szervezet felügyelete alatt munkát végzők könnyebben azonosíthatják, hogy egy esemény incidens vagy nem.

Az Adatvédelmi tisztviselő rendszeres időközönként frissíti az Incidens példatárat a nemzetközi, hazai és a saját szervezeten belüli tapasztalatok alapján.

7.1.4. Incidensek bejelentése szervezeten belüli események esetében

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

Az incidenst észlelő Szervezet telephelyén vagy Home Office-ban munkát végző személy késedelem nélkül (azonnal) értesíti az Adatvédelmi tisztviselőt telefonon a 3. számú függelékben megjelölt kapcsolattartási telefonszámon vagy személyesen.

7.1.5. Gyorselemzés, kárenyhítés

A bejelentést vagy észlelést követően az **Adatvédelmi tisztviselő azonnal** megkezdi az incidens gyanú elemzését.
Már ebben a fázisában is szükséges lehet – az **Adatvédelmi tisztviselő** döntése alapján – további szakértők (**jogász, informatikus, információbiztonsági elemző**) bevonása.
Az **Adatvédelmi tisztviselő – az Adatvédelmi manager** bevonásával - információt gyűjt az incidens gyanúról. Az incidens gyanú körülményeinek vizsgálata és a kezdeti diagnosztikai lépések célja, hogy minél hamarabb, minél részletesebb információ álljon rendelkezésre az incidens gyanúról és a Szervezet döntést tudjon hozni az eseményről, hogy valóban GDPR szerinti adatvédelmi incidens-e az esemény.
Cél, hogy meghatározásra kerüljön:

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

7.1.6. Téves bejelentés

Amennyiben a gyorselemzés során egyértelműen bebizonyosodik, hogy a **bejelentés téves volt,** az incidens gyanú vizsgálata a **Adatvédelmi tisztviselő** döntését követően lezárható.

7.1.7. Döntés az Incidensről

Az azonnali kárenyhítő intézkedések megtételét követően, vagy ha lehetséges azzal egyidőben az **Adatvédelmi tisztviselő** kiértékeli az incidens gyanút a következő szempontok alapján az ***ASZ-08-1 Adatvédelmi incidensek nyilvántartása*** dokumentumban:

- Az érintett adatrekordok száma
- 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, adatvesztéssel járt-e
- Szándékos károkozás történt-e
- A jogsértés (lehetséges) következményei, annak súlyossága

Amennyiben a vizsgálat eredménye és a GDPR 4. cikk a 12. pontja szerinti definíció szerint az esemény incidensnek kell tekinteni, az **Adatvédelmi tisztviselő** döntést hoz az incidensről. Az incidens gyanú bejelentésétől vagy észlelésétől számított legkésőbb 24 órán belül ki kell vizsgálni az eseményt és az **Adatvédelmi tisztviselőnek** döntést kell hoznia az incidensé minősítésről vagy az incidens gyanú eszkalálásáról.

7.1.8. Az incidens egyértelműen nem jár kockázattal Érintettek számára

Amennyiben az esemény a GDPR 4. cikk a 12. pontja szerinti definíció szerint incidensnek minősül, de a korábban megtett biztonsági intézkedések (pl.: titkosítás) következtében az érintettek személyes adataira és szabadságára nézve nem okoz kockázatot az **Adatvédelmi tisztviselő** megállapítja, hogy az esemény nem bejelentés köteles. Az **Adatvédelmi tisztviselő** az ***ASZ-08-1 Adatvédelmi incidensek nyilvántartása*** dokumentumban rögzíti, annak indokait, hogy miért nem jár az esemény kockázattal az érintettek személyes adataira és szabadságára nézve az alábbiak szerint:

- Érint-e különleges adatot
- Érint-e gyermekeket vagy hátrányos helyzetű/ sérült embereket
- Szándékos károkozás történt-e
- Az incidens során kompromittálódott-e a természetes személy(ek) pénzügyi adata
- Az incidens során kompromittálódott-e a természetes személy(ek) email címe vagy telefonszáma
- Az incidens következtében vissza lehet-e élni az érintett személyazonosságával
- Kockázat súlyossága
- Az esemény lehetséges negatív hatásai az érintettekre
- Lehetséges negatív hatás súlyossága
- Incidenssel érintett személyes adatok kategóriái és érzékenysége
- Érintettek sérülékenysége az esemény következtében
- Érintett magánszférájára gyakorolt lehetséges hatások és ezek lehetséges tartama

A bejelentett esemény nem jár kockázattal az érinettre például a következő esetekben:

1. Titkosított (enkriptált) notebook vagy USB adathordozó elvesztése/ eltulajdonítása esetén.
2. Személyes adatok üzemidőn kívüli rendelkezésre állása sérülésének esete, 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.

Amennyiben bizonyítható és dokumentálható, hogy az incidens NEM jár kockázattal és hátással az érintettek személyes adataira és szabadságára, az **Adatvédelmi tisztviselő** a nyilvántartásba vételt követően lezárja az incidenst**.**

Amennyiben az esemény kockázattal jár az érintettre az **Adatvédelmi tisztviselő** döntést hoz az incidens eszkalálásáról.

7.1.9. Az incidens eszkalálása

Az **Adatvédelmi tisztviselő** a 7.1.8. pontban meghozott döntése alapján **az incidenst eszkalálja** az alábbiak szerint.

7.1.9.1. Adatkezelőként végzett tevékenységek esetében

Az Adatvédelmi tisztviselő értesíti és bevonja az incidens kezelésébe a:

- Az incidenssel érintett területek Területi vezetőit
- A Szervezet jogi képviselőjét,
- Szervezet Operatív igazgatóját/Ügyvezetőjét
- és szükség esetén minden egyéb az incidens szempontjából releváns döntési helyzetben lévő kollégát

7.1.9.2. Adatfeldolgozóként végzett tevékenységek esetében

Az **Adatvédelmi tisztviselő** a Szervezet jogi képviselőjével és az Operatív igazgatójával/Ügyvezetőjével történt egyeztetést követően késedelem nélkül értesíti az adatkezelési folyamathoz kapcsolódó az ***ASZ-01-2 Adatfeldolgozói adatkezelések nyilvántartása*** dokumentumban nyilvántartott adatkezelő kapcsolgattatóját és tájékoztatja az incidensről.

7.1.10. Az incidensek nyilvántartása

Az adatvédelmi incidensről hozott döntést követően az Adatvédelmi tisztviselő az incidens további adatait rögzíti az ***ASZ-08-1 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 követelményeknek való megfelelést.

7.1.11. Az incidens eszkalálását követő tevékenységek adatkezelőként végzett folyamatok esetében

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 7.1.6 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 7.1.13 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 7.1.13 pontban meghatározottak alapján és az incidensről **tájékoztatni kell az érintetteket** az 7.1.14 pontban meghatározottak alapján.
   Az incidenst magas kockázatúnak kell tekinteni minimálisan a következő esetekben:
   a) Ha az incidens különleges adatokat vagy gyermekek különleges adatait érinti
   b) Ha az incidens az adott adatkezelési folyamatban kezelt összes adatot érinti
   c) Ha az incidens az érintett pénzügyi adatainak integritását érinti.

7.1.12. Kommunikáció

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

- az illetékes felügyeleti hatóságot (lásd: 7.1.13 pont)
- az érintetteket (lásd: 7.1.14 pont)
- a Szervezet munkatársait, illetve azok adott csoportjait, Ügyvezető igazgatót / Adatvédelmi managert
- 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**.

7.1.12.1. Adatfeldolgozói tevékenységekhez kapcsolódó kommunikációs elvárások

Adatfeldolgozóként végzett adatkezelésekkel kapcsolatos publikus kommunikációt - beleértve a social media kommunikációt, a sajtóközleményeket csak az incidensben érintett adatkezelő írásos engedélyével adhat ki a Szervezet.

7.1.13. Bejelentés a felügyeleti hatóságnak

7.1.13.1. Teljes bejelentés

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/index.php/adatvedelmi-incidensbejelento-rendszer**). 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.

A bejelentések kapcsán a szervezet **Adatvédelmi tisztviselő:**

- nyilvántartást vezet a bejelentésektől,
- köteles meggyőződni a bejelentések hatósághoz történő megérkezéséről,
- további kommunikációt folytat az bejelentett incidensek hatósági megítéléséről és a teendőkről.

7.1.13.2. Szakaszos bejelentés

Amennyiben nem lehetséges az információkat egyidejűleg a bejelentési határidő belül összegyűjteni, azokat további indokolatlan késedelem nélkül, de legkésőbb az észleléstől számított 72 órán belül az Adatvédelmi tisztviselő szakaszos bejelentés formájában bejelenti a hatóság számára.
A bejelentéseket minden esetben írásos formában, a hatóság által biztosított felületen / formában kell megtenni.

7.1.14. 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 igazgatója** 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, ideértve különösen azokat az intézkedéseket – 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 tájékoztatás**t** a Szervezet **Adatvédelmi tisztviselője bevezeti** az ***ASZ-08-1 Adatvédelmi incidensek nyilvántartása táblázatba.***

7.1.15. Javító és kárelhárító intézkedések tervezése és végrehajtása

A kárelhárítási terv kidolgozásáért az adatkezelésben érintett terület vezetője a felelős. A kárelhárítási terv kidolgozásában bevonja a Szervezet IT üzemeltetőjét, az Adatvédelmi managert, az Adatvédelmi tisztviselőt és a Szervezet jogászát.

A Szervezet **Ügyvezetője** felelős a kárelhárító intézkedések végrehajtásához szükséges erőforrások biztosításáért és a kárelhárító intézkedések jóváhagyásáért.
A kidolgozott és jóváhagyott javító kárelhárító terv részleteit az ***ASZ-08-1 Adatvédelmi incidensek nyilvántartásában*** dokumentálja az Adatvédelmi tisztviselő***.***

7.1.16. Incidenskezelési megállapodások más szervezettekkel

A Szervezet az adatfeldolgozói szerződésben megállapodásokat ír alá az incidenskezelési folyamatról minden partnerével,

- akik a Szervezet számára adatfeldolgozást végeznek 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.
A Szervezet az adatfeldolgozókkal kötött szerződései alapján elvárja minden adatfeldolgozójától, hogy a náluk bekövetkezett adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül, de maximum 4 órán belül jelentsék a szerződésben megadott adatvédelmi kapcsolattartónak.
A jelentés tartalmának legalább azokat az információkat kell tartalmaznia, amelyek az adatfeldolgozónak is szükségesek lehetnek az incidens hatásainak megfelelő felméréséhez.

Az adatvédelmi kapcsolattartó elérhetetlensége esetén az adatfeldolgozó kötelezettsége, hogy munkaidőben 2 óránként ismételten megpróbálja a kapcsolatfelvételt.
Az Adatvédelmi manager felelőssége, hogy a kapcsolattartásra megadott elérhetőségeket munkaidőben két óránként ellenőrizze.

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 figyelembevételével 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 - Általános
- Adatkezelési tájékoztató – Munkavállaló
- Adatkezelési tájékoztató – Toborzás

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
    - szerződéses jogalap esetén az adatszolgáltatás a szerződéskötés előfeltétele-e;
    - az adat kezelése 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 ***ASZ01-1 Adatkezelési tevékenységek nyilvántartás-*** ában megadott adatkezelési paraméterekkel összhangban kell elkészíteni.

8.2. Tájékoztatási szabályok

8.2.1. Általános rész

A tájékoztatás 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 adatokat kapcsolattartás céljára használja) vagy
    - ha más címzettel is közlik az adatokat, legkésőbb a személyes adatok **első alkalommal való közlésekor**.

8.2.2. Munkavállalók tájékoztatása

A Szervezet munkavállalói esetében az ***ASZ-07-03 Adatkezelési* tájékoztató-*Munkavállaló*** a munkaszerződés melléklete.
A Szervezetnél megbízási szerződés alapján foglalkoztatott magánszemélyek 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 tájékoztatás megadásának igazolása:

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

8.2.3. A Szervezethez álláspályázat útján jelentkező természetes személyek tájékoztatása

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

- A weboldalon elhelyezett jelölőnégyzet logolásával.

vagy

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

vagy

- Az internetes toborzási portál által nyújtott adatkezelés igazolásával

8.2.4. Természetes személyek, egyéni vállalkozók tájékoztatása

A természetes személyeket és egyéni vállalkozók akik az Adatkezelővel szerződéses jogviszonyban állnak, vagy az Adatkezelővel kötött szerződés alapján az Adatkezelő szolgáltatását igénybe veszik, vagy az Adatkezelő részére szolgáltatást nyújtanak vagy terméket értékesítenek a velük kötött szerződés teljesítésével vagy a szolgáltatás igénybe vételével összefüggésben kezelt adatokról Adatkezelő az ***ASZ-07-05 Adatkezelési tájékoztató—Általános*** dokumentumban tájékoztatja.

8.2.5. Jogi személyek tájékoztatása

A Szervezet olyan szerződéseket köt üzleti partnereivel (jogi személyekkel, akik az Adatkezelővel szerződéses jogviszonyban állnak, az Adatkezelővel kötött szerződés alapján az Adatkezelő szolgáltatását igénybe veszik, vagy az Adatkezelő részére szolgáltatást nyújtanak vagy terméket értékesítenek) 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 Szervezet a partnereivel megállapodik továbbá, hogy jogvita vagy érintetti adatkezeléssel kapcsolatos igénybejelentés esetén késedelem nélkül egymás rendelkezésére bocsátják a tájékoztatással kapcsolatos bizonyítékokat.
Az adatkezelési elvárásokat az ***ASZ-24 Partneri szerződés Adatkezelési melléklet*** dokumentum alapján kell elkészíteni.

A Szervezet a következő weboldalon elérhetővé teszi az ***ASZ-07-05 Adatkezelési tájékoztató—Általános*** dokumentumot:

https://www.uprogram.hu

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
- A szervezet weboldala megtalálható a www.uprogram.hu weboldalon. Az oldal rendszeresen rögzíti a Szervezet által közzétett Általános Adatkezelési tájékoztatót.

8.3. Az érintetti kérelmek, igények teljesítésének támogatása

8.3.1. A kapcsolattartás csatornái

A Szervezet a következő kapcsolattartási csatornákat működteti:

- e-mail
- személyes bejelentési lehetőség
- Amennyiben az érintett kérdés, kérés vagy panasz okán a Szervezethez fordul - függetlenül attól, hogy a tevékenységet adatkezelőként vagy adatfeldolgozóként végzi - ezeket a bejelentkezéseket és az ezek nyomán született intézkedéseket a Szervezet nyilvántartja.

A bejelentéseket és intézkedéseket az ***ASZ-07-01 Érintetti kérelmek nyilvántartása*** dokumentumban kell nyilvántartani.

A nyilvántartásban az alábbi adatok dokumentálása szükséges:

Paraméter	Magyarázat
Kérés azonosító (év-sorszám)	A nyilvántartásban a kérelem sorszáma.
A kérés leírása	Az érintett kérelmének leírása.
A kérés bejelentésének dátuma	A kérelem Szervezethez való beérkezésének dátuma.
Kérés bejelentője (név)	Az érintett neve, akitől a kérelem érkezett.
Kérés bejelentőjének azonosítása (belső azonostó, cím, igazolványszám)	Az érintett pontos azonosítására szolgáló egyedi azonosító.
A kérés tartalma	A kérelem pontos tartalma, hogy mivel fordult az érintett a Szervezethez.
Érintett halálát követően érintetti adatok kiadhatók a következő személyeknek	Az érintett által meghatalmazott személy azonosítására alkalmas adatok.
Érintett adatkezelések	Azok az adatkezelési folyamatok, melyeket érint a benyújtott kérelem.
Adatkezelő / adatfeldolgozó	Annak a meghatározása, hogy az adatkezelési folyamatot a szervezet adatkezelőként vagy adatfeldolgozóként végzi.
Adatkezelő	Adatfeldolgozóként végzett tevékenységhez kapcsolódó érintetti igény esetén az adatkezelési folyamat Adatkezelőjének megnevezése

A bejelentés kezelésének módja	Annak meghatározása, hogy a bejelentést a Szervezet kezeli vagy továbbítja az adatkezelőnek.
Végrehajtásért felelős	Az Adatvédelmi tisztviselő és Adatvédelmi manager.
Teljesítés leírása	A kérelem végrehajtásával kapcsolatosan elvégzett tevékenységek.
Teljesítés lezárásának dátuma	A kérelem lezárásának dátuma.
Kommunikáció lépései	A szervezet rögzíti az összes kommunikációs lépést és azok tartalmát. Adatfeldolgozóként végezett tevékenységekhez kapcsolódó esetekben a Adatkezelő utasítását is rögzíteni szükséges.
Azonosításra bekért kiegészítő adatok	Azon adattípusok melyeket az érintettől bekér a Szervezet amennyiben nem tudja biztosan azonosítani a bejelentést benyújtó személyt.
Megjegyzések	Egyéb megjegyzések a kérelemmel kapcsolatosan.

8.3.2. Az érintett azonosítása

Az érintetti jogok teljesítésénél fontos szempont, hogy a kérelmet benyújtó érintett azonosítása megfelelő legyen. Az azonosítást el kell végezni függetlenül attól, hogy az adott adatkezelési tevékenységet a Szervezet a saját nevében vagy egy másik adatkezelő nevében, mint adatfeldolgozó végzi.
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,
- a Szervezet által kezelt további bármely adatot vagy adatrészletet.

Az érintettek azonosítását az érintetti igényt felvevő kolléga végzi el. Kétség esetén késedelem nélkül bevonja az azonosításba az Adatvédelmi managert és vagy az Adatvédelmi tisztviselőt.
A kiegészítő azonosítás kérésekor kifejezetten ügyelni kell arra, hogy a kiegészítő adatot csak úgy lehet bekérni az érintettől, hogy azt valóban ellenőrizni tudja a Szervezet.

Például:

- Az érintettről postacímet, rendelési adatokat, e-mail címet, telefonszámot tárol a szervezet, akkor a személyazonosításához nem kérhető be az anyja neve vagy a személyi igazolvány száma.

8.3.3. E-mailen érkező kérelem

Amennyiben az érintett kérelmét egy olyan email címről adja fel, melyet a Szervezet tárol és az emaillel azonosítható érinett adataival kapcsolatos a kérelem, abban az esetben az érintettet azonosítottnak kell tekinteni.

Az érintett a kérelmét elsősorban az adatvedelem@uprogram.hu e-mail címre küldheti. Abban az esetben, ha az érintett a GDPR-ral egyértelműen kapcsolatos igényt fogalmaz meg egy másik email címre címezve, a portafiókot kezelő felhasználó késedelem nélkül továbbítja a beérkezett email üzenetet az adatvedelem@uprogram.hu -ra.
Ezt követően a kimenő és bejövő postaládájából is törli az eredeti üzenetet.
Amennyiben egy postafiók üzemeltetője nem biztos az email tartalma alapján, hogy az emailben megfogalmazott igényt GDPR eljárásrend alapján kellene kezeli, úgy késedelem nélkül értesíti a Szervezet Adatvédelmi Managerét és egyeztet a továbbítás szükségességéről.

8.3.4. Telefonos ügyfélszolgálaton érkező kérelem

Az ügyintéző kolléga tájékoztatja az érintettet, hogy a Szervezet írásban és telefonon keresztül is elfogad el érintetti kérelmet, azzal, hogy felkéri az érintettet, hogy amennyiben lehetséges írásban is nyújtsa be érintetti igényét az adatvedelem@uprogram.hu emailcímen.

8.3.5. Személyesen bejelentett kérelem

Az ügyintéző kolléga személyazonosításra alkalmas fényképes igazolvány bemutatását kéri az érintettől majd ellenőrzi az ***ASZ-07-02 Érintetti adatkezelési igény bejelentés űrlap*** kitöltését, ezt követően átveszi az érintett kérelmét.

8.3.6. Adatfeldolgozóként végtett tevékenységekkel kapcsolatos érintetti igények és panaszok kivizsgálása és kezelése

Amennyiben az érintett a Szervezethez fordul érintetti igényének teljesítése érdekében vagy bármely a Szervezet által valamely adatkezelő nevében végzett adatkezelési tevékenységgel kapcsolatos panasza, igénye vagy bejelentése kapcsán, a Szervezet az bejelentésekkel kapcsolatosan az alábbiak szerint jár el:

1. Az bejelentés nyilvántartásba vétele során meghatározza az adatkezelési tevékenységhez kapcsolódó adatkezelőt és késedelem nélkül, de legkésőbb 5 munkanapon belül átadja az érintetti megkeresést az adott folyamathoz kapcsolódó adatkezelőnek.
2. A bejelentés beérkezését követően kivizsgálja a bejelentést és ***ASZ-07-01 Érintetti igények kérelmek nyilvántartás*** dokumentumban rögzíti a kivizsgálás eredményét. Szükség esetén külön jegyzőkönyvet készít a feltárt részletek pontos rögzítése érdekében.
3. Ezt követően tájékoztatja az érintettet, hogy mint adatfeldolgozó nem jogosult az Érintetti igény teljesítésére, így az igényt az adatkezelőnek továbbítja.
4. A kivizsgálás eredményéről a Szervezet Adatvédelmi managere egyeztet az Adatvédelmi tisztviselővel.

8.4. Kommunikáció és eszkaláció

Az 8.3.1. pontban meghatározott csatornákon érkező Érintetti kérelmeket az Adatvédelmi manager kezeli és továbbítja az Adatvédelmi tisztviselőnek. Az Adatvédelmi tisztviselő a

kezelési folyamatba haladéktalanul bevonja, a Szervezet jogi képviselőjét és meghatározza a konkrét tevékenységet a Szervezet számára.
A meghatározott tevékenységről és annak határidejéről az Adatvédelmi tisztviselő – az Adatvédelmi manager bevonásával - tájékoztatja a Szervezet érintett részlegének vezetőjét.

8.4.1. Eszkaláció

Az Adatvédelmi tisztviselő nem elutasítható adatkezelési korlátozási kérelem és tiltakozási kérelem esetén jelenti a Szervezet az **Ügyvezető igazgatójának** az esetet és a GDPR-ban, illetve a jelen szabályzaban foglaltak szerint jár el.

Amennyiben az érintett az adatfeldolgozóként végzett adatkezeléshez kapcsolódóan az eljárás során észrevételt, panaszt vagy bármilyen kifogást fogalmaz meg az eljárással kapcsolatosan az Adatvédelmi tisztviselő késedelem nélkül tájékoztatja az adatkezelőt a beérkezett bejelentéssel kapcsolatosan.

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. Az érintetti kérelem, 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 az igényének - törlés, tiltakozás vagy hozzájárulás visszavonás - teljesítéséta Szervezet az általa üzemeltetett hírlevél küldő rendszer leiratkozás funkcionalitásával hajtja végre. Ebben az esetben az érintetti igényt külön nem kell nyilvántartani, a hírlevél küldő rendszerben a napló fájl rendszert kell az érintetti igény nyilvántartásának tekinteni.

Az adatvedelem@uprogram.hu -ra érkező igények esetében az igény egyedi azonosítót kap.

8.6. Az érintetti igény rögzítése

1. Az Adatvédelmi tisztviselő – az Adavédelmi manager bevonásával - ellenőrzi a következőket:

    a. Az érintett adatait jogszabályi kötelezettség mentén kezeli-e a Szervezet (számviteli, munkajogi, egészségügyi stb.). Ha igen lejárt-e a jogszabályban előírt adatkezelési határidő. Amennyiben lejárt a törvényben meghatározott határidő az adatok törölhetők.
    b. Az érintett adatait szerződéses jogalap mentén kezeli-e a Szervezet, és a megkötött szerződés (melyben az érintett az egyik fél) érvényben van-e?
    Amennyiben érvényben van akkor azok az adatok melyeket e jogalap mentén kezel a Szervezet nem törölhetők, csak a szerződés megszűnésével együtt.
    Amennyiben már nincs érvényben a szerződés, az adatok törölhetők.
    c. Az érintett adatait az érintett létfontosságú érdeke jogalap mentén kezeli-e a Szervezet. Ha a Szervezet az érintett érdeke jogalap mentén kezeli az adatokat az adatok nem törölhetők.

d. Az érintett adatait jogos érdek jogalap mentén kezeli-e a Szervezet. Ha a Szervezet jogos érdek mentén kezeli az adatokat, akkor a korábban elvégzett érdekmérlegelési teszt és az érintett által jelzett igény összevetésével kell az érintetti igény teljesítéséről a döntést meghozni. 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.

2. Az Adatvédelmi tisztviselő – az Adavédelmi manager bevonásával - ellenőrzi, hogy az érintett adatát a Szervezet átadta-e adatfeldolgozónak, vagy címzettnek. Amennyiben az adatot átadta egy adatfeldolgozónak vagy címzettnek, akkor értesíteni kell az adatfeldolgozót vagy a címzettet az alábbiak szerint:
   a. Amennyiben az érintett már rendelkezik adatvédelmi azonosítóval, melyet az Adatfeldolgozó/további Adatkezelő is nyilván tart, abban az esetben a korábbiakban kiadott adatvédelmi azonosítóra hivatkozva kéri a Szervezet az érintett adatainak 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 az adott bejelentőtől, a felhasználóra, és erre tekintettel az érintettet adatvédelmi azonosítóval látta el. Egy következő levélben a Szervezet már csak az adatvédelmi azonosítóra hivatkozva küldi a teendőket. Az első e-mailt, amelyben még a személyes adatok benne voltak, az Adatfeldolgozó / további Adatkezelő köteles letörölni, erről tájékoztatni szükséges.

3. Amennyiben nincs adatfeldolgozói adattovábbítás, akkor az Adatvédelmi manager – az Adatvédelmi tisztviselő utasítása alapján - a Szervezet minden aktív rendszeréből törli az érintett adatait és kizárólag az ***ASZ-07-01 Érintetti igények 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 igények kérelmek nyilvántartás*** tekintetében hozzáférésre jogosultak: Ügyvezető igazgató, Adatvédelmi manager és az Adatvédelmi Tisztviselő.

A Szervezet az **ASZ-*07-01 Érintetti igények kérelmek nyilvántartás - ról*** minden érintetti igény esetén, de negyed évente egy alkalommal mindenképpen mentést végez egy titkosított USB pendrive-ra. Az ***ASZ-07-01 Érintetti igények kérelmek nyilvántartás*** biztonsági mentésének tárolási helye (USB titkosított pendrive fizikai elérhetősége: Adatvédelmi manager irodája – zárt fiók

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

4. Az érintetti törlési igény végrehajtásáról az Adatvédelmi tisztviselő emailben tájékoztatja az érintettet. Az emailt törölni kell az levelező rendszerből az elküldést követően.

8.7. 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.

8.7.1. Tájékoztatás költsége

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

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

8.7.2. 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**, (egy hónapon belül harmadik alkalommal él az Érintett ugyanazon tárgyú a 15-22. cikk szerinti jogai gyakorlására irányuló kérelemmel) az Adatkezelő megtagadhatja a kérelem alapján történő intézkedést.

8.8. 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;
- A kezelt 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 a 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 Adatvédelmi tisztviselő kontrollálja és az Adatvédelmi manager kommunikálja az Érinttet felé.

8.9. 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 folyamatgazda végzi az adatbázisban.
Az Adatvédelmi tisztviselő rendszeresen ellenőrzi az érinettek 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 tájékoztatja az érinettet, 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.

8.10. 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 adatok 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.

8.11. 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 Szervezt 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 Európai 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.

8.12. 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.

*Az hordozható adatok átadásáért felelős: az **Adatvédelmi** **tisztviselő***

8.13. Tiltakozáshoz való jog

8.13.1. 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.

8.13.2. Tiltakozás vagy panasz bejelentés Adatfeldolgozó általi adatkezelés ellen

Amennyiben az érinett tiltakozik egy Szervezet Adatfeldolgozója vagy Al-adatfeldolgozója által végzett tevékenysége ellen, a Szervezet késedelem nélkül kivizsgálja a bejelentést.

- A kivizsgálás megkezdésével egyidejűleg az Adatvédelmi tisztviselő – az Adavédelmi manager bevonásával - megvizsgálja, hogy a bejelentés kapcsán történt-e adatvédelmi incidens. Amennyiben igen az incidens kezelési eljárás szerint jár el a továbbiakban.
- Amennyiben nem történt incidens a Szervezet a kivizsgálás körülményeit és eredményét figyelembe véve értesíti a bejelentőt a vizsgálati eredményről.
- Amennyiben az adatkezelési tevékenységet a Szervezet valamely más Adatkezelő nevében mint, adatfeldolgozó végzi a kivizsgálás megkezdésekor az Adatvédelmi Manager értesíti az adott adatkezelési folyamat adatkezelőjének az ASZ-01-02 nyilvántartásban szereplő adatvédelmi kapcsolatartóját.

Kivizsgálás eredménye:

Amennyiben a kivizsgálás eredménye alapján az Szervezet alfeldolgozója adatvédelmi vétséget követett el, a Szervezet felszólítja a vétség kijavítására, a nem szabályos működés kijavítására vagy beszüntetésére.

8.14. Automatikus döntéshozatal, profilalkotás

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

- az érintett kifejezett hozzájárulása esetén vagy
- ha uniós vagy tagállami jog teszi lehetővé vagy
- ha 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 ELHUNYTAK ADATAINAK KEZELÉSE

Az érinettnek a 2011. évi CXII. törvény az információs önrendelkezési jogról és az

információszabadságról törvény értelmében lehetősége van nyilatkozatot tenni, hogy halálát követő 5 évben az Adatkezelő által róla kezelt adatokat kinek adhatja ki, valamint az érinett jogait ki gyakorolhatja.
Amennyiben az érintett életében írásbeli nyilatkozatot tett az Adatkezelőnél, akkor az elhunyt által meghatalmazott személy bizonyítást követően az érintett halálát követő 5 éven belül jogosult az érintetti jogok gyakorlására.
A beérkezett halálesetre vonatkozó Érintetti adatkezelési nyilatkozatokról a Szervezet nyilvántartást vezet az ***ASZ-28 – Érintetti halálozási nyilatkozatok nyilvántartása*** dokumentumban.

Nyilatkozat hiányában is eljárhat az elhunyt közeli hozzátartozója a GDPR 16. cikk szerinti helyesbítéshez való jog és a 21. cikk szerinti tiltakozáshoz való jog gyakorlásában. Ha az elhalálozás előtt is jogellenes volt az adatkezelés, akkor a meghatalmazott élhet az elhunyt 17. cikk szerinti törléshez való jogával és a 18. cikk szerinti korlátozás jogával.

Az érintett nyilatkozatát elektronikus formában hozzáférés kontrollal ellátott mappában kell tárolni az Adatkezelő szerverén, papír alapú dokumentumot zárt szekrényben az Adatkezelő irodájában. Az adatkezelést a *GDPR rendelettel összefüggő adatkezelés* nyilvántartási sor tartalmazza.

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 adatkezelést 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

Jelen szabályzat hatálya alatt EU-n belülinek az **Európai Gazdasági Térség (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 betartja 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 jogaihoz kapcsolódó kérelmek megválaszolása tekintetében;
- az Adatfeldolgozó jelen szabályzat incidens kezelésről szóló fejezetében meghatározott eljárás mentén jelenti az incidenseket, továbbá 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.

10.1.1. Adatfeldolgozói szerződés alvállalkozóval/teljesítési segéddel

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 szerint a szerződés részeként vagy mellékleteként is kezelhetőek.

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 szerint a szerződés részeként vagy mellékleteként is kezelhetőek.

10.1.3. Al-Adatfeldolgozók menedzsmentje és szerződéskötés

Amennyiben egy adatkezelési tevékenységben a Szervezet az adatfeldolgozó és az adatfeldolgozási tevékenységéhez al-adatfeldolgozót vesz igénybe, ezt csak az adatkezelő írásos engedélyével teheti.
Az adatfeldolgozói szerződésben rögzítettek szerint az alábbi esteket kell a Szervezetnek vizsgálnia:

Az Adatkezelő a vele megkötött szerződésben:

a) általános meghatalmazást adott további adatfeldolgozó alkalmazására, az adatfeldolgozót fel kell venni ASZ-01-2 Adatfeldolgozói nyilvántartásba.
b) engedélyhez kötötte a további adatfeldolgozó alkalmazását, akkor az alfeldolgozó adatkezelésbe történő bevonása előtt engedélyeztetni kell az Adatkezelővel.
c) Megtiltotta további adatfeldolgozó alkalmazását az adatott adatkezelési folyamat teljesítésében, ez esetben az alfeldolgozó nem vehető igénybe.

Az a) és b) estben 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 szerint a szerződés részeként vagy mellékleteként is kezelhetőek.

10.2. Adatfeldolgozói szerződés megkötésének folyamata

1. A Szervezet kapcsolattartójaként eljáró kolléga a szerződés előkészítése során azonosítja az alvállalkozóval/teljesítési segéddel megkötendő szerződés adatkezelési tevékenységeit és amennyiben a tevékenység során az alvállalkozó/teljesítési segéd az Adatkezelő nevében adatfeldolgozói tevékenységet végez a szerződés megkötése előtt jelzi az Adatvédelmi managernek.
2. A szerződést előkészítő kolléga az üzleti tevékenységről szóló szerződéssel együtt köteles az adatfeldolgozói szerződést megkötni a 10.1. pontban megfogalmazottak mentén.

11. ADATÁTADÁS 3. FÉL SZÁMÁRA

A Szervezet az általa kezelt adatokat különböző céllal alvállalkozók/teljesítési segédeknek nak, azaz adatfeldolgozóknak adja át.

11.1. Adatvédelmi Azonosító használata

A Szervezet Adatvédelmi azonosítót alkalmazhat olyan esetben, ahol az érintett élhet a GDPR rendeletben megfogalmazott törlés 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

A Szervezet minden új adatkezelési folyamat bevezetése előtt megvizsgálja, hogy az adott adatkezelési folyamatban az adatok átadásán milyen jellegű kontrollt alkalmaz. A Szervezettel érvényes szerződéses jogviszonyban álló Adatfeldolgozóknak átadott adatok esetében a mindenkori adatfeldolgozói szerződés határozza meg, hogy szükséges-e az adatvédelmi azonosító alkalmazása. A vizsgálatot az adatkezelés jogalapja alapján kell elvégezni és dokumentálni az ***ASZ-01-1 Adatkezelési tevékenységek*** nyilvántartásban.

Az Adatvédelmi Azonosító kiadásának folyamata:

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.
A Szervezet nem határozott meg olyan adatkezelési folyamatot, amelynek esetében alapértelmezetten alkalmazza az Adatvédelmi Azonosítót.

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:

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. Adatvédelmi Azonosító használatának adatkezelési jogalapok szerinti kategorizálása

Az egyes adatkezeléshez kapcsolódó jogalapok esetén az Adatvédelmi Azonosító használata különböző vagy akár szükségtelen is lehet az elvégzendő nagymennyiségű, csoportos vagy azonos adatkezelési tevékenység következtében, vagy egyéb okból az alábbiak szerint:

11.2.1. Adatvédelmi Azonosító használata hozzájáruláson alapuló adatkezelés esetében

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

11.2.2. Adatvédelmi Azonosító használata 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. Adatvédelmi Azonosító használata 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 feladat végrehajtása

A Szervezet alkalmazhat Adatvédelmi Azonosítót.

11.2.6. Adatvédelmi azonosító használata Jogos érdek jogalapon alapuló adatkezelés esetén

A Szervezet alkalmazhat Adatvédelmi Azonosítót annak érdekében, hogy az Érintett bármikor tiltakozhasson a személyes adatainak kezelése 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. Egyedi adatátadási törlés folyamata

12.1.1. Adatvédelmi Azonosító használata Adatvédelmi azonosítóval rendelkező Érintettek esetében

1. Amennyiben 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 ugyanennek 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.

12.1.2. Adatvédelmi Azonosító használata az Érintetti igény bejelentését követően

1. Amennyiben 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. Az 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 ugyanennek a természetes személynek, sem másnak nem adja ki még egyszer. Amennyiben az érinett még egyszer megadja az adatait a Szervezetnek, úgy egy új Adatvédelmi Azonosítót kell a számára kiadni.

12.1.3. Adatvédelmi Azonosító használata Adatkezelés korlátozásának bejelentését követően

Amennyiben az érintett él azzal a jogával, hogy az általa rendelkezésre bocsátott személyes adatok kezelését korlátozza az alábbi indokok valamelyikével:

- Vitatja az adatainak pontosságát,
- Vitatja az adatkezelés jogosságát,
- Igényli az Adatkezelő által törlésre szánt adatok további tárolását jogi igények előterjesztéséhez,
- tiltakozása esetén, míg megállapításra nem kerülnek, hogy mely fél jogos indokai élveznek az ügyben elsőbbséget (mely esetben a korlátozás csak az tiltakozási ügy lezárásáig áll fenn).

A Szervezet az Érintett személyes adatait a korlátozás indokaként megjelölt ügy lezárásáig, kizárólag az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez használhatja.
Amennyiben a Szervezet a megadott Adatvédelmi azonosítóval ellátott adatsort kiadta Adatfeldolgozónak, akkor haladéktalanul köteles azt értesíteni az Adatfeldolgozót az Adatvédelmi azonosítóhoz rendelt adatok korlátozásáról.
A korlátozás feloldásáról az Adatkezelő előzetesen értesíti az érintettet.

13. MUNKAVÁLLALÓK SAJÁT TULAJDONÚ ESZKÖZEINEK HASZNÁLATA

A Szervezet lehetőséget biztosít a munkavállalóknak arra, hogy egyedi engedélyezést követően beállítsák a céges levelezést a Munkavállalók saját tulajdonában lévő mobil eszközeikre.
Az engedélyezési folyamat az alábbiak szerint történik:

1. A munkavállaló emailben jelzi az igényét az Ügyvezető felé.
2. Az Ügyvezető dönt a munkavállaló igényéről és jóváhagyás esetén továbbítja az igényt a jóváhagyással az IT üzemeltető felé. A levél címzettjei között szerepel a Munkavállaló, így értesül a jóváhagyásról.
3. Az IT üzemeltető a Munkavállaló eszközén engedélyezi a levelezést, a szükséges beállításokat elvégzi a mobil eszközön és a Szervezet saját informatikai rendszerében.
4. A Munkavállaló aláírja az **ASZ-04_Sajat_tulajdonu_eszkoz_hasznalati_nyilatkozatot**, amit az IT üzemeltető lead a HR osztályon, ahol a Munkavállaló személyi aktájába kerül lefűzésre.

A Munkavállaló az utolsó munkában töltött napján az IT üzemeltető és a Területi vezető/Ügyvezető igazgató részvételével köteles bemutatni az eszközön a Szervezet adatainak törlését és a levelezésből való kilépését.

14. ÉRINTETTI JOGOK ALKALMAZÁSA ADATVISSZAÁLLÍTÁST KÖVETŐEN

A Szervezet adatmentési és **adatvisszaállítási folyamataiba beépíti**, hogy az informatikai rendszer mentéséből vagy archiválásából történő adatvisszaállítás esetén az adatvisszaállítást követően, de még az éles használat megkezdése előtt az Adatvédelmi manager ellenőrzi a következőket:

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

Az adatvisszaállítást követően az érintettek adatainak ellenőrzéséért felelős: az
Adatvédelmi manager
Az ellenőrzést elvégzi az: ***az Adatvédelmi tisztviselő***

15. ADATTOVÁBBÍTÁS HARMADIK ORSZÁGOKBA

EU-n kívülinek, azaz harmadik országnak tekintendő minden olyan ország, ami nem tagja az **EGT tagállamainak**.
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 vagy

(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 van a Szervezet és a címzett között (GDPR 46. cikk (3)) vagy
3) kötelező erejű vállalati szabályok vannak érvényben az adatfeldolgozó és a Szervezet között vagy
4) amennyiben az 1-3 pontban megfogalmazott feltételek nem állnak rendelkezésre az adattovábbításhoz a Szervezet tájékoztatja az Érinettet a 3. országba történő adattovábbítás veszélyeiről és kifejezett hozzájárulását kéri az adatok továbbításához, az ***ASZ-22 3. ország adattovábbítási nyilatkozat*** alapján.

Amennyiben a Szervezet által szolgáltatás igénybevételéhez és/vagy 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, de a hozzájárulást be kell kérni.

A 3. országba történő adattovábbítási folyamat előtt a megfelelő biztonsági garanciák ellenőrzéséért felelős: az ***Adatvédelmi tisztviselő***

15.1. Szervezet által azonosított harmadik országokba történő adattovábbítás egyedi eljárásai

A Szervezet az alábbi adatkezelési folyamatok esetében határozza meg a 3. országba történő adattovábbítást egyedi elvárásait.

15.1.1. Kapcsolattartás EGT-n kívüli partnerekkel

Azon munkavállalók esetében, akik kereskedelmi vagy szakmai kapcsolattartást végeznek a 3. országbeli partnerek kapcsolattartóival. A munkakör betöltése előtt a kapcsolattartási feladatot rögzíteni kell a munkavállaló munkaszerződésében, munkaköri leírásában, miszerint a Szervezet által kezelt személyes adatok közül kizárólag a kapcsolattartáshoz szükséges adatok kerülnek kiadásra a kapcsolattartás során.

16. OKTATÁS ÉS KÉPZETTSÉGI ELVÁRÁSOK

16.1. Felkészültség

Az Adatvédelmi tisztviselő, az Adatvédelmi manager és az Adatkezelési folyamatgazdák esetében a szükséges szakmai felkészültséget a munkaköri leírásukban vagy a megbízási szerződésükben kell meghatározni az alábbiak szerint:
Elvárás:
Adatvédelmi Tisztviselő esetében

- minimum két napos adatvédelmi oktatáson való részvétel vagy Jogi diploma vagy információbiztonsági adatvédelmi szakirányú végzettség vagy releváns munkakörben szerzett szakmai tapasztalat.
- rendszeres képzés/önképzés

Adatvédelmi manager esetében

- Rendszeres képzés/önképzés
- Jelen Adatvédelmi és adatkezelési Szabályzat beható ismerete
-

Adatkezelési folyamatgazdák estében:

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

16.2. 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 17. pontjában részletezettek szerint.

A tudatosító képzések megszervezéséért felelős:az ***Adatvédelmi manager***
Az ellenőrzést elvégzi az: ***az Adatvédelmi tisztviselő***

17. 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 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.

18. ADATVÉDELMI KÉPZÉS

A Szervezet irányítása alatt munkát végző személyek rendszeres, differenciált adatvédelmi képzésben részesülnek az adatkezeléssel való kapcsolatuk és az ebben rejlő kockázatok alapján.
Általános adatvédelmi tudatosító képzés
GDPR alapok – elektronikus oktatási anyag
Adatkezelési elvek

- Adatkezelési elvek, jogalapok

- Érintett jogainak teljesítési lehetőségei
- Adatvédelemi incidens szervezeten belüli eszkalációs rendje

19. AZ ADATKEZELÉSI FOLYAMATOK ÉRTÉKELÉSE

19.1. Folyamatos megfigyelés

A Szervezet tervezett módon belső auditokat végez, annak ellenőrzésére, hogy az adatkezelési folyamatai megfelelnek-e a GDPR rendelet szabályainak, történtek-e időközben változások.

Az Adatvédelmi tisztviselő folyamatosan ellenőrzi az alábbi teljesítmény mutatókat:

- Az Adatkezelési folyamatgazda kollégák és az Adatvédelmi manager 1 hónapja nem fordultak kérdéssel az Adatvédelmi tisztviselőhöz
- Fél éve nem volt Érintetti panaszkezelési igény

Az Adatvédelmi manager folyamatosan ellenőrzi az alábbi teljesítmény mutatókat:

- A szervezet vezető beosztású kollégái 1 hónapja nem jelentettek adatkezelési folyamat változtatást

19.2. Időszakos ellenőrzés

Az Adatvédelmi tisztviselő tervezett módon ellenőrzéseket hajt végre az adatvédelmi szabályozási rendszer működésének megfelelősége érdekében.
Amennyiben a 19.1 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

- Vendég beléptetés, video megfigyelés és nyilvántartás
- Marketing célú megkeresések, hírlevél
- Kereskedelmi kommunikáció, ügyfél kezelés
- Adatfeldolgozók menedzsmentje

19.3. 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 **április hónap utolsó** munkanapján végzi el.

> *Az Adatkezelési folyamatok felülvizsgálatáért a felelős: az **Adatvédelmi manager***
> *Az ellenőrzést elvégzi : **az 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 adatok törlésének ellenőrzése
- A rögzített incidensek következmények kivizsgálása és szükség esetén a folyamatok módosítása
- Az adatfeldolgozók által végzett tevékenységek minimálisan véletlenszerű ellenőrzése.

19.4. 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.
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 manager végzi el és az Adatvédelmi tisztviselő ellenőrzi.
A Szervezet a belső auditok során feltárt hiányosságokat jegyzőkönyvben rögzíti, illetve a hiányosságok megszüntetését követően szükség esetén az Adatvédelmi manager – az Adatvédelmi tisztviselő ellenérzése mellett - az adatkezelési dokumentáción átvezeti a módosításokat. Az auditokat az auditálásra vonatkozó szakmai ajánlások szerint kell elvégezni, és az eredményeket dokumentált információként meg kell őrizni.

20. AZ ADATKEZELÉSI FOLYAMATOK BIZTONSÁGÁNAK FEJLESZTÉSE

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

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

E tevékenységek során feltárt nem megfelelő működések kijavítására a Szervezet intézkedéseket hoz.
Az adatvédelmi szabályozási 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 évenkénti megszervezéséért a felelős: az ***Adatvédelmi tisztviselő***

21. MELLÉKLETEK / FÜGGELÉKEK

1. sz Függelék Kapcsolattartók

Az Adatvédelmi manager elérhetőségei:

Neve: ……..
E-mail címe: adatvedelem@uprogram.hu
Telefonszáma: ……

Az Adatvédelmi tisztviselő elérhetőségei:

Neve: Gill & Murry Zrt.
E-mail címe: sandor@gillandmurry.com
Telefonszáma: Sándor Zsolt András +36 70 401 2951

2. sz Függelék – Kapcsolódó dokumentumok listája

3. Azonosító	Megnevezés	Forma	Elérhetőség
ASZ-01	Adatvédelmi Szabályzat		
ASZ-01-1	Adatkezelési tevékenység nyilvántartás		
ASZ-01-2	Adatfeldolgozói adatkezelések nyilvántartása		
ASZ-02	Munkavállalói titoktartási nyilatkozat		
ASZ-03-01	Adatvédelmi tisztviselő feladatai és felelősségei		
ASZ-03-02	Adatvédelmi manager feladatai és felelősségei		
ASZ-04	Saját tulajdonú eszköz használati nyilatkozat		
ASZ-05-01	Hatásvizsgálatot megelőző kockázatértékelés		
ASZ-06-01	Érdekmérlegelés		
ASZ-06-04	Adatkezelési cél átminősítés nyilvántartás		
ASZ-07-01	Érintetti igények, kérelmek nyilvántartása		
ASZ-07-02	Érintetti adatkezelési igény bejelentő űrlap		
ASZ-07-03	Adatkezelési Tájékoztató Munkavállalói		
ASZ-07-04	Adatkezelési Tájékoztató – Toborzás		
ASZ-07-05	Általános Adatkezelési tájékoztató		
ASZ-08-01	Incidenskezelési nyilvántartás		
ASZ-08-02	Incidens kockázatelemzés		
ASZ-09-01	Adatátadási nyilvántartás		
ASZ-22	3. Ország adattovábbítási nyilatkozat		
ASZ-23	Szülői hozzájárulás		
ASZ-24	Partneri szerződés adatkezelési kiegészítés		
ASZ-28	Érintetti halálozási nyilatkozatok nyilvántartása		
ASZ-29	Incidens példatár		

ASZ-30	Adatfeldolgozói mintaszerződés - adatkezelő		
ASZ-31	Adatfeldolgozói mintaszerződés - adatfeldolgozó		
ASZ-32	Al-Adatfeldolgozói mintaszerződés		

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	Gill&Murry Zrt.	+36 70 401 2951 Sándor Zsolt	sandor@gillandmurry.com
Adatvédelmi Manager			
Információbiztonsági felelős			
IT üzemeltetés vezető			
Szervezet Jogásza			
Ügyvezető igazgató	Ungi Veronika		

1.SZ MELLÉKLET - HATÁSVIZSGÁLAT

22. AZ ADATVÉDELMI HATÁSVIZSGÁLAT LEFOLYTATÁSA

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

22.1. 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.

5.1 Alkalmazott munkamódszer

A Szervezet az adatkezelési határvizsgálatot elvégezheti a jelen mellékletben meghatározottajk szerint vagy a NAIH weboldaláról letölthető DPIA szoftver segítségével.

22.2. A tervezett adatkezelés leírása

A Szervezet elkészíti a tervezett adatkezelési műveletek módszeres leírását, beleértve az adatkezelés céljainak ismertetését, és adott esetben az adatkezelő által érvényesíteni kívánt jogos érdek bemutatását.
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 adatok tárolásához használt eszközöket (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák);
5) figyelembe vették-e olyan jóváhagyott magatartási kódex előírásait, melyhez a Szervezet csatlakozott.

22.3. 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 vizsgálatát az ***ASZ-05-02 Adatvédelmi hatásvizsgálat*** 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:

Ha a kérdések bármelyikére **nem** a válasz, abban az esetben **a Szervezet nem kezdheti meg az adatkezelést 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 szabályozási környezet változik.

*Az szükségességi-arányossági vizsgálatot az **Adatvédelmi manager** végzi el az adatkezelés megkezdése előtt.*
*Az ellenőrzést elvégzi : az **Adatvédelmi Tisztviselő***

22.4. Kockázatok meghatározása

Az adatvédelmi hatásvizsgálat az adatvédelmi kockázatok feltárását célozza. Ha nem vagy nem megfelelően van megvalósítva egy követelmény, akkor fennál a veszélye, hogy az érintettek személyes adatainak kezeléséhez fűződő jogai sérülnek.
A hatásvizsgálatot az ***ASZ-05-02 Adatvédelmi hatásvizsgálat*** 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 kell meghatározni az incidens bekövetkezésekor lehetséges kárt, azaz a személyes adatok bizalmassága, integritása és/vagy rendelkezésre állása sérülésének mértékét. Az adatvédelmi hatás mértéke szakértői becsléssel kerül meghatározásra.

22.4.1. A kockázatmenedzsment folyamat lépései

1. Az előzetes kockázatelemzés során adatvédelmi hatásvizsgálatra kijelölt adatkezelési folyamatokat csoportosítása. 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 kockázatait csökkentő intézkedésekre.
5. Kockázatkezelési terv készítése.

22.4.2. 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 fenyegetéseket, 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

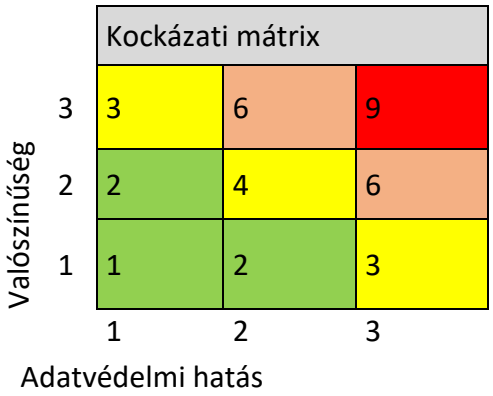
22.4.3. Hatás

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

22.4.4. 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

22.5. Kockázatkezelés

22.5.1. 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 észszerűen megtehető intézkedések nem csökkentik megfelelően a kockázatot a Szervezet a hatóságtól előzetes konzultációt kér.

közepes	**Kezelendő kockázat,** az adatkezelésmegkezdése 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 észszerűen 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.

22.5.2. 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*** tartja 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 manager***
Az ellenőrzést elvégzi : az ***Adatvédelmi Tisztviselő***

22.6. Dokumentáció

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

22.7. Nyomon követés és felülvizsgálat

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

a) Az adatkezelési folyamat megváltozik
b) Az adatkezelési folyamatban résztvevő adatfeldolgozó megváltozik
c) A szabályozási környezet megváltozik
d) Az Adatvédelmi manager, 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) Egy adott adatkezelésre vonatkozó utolsó hatásvizsgálat 2 évnél régebbi.

2.SZ MELLÉKLET

Aktív rendszerek listája:

- Vectory – számviteli szoftver
- Tenant – belsős ügyviteli, adminisztrációs program
- Previse belsős ügyviteli, adminisztrációs program
- Nexon – bérszámfejtő szoftver
- Microsoft Exchange levelező rendszer
- Mywork – CRM rendszer
- Jantar rendszer – beléptető rendszer
- Logipix – kamera, beléptető rendszer
- Intelio – kamera rendszer

<A dokumentum vége>