Tempus Közalapítvány
Adatvédelmi Szabályzata

6.sz. módosítás

Tartalomjegyzék

1 NYILATKOZAT

A Tempus Közalapítvány (továbbiakban: TKA) személyes adatokat kezel a jogszabályokban és szerződéseiben meghatározott tevékenységének hatékony és a jogszabályoknak megfelelő módon történő ellátására. Ezen adatok gyűjtése a munkavállalókat, pályázókat és további szerződéses ügyfeleket érinti (a továbbiakban: érintettek) és (*különösen, de nem kizárólag*) magában foglalja a név, cím, email cím, születési dátum, IP cím, azonosító számok, személyes és bizalmas adatok, különleges adatok gyűjtését is.

A TKA elkötelezett az információk gyűjtése, kezelése, tárolása és megsemmisítése során a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679 rendelet (a továbbiakban: GDPR), illetve Magyarország adatvédelmi jogszabályoknak történő megfelelésnek.

A TKA szabályozásokat, eljárásokat, ellenőrzési mechanizmusokat és intézkedéseket alakított ki a GDPR szabályoknak és az ott írt elveknek történő lehető legteljesebb mértékű és folyamatos megfelelés érdekében (ideértve az alkalmazottak oktatását, eljárási dokumentumok, audit intézkedések és értékelések készítését is). A TKA által kezelt érintettek személyes és/vagy különleges adatai biztonságának és biztonságosságának biztosítása és fenntartása a TKA adatvédelmi rendszerének központi eleme és a TKA minden eljárás és funkció biztosítása során tartja magát a GDPR-ban nevesített szabályokhoz és az ahhoz kapcsolódó elvekhez.

Ennek keretében a TKA a „Beépített Adatvédelem” (Privacy by Design) megközelítést alkalmazza, melynek a célja a proaktivitás.

Jelen Adatvédelmi Szabályzathoz kapcsolódó jogszabályok

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 irányelv hatályon kívül helyezéséről
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [az Infotv-nek a GDPR hatálya alá eső adatkezelésekre alkalmazandó szabályai – lásd. Infotv. 2. § (2) és (4) bekezdése]
Ptk.	a Polgári Törvénykönyvről szóló 2013. évi V. törvény
Mt.	a Munka Törvénykönyvéről szóló 2012. évi I. törvény
Alaptörvény	Magyarország Alaptörvénye

2 SZABÁLYZAT CÉLJA ÉS HATÁLYA

A jelen szabályzat célja, hogy a GDPR szabályok hatálya alatt a TKA megfeleljen a jogszabályi, törvényhozói és szabályozói környezetnek; valamint annak biztosítása, hogy minden személyes és különleges kategóriába eső információ biztonságos, azok használata során védve van és a

jogszabályoknak megfelelően kerül feldolgozásra, tárolásra, valamint továbbításra, elköteleződve a személyes adatok szervezeten belül történő biztonságos kezelésére.

A GDPR szabályok a megbízhatóságot és irányítást előmozdító rendelkezéseket tartalmaznak, és e szabályoknak történő megfelelés érdekében a TKA átfogó és hatékony irányítási intézkedéseket alkalmaz. Ezen eszközök célja végeredményben minimalizálni az adatok védelme megsértéséből fakadó kockázatokat; valamint fenntartani a személyes adatok védelmét.

2.1 A Szabályzat Hatálya

Jelen **Szabályzat személyi hatálya** kiterjed az Adatkezelő irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyekre (a munkavégzésre irányuló jogviszony jellegétől függetlenül), továbbá azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák, továbbá azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelés érinti. Az Adatkezelő megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra az Adatkezelő által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy az Adatkezelő által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

A **Szabályzat tárgyi hatálya** az Adatkezelő mindazon adatkezeléseire kiterjed – függetlenül attól, hogy az adatkezelés elektronikusan vagy papíralapon történik –, amelyek

a.) az oktatási és egyéb tevékenység nyújtásához kapcsolódó adatkezelést valósítanak meg a Szabályzatban felsorolt jogszabályok és belső utasítások szerint;
b.) foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg (a Adatkezelővel munkaviszonyban vagy egyéb foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek);
c.) az Adatkezelővel szerződéses kapcsolatban álló jogi és természetes személyek, Adatkezelők képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

2.2 Fogalmak

Jelen Szabályzat alkalmazása során összhangban a GDPR 4. cikkében és az Infotv. 3. §-ában foglaltakkal - az alábbi fogalmakat kell alkalmazni:

- ***GDPR*** a jelen dokumentum értelmében az Általános Adatvédelmi Rendeletet jelenti, és minden olyan adatvédelmi jogszabály együttes megjelölésére is használandó, amelynek a TKA megfelel.
- ***Személyes adat*** azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
- ***Különleges adat*** a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes 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
- ***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.

- ***Érintett*** azt a természetes személyt jelenti, aki a személyes adat tárgya.
- ***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.
- ***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.
- ***Profilalkotás*** személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.
- ***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.
- ***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.
- ***Személyes adatok határokon átnyúló adatkezelése*** személyes adatoknak olyan kezelése:

  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

- ***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.

- ***Felügyeleti Hatóság*** egy tagállam által létrehozott független közhatalmi szerv, Magyarország esetében a Nemzeti Adatvédelmi és Információszabadság Hatósága.

- ***Adattovábbítás*** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele

- ***Harmadik országba történő adattovábbítás*** olyan adattovábbítás, amely az Európai Gazdasági Térségről szóló megállapodásban nem részes államok területén kívülre történik

3 ALAPELVEK

A GDPR 5. cikke megköveteli, hogy a személyes adatok:

a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni

(„jogszerűség, tisztességes eljárás és átláthatóság")

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

c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk ***(„adattakarékosság")***

d) pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék ***(„pontosság")***

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, a rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel ***(„korlátozott tárolhatóság")***

f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve ***(„integritás és bizalmas jelleg").***

Az 5. cikk (2) bekezdése megköveteli, hogy *az adatkezelő felelős a fentieknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („****elszámoltathatóság****")* és megköveteli, hogy a cégek bemutassák, hogy hogyan felelnek meg a fenti elveknek, részletezve és összefoglalva azokat az intézkedéseket és ellenőrző mechanizmusokat, amelyekkel a személyes adatok védelme érdekében és az adatkezelés kockázatainak csökkentése érdekében rendelkeznek.

4 CÉLOK

A TKA elkötelezett amellett, hogy minden általa kezelt személyes adat gyűjtése és kezelése a vonatkozó jogszabályoknak és elveknek megfelelően történjen.

A TKA a következő célokat az ennek való megfelelés érdekében, valamint azért tűzte ki, hogy intézkedéseket, eljárásokat és ellenőrzési mechanizmusokat alakítson ki a céloknak megfelelő biztosítására és fenntartására.

TKA biztosítja az alábbiakat:

- Védjük az egyének jogait az ismert és róluk a TKA által, tevékenysége körében kezelt személyes adatok tekintetében.
- A GDPR szabályoknak való megfelelés érdekében adatvédelmi szabályzatot, eljárást, audit tervet és képzési programot alakítunk ki, alkalmazunk és tartunk fenn.
- A TKA által kifejtett tevékenységek felügyelete a GDPR szabályoknak és elveknek való megfelelés érdekében történik.
- Adatot csak olyan esetben kérünk, kezelünk vagy tárolunk, ha a kezelésre vonatkozó jogszabályi követelményeknek megfelelünk.
- Különleges kategóriájú adatot kizárólag a GDPR szabályoknak megfelelően kezelünk.
- A hozzájáruló nyilatkozatot a megszerzés időpontjában rögzítjük és a Felügyeleti Hatóság kérésére bizonyítjuk a hozzájárulás meglétét.
- Minden munkavállaló *(ideértve az újonnan belépőket és megbízottakat is)* a GDPR szerint fennálló kötelezettségekkel kapcsolatban megfelelően tájékozott és a GDPR elvekkel és szabályokkal kapcsolatban teljes körű oktatásban részesült és tisztában van a fentieknek a TKA tevékenységére vonatkozó alkalmazásával.
- Ügyfeleink biztonságban érezhetik magukat személyes adataik számunkra történő átadásakor és tisztában vannak azzal, hogy azok kezelése a GDPR szerinti jogaiknak megfelelően történik.
- A GDPR szabályoknak való megfeleléssel kapcsolatban folyamatos ellenőrző, felülvizsgálati és javító rendszert tartunk fenn, hogy még a kockázatok megjelenése előtt azonosítsuk a hiányosságokat és a meg nem felelést.
- Figyelemmel kísérjük a Felügyeleti Hatóság, Európai Adatvédelmi Testület (European Data Protection Board, EDPB) és GDPR-ral kapcsolatos híreket és újdonságokat annak érdekében, hogy tisztában legyünk az újdonságokkal, jelzésekkel és további követelményekkel.
- Az adatvédelemmel kapcsolatos bármely jogsértés vagy panasz azonosítására, kivizsgálására, figyelemmel kísérésére és jelentésére átfogó és írásos Panaszkezelési és Adatvédelmi incidens ellenőrzési mechanizmust és eljárást alkalmazunk.
- Kijelöltük az adatvédelmi tisztviselőt, aki felelős a GDPR szabályok és elvek teljeskörű felügyeletéért és implementációjáért és tájékozott a szabályokkal kapcsolatban és azzal, hogy azok miként érintik a TKA-t.
- Egyértelmű jelentéstételi és felügyeleti láncot alkalmazunk az adatvédelmi megfelelőséggel kapcsolatban.
- Minden személyes adatot a GDPR határidőknek és követelményeknek megfelelően tárolunk és semmisítünk meg.
- Bármely olyan tájékoztatás, amelyet az érintettnek a róla tárolt vagy használt személyes adattal kapcsolatban adunk, tömören, átláthatóan, érthetően és könnyen hozzáférhető formában, tiszta és egyértelmű nyelvezettel ellátva kerül kibocsátásra.
- A munkavállalók tisztában vannak a GDPR alapján fennálló saját jogaikkal és a 13. és 14. cikkek szerinti információ közzétételben részesülnek.

5 SZABÁLYOZÁSI ELJÁRÁSOK

5.1 ELSZÁMOLTATHATÓSÁG ÉS MEGFELELÉS

A vállalt adatkezelés természetére, hatályára, összefüggéseire és céljaira tekintettel a TKA eljárásokat végez az adatkezelések hatásainak azonosítására, értékelésére, mérésére és figyelemmel kísérésére.

A TKA által az adatvédelmi jogszabályoknak, szabályozásoknak való megfelelés biztosítására és bizonyítására alkalmazott technikai és szervezeti intézkedéseket a jelen dokumentum és a kapcsolódó szabályozások tartalmazzák. Ezek az alábbiakat foglalják magukban:

- Informatikai (Információbiztonsági) szabályzat
- Iratkezelési Szabályzat
- Kamera használati szabályzat
- Kiküldetési szabályzat
- Távmunka szabályzat
- Gyakornokok foglalkoztatásáról szóló szabályzat
- HR szabályzat

5.1.1 BEÉPÍTETT ADATVÉDELEM

A Beépített Adatvédelmi megközelítés célja, hogy a megelőzés érdekében - eljárásaink, rendszereink és tevékenységünk segítségével csökkenteni lehessen a személyes adatok kezelésével kapcsolatos kockázatokat.

Adattakarékosság

A GDPR 5. cikkének c) pontja alapján a személyes adatoknak "*a szükségesre kell korlátozódniuk*", amely az általunk alkalmazott minimalista megközelítésünk alapköve. Az adatot csak olyan esetben szerezzük meg, tároljuk, kezeljük és osztjuk meg, amennyiben az szolgáltatásaink elvégzéséhez és jogi kötelezettségeink teljesítéséhez elengedhetetlen és csak olyan hosszú ideig tároljuk, ameddig az szükséges.

Úgy szerveztük meg rendszereinket, eljárásainkat és tevékenységeinket, hogy a személyes adatok gyűjtését - a meghatározott cél elérése érdekében - a közvetlenül releváns és szükséges mértékre korlátozzuk. Az adat minimalizálás segíti az adatvédelmi kockázat és adatsértések csökkentését és támogatja a GDPR szabályoknak történő megfelelést.

Intézkedések annak biztosítására, hogy csak a szükséges adatok kerüljenek összegyűjtésre: -

- Elektronikus adatgyűjtés (*például formanyomtatványok, honlapok, kérdőívek*) esetén csak a gyűjtés és későbbi kezelés szempontjából releváns mezőket szerepeltetjük.
- Fizikai adatgyűjtést (*például személyesen, telefonon stb.*) parancsfájlok és belső nyomtatványok használatával támogatjuk, ahol a kért adatgyűjtést az előre meghatározott mezők használata biztosítja. Ebben az esetben is csak a releváns és szükséges adatokat gyűjtjük.
- Egyedi megállapodásokat kötöttünk olyan harmadik fél adatkezelőkkel, akik számunkra személyes adatokat küldenek (*függetlenül attól, hogy adatkezelőként vagy adatfeldolgozóként járunk-e el*). Ez azt jelenti, hogy csak az általunk végzett adatfeldolgozási tevékenységhez kapcsolódó releváns és szükséges adatok kerülnek megküldésre.

- Iratmegsemmisítési eljárásunk van arra az esetre, ha az adat alany vagy harmadik személy az általunk megkövetelten túlmutatóan, további személyes adatot küld részünkre.

Korlátozás

A *Beépített Adatvédelem* megközelítés azt jelenti, hogy a TKA a személyes adatokkal kapcsolatban végzett tevékenységekkel kapcsolatban korlátozási módokat alkalmaz. A korlátozott hozzáférés alapvetően beépült a TKA eljárásaiba, rendszereibe és struktúrájába és ez biztosítja, hogy kizárólag azok férnek hozzá a személyes adatokhoz, akik erre felhatalmazással és/vagy releváns céllal rendelkeznek.

5.1.2 INFORMÁCIÓ ÁTADÁS ÉS ÁRAMLÁS

A TKA minden, általa adatkezelői vagy adatfeldolgozói minőségében megszerzett, feldolgozott és megosztott személyes adatot azonosít, kategorizál és regisztrál, és megfelel az adatkezelési nyilvántartásokban és tájékoztatókban foglaltaknak, amely az alábbiakat foglalja magában:

A TKA által kezelt személyes adatok:

- honnan származnak;
- azokat kikkel közöljük;
- mi az adatfeldolgozás jogalapja;
- milyen formátumban érhető el;
- ki a felelős személy;
- közlések és átadások.

5.2 AZ ADATKEZELÉS JOGALAPJA *(JOGSZERŰSÉG)*

A TKA által végzett személyes adatkezelési tevékenységek központi eleme a GDPR 6. cikkének való megfelelés, valamint a feldolgozási kötelezettségek jogszerűségének biztosítása és igazolása. A személyes adatokon végzett bármilyen adatkezelési tevékenység megkezdése előtt mindig azonosítjuk az erre feljogosító jogalapot és azt összevetjük a rendelet szabályaival.

A jogalap rögzítésre kerül a nyilvántartásban és amennyiben alkalmazandó, adatközlési kötelezettségeink körében átadásra kerül az érintett, valamint a Felügyeleti Hatóság számára. ***Az adatot csak olyan esetben szerezzük meg, kezeljük vagy tároljuk, amennyiben az adatfeldolgozási követelmények jogszerűségének kritériumát az alábbiak szerint teljesítjük: -***

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

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;

c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

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 szabadságjogai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

5.2.1 KÜLÖNLEGES KATEGÓRIÁJÚ ADAT FELDOLGOZÁSA

A GDPR 9. cikk (1) a Különleges Kategóriájú Személyes Adatot az alábbiak szerint definiálja: -

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 kezelése tilos – kivéve, amennyiben a 9. cikk (2) bekezdésében foglalt indokok miatt ez megengedett.

Amennyiben a TKA különleges kategóriájú adatnak minősülő személyes adatot kezel, azt a GDPR 9. cikkének (2) bekezdéseiben foglalt, alábbi esetek valamelyikének fennállásakor teszi.

Csak olyan esetben kezelünk különleges kategóriájú személyes adatot, amennyiben: -

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 a GDPR 9. cikk (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 az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;

d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;

e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;

f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;

g) az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges

tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

h) 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 9. cikk (3) bekezdésben említett feltételekre és garanciákra figyelemmel;

i) az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;

j) az adatkezelés a 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

Amennyiben a TKA a fenti kategóriákba tartozó személyes adatot kezel, a kezelést megelőzően a TKA különleges rendelkezéseket és intézkedéseket alkalmaz.

Az alkalmazott intézkedések az alábbiak: -

- Az adatkezelés megkezdését megelőzően ellenőrizzük a GDPR 9. cikk (1) és (2) bekezdésének követelményeit
- Az adatkezelés alkalmával megfelelő szabályozási dokumentum birtokában meghatározzuk az alábbiakat: -
    - eljárásainkat a GDPR elveknek történő megfelelés biztosítása érdekében
    - a feltételnek megfelelő kezelt, személyes adat visszatartása és megsemmisítésére vonatkozó szabályozásokat
    - megőrzési időszakokat és indokokat *(például jogi, törvényi stb.)*
    - ebben a tárgykörben meglévő szabályozás áttekintésére és frissítésére vonatkozó eljárásokat

5.2.2 AZ ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA

A TKA minden adatkezelési tevékenységről nyilvántartást vezet (1.sz. melléklet), és a nyilvántartásokat olyan írásbeli, tiszta és érthető formában tartja fenn, hogy az a Felügyeleti Hatóság kérésére azonnal elérhető legyen.

Adatkezelőként (vagy képviselőként) eljárva a felelősségi körünkben végzett adatkezelési tevékenységeink belső nyilvántartásai az alábbi információkat tartalmazzák: -

a) az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;

b)az adatkezelés céljai;

c)az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;

d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;

e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;

f) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;

g) ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

Adatkezelőként (vagy képviselőként) eljárva a felelősségi körünkben az adatkezelő nevében végzett adatkezelési tevékenységeink belső nyilvántartásai az alábbi információkat tartalmazzák: -

a.) az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az Adatvédelmi Tisztviselőnek a neve és elérhetőségei;

b.) Az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;

c.) Adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása *(beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a megfelelő garanciák leírását);*

d.) A (*GDPR 32. cikk (1) bekezdésében említett*) technikai és szervezési intézkedések általános leírása a jelen dokumentum 13. pontja szerint.

5.3 HARMADIK FÉL ADATFELDOLGOZÓI TEVÉKENYSÉGE

A TKA, szerződéses jogviszony keretében külsős adatfeldolgozókat vesz igénybe bizonyos adatkezelési tevékenységek végzése céljából. Eljárást folytatunk a cégen kívül kezelt minden személyes adat azonosítása, kategorizálása és nyilvántartása érdekében, abból a célból, hogy az adat, az adatkezelési tevékenység, adatfeldolgozó és a jogalap mind nyilvántartásra és áttekintésre kerüljenek, és könnyen elérhetők legyenek. ***Ilyen külsős adatkezelési tevékenységnek minősülnek különösen*** *(de nem kizárólag**) az alábbiak: -***

a.) Tevékenység megvalósításához szükséges informatikai rendszerek

b.) Bérszámfejtés

c.) Könyvelés

d.) IT Szolgáltatások

A szerződéskötés előtt minden adatfeldolgozót megismerünk és megbizonyosodunk arról, hogy az adatfeldolgozó az általunk megbízott munka elvégzésére megfelelő, kielégítő és hatékony.

Eljárásaikat és tevékenységeiket a szerződés megkötését megelőzően és a szerződés időtartama alatt nyomon követjük, hogy megbizonyosodjunk arról, hogy azok az adatvédelmi jogszabályoknak megfelelnek.

Egyedi szolgáltatói megállapodásokat (SLA) és szerződéseket kötünk minden adatfeldolgozóval,

amelyek többek között az alábbi rendelkezéseket is tartalmazzák: -

a.) Az adatfeldolgozók adatvédelmi kötelezettségeit;

b.) Elvárásainkat, jogainkat és kötelezettségeinket;

c.) Az adatkezelés időtartamát, céljainkat és elképzeléseinket;

d.) Az érintettek jogait és garanciális intézkedéseit;

e.) Az adatfeldolgozás természetét és célját;

f.) Az érintettekre vonatkozó személyes adat fajtáját és kategóriáit.

Az adatfeldolgozókat tájékoztatjuk, hogy az előzetesen, külön megadott engedélyünk hiányában nem vonhatnak be más adatfeldolgozót és bármely olyan, a meglévő adatfeldolgozóinkon felüli szándékolt változtatást, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, írásban, a változás implementálását megelőzően kell bejelenteni számunkra.

A fenti meghatározott bizonyos szerződésnek vagy más jogi aktusnak tartalmaznia kell különösen azt, hogy az adatfeldolgozó:

- A személyes adatokat kizárólag írásbeli utasításunk alapján kezeli,
- Engedélyünket kéri a személyes adat valamely harmadik ország vagy nemzetközi szervezet számára való továbbításához (kivéve, ha azt az adatfeldolgozó számára a rá alkalmazandó jogszabály írja elő),
- Erről a továbbításra vonatkozó jogi előírásról az adatfeldolgozó minket az adatkezelést megelőzően értesít,
- Biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak,
- Mindenkor meghozza a személyes adatok védelméhez szükséges intézkedéseket,
- Tiszteletben tartja, támogatja és megfelel azon adatbiztonságra vonatkozó kötelezettségeinknek, hogy az érintettek jogainak érvényesítésekor megkeresésükre válaszoljunk,
- Segíti a TKA-t az adatbiztonsági, kockázatcsökkentési, adatsértés jelzési és adatvédelmi hatás vizsgálatokra vonatkozó kötelezettségeknek való megfeleléssel kapcsolatban,
- Kérésre az adatkezelési szolgáltatás nyújtásának befejezését követően a TKA kérése alapján minden személyes adatot töröl vagy visszajuttat a TKA számára, és törli a meglévő másolatokat, amennyiben lehetséges,
- A TKA rendelkezésére bocsát minden olyan információt, amely itt és a szerződésben meghatározott kötelezettségek teljesítésének igazolásához szükséges,
- Megengedi és elősegíti a szerződés szerinti auditokat, ellenőrzési és egyéb vizsgálatokat és jelentéstételt,
- Azonnal tájékoztatja a TKA-t bármely jogsértésről, meg nem felelésről vagy arról, ha a szerződés szerinti feladatának ellátására képtelen.

5.4 ADATOK MEGŐRZÉSE ÉS AZOKKAL RENDELKEZÉS

A TKA meghatározott eljárásokkal rendelkezik a jogszabályokban, szerződésekben foglalt adatmegőrzési határidőknek, és a GDPR követelményeknek való megfelelés tekintetében, annak érdekében, hogy csak a feltétlen szükséges ideig őrizze és kezelje a személyes adatot. Minden személyes adat felett oly módon rendelkezünk, hogy az az érintettek jogait és magánéletét védje (*például adatmegsemmisítés zúzás által, bizalmas hulladék megsemmisítése, biztonságos elektronikus törlés*) és a személyes adatok védelmét mindenkor előnyben részesítjük.

6 ADATVÉDELMI HATÁSVIZSGÁLAT (DPIA, DATA PROTECTION IMPACT ASSESSMENT)

Amennyiben a TKA olyan adatkezelést végez, amely új technológiákat alkalmaz, és/vagy amennyiben az adatkezelés a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal jár, minden esetben Adatvédelmi Hatásvizsgálatot (Data Protection Impact Assessment; DPIA) végzünk.

A GDPR 35 (3) cikke alapján az adatkezelési tevékenységet valószínűsíthetően magas kockázattal járónak minősítjük, amennyiben az az alábbiakat tartalmazza: -

- Természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is –alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
- A személyes adatok különleges kategóriáinak nagy számban történő kezelése;
- Büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése;
- Nyilvános helyek nagymértékű, módszeres megfigyelése (például CCTV);
- Ha az adatkezelési tevékenység valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve;
- Ha az adatkezelés új technológiákat alkalmaz;
- Új, korábban nem alkalmazott adatkezelési tevékenység esetén;
- Jelentős mennyiségű személyes adat regionális, nemzeti vagy szupranacionális szintű kezelése, amelyek az érintettek jelentős számára hatással lehet;
- Ha az adatkezelési műveletek megnehezítik az érintettek számára, hogy a jogaikat gyakorolják.

Az adatvédelmi hatásvizsgálatok végzése lehetővé teszi számunkra azt, hogy a leghatékonyabb módon biztosítsuk az adatvédelmi kötelezettségeinknek való megfelelést és az adatkezelés során a legmagasabb szintű adatvédelmet biztosítsuk. Ez a Beépített Adatvédelmi megközelítésünk része és lehetővé teszi számunkra, hogy az adatkezelés megkezdése előtt értékelhessük a hatást és kockázatot - így a problémát a forrásánál azonosítva és javítva, ezáltal csökkentve a költséget, adatsértést és kockázatot.

Az adatvédelmi hatásvizsgálatok végzése lehetővé teszi számunkra azt, hogy a lehetséges adatvédelmi megoldásokat és enyhítő intézkedéseket a kockázatok azonosítása és azok hatásainak csökkentése érdekében azonosítsuk. Az adatvédelmi hatásvizsgálatok tartalmazzák a megoldásokat és javaslatokat, a kockázatok pedig valószínűségük és hatásuk tekintetében kerülnek értékelésre. A kockázatokkal kapcsolatos megoldások és enyhítő intézkedések célja annak biztosítása, hogy a kockázatok besorolása az alábbiak szerint meghatározható legyen: -

- Eltávolított (azonosított és megszüntetett); vagy
- Csökkentett; vagy
- Elfogadott.

6.1 ADATVÉDELMI HATÁSVIZSGÁLATI ELJÁRÁS

Az adatvédelmi hatásvizsgálati eljárás lefolytatására mindig kijelölésre kerül egy vezető, aki követi az eljárást, feljegyzi a szükséges információt és az eredményeket közli a felsővezetés tagjaival. Minden adatvédelmi hatásvizsgálati eljárás végzése során közreműködik az Adatvédelmi Tisztviselő, aki a GDPR szabályok szerinti eljárásokban való megfeleléshez nyújt segítséget és támogatást.

Az adatvédelmi hatásvizsgálati eljárás vezetője az alábbi kérdésekre adott válaszok értékelésével felméri, hogy szükséges-e a vizsgálat lefolytatása. Amennyiben egy vagy több kérdésre is „***igen***" a válasz, adatvédelmi hatásvizsgálati eljárás lefolytatása válik szükségessé.

A szűrő kérdések (többek között) az alábbiak lehetnek: -

- Az adatkezelés igényli természetes személyekre vonatkozó egyes személyes jellemzők módszeres (*automatizált módszerekkel történő*) és kiterjedt értékelését?
- Az adatkezelés személyes adatok különleges kategóriáit érinti és a személyes adatok nagy számban történő kezelését eredményezi?
- Az adatkezelés büntetőjogi felelősség megállapítására vonatkozó határozatok és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelésére vonatkozik?
- Az adatkezelés nyilvános helyek nagymértékű, módszeres megfigyelését (például CCTV) eredményezi?
- A projekt érinti természetes személyekről gyűjtött új adatokat?
- A projekt kényszeríti természetes személyeket arra, hogy magukról adatokat közöljenek?
- A természetes személyekkel kapcsolatos adat valószínűsíthetően magas kockázattal jár a természetes személyek alapvető jogaira és szabadságjogaira nézve?
- A természetes személyekkel kapcsolatos adat közlésre kerül olyan szervezetek vagy személyek számára, akik korábban nem rendelkeztek hozzáféréssel az adathoz vagy megfelelő garanciákkal?
- Az adatkezelés alkalmaz új technológiákat vagy rendszereket, amelyek a magánéletbe beavatkozó jellegűnek minősíthetőek?
- Az adatkezelés eredményezheti olyan döntések meghozatalát vagy olyan cselekmények meghozatalát természetes személyek ellen, amelyek jelentős hatással lehetnek rájuk?
- A projekt megköveteli, hogy az adatkezelő oly módon lépjen kapcsolatba a természetes személyekkel, amely magánéletükre nézve beavatkozó jellegű lehet?

Az adatvédelmi hatásvizsgálati eljárás az előre meghatározott dokumentum szerint zajlik és - a megfelelőség, valamint annak bizonyítására, hogy minden magas kockázati besorolású adatkezelési tevékenység annak megkezdése előtt értékelésre kerül - minden mozzanat feljegyzésre kerül. Az adatvédelmi hatásvizsgálati eljárást tartalmazó dokumentum a hatásvizsgálat elkészítésének első napjától számított 6 évig megőrzésre kerül és a Felügyeleti Hatóság számára, annak kérésére elérhető.

A TKA az adatvédelmi hatásvizsgálatot a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján közétett, valamint a GDPR-ban rögzítettek szerint végzi el.

Az adatvédelmi hatásvizsgálati eljárás az alábbiakat tartalmazza: -

1. Az adatvédelmi hatásvizsgálati eljárás céljai és szándékai;
2. Az adatvédelmi hatásvizsgálati eljárás hatálya *(amennyiben az több, mint egy adatkezelési tevékenységre vonatkozik);*
3. Az adatkezelési eljárás jogalapjának megjelölése;
4. Az adatvédelmi hatásvizsgálati eljárást milyen tevékenység/magas kockázati tényező indokolja (*például a fenti kezdeti szűrő kérdések közül melyek kerültek azonosításra)?*
5. Az adatkezelési műveletek leírása;
6. Az adatkezelés céljainak ismertetése, az adatkezelő által érvényesíteni kívánt jogos érdek;
7. Az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálata;
8. Az érintett jogait és szabadságait érintő kockázatok vizsgálata (*ideértve a lehetséges magánéletbe való beavatkozást is);*
9. A vállalati kockázatok vizsgálata *(ideértve a szabályozói cselekményeket, meg nem felelést, hírnév sérelmét, közvélemény bizalmának elvesztését stb.);*
10. Megfelelési ellenőrzés végrehajtása a GDPR szabályok, alkalmazandó jogszabályok és bármely Magatartási Kódexek tekintetében;
11. Az azonosított kockázatokról nyilvántartás vezetése;
12. Amennyiben megfelelő, kikérjük az érintett(ek) vagy képviselőik véleményét a szándékunkban álló adatkezelésről;
13. Az intézkedések fenntartása a kockázat azonosítása, csökkentése és eltávolítása tekintetében *(például biztonság, javasolt megoldások, kárenyhítő cselekmények stb.);*
14. Adatáramlás – mi az adat, honnan származik és ki számára kerül továbbításra;
15. Az adatvédelmi hatásvizsgálati eljárás eredményeinek nyilvántartása, rizikó besorolás hozzáadása és következő lépések meghatározása.

7 Az Érintett Jogaival Kapcsolatos Eljárások

7.1 Hozzájárulás és a tájékoztatáshoz való jog

A személyes és bizonyos esetekben különleges kategóriájú adatok gyűjtése alapvető eleme a TKA által kínált termékek és szolgáltatások nyújtásának és ezért különleges ellenőrzési mechanizmusokat és intézkedéseket alakítottunk ki a GDPR szabályokban írt hozzájárulás feltételeinek történő megfelelés érdekében.

A GDPR az érintett hozzájárulását úgy definiálja, hogy az „*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.*”

Ahol az adatkezelés hozzájáruláson alapul, a TKA minden hozzájárulási mechanizmus tekintetében biztosítja, hogy: -

- A hozzájárulás iránti kérelem átlátható, érthető a nyelvezete és minden olvashatatlan feltételtől, zsargontól vagy részletes jogi feltételektől mentes.
- Önkéntes konkrét és megfelelő hozzájáruláson alapul és félreérthetetlenül jelzi a természetes személy szándékát.

- Beleegyezését mindig olyan nyilatkozat vagy egyértelmű megerősítő aktus által jelzi, amely hozzájárulását jelzi az őt érintő személyes adatok kezeléséhez.
- A hozzájárulási mechanizmus előre megadott, átlátható tiszta, minden részletet tartalmazó és könnyen alkalmazandó, valamint érthető.
- Előre behúzott vagy megjelölt négyzetek használata **sohasem** megfelelő.
- Azon esetekben, ahol a hozzájárulás más témák mellett szerepel (*például általános szerződési feltételek, megállapodások, szerződések)*, biztosítjuk, hogy a hozzájárulás a többi témától külön szerepel és nem előfeltétele bármely szolgáltatás nyújtásának (*kivéve amennyiben az a szolgáltatáshoz szükséges*).
- A saját szervezetünk neve mellett adathasználóként bármely olyan harmadik személy adatait is feltüntetjük, aki használni fogja vagy a beleegyezés alapján jár el.
- A hozzájárulás mindig igazolható és ellenőrzési mechanizmusaink vannak annak biztosítására, hogy minden esetben bizonyítani tudjuk a hozzájárulás meglétét.
- Részletes nyilvántartást vezetünk a hozzájárulásról és minimum azt bizonyítjuk, hogy: -
    - a természetes személy hozzájárult személyes adatának használatához és kezeléséhez;
    - a természetes személy tájékoztatásra került a saját szervezetünk nevéről és bármely olyan harmadik személyről, aki az adatát használni fogja;
    - a természetes személyt a beleegyezés megadásakor miről tájékoztattuk;
    - hogyan és mikor szereztük meg a beleegyezést.
- Biztosítjuk, hogy a hozzájárulás visszavonása is olyan egyszerű, tiszta és egyértelmű, mint annak megadása és több lehetőség áll az érintett rendelkezésére, ideértve: -
    - A levelezésben vagy elektronikus kommunikációban elutasítási / leiratkozási linkek megléte;
    - A honlapon és minden írásos kommunikációban az elutasítási / leiratkozási eljárás magyarázata, lépesekkel;
    - Lehetőség a szóbeli, írásban vagy email útján történő elutasításra / leiratkozásra.
- A hozzájárulást visszavonó kérelmek azonnal és minden hátrány nélkül feldolgozásra kerülnek.
- Ahol szolgáltatások gyermekek számára kerülnek nyújtásra, életkor igazolási és szülői hozzájáruló intézkedéseket fejlesztettünk ki és alkalmazunk a hozzájárulás megszerzése érdekében.
- Ellenőrzések és eljárások kerültek kifejlesztésre és alkalmazásra a hozzájárulás frissítése érdekében, különösen, ahol szülői hozzájárulás megszerzése szükséges.
- Különleges kategóriájú adatok esetében a megszerzett hozzájárulás kifejezett *(tisztán és részleteiben nyilatkoztatva, az összetéveszthetőség vagy kétség kizárása mellett*), minden esetben az adatkezelés céljának / céljainak megjelölésével.

7.1.1 A HOZZÁJÁRULÁS ELLENŐRZÉSE

A TKA szigorú nyilvántartást vezet az érintettek személyes adatainak kezelésére szolgáló hozzájárulásról és mindig képes bizonyítani, hogy az érintett hozzájárulását adta személyes adatainak kezeléséhez, amennyiben az szükséges. Emellett biztosítjuk azt is, hogy a hozzájárulás visszavonása ugyanolyan tiszta, egyszerű és átlátható folyamat, mint a hozzájárulás megadása volt.

Olyan esetekben, ahol az érintett hozzájárulása olyan írásbeli nyilatkozat formájában került megadásra, amely más témákat is érint, a hozzájárulásra vonatkozó kérelem olyan formában kerül bemutatásra, amely tisztán megkülönböztethető a többi témától, érthető és könnyen hozzáférhető formájú, valamint tiszta és egyértelmű nyelvezettel rendelkezik. Az Adatvédelmi Tisztviselő minden ilyen írásbeli nyilatkozatot áttekint és - azok használatának megkezdése előtt - engedélyez.

A GDPR úgy rendelkezik, hogy amennyiben az adatkezelés hozzájáruláson alapul és a személyes adat olyan gyermekre vonatkozik, aki a 16. életévét nem töltötte be, az adatok TKA általi kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló személy adta meg, illetve engedélyezte.

Az adat megszerzéséhez, kezeléséhez, tárolásához és közléséhez (*amennyiben alkalmazandó*) szükséges hozzájárulást a TKA az alábbi módokon szerezheti meg: -

- Személyes találkozás alkalmával
- Telefon útján
- Írásban
- Email/SMS útján
- Elektronikus úton *(például honlapon lévő formanyomtatványon keresztül*)

Az elektronikus hozzájárulás nem előre bejelölt jelölő négyezetet tartalmazó, opt-in cselekményt jelent, hanem a természetes személy számára lehetőséget ad arra, hogy hozzájárulását a szükséges tájékoztatás közlését követően adhassa meg. A hozzájárulás megadását - a személyes adat feldolgozása, tárolása és közlése érdekében - email, SMS vagy a hozzájárulás írásbeli megerősítése követi. Az Adatkezelési Nyilatkozatok minden hozzájárulási formában és személyes adat gyűjtése során használandók annak biztosítására, hogy megfelelünk a GDPR által megkövetelt könnyen olvasható és elérhető formában történő információ közlésre vonatkozó követelménynek.

7.1.2 A Hozzájárulás Alternatívái

A TKA tudomásul veszi, hogy az adatkezelésnek hat jogszerű alapja van és a hozzájárulás nem mindig a legmegfelelőbb választás. Minden adatkezelési tevékenységet áttekintettünk és a hozzájárulást kizárólag akkor használjuk, amikor a természetes személynek van választási lehetősége.

Amikor áttekintjük az adatkezelési tevékenységet a hozzájárulási követelményeknek való megfelelés céljából, megbizonyosodunk arról, hogy az alábbi esetek közül egyik sem áll fenn: -

- Ahol hozzájárulást kérünk, de annak ellenére végeznénk adatkezelést, hogy az esetleg nem kerül megadásra (*vagy visszavonásra kerül*). Amennyiben más jogalap alapján – a hozzájárulástól függetlenül – végeznénk adatkezelést, felismerjük, hogy az a használatra nem a megfelelő jogalap;
- Amennyiben a személyes adat kezeléséhez egy általunk nyújtott szolgáltatás előfeltételeként hozzájárulást kérünk, az nem opcionálisan adandó és a hozzájárulás nem megfelelő;
- Ahol a jogviszonyban nem egyenrangú felek állnak, például munkavállalók esetén.

7.1.3 Információ Szolgáltatás

Amennyiben személyes adatot közvetlenül a természetes személytől szerzünk *(például hozzájárulás formájában, munkavállalóktól, írásbeli anyagok és/vagy elektronikus formátum alapján (például honlap formanyomtatványok, hírlevelek, e-mailek stb.)*, az alábbi információkat minden esetben

közöljük, hozzájáruló/vagy adatkezelési nyilatkozat formájában: -

- Az adatkezelő azonosítását és kapcsolattartási adatait és amennyiben alkalmazandó, az adatkezelő képviselőjének azonosítását és kapcsolattartási adatait.
- Az adatvédelmi tisztviselőnk kapcsolattartási adatait.
- A személyes adatok kezelésére vonatkozó adatkezelés célja(i)t.
- Az adatkezelés jogalapját.
- Amennyiben az adatkezelés a GDPR 6. cikk (1) bekezdésének f) pontja alapján történik, *„az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges”*, a jogos érdek részletezését.
- A személyes adatok címzettjeit, illetve a címzettek kategóriáit (*amennyiben alkalmazandó*).
- Adott esetben annak tényét, hogy a *TKA* harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá az Európai Bizottság megfelelőségi határozatának meglétét vagy annak hiányát.
    - amennyiben a TKA az Európai Bizottság megfelelőségi határozata hiányában harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, a TKA által eszközölt megfelelő és alkalmas garanciák megjelölését, valamint az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozást
- A személyes adatok tárolásának időtartamát, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjait.
- Az érintett azon jogát, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról.
- A GDPR 6. cikk (1) bekezdésének a) pontján vagy a 9. cikk (2) bekezdésének a) pontján alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jogot, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét.
- A felügyeleti hatósághoz címzett panasz benyújtásának jogát.
- Azt, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint az érintett köteles-e a személyes adatokat megadni, továbbá milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása.
- A GDPR 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal tényét, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információkat, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

A fenti információt az érintett számára az adat gyűjtésének időpontjában kell rendelkezésre bocsátani és a hozzájárulásra vonatkozó nyilvántartásokat a hozzájárulás megadásától számított 6 éves időtartamig kell megőrizni és tárolni, kivéve, amennyiben jogi követelmény írja elő a hosszabb ideig történő tárolást.

7.2 ADATKEZELÉSI NYILATKOZAT

Az Adatkezelési Nyilatkozat a természetes személyek számára személyes adataik gyűjtésekor *(vagy az adat közvetlen megszerzésekor meglévő legkorábbi lehetőség alkalmával)* kerül átadásra. Az Adatkezelési Nyilatkozat tartalmazza a GDPR 13 és 14. cikkei szerinti követelményeket és a természetes személyek számára tartalmazza a szükséges és jogi információkat arról, hogy hogyan, miért és mikor kezeljük adataikat, valamint jogaikat és kötelezettségeiket.

Az Adatkezelési Nyilatkozatot úgy alkottuk meg, hogy a köz számára nyilatkozzunk arról, hogy TKA miként alkalmazza az adatvédelmi elveket az általunk kezelt adatok tekintetében. Az Adatkezelési Nyilatkozat minden természetes személy számára átadásra kerül, akinek adatát kezeljük *(például ügyfeleknek, munkavállalóknak, harmadik feleknek stb.)* és csak a természetes személyre vonatkozó specifikus, valamint a jogszabály által megkövetelt információt tartalmazza. Az Adatkezelési Nyilatkozat könnyen hozzáférhető, olvasható, zsargon mentes és - az adatgyűjtés formájától függően - több formában elérhető dokumentum: -

Olyan esetekben, amikor a személyes adat megszerzését és kezelését hozzájárulás alapján végezzük, biztosítjuk, hogy:

- A hozzájárulás kérése érthetően és jól láthatóan jelezve legyen;
- Megkérjük a természetes személyeket arra, hogy megerősítőleg adják beleegyezésüket;
- Elegendő információt adunk nekik ahhoz, hogy megalapozott döntést hozzanak;
- Elmagyarázzuk az adatok használatának különböző módozatait;
- Érthetően és egyszerűen biztosítjuk számukra arra, hogy jelezzék beleegyezésüket a különböző típusú adatkezelésekkel kapcsolatban.

7.3 NEM AZ ÉRINTETTŐL SZÁRMAZÓ SZEMÉLYES ADAT

Olyan esetekben, ahol a TKA olyan személyes adatot szerez meg és/vagy kezel, amely közvetlenül **nem** az érintettől származik, a TKA biztosítja a GDPR 14. cikk (1) foglaltakat, hogy az információ (adatkezelő neve, elérhetősége, érintett személyes adatok kategóriái stb.) az érintett számára a személyes adat megszerzésétől számított 30 napon belül átadásra kerül (*kivéve, arról történő tájékoztatás esetén, hogy a személyes adat jogszabályi vagy szerződéses követelmény*).

Az érintett számára szintén tájékoztatást adunk az alábbiakról:

- A személyes adatok kategóriáiról;
- A személyes adat származásának forrásáról és arról, hogy az a köz számára elérhető forrásból származik-e.

Az információt legkésőbb az első kommunikáció vagy közlés megtételekor kell közölni, amennyiben a személyes adatot az érintettel történő kommunikációra használják, vagy más címzettel történő közlés valószínűsíthető. Amennyiben a TKA a továbbiakban bármely személyes adatot az eredeti céltól ***eltérő*** célra kíván kezelni, a kezelést megelőzően ezen szándékot jelezzük az érintettnek és amennyiben alkalmazandó, kizárólag hozzájárulása alapján kezeljük.

A jelen szabályzat szerint szolgáltatott információ szolgáltatásakor követjük az elérhető legjobb gyakorlatokat, azonban fenntartjuk magunknak a jogot, hogy nem adunk tájékoztatást az érintettnek, amennyiben:

- Már rendelkezésére áll az információ, és bizonyítani tudjuk az információ korábbi átvételét;
- Az információ szolgáltatása lehetetlennek bizonyul és/vagy aránytalan terhet jelentene;
- Az adatszerzés vagy -közlés szabályait a TKA-ra nézve kötelező uniós vagy tagállami jog kifejezetten tartalmazza és megfelelő intézkedéseket biztosít az érintett jogi érdekének védelmére;
- Amennyiben a személyes adat bizalmas jellegű marad az uniós vagy tagállami jog szerinti szakmai titoktartási szabályoknak megfelelően, ideértve a törvényes titoktartási kötelezettséget.

7.3.1 A MUNKAVÁLLALÓ SZEMÉLYES ADATA

A GDPR iránymutatás szerint nem használjuk a hozzájárulást a munkavállaló személyes adata megszerzésének vagy kezelésének jogalapjaként. A kapcsolódó szabályzatainkat folyamatosan

frissítjük annak biztosítására, hogy munkavállalóink megkapják a megfelelő információkat és tisztában legyenek azzal, hogyan és miért kezeljük adataikat.

7.4 A HOZZÁFÉRÉSHEZ VALÓ JOG

Megfelelő intézkedéseket biztosítunk annak érdekében, hogy az érintettek adatkezelése a GDPR 13 és 14. cikkek szerinti információ szolgáltatás és a 15- 22 és 34 cikkek (*együttesen: az Érintettek Jogai*) szerint történő kommunikáció során tömören, átláthatóan, érthetően és könnyen hozzáférhető formában, tiszta és egyértelmű nyelvezettel ellátva kerüljön kibocsátásra. Ezen információt díjmentesen, írásban, vagy más, az érintett által engedélyezett formában, az érintett azonosításának előzetes ellenőrzése mellett bocsátjuk rendelkezésre (*például szóban vagy elektronikus úton*).

Az érintett számára az információt a lehető leghamarabb, de a kérelem átvételétől számított legfeljebb 30 napos időtartamon belül kell szolgáltatni. Ahol az információ visszakeresése vagy szolgáltatása különösen bonyolult vagy nyomós okból csak késedelmesen teljesíthető, - amennyiben szükséges -, a határidő további két hónappal meghosszabbítható. Azonban ez csak különleges körülmények esetén lehetséges és az érintettet a visszakeresési eljárás alatt fellépő bármely késedelemről vagy a késedelem okáról folyamatosan, írásban tájékoztatni kell.

Azon esetekben, amikor nem felelünk meg az adatszolgáltatási kérésnek, az érintettet tájékoztatni kell 30 napon belül az elutasítás okáról, valamint arról, hogy panaszt nyújthat be a Felügyeleti Szervnek.

A részletes szabályokat a TKA Informatikai szabályzatai tartalmazzák.

7.4.1 AZ ÉRINTETTEK HOZZÁFÉRÉSI KÉRÉSEI

Amennyiben az érintett annak igazolására kér minket, hogy vele kapcsolatban személyes adatát megszereztük vagy kezeljük és hozzáférést kér ezen adatokhoz; az alábbiakról tájékoztatjuk: -

- Az adatkezelés céljai;
- Az érintett személyes adatok kategóriái;
- Azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják;
- Ha az adatot harmadik országbeli címzettekkel, illetve a nemzetközi szervezetekkel közölték vagy fogják közölni, a megfelelő garanciák megjelölése;
- Adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- Az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- A valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- Ha a TKA személyes adatokat nem az érintettől gyűjtötte, 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.

A hozzáférési kérés beérkezést követően átadásra kerül az Adatvédelmi Tisztviselő részére és a kérésről feljegyzés készül. A természetes személyről tárolt adatot ellenőrizzük, továbbá azt, hogy milyen formában kerül tárolásra, kivel közöltük és a hozzáférésre vonatkozó milyen különleges időkeret alkalmazandó.

Az Érintett Hozzáférési Kérését minden esetben 30 napon belül, ingyenesen fel kell dolgozni. Amennyiben a természetes személy kérését elektronikus formátumban teszi meg, az információt a szokásosan használt elektronikus formában szolgáltatjuk, kivéve, amennyiben alternatív formában történő választ kér.

7.5 ADATHORDOZHATÓSÁG

A TKA az érintettre vonatkozó személyes adatot kérésre, könnyen közölhető és olvasható formátumban adja meg. Vállaljuk, hogy teljesítjük az egyének adathordozhatósággal kapcsolatos jogait, biztosítva, hogy minden személyes adat elérhető és tagolt, széles körben használt, és azt olyan géppel olvasható formátumban bocsátjuk az érintettek rendelkezésére, amely lehetővé teszi számukra azt, hogy személyes adatát saját céljaira különböző szolgáltatások során történő használatra megszerezze és újra felhasználja. Ez abban az esetben lehetséges, ha az érintett a személyes adatokat a hozzájárulása alapján bocsátotta rendelkezésre, illetve, ha az adatkezelés szerződés teljesítéséhez szükséges.

Az érintett kérésére - amennyiben a fenti feltételek teljesülnek és technikailag lehetséges -, a személyes adatot közvetlenül továbbítjuk a TKA-tól a kijelölt adatkezelőnek.

Minden információkérés az érintett vagy a kijelölt adatkezelő számára díjmentesen és a kérés beérkezésétől számított 30 napon teljesítendő. Amennyiben bármilyen oknál fogva nem intézkednénk az adathordozhatóságra vonatkozó kéréssel kapcsolatban, 30 napon belül az érintett számára teljes, írásbeli magyarázatot küldünk az elutasítás vagy a késedelem okairól, valamint tájékoztatást a felügyeleti hatóság felé fennálló panasztételi jogról és a jogorvoslati jogról.

Az adathordozhatósághoz való jog alapján fennálló minden továbbítási kérést értékelünk annak szempontjából, hogy az más adat alanyt ne érintsen. Amennyiben a személyes adat az adattovábbítást más adatkezelő számára kérő érintetten kívül más természetes személyeket is érint, ez semmilyen esetben sem érintheti a többi érintett jogait és szabadságát.

7.6 HELYESBÍTÉS ÉS TÖRLÉS

7.6.1 PONTATLAN VAGY NEM TELJES ADAT JAVÍTÁSA

A GDPR 5. cikk (d) pontja értelmében a TKA által őrzött és kezelt minden adatot, amennyiben lehetséges, pontosan és szükség esetén naprakészen kell tartani. Amennyiben pontatlanságot azonosítunk és/vagy az érintett, vagy a közös adatkezelői minőségben lévő másik fél arról tájékoztat minket, hogy az általunk kezelt adat pontatlan, minden észszerű intézkedést megteszünk annak érdekében, hogy a pontatlan személyes adatokat haladéktalanul helyesbítsük.

Az Adatvédelmi Tisztviselő értesítést kap az érintettek kéréséről személyes adataik frissítése céljából és felelős a kapott információ érvényesítéséért - és amennyiben jelzésre került -, a hibák kijavításáért. A kezelt adat az érintett utasítása szerint kerül módosításra a nyilvántartás ellenőrzése mellett, biztosítva azt, hogy az érintettre vonatkozó minden adat – amennyiben az nem teljes vagy nem pontos - frissítésre kerül. Frissítés esetén adott esetben kiegészítést vagy kiegészítő nyilatkozatot teszünk.

Amennyiben az érintett tájékoztatása szerint az adat nem pontos, a hibát 30 napon belül kijavítjuk és – amennyiben a kérdéses személyes adatot továbbítottuk - az érintett harmadik felet értesítjük a javításról. Az érintettet a javításról írásban tájékoztatjuk és adott esetben azon harmadik fél személyéről is tájékoztatjuk, aki számára az adat átadásra került.

Amennyiben bármilyen oknál fogva nem intézkednénk a javításra és/vagy kiegészítésre vonatkozó kéréssel kapcsolatban, 30 napon belül az érintett számára teljes, írásbeli magyarázatot küldünk, valamint tájékoztatást a felügyeleti hatóság felé fennálló panasztételi jogról és a jogorvoslati jogról.

7.6.2 TÖRLÉSHEZ VALÓ JOG

Az "Elfeledtetéshez való jog" -ként is ismert jog alapján, a TKA teljes mértékben megfelel a GDPR 5. cikk (e) pontjának és biztosítja, hogy az érintett azonosítására szolgáló személyes adat csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig kerül tárolásra. Vagy egy törlési időpont kerül meghatározásra vagy folyamatosan figyelemmel kísérjük annak érdekében, hogy azt - amennyiben az továbbiakban már nem szükséges -, azonnal megsemmisítsük.

Ezen intézkedések lehetővé teszik az érintettek törlésre vonatkozó kérelmének való megfelelést, mivel - amennyiben már nem áll fenn kényszerítő ok a folyamatos adatkezelésre - a természetes személy kérheti a személyes adat törlését vagy eltávolítását. Habár az alapvető eljárásaink már törlik az adatokat, amennyiben azok a továbbiakban már nem szükségesek, mégis rögzített eljárást követünk a törlési kérelmek tekintetében annak biztosítására, hogy minden fennálló jognak megfeleljünk és semmilyen adatot ne tároljunk tovább, mint az szükséges.

Amennyiben törlésre és/vagy személyes adatok eltávolítására vonatkozó kérést kapunk az érintettől, a következő eljárást követjük: -

1. A kérést kiosztjuk az Adatvédelmi Tisztviselőnek és feljegyezzük.
2. Az Adatvédelmi Tisztviselő az érintettre vonatkozó minden személyes adatot beazonosít és ellenőrzi, hogy az még mindig kezelés alatt áll-e és még mindig szükséges-e kezelése, továbbá megfelelő a kezelés jogalapja és az eredeti szándékolt cél továbbra is fennáll-e.
3. A kérést áttekinti, hogy megbizonyosodjon arról, hogy a kérés megfelel-e az alábbi egy vagy több törlési oknak: -
    a. a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
    b. az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
    c. az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
    d. a személyes adatokat jogellenesen kezelték;
    e. a személyes adatokat jogi kötelezettség teljesítéséhez törölni kell;
    f. a személyes adatok gyűjtésére gyermekek számára az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor;
4. Amennyiben a törlésre vonatkozó kérésnek a fentiek közül legalább egy jogi alapja fennáll, a kérés megérkezését követő 30 napon belül a törlés teljesítésre kerül.
5. Az Adatvédelmi Tisztviselő írásban értesíti az érintettet, hogy a törléshez való jogot biztosítja és részleteket szolgáltat a törölt adatról és a törlés időpontjáról, vagy amennyiben nem lehetséges a törlés, annak okáról.

6. Amennyiben a TKA bármely személyes adatot közzétett és a törléshez való jog biztosításra került, minden ésszerű lépést és intézkedést megteszünk a nyilvános hivatkozások, linkek és adat másolatok eltávolítása érdekében, továbbá kapcsolatba lépünk az érintett adatkezelőkkel és/vagy adatfeldolgozókkal és tájékoztatjuk őket az érintettek személyes adatok törlésére vonatkozó kéréséről.

Amennyiben bármilyen oknál fogva nem intézkednénk a javításra és/vagy kiegészítésre vonatkozó kéréssel kapcsolatban, 30 napon belül, az érintett számára teljes, írásbeli magyarázatot küldünk, valamint tájékoztatást a felügyeleti hatóság felé fennálló panasztételi jogról és a jogorvoslati jogról. ***Ezen adat törlésre vonatkozó visszautasítás az alábbi tájékoztatásokat tartalmazza: -***

- A véleménynyilvánítás szabadságáról és a tájékozódáshoz való jog gyakorlásáról.
- Szerződéses vagy jogszabályi kötelezettség keretében végzett feladat végrehajtásáról.
- Jogi igények előterjesztéséről, érvényesítéséről, illetve védelméről.

7.7 AZ ADATKEZELÉS KORLÁTOZÁSÁHOZ VALÓ JOG

Meghatározott körülmények fennállása esetén a TKA a személyes adat kezelését annak érdekében korlátozza, hogy az érintett kérésére vonatkozó jogi követelményt érvényesítse, igazolja vagy annak megfeleljen. A korlátozás alatt álló adat eltávolításra kerül a normális információáramlás köréből és az információs audit körében korlátozás alatt állóként kerül nyilvántartásra. Az érintettel kapcsolatos, korlátozás alatt álló adatra vonatkozó bármely beszámoló és/vagy rendszer frissítésre kerül, és a használókat tájékoztatjuk a korlátozással kapcsolatos kategóriáról és az okokról. Ahol az adatkezelés korlátozottá válik, tárolásra kerül és nem kezelhető bármilyen formában.

A TKA az adatkezelés korlátozására vonatkozóan az alábbi körülményeket vizsgálja: -

- Amennyiben az érintett vitatja a személyes adatok pontosságát, és ellenőrizzük a személyes adatok pontosságát és/vagy helyesbítését.
- Amennyiben az érintett ellenzi az adatok törlését (*ahol az a közérdek céljára vagy jogi érdek céljának teljesítésére szükséges volt)*, és azt vizsgáljuk, hogy jogos indokaink elsőbbséget élveznek-e az érintett jogos indokaival szemben.
- Ha az adatkezelés jogellenes, az érintett az adatok törlése helyett azok felhasználásának korlátozását kérheti.
- Amennyiben az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, az érintett igényelheti azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez.

Az Adatvédelmi Tisztviselő áttekinti és engedélyezi a korlátozásra vonatkozó kéréseket és intézkedéseket, valamint tárolja az érintettektől, vagy a megfelelő harmadik felektől származó, illetve a nekik küldött értesítések másolatait. Amennyiben az adat korlátozott és ezen adatot harmadik féllel közöltük, a harmadik felet tájékoztatjuk az érvényben lévő korlátozásról és annak okáról, valamint a korlátozás felfüggesztéséről.

Az adatkorlátozást kérő érintetteket a korlátozás alkalmazását követő 30 napon belül tájékoztatjuk, továbbá tájékoztatást adunk bármely olyan harmadik félről is, akivel az adatot közöltük. Az érintett számára szintén írásban megküldünk bármely olyan határozatot, amely az adatkezelés korlátozásának felfüggesztésére vonatkozik. Amennyiben bármilyen oknál fogva nem intézkednénk a korlátozásra vonatkozó kéréssel kapcsolatban, 30 napon belül az érintett számára írásbeli magyarázatot küldünk, valamint tájékoztatjuk a felügyeleti hatóság felé fennálló panasztételi jogról és a jogorvoslati jogról.

7.8 TILTAKOZÁSOK ÉS AUTOMATIZÁLT DÖNTÉSHOZATAL

Az érintetteket az első kapcsolatfelvétel alkalmával az Adatvédelmi Nyilatkozatban a többi információtól elkülönítve, tiszta és olvasható formában tájékoztatjuk az adatkezelésre vonatkozó tiltakozási jogukról. ***A természetes személyek jogában áll tiltakozni: -***

- Amennyiben az adatkezelés létfontosságú érdekek védelme miatt szükséges, közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (*ideértve a profilozást is*);

- Közvetlen üzletszerzés esetén (*ideértve a profilozást is*);
- Amennyiben az adatkezelés tudományos/történelmi kutatás és statisztika céljára történik.

Amikor a TKA a személyes adatokat jogi kötelezettség teljesítése céljából jogos érdekkel kapcsolatban vagy tudományos célra kezeli, az érintett tiltakozása csak olyan esetben vehető figyelembe, ha az a „*saját helyzetével kapcsolatos okokból"* történik. Fenntartjuk a jogot ezen személyes adat további kezelésére az alábbi esetekben:

- Ha tudjuk bizonyítani, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben;

- Ha az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódik.

Amennyiben az érintett a személyes adat kezelése ellen érvényes okok alapján tiltakozik, a TKA abbahagyja arra a célra végzett adatkezelést és az érintettet erről írásban, a kifogás beérkezésétől számított 30 napon belül értesíti.

Rendszer auditot végeztünk az emberi beavatkozást nem igénylő automatizált döntéshozatali eljárások azonosítására. Ezen ugyanazon elem céljára, az implementálás előtt új rendszereket és technológiákat is értékelünk. A TKA figyelembe veszi, hogy az emberi interakciótól mentes döntések elfogultak lehetnek a természetes személyekkel kapcsolatban, és a GDPR 9. és 22. cikke alapján célunk olyan intézkedéseket tenni, amelyek az érintettek számára adott esetben garanciákat biztosítanak. Adatvédelmi Nyilatkozataink útján az első kapcsolatfelvétel során és honlapunkon tájékoztatjuk az érintetteket jogaikról, hogy ne terjedjen ki rájuk az olyan döntés hatálya, amely: -

- Kizárólag automatizált adatkezelésen alapul,
- Amely rájuk nézve joghatással járna vagy őket hasonlóképpen jelentős mértékben érintené.

Korlátozott körülmények között a TKA az automatizált döntéshozatali eljárásokat a jogszabályoknak megfelelően használja. ***Ezen esetek az alábbiak:***

- Amennyiben az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges,

- Amennyiben meghozatalát jogszabály teszi lehetővé (*például csalás vagy adókijátszás megelőzése*),

- Amennyiben az érintett kifejezett hozzájárulásán alapul,
- Amennyiben a döntésnek rá nézve nincs joghatása vagy az őt jelentős mértékben nem érinti.

Amennyiben a TKA automatizált döntéshozatali eljárást alkalmaz, erről mindig értesítjük az érintettet és tájékoztatjuk jogairól. Biztosítjuk továbbá, hogy az érintettek kérhetik az emberi beavatkozást, kifejezhetik véleményüket, kérhetik a döntés magyarázatát, és azt kifogásolhatják is.

8 FELÜGYELETI ELJÁRÁSOK

8.1 BIZTONSÁG ÉS ADATSÉRTÉS KEZELÉSE

Az adatok védelmével kapcsolatos "Beépített Adatkezelés" értelmében a kezelt adat legmagasabb szintű biztonságát vállaljuk, ideértve elsősorban a megosztás, közlés és továbbítás során történő biztonságot. ***Informatikai (Információbiztonsági) Szabályzatunk*** részletes intézkedéseket és ellenőrzési mechanizmusokat tartalmaz a személyes adatok védelmével és azok biztonságának biztosításával kapcsolatban, a beleegyezés megszerzésétől a törlésig.

Ellenőrzési tevékenységet végzünk annak biztosítására, hogy az általunk tárolt és kezelt személyes adatok kiszámíthatók és nyilvántarthatók legyenek, amellett, hogy az érintettekre vonatkozó adatsértés hatályával és hatásával kapcsolatban kockázatértékelést is végzünk. Megfelelő technikai és szervezeti intézkedéseket alkalmazunk a kockázatnak megfelelő biztonsági szint biztosítására.

Amellett, hogy minden intézkedést megteszünk az adatsértések kockázatainak csökkentésére, a TKA – a Felügyeleti Hatóság és az érintetteknek történő értesítés megadása mellett (amennyiben alkalmazandó) – kifejezett ellenőrzési és eljárási mechanizmusokat fejlesztett ki az ilyen helyzetek kezelésére.

8.2 JELSZAVAK

A jelszavak használata a TKA védelmi stratégiájának központi eleme, és a szervezeten belül mindenhol használjuk az információk védelme és a rendszerekhez történő hozzáférés korlátozása céljából. Több szintű megközelítést alkalmazunk, amely magában foglalja a felhasználói, management, eszköz, rendszer és hálózati szintű jelszavakat az átfogó és mindenre kiterjedő megközelítés jegyében.

A jelszavak magas szintű védelmet biztosítanak a forrásokhoz és adatokhoz való hozzáférés vonatkozásában; valamint használatuk kötelező követelmény minden, egy vagy több fiókért vagy rendszerért felelős, illetve olyan munkavállaló és/vagy harmadik fél számára, aki hozzáfér a jelszót igénylő forráshoz.

A jelszavakkal kapcsolatos részletes szabályokról a TKA Informatikai szabályzata rendelkezik.

8.3 KORLÁTOZOTT HOZZÁFÉRÉS

A TKA esetenként és saját belátása szerint jogosult minden vagy egy-egy fájlt biztonságos számítógépes hálózatra helyezni, korlátozott hozzáférést biztosítva minden/bizonyos személyi adatokhoz. Ahol ez alkalmazásra kerül, a személyes adatokhoz történő hozzáférés kizárólag azon személy/szervezeti egység részére megengedett, akinek ezen adathoz történő hozzáféréshez és használathoz különleges és törvényes célja van.

A TKA nem engedélyezi, hogy a tárgyaló szobákban, vagy látható formában, például nem zárolt számítógépes kijelzőkön vagy fax gépeken, nyomtatókon stb. személyes adatot felügyelet nélkül hagyjanak. Az épületen belül mindenhol biztonságosan ellenőrzött, korlátozott hozzáférés van azon területekhez, ahol személyes adat kerül tárolásra (mind elektronikusan, mind fizikailag). Kizárólag az adatok hozzáférésére vagy területek biztosítására feljogosított alkalmazott jogosult ezen területeken tartózkodni. Minden, személyes és bizalmas adatot fizikailag tartalmazó másolatot biztonságosan kell tárolni.

8.4 SZEMÉLYAZONOSÍTÓ OKMÁNYOK ÉS VÉGZETTSÉGET IGAZOLÓ DOKUMENTUMOK ELLENŐRZÉSE

A TKA biztosítja, hogy a munkavállalói személyazonosító okmányokról és végzettséget igazoló dokumentumokról másolati példányt semmilyen esetben nem készít, szükség esetén azokat az irodában, az érintett munkavállaló jelenlétében ellenőrzi, és haladéktalanul visszaadja a munkavállalónak.

Nem munkavállaló természetes személy esetében a következő két feltétel **együttes** fennállása esetén van lehetőség bekérni a személyazonosító okmány és/vagy a végzettséget igazoló dokumentum másolatát:

- a dokumentum bekérése az adatkezeléshez feltétlenül szükséges;
- egyáltalán nincs lehetőség a dokumentum helyszínen, az érintett személy jelenlétében történő ellenőrzésére.

A TKA adatkezelési nyilvántartásában határozza meg azokat az adatkezelési eseteket, amikor ezen dokumentumok bekérése szükségszerű.

9 ADATTOVÁBBÍTÁSOK ÉS ADATMEGOSZTÁS

A TKA arányos és hatékony intézkedéseket tesz az általa mindenkor őrzött és kezelt személyes adat védelme érdekében, és ismerve a személyes adatok közlésének és továbbításának magas kockázati jellegét, a továbbítandó adat védelmének és biztonságának még magasabb szintű elsőbbséget biztosítunk. A Magyarországon és az Európai Unión belül történő adattovábbítások kevésbé jelentenek kockázatot, mintha az a harmadik országok vagy nemzetközi szervezetek felé történne, mivel a GDPR lefedi az EU (és EGT) tagállamok számára alkalmazandó szabályokat.

A továbbítás jóváhagyott, biztonságos módját használjuk és kijelölt kapcsolattartóink vannak minden olyan tagállami vagy harmadik országbeli szervezetnél, amelyekkel együtt dolgozunk. Minden továbbított adat feljegyzésre kerül a nyilvántartásunkban annak érdekében, hogy a nyomon követés könnyen elérhető és a felhatalmazás hozzáférhető legyen. Az Adatvédelmi Tisztviselő minden adattovábbítás esetében felhatalmazást ad és a biztonsági módszereket és eszközöket igazolja.

Amennyiben a személyes adatok továbbítása olyan harmadik országok és nemzetközi szervezetek részére történik, ahol az Európai Bizottság megállapította, hogy a harmadik ország vagy a nemzetközi szervezet megfelelő védelmi szintet biztosít, ezen adattovábbítások áttekintésre kerülnek az Adatvédelmi Tisztviselő által és ugyanazon eljárást alkalmazzuk, mint az EU-n belüli adattovábbítás esetében. Az Adatvédelmi Tisztviselő felelős az Európai Bizottság által átadott, jóváhagyott harmadik országok listájának figyelemmel kíséréséért és kizárólag a jelen bekezdés szerint továbbít adatokat az ott megjelölt országokba, szervezetek vagy ágazatok számára.

9.1 ADATTOVÁBBÍTÁSI KIVÉTELEK

A TKA nem továbbít személyes adatot bármely harmadik ország vagy nemzetközi szervezet részére anélkül, hogy az Európai Bizottság vagy a Felügyeleti Hatóság engedélye és a megfelelő garanciák ne állnának rendelkezésére. ***A továbbításnak az alábbi feltételek közül legalább egynek kell megfelelnie:*** **-**

- az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;

- az adattovábbítás az érintett és a TKA közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
- az adattovábbítás a TKA és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
- az adattovábbítás fontos közérdekből szükséges;
- az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
- az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
- a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, *(és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető),* de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek. Az e kivétel szerinti adattovábbítás nem érintheti a nyilvántartásban szereplő személyes adatok vagy személyes adatok kategóriáinak összességét. Ha a nyilvántartásba kizárólag olyan személyek tekinthetnek be, akiknek ehhez jogos érdeke fűződik, az adattovábbításra kizárólag e személyek kérelmére kerülhet sor, illetve abban az esetben, ha ők a címzettek.

Amennyiben az adattovábbítás nem alapulhat a GDPR 45. cikk és 46. cikk rendelkezésein és a fenti eltérések nem alkalmazandók, a TKA megfelel a 49. cikk szerinti rendelkezésnek, miszerint az adat továbbítható harmadik ország vagy nemzetközi szervezet részére, amennyiben minden alábbi feltétel alkalmazandó. ***Az adattovábbítás:***

- nem teljesíthető közhatalmi jogkörében eljáró közhatalmi szerv által,
- nem ismétlődő,
- csak korlátozott számú érintettre vonatkozik,
- a TKA olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, és
- a TKA az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében

Amennyiben a fentiek szerint adatot kell továbbítani jogi és/vagy kényszerítő erejű jogos indokok alapján, a továbbítás előtt a felügyeleti hatóságot tájékoztatni kell az adattovábbításról és a megfelelő garanciákról. Az adatkezelő a GDPR 13. és a 14. cikkben említett információk nyújtásán kívül az érintettet tájékoztatja az adattovábbításról, az adattovábbítást érintő használt garanciákról, valamint az adatkezelő kényszerítő erejű jogos érdekéről.

10 AUDIT ÉS MONITORING

A jelen szabályzat és eljárási dokumentum részletezi a TKA által a személyes adatok védelme, az érintettek jogainak fenntartása, kockázatenyhítés, adatsértések csökkentése és a GDPR és kapcsolódó jogszabályoknak és magatartási kódexeknek történő megfelelés érdekében használt kiterjedt ellenőrzési módszereket és mechanizmusokat.

Az Adatvédelmi Tisztviselő teljes körű felelősséggel rendelkezik az érvényben lévő eljárások, eszközök és ellenőrzési mechanizmusok értékelésével, tesztelésével, áttekintésével és javításával, és adott esetben a kuratórium, valamint a főigazgató számára történő javítási akció tervekkel összefüggő jelentéstétellel

kapcsolatban. Az adat csökkentési módszereket gyakran áttekintjük és az új technológiákat - az adatok és az egyének védelme érdekében - legjobb tudomásunk szerint értékeljük.

Az Adatvédelmi Tisztviselő nyilvántartja a felülvizsgálati, audit és folyamatos monitoring eljárásokat és a másolatokat a kuratórium, valamint a főigazgató számára megküldi, valamint kérésre a Felügyeleti Hatóság rendelkezésére bocsátja.

A belső adatvédelmi auditok céljai, hogy:

- Megfelelő szabályzatok és eljárások legyenek érvényben;
- Annak igazolása, hogy a szabályzatok és eljárások követésre kerülnek;
- Az érvényben lévő intézkedések és ellenőrzési mechanizmusok megfelelőségének és hatékonyságának tesztelése;
- A megfelelőséggel kapcsolatos jogsértések vagy potenciális jogsértések azonosítása;
- A kockázatok azonosítása és az érvényben lévő enyhítő eszközök értékelése a kockázatok csökkentése érdekében;
- Megoldásokkal és akció tervekkel kapcsolatos javaslattétel a kuratórium, valamint a főigazgató felé az érintettek védelme és személyes adatainak biztosítására vonatkozó javítások céljából;
- A GDPR-nak történő megfelelés figyelemmel kísérése, valamint a legjobb gyakorlatok bemutatása.

11 OKTATÁS

Erős elkötelezettségünk és szigorú ellenőrzési mechanizmusunk által biztosítjuk, hogy minden munkavállalónk tisztában van a GDPR szabályokkal és elvekkel, azokhoz hozzáféréssel rendelkezik és folyamatos oktatásban, támogatásban és értékelésben részesül. A következő eszközökkel támogatjuk munkavállalóinkat:

- GDPR Workshopok és Képzési Tanfolyamok;
- Értékelő Tesztek;
- Szövegek és emlékeztető anyagok;
- A GDPR szabályokhoz, eljárásokhoz, ellenőrző listákhoz és kapcsolódó anyagokhoz történő hozzáférés.

A munkavállalókat folyamatosan támogatjuk és oktatjuk a GDPR követelményekről és az adatvédelemmel kapcsolatos saját céljainkról és kötelezettségeinkről.

12 BÍRSÁGOK

A TKA tisztában van a GDPR és Felügyeleti Hatóság által támasztott kötelezettségeinkkel és felelősségünkkel és tudomással bír a Rendelet alapján fennálló adatsértések komolyságáról.

Tiszteletben tartjuk a Felügyeleti Hatóság jogszabály erejénél fogva történő felhatalmazását bírság kiszabására és kikényszerítésére a rendelkezések megsértése, a kockázatok csökkentésének elmulasztása és a tudatosan folytatott nem megfelelő működés esetén.

Munkavállalóink tudomással bírnak a bírságok komolyságáról és azoknak a jogsértéssel történő arányosságáról. ***Tisztában vagyunk azzal, hogy:***

- Az adatkezelő, az adatfeldolgozó, a tanúsító szervezet és az ellenőrző szervezet legfeljebb 10 000 000 EUR összegű bírsággal, vagy az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-át kitevő összeggel sújtható; azzal, hogy a kettő közül a magasabb összeg alkalmazandó.
- Az adatkezelés elveinek, a hozzájárulás feltételeinek, az érintettek jogainak, a személyes adatoknak harmadik országbeli címzett vagy nemzetközi szervezet részére történő továbbítása megsértése, különleges adatkezelési esetek (*IX. Fejezet*) és a felügyeleti hatóság utasításának be nem tartása esetén legfeljebb 20 000 000 EUR összegű bírsággal, illetve az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeggel sújtható, azzal, hogy a kettő közül a magasabb összeg alkalmazandó.

13 FELELŐSSÉGEK

A TKA a GDPR 37. cikk alapján adatvédelmi tisztviselőt köteles kinevezni, mivel közfeladatot ellátó szerv.

Az adatvédelmi tisztviselő neve és elérhetősége:

név: dr. Ugrai Gábor

elérhetőség: gabor.ugrai@tpf.hu és adatvedelem@tpf.hu

Az Adatvédelmi Tisztviselő feladata a személyes adatok védelmével kapcsolatos kockázatok azonosítása és csökkentése, tájékoztatás, valamint szakmai tanácsadás az adatkezelést végző munkavállalók és a kuratórium, valamint a főigazgató részére, továbbá az az adatvédelmi jogszabályok naprakész ismerete. Az Adatvédelmi Tisztviselő együttműködik a HR és IT munkatársakkal annak biztosítására, hogy a munkavállalók minden eljárás, rendszer alkalmazásakor és egyéb tevékenységeik során betartják a GDPR szabályait.

Az Adatvédelmi Tisztviselő teljes mértékben felelős az átvilágítás, adatvédelmi hatásvizsgálatok, kockázatértékelések és az olyan esetekben történő adat továbbításokért, ahol személyes adat érintett, valamint köteles megfelelő és hatékony nyilvántartást vezetni és a kuratórium, valamint a főigazgató felé - a GDPR-nak és saját belső célkitűzéseinknek és kötelezettségeinknek megfelelően - beszámolni.

A személyes vagy különleges kategóriájú adatot kezelő és feldolgozó munkavállalók számára kiterjedt adatvédelmi képzést kell tartani annak biztosítására, hogy a munkavállalók szakképzettek és hozzáértők legyenek az általuk végzett pozíció ellátására.

14. ADATVÉDELMI INCIDENS

Az adatvédelmi incidens kategorizálása:

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

súlyos incidens: olyan incidens (pl. adatvesztés, adatsérülés), mely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl.: a jogosulatlan hozzáféréssel érintett adatok esete; az olyan adatsérülés, adatvesztés, amelynél az adatok naplózott állományból nem

állíthatóak helyre). Magas kockázatúnak minősül az az eset, amely fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, pl. az érintetteknek a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, pénzügyi veszteséget, jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok integritásának, illetve bizalmas jellegének sérülését eredményezheti,

- **enyhe incidens**: minden incidens, amely nem tartozik a súlyos incidens fogalma alá (pl. átmeneti szolgáltatásleállás, -kiesés az Adatkezelő munkavállalói által használt olyan belső rendszerekben, amely nem jár adatsérüléssel vagy adatvesztéssel).

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

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

Az adatvédelmi incidens bejelentése

Az Adatkezelő irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező azon természetes személy (a munkavégzésre irányuló jogviszony jellegétől függetlenül), aki az Adatkezelő által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy az Adatkezelő szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban adatvédelmi incidenst vagy annak gyanúját észleli, köteles azt haladéktalanul bejelenteni a jogi igazgatóságnak, továbbá az adatvédelmi tisztviselőnek (gabor.ugrai@tpf.hu vagy az adatvedelem@tpf.hu e-mail címen)

Amennyiben az adatvédelmi incidens bejelentése szóban (telefonon vagy személyesen) történik (beleértve az Adatkezelő telefonos elérhetőségein tett közérdekű bejelentéseket is), azt a szóbeli közlést követő legfeljebb 1 napon belül írásban is meg kell erősíteni. Ilyen esetben a szóbeli közlés időpontját külön fel kell tüntetni.

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

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

Az adatvédelmi incidens kivizsgálása

Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozókra egyaránt) felmerülése esetén az Adatkezelő adatvédelmi tisztviselője, a főigazgató, a jogi és operatív igazgatóság és az informatikai szakterület, továbbá szükség esetén az adott szakterületért felelős szervezeti egység kijelölt munkatársának (a továbbiakban együtt: incidensvizsgáló bizottság) közreműködésével megvizsgálja, és kategorizálja a bekövetkezett incidenst és meghatározza az esetleges elhárítás érdekében szükséges további intézkedéseket. A bejelentőt – szükség esetén – további információk közlésére kell felkérni. Az incidensvizsgáló bizottságot az főigazgató hívja össze, az említett személyeknek szükség esetén munkaidőn kívül is rendelkezésre kell állniuk. Az incidensvizsgáló bizottság munkáját a főigazgató koordinálja, és képviseli az Adatkezelő egyéb szervezeti egységei felé.

Az incidensvizsgáló bizottság üléseiről emlékeztetőt, döntéseiről indoklást is tartalmazó jegyzőkönyvet, vizsgálatairól pedig intézkedési javaslatokat is tartalmazó jelentést kell készíteni. Az incidensvizsgáló bizottság munkáját tartalmazó dokumentumok kezelésére a Adatkezelő mindenkori iratkezelési szabályai az irányadók. Az incidensvizsgáló bizottság korlátozhatja a munkájáról szóló dokumentumokba betekintők körét.

A bejelentés előzetes megvizsgálása során az alábbi szempontokat kell figyelembe venni:

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

Ha a bejelentés előzetes megvizsgálása azzal az eredménnyel jár, hogy az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) esemény nem érintett személyes adatokat, akkor a vizsgálatot az Adatkezelő mindenkor hatályos Informatikai Biztonsági Szabályzatában foglaltak szerint jár el. Az incidensvizsgáló bizottság – a jogi és operatív igazgatóság útján – legkésőbb az incidens bejelentés vagy az incidensről való tudomásszerzés közül a korábbi időpontot követő 1 munkanapon belül tájékoztatja a következő személyeket az előzetes vizsgálat eredményéről, a GDPR 33. cikkében írt hatósági bejelentés szükségességéről, az érintettek tájékoztatásának szükségességéről és módjáról, valamint arról, hogy szükséges-e az incidens részletes vizsgálata:

- az Adatkezelő főigazgatóját;

- a jogi és operatív igazgatót;

- informatikai rendszert is érintő incidens esetén az informatikai szakterület vezetőjét;

- a szakmailag illetékes szervezeti egység vezetőjét;

Az incidensvizsgáló bizottság javaslata alapján a főigazgató legkésőbb a bizottság javaslatának kézhezvételét követő 1 munkanapon belül dönt a GDPR 33. cikkében írt adatvédelmi felügyeleti hatósági bejelentés szükségességéről. A főigazgató döntéséről a jogi és operatív igazgatóság értesíti az egyéb személyeket is.

Az adatvédelmi incidens részletes vizsgálatának szükségességéről az incidensvizsgáló bizottság dönt. A részletes vizsgálatot a vizsgálat megkezdése után a lehető leghamarabb le kell zárni.

A vizsgálat során elsősorban az alábbi módszerek alkalmazhatóak:

- személyes megbeszélés az adatvédelmi incidenst észlelő személyekkel, valamint az érintett szervezeti egységek munkatársaival és vezetőivel,

- írásbeli tájékoztatás kérése az érintett szervezeti egységektől,

- dokumentumok vizsgálata,

- informatikai rendszerek, hálózatok és eszközök vizsgálata, beleértve a naplóállományok vizsgálatát is.

Amennyiben az incidensvizsgáló bizottság a részletes vizsgálat során úgy ítéli meg, hogy azonnali intézkedések szükségesek annak biztosítására, hogy az adatvédelmi incidenssel azonos probléma forrásból eredő incidens a jövőben ne valósuljon meg, úgy a szükséges intézkedések megtétele érdekében haladéktalanul tájékoztatja az érintett szervezeti egységek vezetőit.

Az incidensvizsgáló bizottság a részletes vizsgálat megállapításairól, illetve a javasolt intézkedésekről a részletes vizsgálat befejezését követő 2 munkanapon belül vizsgálati jelentést készít. A vizsgálati jelentés tartalmazza az adatvédelmi incidens elhárításához és további incidens megelőzéséhez szükséges intézkedésekre vonatkozó, az illetékes vezető részére tett javaslatot is.

A jelentés alapján a vizsgálatban érintett szervezeti egységek vezetői 15 napon belül a megvalósításhoz szükséges határidőre tett javaslatot is tartalmazó intézkedési tervet készítenek és azt megküldik az jogi és operatív igazgatóság útján az incidensvizsgáló bizottságnak.

Az intézkedési tervet és a megvalósításhoz szükséges határidőt tartalmazó szakterületi javaslatot az incidensvizsgáló bizottság a kézhezvételtől számított 3 munkanapon belül véleményezi, majd jóváhagyásra megküldi a főigazgató részére.

Az adatvédelmi incidens elhárítása és a további incidensek megelőzése céljából megvalósított egyes intézkedésekről az incidenssel érintett szervezeti egység vezetője tájékoztatást küld az adatvédelmi tisztviselő és a jogi és operatív igazgatóság részére.

A jogi és operatív igazgatóság az intézkedési tervben foglaltak végrehajtásáról, az összes intézkedés befejezését követő 3 munkanapon belül tájékoztatást küld a főigazgató részére.

Az érintett(ek) tájékoztatása a súlyos adatvédelmi incidensről

Súlyos adatvédelmi incidens esetén az Adatkezelő – az érintettel, érintettekkel kapcsolatban rendelkezésére álló elérhetőségeken, ennek hiányában vagy amennyiben az ily módon történő tájékoztatás aránytalan terhet jelentene (GDPR 34. cikk) az Adatkezelő honlapján közzétett közlemény útján – indokolatlan késedelem nélkül tájékoztatja az érintettet (érintetteket) az adatvédelmi incidensről. Az érintett(ek) tájékoztatásának módjára az incidensvizsgáló bizottság javaslatot tesz. Az érintettek tájékoztatását – az érintett szervezeti egységek bevonásával – a jogi és operatív igazgatóság koordinálja az adatvédelmi tisztviselő közreműködésével.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat és intézkedéseket:

- Az adatvédelmi tisztviselő és a jogi és operatív igazgatóság vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

- az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintettet nem kell tájékoztatni, amennyiben az incidens nem jár magas kockázattal, és a következő feltételek bármelyike teljesül:

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

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

<u>Az adatvédelmi incidens bejelentése a Hatóságnak</u>

Az adatvédelmi incidensről szóló bejelentést a Hatóság mindenkori kapcsolati pontjára kell eljuttatni.

A bejelentés összeállításának és beadásának felelőse az adatvédelmi tisztviselő. Az adatvédelmi incidensről szóló bejelentéshez szükséges információkat az adatvédelmi tisztviselő, valamint a jogi és operatív igazgatóság rendelkezésére kell bocsátani.

Az adatvédelmi incidensről szóló bejelentésben legalább:

- 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 az adatvédelmi tisztviselő, a jogi és operatív igazgatóság vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

- ismertetni kell az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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

Az adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidensekről az adatvédelmi tisztviselő nyilvántartást vezet. E szabályzat nem érinti az egyéb jogszabályok szerint a biztonsági események kezelésével kapcsolatban vezetendő nyilvántartásokra vonatkozó szabályok alkalmazását.

A nyilvántartásban rögzíteni kell:

- az incidensben érintett személyes adatok körét; és számát,

- az adatvédelmi incidenssel érintettek körét, és számát,

- az adatvédelmi incidens tudomásszerzés időpontját,

- az adatvédelmi incidens körülményeit, hatásait,

- az adatvédelmi incidens elhárítására megtett intézkedéseket,

- az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

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

15. JOGORVOSLATI LEHETŐSÉG

Név: Nemzeti Adatvédelmi és Információszabadság Hatóság

Székhely: 1055 Budapest Falk Miksa u. 9-11.

Postacím: 1363 Budapest, Pf.: 9.

Webcím: www.naih.hu

Email cím: info@naih.hu

Telefon: +36 (1) 391-1400

Telefax: +36 (1) 391-1410

Jelen szabályzat aláírása napján lép érvénybe és határozatlan ideig érvényes.

Budapest, 2023.

Bodrogi Richárd
Főigazgató