Adatkezelési Szabályzat

Veszprém-Balaton 2023 Zrt.

(a továbbiakban: Adatkezelő vagy Szervezet)

Az általa kezelt személyes adatok vonatkozásában

Adatvédelmi Tisztviselő: dr. Bazsala Judit

Adatkezelő képviselője: Markovits Aliz ügyvezető igazgató

Tartalomjegyzék

1. Preambulum 4
2. Általános rendelkezések 6
2.1. A Szabályzat célja és hatálya 6
2.2. Az adatvédelem alapfogalmai 6
3. Személyes adatok kezelésének módszertani szabályai 8
3.1. Személyes adatok kezelésére vonatkozó alapelvek 8
3.2. Személyes adatok kezelésének jogalapja 8
4. A Szervezetnél megvalósuló adatkezelések 9
4.1. A munkaviszony létesítésével, fenntartásával és megszűnésével kapcsolatos adatkezelések 9
4.2. Munkaköri alkalmasság ..... **Hiba! A könyvjelző nem létezik.**
4.3. Személyazonosító igazolványok fénymásolása 10
4.4. Bér- és munkaügyi nyilvántartás 10
4.5. Munkavédelem 11
4.6. Munkára alkalmas állapot munkavédelmi vizsgálata ..... **Hiba! A könyvjelző nem létezik.**
4.7. Munkavállalók céges mobiltelefonjával kapcsolatos adatkezelés 12
4.8. Közösségi oldal működtetésével összefüggő adatkezelés 12
4.9. Marketing-tevékenységgel és elérhetőséggel kapcsolatos adatkezelés 13
5. A Szervezet adatvédelmi rendszere 14
5.1. Az adatvédelem Szervezeten belüli szervezete 14
5.2. Adatbiztonsági szabályok 16
6. Adatvédelmi incidens 17
6.1. Az adatvédelmi incidens fogalma 17
6.2. Az adatvédelmi incidens kezelése 18
6.3. Adatvédelmi incidens nyilvántartása 19
7. Az adatvédelmi hatásvizsgálat, az előzetes konzultáció és az érdekmérlegelés bemutatása 19
7.1. Az adatvédelmi hatásvizsgálat 19
7.2. Előzetes konzultáció 20
7.3. Érdekmérlegelés 20
8. Az érintett jogainak érvényesítése 21
8.1. Átlátható tájékoztatás, kommunikáció és az érintett joggyakorlásának elősegítése 21
8.2. Az érintett hozzáférési joga 22
8.3. A helyesbítéshez való jog 23
8.4. Az adattörléshez való jog 23
8.5. Az adatkezelés korlátozásához való jog 24

8.6. Az adathordozhatósághoz való jog 24
8.7. A tiltakozáshoz való jog 25
8.8. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást 25
8.9. Jogorvoslati jog 26
9. Záró rendelkezések 26
10. MELLÉKLETEK 27

1. PREAMBULUM

A Veszprém-Balaton 2023 Zrt. és kapcsolódó vállalatai (a továbbiakban: Szervezet, Szervezetek) belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi és adatkezelési szabályzatot (a továbbiakban: Szabályzat) alkotja.

Adatkezelő adatai:

Veszprém-Balaton 2023 Zártkörűen Működő Részvénytársaság

Székhelye: Veszprém 8200, Óváros tér 26.

Cégjegyzék száma: 19-10-500277

E-mail: info@veszprembalaton2023.hu

Telefon: 0688 794 028

Adatfeldolgozó adatai:

Molnár és Társa Kft.

Székhely: Balatonfűzfő 8175, Irinyi utca 8. 8/5

Cégjegyzékszám: 19-09-508818

E-mail: molnartsa@freemail.hu

Telefon: 30/431-6373

FourMed Egyészségügyi Szolgáltató Kft.

Székhely: Veszprém 8200, Kabay János utca 2.

Cégjegyzékszám: 19-09-502293

E-mail: fourmed@gmail.com

Telefon: 0688-421-251

CODEBASE Szoftverfejlesztő, Kereskedelmi és Szolgáltató Kft.

Székhely:1037 Budapest, Bokor utca 15. 1. em. 27.

Cégjegyzékszám: 01-09-725607

Adószám: 13246422-2-41

Macrotel Kft.

Székhelye: Veszprém 8200, Gerenda út 4.

Cégjegyzék száma: 19-09-506709

E-mail: pichnerp@marcotel.hu

Telefon:003630/283-8063

Adatkezelési Szabályzat

Veszprém-Balaton 2023 Zrt.

(a továbbiakban: Adatkezelő vagy Szervezet)

Az általa kezelt személyes adatok vonatkozásában

Adatvédelmi Tisztviselő: dr. Bazsala Judit

Adatkezelő képviselője: Markovits Aliz ügyvezető igazgató

Tartalomjegyzék

1. Preambulum 4
2. Általános rendelkezések 6
2.1. A Szabályzat célja és hatálya 6
2.2. Az adatvédelem alapfogalmai 6
3. Személyes adatok kezelésének módszertani szabályai 8
3.1. Személyes adatok kezelésére vonatkozó alapelvek 8
3.2. Személyes adatok kezelésének jogalapja 8
4. A Szervezetnél megvalósuló adatkezelések 9
4.1. A munkaviszony létesítésével, fenntartásával és megszűnésével kapcsolatos adatkezelések 9
4.2. Munkaköri alkalmasság ..... **Hiba! A könyvjelző nem létezik.**
4.3. Személyazonosító igazolványok fénymásolása 10
4.4. Bér- és munkaügyi nyilvántartás 10
4.5. Munkavédelem 11
4.6. Munkára alkalmas állapot munkavédelmi vizsgálata ..... **Hiba! A könyvjelző nem létezik.**
4.7. Munkavállalók céges mobiltelefonjával kapcsolatos adatkezelés 12
4.8. Közösségi oldal működtetésével összefüggő adatkezelés 12
4.9. Marketing-tevékenységgel és elérhetőséggel kapcsolatos adatkezelés 13
5. A Szervezet adatvédelmi rendszere 14
5.1. Az adatvédelem Szervezeten belüli szervezete 14
5.2. Adatbiztonsági szabályok 16
6. Adatvédelmi incidens 17
6.1. Az adatvédelmi incidens fogalma 17
6.2. Az adatvédelmi incidens kezelése 18
6.3. Adatvédelmi incidens nyilvántartása 19
7. Az adatvédelmi hatásvizsgálat, az előzetes konzultáció és az érdekmérlegelés bemutatása 19
7.1. Az adatvédelmi hatásvizsgálat 19
7.2. Előzetes konzultáció 20
7.3. Érdekmérlegelés 20
8. Az érintett jogainak érvényesítése 21
8.1. Átlátható tájékoztatás, kommunikáció és az érintett joggyakorlásának elősegítése 21
8.2. Az érintett hozzáférési joga 22
8.3. A helyesbítéshez való jog 23
8.4. Az adattörléshez való jog 23
8.5. Az adatkezelés korlátozásához való jog 24

8.6. Az adathordozhatósághoz való jog 24
8.7. A tiltakozáshoz való jog 25
8.8. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást 25
8.9. Jogorvoslati jog 26
9. Záró rendelkezések 26
10. MELLÉKLETEK 27

1. PREAMBULUM

A Veszprém-Balaton 2023 Zrt. és kapcsolódó vállalatai (a továbbiakban: Szervezet, Szervezetek) belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi és adatkezelési szabályzatot (a továbbiakban: Szabályzat) alkotja.

Adatkezelő adatai:

Veszprém-Balaton 2023 Zártkörűen Működő Részvénytársaság

Székhelye: Veszprém 8200, Óváros tér 26.

Cégjegyzék száma: 19-10-500277

E-mail: info@veszprembalaton2023.hu

Telefon: 0688 794 028

Adatfeldolgozó adatai:

Molnár és Társa Kft.

Székhely: Balatonfűzfő 8175, Irinyi utca 8. 8/5

Cégjegyzékszám: 19-09-508818

E-mail: molnartsa@freemail.hu

Telefon: 30/431-6373

FourMed Egyészségügyi Szolgáltató Kft.

Székhely: Veszprém 8200, Kabay János utca 2.

Cégjegyzékszám: 19-09-502293

E-mail: fourmed@gmail.com

Telefon: 0688-421-251

CODEBASE Szoftverfejlesztő, Kereskedelmi és Szolgáltató Kft.

Székhely:1037 Budapest, Bokor utca 15. 1. em. 27.

Cégjegyzékszám: 01-09-725607

Adószám: 13246422-2-41

Macrotel Kft.

Székhelye: Veszprém 8200, Gerenda út 4.

Cégjegyzék száma: 19-09-506709

E-mail: pichnerp@marcotel.hu

Telefon:003630/283-8063

Signator Audit Könyvvizsgáló Kft.

Székhelye: Veszprém 8200, Radnóti tér 2

Cégjegyzék száma: 19-09-500315

E-mail: signator@signator.hu

Telefon: 0630/901-2777

Csapó, Kiss és Mohos Ügyvédi Iroda

Székhelye: Veszprém 8200, Ádám Iván u 10.

Telefon: 003630/946-3452

Veszprém-Balaton Régió Kultúrájáért Közalapítvány

Székhely: Veszprém 8200, Óváros tér 9.

Nyilvántartási szám: 19-01-0000227

Jelen rendelkezéseket a Szervezet többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és a bármely más, jelen szabályzat hatálybalépése előtt hatályba lépett szabályzat előírásai között, úgy abban az esetben a jelen Szabályzatban foglalt rendelkezések az irányadók.

Jelen szabályzatban használt rövidítések:

Infotv. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

GDPR az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (Általános Adatvédelmi Rendelet)

Mt. a munka törvénykönyvéről szóló 2012. évi I. törvény

Mvt. a munkavédelemről szóló 1993. évi XCIII. törvény

Ptk. a polgári törvénykönyvről szóló 2013. évi V. törvény

Szvtv. a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény

NAIH vagy Hatóság Nemzeti Adatvédelmi és Információszabadság Hatóság

2. ÁLTALÁNOS RENDELKEZÉSEK

2.1. A Szabályzat célja és hatálya

Jelen Szabályzat célja, hogy a GDPR rendelkezéseivel összhangban szabályozza a Szervezet működése során alkalmazott nyilvántartások vezetését, biztosítsa az adatkezelés és az ezzel összefüggő adatvédelem szabályozásának törvényes rendjét, a személyes adatok védelméhez fűződő információs önrendelkezési jog és az adatbiztonság érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását, jogosulatlan nyilvánosságra hozatalát és bármely jogosulatlan felhasználását.

A Szabályzat személyi hatálya a Szervezet és partnerei tisztviselőire, munkavállalóira, gyakornokaira, szerződéses partnereire, üzletfeleire terjed ki.

A Szabályzat alkalmazásában természetes személynek kell tekinteni az egyéni vállalkozó, egyéni cég, őstermelő ügyfeleket, vevőket és szállítókat is. A Szabályzat hatálya ugyanakkor nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre, illetve amely különösen olyan vállalkozásokra vonatkozik, amelyeket jogi személyként hoztak létre, beleértve a jogi személy nevét és formáját, valamint a jogi személy elérhetőségére vonatkozó adatokat, de ide kell érteni a jogi személy kapcsolattartójának a kapcsolattartáshoz szükséges személyes adatait.

A Szabályzat tárgyi hatálya kiterjed:

- a Szervezetnél keletkezett valamennyi adatra, függetlenül annak megjelenési formájától;
- az informatikai rendszerben kezelt vagy feldolgozott adatra;
- az adatkezelés eredményeképpen létrejött adatra;
- a Szervezetnél alkalmazott valamennyi hardver- és szoftvereszközre, mint adatbiztonsági eszközökre;
- a Szervezet tevékenységével kapcsolatos, működése során keletkező közérdekű adatra vagy közérdekből nyilvános adatra.

2.2. Az adatvédelem alapfogalmai

A jelen Szabályzat fogalmi rendszere megegyezik a GDPR 4. cikkében meghatározott értelmező fogalommagyarázatokkal. Ennek megfelelően a főbb fogalmak:

- „személyes adat": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online

azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

- „adatkezelés": a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
- „az adatkezelés korlátozása": a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
- „profilalkotás": személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;
- „álnevesítés": a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;
- „nyilvántartási rendszer": a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
- „adatkezelő": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
- „adatfeldolgozó": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
- „címzett": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;
- „harmadik fél": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
- „az érintett hozzájárulása": az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
- „adatvédelmi incidens": a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
- „vendég": a Szervezet területén lévő, illetőleg a vele szerződött szolgáltatók által nyújtott szolgáltatásokat igénybe vevő, illetőleg igénybevételi szándékáról nyilatkozatot tett természetes személy, érintett
- „adatgazda": annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.

3. SZEMÉLYES ADATOK KEZELÉSÉNEK MÓDSZERTANI SZABÁLYAI

3.1. Személyes adatok kezelésére vonatkozó alapelvek

Jogszerűség, tisztességes eljárás, átláthatóság

A személyes adatok kezelése csak meghatározott jogalap (hozzájárulás vagy más törvényes jogalap) alapján történhet. A személyes adatokat tisztességesen és az érintett által átlátható módon kell kezelni. Az adatkezeléssel kapcsolatos információkat pontos, átlátható, érthető és könnyen hozzáférhető formában, egyszerű és érthető nyelvezettel kell megadni.

Célhoz kötöttség

A személyes adatok csak meghatározott, egyértelmű és jogszerű célból gyűjthetők. A személyes adatok további kezelése is csak e célokkal összhangban történhet. A célhoz kötöttséggel közvetlenül összefüggő, az adatkezelő és az érintett érdekei közti mérlegelés sok esetben megteremti az adatkezelés jogalapját. Ezért az adatkezelés konkrét célját minden esetben meg kell határozni.

Adattakarékosság

Az adattakarékosság alapelvének értelmében az adatgyűjtés és az adatkezelés azokra az adatokra korlátozandó, amelyek a kívánt cél eléréséhez ténylegesen szükségesek.

Pontosság

Az adatkezelés során igazolható módon biztosítani kell az adatok pontosságát, teljességét és naprakészségét, valamint a pontatlan adatok haladéktalan törlését vagy helyesbítését. A Szervezet által, illetve a Szervezetnél ezen alapelv érvényesülése érdekében a Szervezet köteles a kezelt személyes adatok aktualizálására rutinszerű eljárásokat bevezetni.

Korlátozott tárolhatóság

A személyes adatok érintettek azonosítását lehetővé tevő formában való tárolása az adatkezelés céljának eléréséhez szükséges ideig lehetséges. Továbbá be kell tartani a jogszabályban előírt határidőket is.

Integritás, bizalmi jelleg

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok elégséges biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. Ezért elsősorban IT és szervezeti vonatkozásban (pl.: hozzáférési és jogosultsági eljárásrendek, kódolás) kell megfelelő intézkedéseket foganatosítani, figyelembe véve különösen a GDPR 32. cikkében (az adatkezelés biztonsága) és 35. cikkében (adatvédelmi hatásvizsgálat) foglalt rendelkezéseket.

Elszámolhatóság

Az elszámoltathatóság alapelve a GDPR 5. cikk 2. bekezdése értelmében a Szervezetnek az előzőekben bemutatott alapelveknek való megfelelést tudnia kell dokumentumokkal alátámasztva igazolni.

3.2. Személyes adatok kezelésének jogalapja

A GDPR 6. cikkében foglaltak szerint a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- 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;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

A Szervezet az adatkezelés során az alábbi jogszabályok alapján végzi tevékenységét:

- Magyarország Alaptörvénye
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete 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
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
- 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról,
- 2009. évi CLV. törvény a minősített adat védelméről,
- 2005. évi CXXXIII. törvény a személy és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (Szvt.)
- 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről
- 2016. évi CL. törvény az általános közigazgatási rendtartásról
- 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.)
- 2000. évi C. törvény a számvitelről
- 1997. évi CLV. törvény a fogyasztóvédelemről
- 1995. évi CXVII. törvény a személyi jövedelemadóról
- 1993. évi XCIII. törvény a munkavédelemről (Mvt.)
- 2012. évi I. törvény a munka törvénykönyvéről (Mt.)
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 1997. évi CLIV. törvény az egészségügyről (Eütv.)
- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről (Eüak,)

4. A SZERVEZETNÁL MEGVALÓSULÓ ADATKEZELÉSEK

4.1. A munkaviszony létesítésével, fenntartásával és megszűnésével kapcsolatos adatkezelések

A Szervezethez történő jelentkezés folyamata:

A megfelelő munkavállaló kiválasztásáért az ügyvezető, az illetékes szervezeti egység vezetője, illetőleg a HR felelős, aki a jelen adatkezeléssel összefüggő feladatok ellátása során az adatvédelmi tisztviselővel együttműködve kötelesek az érintettek jogait biztosítani.

A Szervezet előtt az alábbi módon tárulnak fel személyes adatok a munkaerő kiválasztásával kapcsolatosan:

A sajtóban, valamint az interneten megjelenő hirdetés útján történik munkaerő toborzás, továbbá a Szervezet saját munkavállalói között és azok ajánlására is kereshet a megüresedett álláshelyre munkavállalót, illetve kérés nélküli jelentkezők közül is történik kiválasztás. A Szervezet a munkára jelentkezés céljából érkezett személyes adatokat tartalmazó önéletrajzok (továbbiakban: CV vagy önéletrajz) esetén nem tesz különbséget azok érkezésének módja között: azonos elbírálás alá esik a papíralapon és az elektronikus módon érkezett CV. Konkrét álláspályázatra történő jelentkezés esetén az önéletrajzokat a Szervezet a beküldéstől, illetve a toborzás lezárásától számított legfeljebb 6 hónapig kezeli, amely időszak alatt a pályázó bármikor kérheti az adatkezelés megszüntetését. Amennyiben a Szervezet ennél hosszabb ideig kívánja a jelentkező adatait kezelni, úgy arra a jelentkezőtől kifejezett felhatalmazást kér.

A hr@veszprembalaton2023.hu e-mail címre bármilyen formában vagy céllal beérkezett jelentkezéseket a Szervezet levelezőrendszere tárolja, illetve külön is menti őket a hálózaton tárolt személyügyi részlegmappán belül kijelölt mappába. A HR minden esetben válaszüzenetet küld, melyben tájékoztatja a jelentkezőt a CV megőrzéséről vagy törléséről, illetve a további döntésekről.

Adatkezelés célja	Kezelt adatok köre	Adatkezelés jogalapja	Adattárolás határideje	Adattárolás módja
a megüresedő álláshelyek betöltésére a munkaviszony későbbi létesítése céljából, megfelelő leendő munkavállaló kiválasztása	név, születési dátum, anyja neve, lakcím, képzési adatok, az érintett által megadott egyéb adatok, ajánló személyazonosító adatai, háttérellenőrzés sikerességének ténye	az érintett önkéntes hozzájárulása [GDPR 6. cikk (1) bek. a) pont], amely hozzájárulást az érintett az önéletrajzának és az ehhez kapcsolódó dokumentumoknak a megküldésével adja meg.	az érintett törlési kérelméig, maximum a beérkezéstől számított 1 év	Papíron, elektronikusan

A Szervezet munkavállalóinak munkaköri alkalmasságát a Szervezet a jogszabályi kötelezettségének megfelelően rendszeresen ellenőrzi. A Szervezet jogszabályi kötelezettségénél fogva foglalkozás-egészségügyi szakorvossal áll szerződéses kapcsolatban. A munkaköri alkalmassággal kapcsolatos egészségügyi adatokat a Szervezet nem ismeri meg, és nem kezeli egyetlen érintett adatát a célon túlterjeszkedő mértékben. A Szervezet csak a munkakör alkalmasság tényét bizonyító adatot kezeli.

A Szervezet – összhangban a NAIH álláspontjával – nem készít fénymásolatot személyazonosító igazolványokról természetes személyek azonosítása céljából. Az adatrögzítés és az adatminőség elvének megtartása céljából a Szervezet azonban az újonnan belépő vagy adatot módosító munkavállalók azonosító igazolványait megtekintésre bekérheti.

4.2. Bér- és munkaügyi nyilvántartás

A Szervezet munkavállalóiról személyzeti, illetve bér- és munkaügyi nyilvántartást vezet. A felvett munkavállalók adatait elektronikusan és papíralapon is tárolja a Szervezet. A munkavállalóknak azon személyes adatai kerülnek felvételre, amelyek a munkaviszony létesítéséhez szükségesek.

A személyzeti nyilvántartás adatai a munkavállaló munkaviszonyával kapcsolatos tények megállapítására és statisztikai adatszolgáltatásra használhatók fel. A munkavállalói adatok kezelésére vonatkozóan munkavállalói tájékoztató készült, amelynek célja a munkavállalók előzetes tájékoztatása az adatkezelésről.

A munkaviszony kapcsán beszerzett harmadik személy adatai (például pótszabadság, családi adókedvezmény kapcsán vagy baleset esetén értesítendő személy megjelölésekor) a szükséges adattartamot meg nem haladóan vehetők fel és kezelhetők.

Adatkezelés célja	Kezelt adatok köre	Adatkezelés jogalapja	Adattárolás határideje	Adattárolás módja
munkaviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása.	Lásd táblázat alatt	törvényi felhatalmazás [GDPR 6. cikk (1) bek. c) pont] (Mt 10. § (1) és (3)], valamint az adó és TB jogszabályok vonatkozó rendelkezései	A munkaviszony megszűnését vagy az nyugdíjkorhatár elérését követő 5 évig.	Papíron és elektronikusan

Kezelt adatok köre

név, születési név, születési hely és idő, állampolgárság, anyja születési neve, lakcím, tartózkodási cím (amennyiben eltérő a lakóhelytől), magán nyugdíjpénztári [tagság ténye, belépés ideje (év, hó, nap), bank neve és kódja, adóazonosító jele], társadalombiztosítási azonosító jele (TAJ szám), nyugdíjas törzsszám (nyugdíjas munkavállaló esetén), munkakönyv másolat (ha van), folyószámla száma, munkaviszony kezdő napja, biztosítási jogviszony típusa, heti munkaórák száma, telefonszám, családi állapot, végzettséget igazoló okmány másolati példánya, munkaalkalmassági egészségügyi igazolás, munkaköre, orvosi alkalmasság ténye, erkölcsi bizonyítvány [kiállításának dátuma, okmány száma, kérelem azonosítója], a leszámolást követően a munkaköri alkalmassági záró orvosi vizsgálat elvégzésének ténye, a csökkent munkaképességű munkavállaló csökkent munkaképességét megalapozó szakértői határozat, főálláson kívüli munkavégzés esetén [jogviszony jellege, munkáltató neve és székhelye, a főálláson kívüli munkahelyen teljesített havi átlagos munkaidő, elvégzendő tevékenység], előző munkaviszonnyal kapcsolatos igazolások [igazolás a biztosítási jogviszonyról és az egészségbiztosítási ellátásról, munkáltatói igazolás a jogviszony megszűnéséről, előző évi adóalap], az Mt. 120. § alapján járó pótszabadság igénybevételével kapcsolatosan [a rehabilitációs szakértői szerv a megváltozott munkaképesség megállapítását igazoló okmány fénymásolata, fogyatékossági támogatásra jogosultságot igazoló okmány fénymásolata, vakok személyi járadékára jogosultságot igazoló okmány fénymásolata] pótszabadság, családi adókedvezmény igénybevétele, adómentes természetbeni juttatásnak minősülő kedvezményes utazási igazolvány igénylésének vagy adómentes iskolakezdési támogatás céljából a munkavállaló a) 16. életévét be nem töltött hozzátartozójának b) 16. életévét betöltött hozzátartozójának, élettársának [neve, születési neve, születési helye és ideje, lakcíme, anyja neve, társadalombiztosítási azonosító jele (TAJ szám), adóazonosító jele, érvényes diákigazolvány meglétének ténye].

4.3. Munkavédelem , tűzvédelem, balesetvédelem

A Szervezet Munkavédelmi Szabályzatának elkészítését, karbantartását és bizonyos, a munkavédelemmel összefüggő oktatásokkal, illetőleg ellenőrzésekkel kapcsolatos szakmai tevékenységet külső szakértő megbízási szerződés alapján látja el. A Szervezet a megbízott vállalkozásnak nem ad át munkavállalói személyes adatot, azonban a munkavédelemmel összefüggésben eljárások, illetőleg a rendszeres oktatások során, valamint az esetleges munkabalesetek alkalmával, illetőleg ellenőrzések esetén a megbízott vállalkozás a megbízó érdekében eljárva az érintettektől vesz fel, illetve kezel személyes adatot.

Adatkezelés célja	Kezelt adatok köre	Adatkezelés jogalapja	Adattárolás határideje	Adattárolás módja
a munkabalesetek, foglalkozási megbetegedések és fokozott expozíciók kivizsgálása	anyja neve, társadalombiztosítási azonosító jele (taj-száma), születési hely és időpont, nem, állampolgárság, lakóhely (lakcím)	törvényi felhatalmazás [GDPR 6. cikk (1) bek. c) pont] (Mvt. 60. §(3) bekezdés)	a vizsgálat eredménye által megalapozott igények érvényesítésére nyitva álló határidő	Elektronikusan és papíron

4.4. Munkavállalók céges mobiltelefonjával kapcsolatos adatkezelés:

A céges mobiltelefonokat érintő rendelkezéseket a Szervezet Mobiltelefonhasználati Szabályzata tartalmazza.

4.5. Gyakornokok

A Munka Törvénykönyvéről szóló 2012. évi I. törvény, a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény 44. §, valamint a felsőoktatási szakképzésről és a felsőoktatási képzéshez kapcsolódó szakmai gyakorlat egyes kérdéseiről szóló 230/2012. (VIII. 28.) Korm. rendelet 17. § és 18. § alapján, továbbá az egyes intézményekkel kötött együttműködési megállapodás nyomán a Szervezet gyakornokokat foglalkoztat. A gyakornokokra a munkavégzés időtartama alatt a Szervezet munkavállalóival azonos szabályok vonatkoznak.

A gyakornokokkal külön gyakornoki szerződés kerül aláírásra. A szerződés és a jogszabályi kötelezések alapján a gyakornok adatkezelés az alábbi:

Adatkezelés célja	Kezelt adatok köre	Adatkezelés jogalapja	Adattárolás határideje	Adattárolás módja
A gyakornoki jogviszony létesítése, fenntartása, elszámolás	név, születési név, anyja születési neve, születési hely és idő, lakcím, hallgatói azonosítószám, telefonszám, email-cím, adóazonosító jel, bankszámlaszám	GDPR 6. cikk (1) bek. c) pont] (Mt 10. § (1) és (3)], valamint az adó és TB jogszabályok vonatkozó rendelkezései 230/2012, Korm, rend. 18/B.§ b) pont	A gyakornoki jogviszony lezárását követő 2 év	Papíron és elektronikusan

4.6. Közösségi oldal működtetésével összefüggő adatkezelés

A szervezet saját honlapot üzemeltet, www.veszprembalaton2023.hu. A honlapon a szervezet közzéteszi a működésére vonatkozó legfontosabb adatokat, az általa hirdetett eseményeket, programokat. A honlap a látogatói élmény fokozása és statisztikai adatok gyűjtése céljából cookie-kat alkalmaz.

A szervezet félévente ellenőrzi a honlap cookie beállításait automatizált lekérdezéssel, a használt cookie-ket a honlapján található adatvédelmi irányelvekben folyamatosan naprakészen tartja.

A Szervezet tevékenységének, felépítésének, álláslehetőségeinek, szervezettel kapcsolatos újdonságainak bemutatása, valamint a Szervezet által szervezett, illetve részvételével megrendezésre kerülő események végett az alábbi adatfeldolgozók közreműködésével Facebook, Instagram, LinkedIn, Youtube oldalakat üzemeltet.

A Szervezet közösségi médiában fenntartott oldalain a „Megosztás" parancsikonra kattintással az érintett hozzájárul a Szervezet híreinek és ajánlatainak közzétételéhez a saját üzenő falán. A Szervezet ezeken az oldalakon képeket/filmeket is közzétesz a különböző eseményekről stb. Amennyiben nem tömegfelvételről van szó, a Szervezet mindig kikéri az érintett írásbeli hozzájárulását a képek közzététele előtt.

A közösségi média oldalak adatkezeléséről a honlapjukon található adatvédelmi irányelvek és szabályzatból lehet tájékozódni.

Adatkezelés célja	Kezelt adatok köre	Adatkezelés jogalapja	Adattárolás határideje	Adattárolás módja
a Szervezet tevékenységének, felépítésének, álláslehetőségeinek, céggel kapcsolatos újdonságainak bemutatása, népszerűsítése	IP cím, statisztikai cookie-k, a közösségi oldalakon a közösségi oldal adatvédelmi szabályai szerinti adatok a közösségi oldal által	az érintett önkéntes hozzájárulása [GDPR 6. cikk (1) bek. a) pont]	A honlap fenntartásának dátuma, a VEB2023 projekt záró elszámolásának elfogadásától számított 10 év.	Elektronikusan

4.7. Marketing, hírlevéllel kapcsolatos adatkezelés:

Marketing tevékenység célja a **„Veszprém-Balaton 2023 Európa Kulturális Fővárosa"** programsorozat népszerűsítése, a Szervezet tevékenységnek minél szélesebb körű megismertetése.

A szervezet a látogatókkal való kapcsolattartás és a szolgáltatásai népszerűsítése érdekében rendszeres vagy eseti hírlevél küldésével a Szervezet kapcsolatot tart partnereivel, tájékoztatást nyújt a fontosabb eseményekről, rendezvényekről, adatokról.

Adatkezelés célja	Kezelt adatok köre	Adatkezelés jogalapja	Adattárolás határideje	Adattárolás módja
kapcsolattartás a potenciális partnerekkel, hírlevél küldése rendezvényekről és kapcsolódó tájékoztatásokról	név, e-mail cím	az érintett hozzájárulása, valamint az Adatkezelő jogos érdeke, a partnerekkel, kialakított üzleti kapcsolatok fenntartása, fejlesztése [GDPR 6. cikk (1) bek. a) illetőleg f) pont]	a hírlevélről való leiratkozásig – az Adatkezelőnek címzett e-mail-lel vagy a hírlevélben a leiratkozás ikonra történő kattintással	Elektronikusan

4.8. Pályázatokkal kapcsolatos adatkezelések

A Szervezet pályázati felhívásokat tesz közzé a honlapján különböző tárgykörökben, melynek kapcsán személyes adatokat kezel. Ilyen témakörök együttműködés, projektmegvalósítás.

Adatkezelés célja	Kezelt adatok köre	Adatkezelés jogalapja	Adattárolás határideje	Adattárolás módja
kapcsolattartás a pályázókkal, a nyertes pályázatok során a végrehajtás koordinálása, elszámolása	A pályázók adatai, illetve a pályázó kapcsolattartójának kapcsolattartási adatai (név, munkahelyi email cím, munkahelyi telefonszám	az érintett hozzájárulása, amelyet a pályázati adatlap benyújtásával egyidejűleg, a pályázati adatlapon tesz meg. az adatkezelő jogos érdeke, a partnerekkel, kialakított üzleti kapcsolatok fenntartása, fejlesztése [GDPR 6. cikk (1) bek. a) illetőleg f) pont]	VEB2023 projekt záró elszámolásának elfogadásától számított 10 év.	Elektronikusan és papíron

5. A SZERVEZET ADATVÉDELMI RENDSZERE

5.1. Az adatvédelem Szervezeten belüli szervezete

A Szervezet igazgatósága a Szervezet sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, és kijelöli az adatkezelés felügyeletét ellátó személyt.

A Szervezet munkatársai munkájuk során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

A Mt. 11/A. § (1) A munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető. Ennek keretében a munkáltató technikai eszközt is alkalmazhat, erről a munkavállalót előzetesen írásban tájékoztatja.

(2) A munkavállaló a munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert (a továbbiakban: számítástechnikai eszköz) – eltérő megállapodás hiányában – kizárólag a munkaviszony teljesítése érdekében használhatja.

(3) A munkáltató ellenőrzése során a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt a munkaviszonnyal összefüggő adatokba tekinthet be.

(4) A (3) bekezdés szerinti ellenőrzési jogosultság szempontjából munkaviszonnyal összefüggő adatnak minősül a (2) bekezdésben meghatározott korlátozás betartásának ellenőrzéséhez szükséges adat.

A Szervezet adatvédelmi rendszerének felügyeletét az igazgatóság látja el egy általa megbízott adatvédelmi tisztviselő útján.

A Szervezet biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint biztosítja számára, hogy a feladatai ellátása során utasításokat senkitől ne fogadjon el, ezen feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható. Az adatvédelmi tisztviselő szervezetileg közvetlenül a Szervezet ügyvezetőjének tartozik felelősséggel.

Az igazgatóság adatvédelemmel kapcsolatos feladatai:

- felelős a Szervezet által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
- felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
- felügyeli az adatvédelmi tisztviselő tevékenységét;
- vizsgálatot rendelhet el;
- kiadja a Szervezet adatvédelemmel kapcsolatos belső szabályait.

Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai:

- közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, segítséget nyújt az érintett jogainak biztosításában;
- minden év január 15-ig jelentést készít az igazgatóság részére a Szervezet adatvédelmi feladatainak végrehajtásáról;
- jogosult jelen szabályzat betartását az egyes szervezeti egységeknél ellenőrizni;
- vezeti a belső adatkezelési és adattovábbítási nyilvántartást;
- részt vesz a NAIH által szervezett adatvédelmi tisztviselők konferenciáján;
- figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását;
- közreműködik a NAIH-tól a Szervezethez érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;
- általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg;
- ellenőrzi az adatvédelmi jogszabályoknak, valamint a Szervezet belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosságnövelését és képzését, valamint a kapcsolódó auditokat is;
- gondoskodik az adatvédelmi ismeretek oktatásáról.
- közreműködik a Szervezethez érkező adatvédelemmel kapcsolatos megkeresések, kérdések, panaszok intézésében, végzi az adatvédelemmel kapcsolatos, jogszabályban rá ruházott további feladatokat

Az IT vezető adatvédelemmel kapcsolatos feladatai:

- közreműködik, segítséget nyújt, ill. javaslatot tesz a belső adatvédelmi felelősnek az informatikai adatkezeléssel összefüggő döntések előkészítésében;
- ellenőrzi az informatikai adatkezelésre vonatkozó jogszabályok, ill. a vonatkozó belső szabályzatok adatbiztonsági követelményeknek a megtartását;
- részt vesz a belső adatvédelmi és adatkezelési szabályzat informatikát érintő kérdéseinek tisztázásában és kidolgozásában;
- biztosítja a belső adatkezelési nyilvántartás vezetésének informatikai hátterét;
- eleget tesz az adatvédelmi tisztviselő felé fennálló kötelezettségeknek;
- javaslatot tesz az adatvédelmi tisztviselő felé az adatvédelmet érintő intézkedések meghozatalára;
- aktualizálj a/aktualizáltatja az Informatikai Biztonsági Szabályzatot;
- szükség szerint, de legalább évente egy alkalommal (minden év október 31. napjáig) írásbeli jelentést készít az adatvédelmi tisztviselő felé az adatvédelem informatikai megvalósulásáról.

Az egyes szervezeti egységek vezetőinek adatvédelemmel kapcsolatos feladatai:

- felelősek az irányításuk alá tartozó szervezeti egység adatkezeléseinek jogszabályoknak és jelen Szabályzatnak, vagy a kapcsolódó szabályzatoknak való megfelelőségéért;

- felelősek azért, hogy az általuk vezetett szervezeti egység adatkezelései során a jelen Szabályzat 5.2. részében foglalt adatbiztonsági előírások maradéktalanul teljesüljenek;
- ellenőrzik az adatvédelemmel kapcsolatos előírások, így különösen jelen Szabályzat rendelkezéseink betartását;
- az adatvédelmi tisztviselő segítségét kérik, amennyiben a személyes adatok, üzleti titkok, közérdekű adatok kezelésével összefüggésben kérdésük merül fel;
- együttműködnek az adatvédelmi tisztviselővel az adatvédelemmel kapcsolatos szabályok érvényesülése érdekében;
- biztosítják, hogy beosztottaik az adatvédelmi tisztviselő által szervezett, illetve tartott adatvédelemmel kapcsolatos képzéseken részt vehessenek.
- A személyes adatot kezelő munkavállaló adatvédelemmel kapcsolatos feladatai:
- kezeli és megőrzi a feladata ellátása során birtokába került adatokat;
- ügyel a személyes adatokat tartalmazó nyilvántartások biztonságos kezelésére és tárolására;
- gondoskodik arról, hogy az általa kezelt adatokhoz illetéktelen személy ne férhessen hozzá;
- betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat;
- haladéktalanul jelzi vezetője felé, amennyiben az adatvédelmi ügyben a felettes vagy az adatvédelmi tisztviselő segítségére szorul;
- részt vesz az adatkezeléssel, adatvédelemmel összefüggő oktatásokon.

5.2. Adatbiztonsági szabályok

A GDPR 32. cikke rögzíti, hogy az adatkezelő és adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve – többek között – adott esetben:

- a személyes adatok álnevesítését és titkosítását;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A papíralapon kezelt személyes adatok biztonsága érdekében a Szervezet, összhangban a hatályos Iratkezelési szabályokat rögzítő szabályzat előírásaival, az alábbi intézkedéseket alkalmazza:

- az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
- a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;
- a Szervezet adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;
- a Szervezet adatkezelést végző munkavállalója a munkavégzés befejeztével a papíralapú adathordozót elzárja;
- a jelen Szabályzatban meghatározott adatkezelések iratainak archiválását évente egyszer el kell végezni, az archivált iratokat a Szervezet Iratkezelési szabályzatának megfelelően kell szétválogatni és irattári kezelésbe venni.

- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra a Szervezet Informatikai Biztonsági Szabályzatában foglalt rendelkezések az irányadók.

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Szervezet, összhangban a Szervezet Informatikai Biztonsági Szabályzatának előírásaival, az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- az adatkezelés során használt számítógépek a Szervezet tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír a Szervezet;
- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről Szervezet rendszeresen, illetve indokolt esetben gondoskodik;
- a Szervezet az adatait a Microsoft O365 felhő alapú szolgáltatásaiban tárolja és kezeli. Az adattárolás európai központokban történik. A Microsoft a megfelelőségi nyilatkozatokat az alábbi oldalon tette nyilvánossá: https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3
- az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
- a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
- a hálózaton tárolt adatok biztonsága érdekében a szerveren folyamatos tükrözéssel kerüli el a Szervezet az adatvesztést;
- a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez, a mentés a központi szerver teljes adatállományára vonatkozik, és mágneses adathordozóra történik;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;
- a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

6. ADATVÉDELMI INCIDENS

6.1. Az adatvédelmi incidens fogalma

Az adatvédelmi incidens alatt a Rendelet 4. cikk 12. pontja értelmében a biztonság olyan sérülését értjük, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot nem adatvédelmi incidens, azonban valamennyi adatvédelmi incidens biztonsági incidens.

Az adatvédelmi incidensek jellemzően az alábbi három fő kategóriába sorolhatók:

- "bizalmassági incidens": személyes adatok jogellenes vagy véletlen közlése vagy az azokhoz való jogosulatlan hozzáférés;
- "integritási incidens": személyes adatok jogellenes vagy véletlen megváltoztatása;
- "elérhetőségi incidens": személyes adatok véletlen vagy jogellenes megsemmisítése, a személyes adatokhoz való hozzáférés véletlen vagy jogellenes elvesztése.

6.2. Az adatvédelmi incidens kezelése

A Szervezet minden munkavállalója – beleértve az egyéb jogviszonyban foglalkoztatott személyeket is – köteles a Szervezeten belül történt adatvédelmi incidenst haladéktalanul jelenteni a szervezeti egysége vezetőjének, valamint az adatvédelmi tisztviselőnek.

A bejelentés adatvédelmi tisztviselőhöz érkezését követően az adatvédelmi tisztviselő haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését. Az adatvédelmi tisztviselő megvizsgálja a bejelentést és amennyiben szükséges a bejelentőtől további adatokat kér az incidensre vonatkozóan. Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel, az adatvédelmi tisztviselő a vizsgálat lefolytatásához szükséges munkatársak bevonásával lefolytatja a vizsgálatot.

A vizsgálatnak tartalmaznia kell, hogy az adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e az érintettek tájékoztatása az incidensről.

Az adatvédelmi incidens kockázati besorolásai:

- Alacsony kockázat: a természetes személyekre lényegében nincs kihatással az incidens vagy az részükre csupán kisebb kellemetlenséget okoz, amelyet gond nélkül meg tudnak oldani.
- Közepes kockázat: a természetes személyek jelentős kellemetlenségeket tapasztalhatnak, amelyeket nehézségek árán meg tudnak oldani.
- Magas kockázat: a természetes személyek jelentős következményekkel szembesülhetnek az incidens kapcsán, amelyeket képesek lehetnek leküzdeni, azonban csak komoly nehézségek árán.
- Nagyon magas kockázat: a természetes személyek jelentős vagy akár visszafordíthatatlan következményekkel szembesülhetnek, amelyeket adott esetben nem képesek leküzdeni.

Ezt követően az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a Szervezet tudomására jutott, bejelenteni köteles az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

A 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 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.

Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatni köteles az érintettet is az adatvédelmi incidens bekövetkezéséről. Az adatkezelő köteles legalább az alábbiak szerinti tájékoztatást adni az érintettek részére:

- ismertetni kell az adatvédelmi incidens jellegét;
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

- ismertetni kell a Szervezet 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, ha a következő feltételek bármelyike teljesül:

- a Szervezet, mint 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;
- a Szervezet az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- 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.

6.3. Adatvédelmi incidens nyilvántartása

A GDPR előírásai alapján az adatvédelmi incidensről az adatvédelmi tisztviselő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az adatvédelmi incidens orvoslására megtett intézkedéseket,
- az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat 5 évig meg kell őrizni. Az adatvédelmi incidensek nyilvántartásának mintáját a vonatkozó melléklet munkalapja tartalmazza.

7. AZ ADATVÉDELMI HATÁSVIZSGÁLAT, AZ ELŐZETES KONZULTÁCIÓ ÉS AZ ÉRDEKMÉRLEGELÉS BEMUTATÁSA

7.1. Az adatvédelmi hatásvizsgálat

Amennyiben valamely új adatkezelési folyamat – annak jellegére, hatókörére, körülményeire, céljaira tekintettel - valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelés megkezdését megelőzően a Szervezet hatásvizsgálatot folytat le arra vonatkozóan, hogy az adatkezelési folyamat a személyes adatok védelmét hogyan érinti. Egymáshoz hasonló adatkezelési műveletek, amelyek hasonló kockázatokat jelentenek egyetlen egy hatásvizsgálat keretében is elvégezhetők.

A hatásvizsgálatot főszabály szerint az adatvédelmi tisztviselő végzi. Amennyiben nem ő végzi, úgy a Szervezet köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát.

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

A személyes adatok kezelésével kapcsolatosan az Adatkezelő kötelezettsége továbbá a kockázatelemzés, amelynek lépései a következők:

- a személyes adatok kezelésével kapcsolatos kockázatok azonosítása,

- kockázati lista felállítása,
- az egyes kockázatok valószínűsíthető fő okainak és várható negatív hatásainak meghatározása és
- ezek alapján a preventív és a korrektív kockázatkezelési folyamatok kidolgozása.

Szükséges a kockázatforrások feltárása, melyen belül meg kell határozni a kockázati preventív és korrektív célkezelés elemeit, az erőforrás-kezelés rendszerét és el kell különíteni az objektív és szubjektív kockázati elemeket. Az elemzés során el kell jutni a teljes kockázatértékelési rendszer kialakításáig, amelyben teljes kockázatpotenciál és kockázat prioritási sorrend (nem az intézkedési rendszerrel azonos) megállapítása kell, hogy megtörténjen. Az elemzés menetét és eredményeit írásba kell foglalni.

A kockázatpotenciálnál meg kell határozni a valószínűség szempontjából

- kicsi
- közepes
- nagy bekövetkezésű kockázatokat,

illetve horderő szempontjából

- kicsi
- közepes
- nagy horderejű kockázatokat.

Az a meghatározás alapozza meg a későbbi kockázatkezelési eljárás módját mind a preventív, mind a korrektív eljárás tekintetében. A kockázatelemzés végrehajtásáért az adatvédelmi tisztviselő felel.

7.2. Előzetes konzultáció

Amennyiben az elvégzett hatásvizsgálat azt állapítja meg, hogy az adatkezelési folyamat valószínűsíthetően magas kockázattal jár, akkor a Szervezet az adatkezelési folyamat megkezdését megelőzően konzultációt kezdeményez a Hatósággal.

A konzultáció kezdeményezése során a Szervezet csatolja:

- az elvégzett hatástanulmányt,
- az adatvédelmi tisztviselő nevét, elérhetőségét,
- az adatkezelési folyamatban részt vevő adatkezelő(k), adatfeldolgozó(k) feladatköreinek felsorolását,
- az adatkezelés célját, módját és
- az érintettek jogainak, szabadságainak biztosításának védelmében hozott intézkedéseket, garanciákat.

7.3. Érdekmérlegelés

A GDPR 6. cikk (1) bekezdés f) pontja szerint lehetőség van hozzájárulás nélküli adatkezelésre, ha ezt valamilyen jogos érdek lehetővé teszi, feltéve, hogy a Szervezet, mint adatkezelő eleget tesz tájékoztatási kötelezettségének. Amennyiben a jogalapot a GDPR 6. cikk (1) bekezdés f) pontja jelenti, az adatkezelési folyamat, akkor és annyiban lesz jogszerű, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

Az adatkezelés jogszerűségének vizsgálatához a Szervezet elvégez egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

Az érdekmérlegelési teszt során a Szervezet azonosítja jogos érdekét az adatkezeléshez, valamint a súlyozás ellenpontját képező érintetti érdeket és az érintett alapjogot. Az egymással ellentétes jogok és

érdekek súlyozásának feltételét mindig az adott eset sajátos körülményeire való tekintettel vizsgálja a Szervezet. A Szervezet a mérlegelés során figyelembe veszi különösen a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabálysértés súlyosságát stb.

Az érdekmérlegelési teszt részeként a szükségesség és arányosság vizsgálatát is elvégzi a Szervezet, amelynek értelmében a személyes adatok védelme alóli kivételeknek és a védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk. A kezelhető adatok jellege és mennyisége nem haladhatja meg a jogszerű érdekek érvényesítése céljából szükséges mértéket. Az arányosság vizsgálata a célok és a megválasztott eszközök közötti kapcsolat értékelését foglalja magában. A választott eszközök a szükségesség mértékét nem haladhatják meg, azonban az eszközöknek is alkalmasnak kell lenniük a meghatározott cél elérésére. A súlyozás elvégzése alapján a Szervezet megállapítja, hogy kezelhető-e a személyes adat.

A teszt eredményéről az érintettek tájékoztatást kapnak, melyből egyértelműen kiderül, hogy mely jogos érdek alapján és miért tekinthető arányos korlátozásnak az, hogy a Szervezet az érintett beleegyezése nélkül kezeli a személyes adatot, tehát a Szervezet adatkezeléséhez fűződő jogos érdeke miért múlja felül az érintett érdekeit, illetve jogait. A Szervezet tájékoztatja az érintetteket a hozzájárulás hiányára tekintettel alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről. Nem írható elő az ellentétes érdekek és jogok közötti súlyozás eredménye anélkül, hogy eltérő eredményt tenne lehetővé a Szervezet az adott eset sajátos körülményeire tekintettel, ezért a Szervezet minden egyes esetben külön érdekmérlegelési tesztet végez el.

8. AZ ÉRINTETT JOGAINAK ÉRVÉNYESÍTÉSE

8.1. Átlátható tájékoztatás, kommunikáció és az érintett joggyakorlásának elősegítése

A Szervezetnek az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell nyújtania, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

A Szervezetnek elő kell segítenie az érintett jogainak a gyakorlását.

A Szervezet indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 30 napon belül tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről. E határidő a Rendeletben írt feltételekkel további 60 nappal, viszont a késedelem konkrét okairól az érintettet tájékoztatni szükséges.

Ha a Szervezet nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 30 napon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

Az adatkezelő az információkat és az érintett jogairól szóló tájékoztatást és intézkedést díjmentesen biztosítja, azonban a Rendeletben írt esetekben díj számítható fel.

Az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról az adatkezelés megkezdését megelőzően tájékoztatást kapjon. Ennek keretében az érintettet tájékoztatni kell:

- az adatkezelő és képviselője kilétéről és elérhetőségeiről,
- az adatvédelmi tisztviselő elérhetőségeiről (ha van ilyen),
- a személyes adatok tervezett kezelésének céljáról, valamint az adatkezelés jogalapjáról,

- jogos érdek érvényesítésén alapuló adatkezelés esetén, az adatkezelő vagy harmadik fél jogos érdekeiről,
- a személyes adatok címzettjeiről – akikkel a személyes adatot közlik - , illetve a címzettek kategóriáiról, ha van ilyen;
- adott esetben annak tényéről, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

A tisztességes és átlátható adatkezelés biztosítsa érdekében a Szervezetnek az érintettet a következő kiegészítő információkról kell tájékoztatnia:

- a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
- az érintett azon jogáról, 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;
- az érintett hozzájárulásán alapuló adatkezelés esetén arról, hogy a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
- a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
- arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e a személyes adatokat megadni, továbbá, hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;
- az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról, és arra vonatkozóan érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

A munkavállalói adatok kezelésére vonatkozóan a szabályzat mellékleteként munkavállalói tájékoztató készült, amelynek célja a munkavállalók előzetes tájékoztatása az adatkezelésről.

8.2. Az érintett hozzáférési joga

A GDPR 15. cikke alapján az érintett kérelmezheti a rá vonatkozó személyes adatokhoz való hozzáférést az alábbiak szerint:

(1) Az érintett jogosult arra, hogy az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- az adatkezelés céljai;
- az érintett személyes adatok kategóriái;
- azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
- adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- az érintett azon joga, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

(2) Az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az Adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

8.3. A helyesbítéshez való jog

A GDPR 16. cikke alapján az érintett jogosult az Adatkezelőtől a rá vonatkozó személyes adat helyesbítését kérni.

Az érintett erre vonatkozó kérése esetén az Adatkezelő köteles indokolatlan késedelem nélkül helyesbíteni a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

Helyesbítés esetén a helyesbített személyes adatot mindazokkal közölni kell, akikkel a Szervezet közölte az eredeti személyes adatot.

8.4. Az adattörléshez való jog

A GDPR 17. cikke alapján az érintett jogosult az Adatkezelőtől a rá vonatkozó személyes adat törését kérni az alábbiak szerint:

(1) Az érintett jogosult arra, hogy az Adatkezelőtől a rá vonatkozó személyes adatok törlését kérje, az Adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett tiltakozik a közérdekből, közhatalmi jogosítvány gyakorlása érdekében vagy az adatkezelő (harmadik fél) jogos érdekében történő adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a tiltakozik a közvetlen üzletszerzés érdekében történő adatkezelés ellen;
- a személyes adatokat jogellenesen kezelték;
- a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami jogban (magyar jogban) előírt jogi kötelezettség teljesítéséhez törölni kell;
- a személyes adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

(2) Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és az (1) bekezdés értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

(3) Az Érintett törlési jogának korlátozására csak a GDPR-ban írt alábbi kivételek fennállása esetén kerülhet sor, azaz a fenti indokok fennállása esetén a személyes adatok további megőrzése jogszerűnek tekinthető:

- ha a véleménynyilvánítás és a tájékozódás szabadságához való jog gyakorlása, vagy
- ha valamely jogi kötelezettségnek való megfelelés, vagy
- ha közérdekből végzett feladat végrehajtása, vagy
- ha az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása miatt, vagy
- ha népegészségügy területén érintő közérdekből,
- ha közérdekű archiválás céljából, vagy
- ha tudományos és történelmi kutatás céljából vagy statisztikai célból, vagy
- ha jogi igények előterjesztéséhez, érvényesítéséhez illetve védelméhez szükséges.

A törléssel összefüggésben is fontos kötelezettség, hogy a kezelt személyes adatot mindazokkal töröltetni kell, akikhez a személyes adat a Szervezeten keresztül eljutott.

8.5. Az adatkezelés korlátozásához való jog

A GDPR 18. cikke alapján az érintett jogosult az Adatkezelőtől a rá vonatkozó személyes adat kezelésének korlátozását kérni az alábbiak szerint:

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

- az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az Adatkezelő ellenőrizze a személyes adatok pontosságát;
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- az érintett tiltakozott a közérdekből, közhatalmi jogosítvány gyakorlása érdekében vagy az adatkezelő (harmadik fél) jogos érdekében történő adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

(2) Ha az adatkezelés a fentiek alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

(3) Az Adatkezelő az érintettet, akinek a kérésére az (1) bekezdés alapján korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell.

8.6. Az adathordozhatósághoz való jog

A GDPR 20. cikke alapján az érintett jogosult a rá vonatkozó személyes adatok hordozhatóságára az alábbiak szerint:

(1) Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

- ha az adatkezelés jogalapja az Érintett hozzájárulása, vagy az Érintettel kötött szerződés teljesítése
- és az adatkezelés automatizált módon történik.

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

(3) Az adatok hordozhatóságához való jog gyakorlása nem sértheti a törléshez való jogot. Az adathordozás joga nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

(4) Az adatok hordozhatóságához való jog nem érintheti hátrányosan mások jogait és szabadságait.

Az adathordozhatósághoz való jog gyakorlása nem sértheti a Rendelet 17. cikkét (A törléshez való jog („az elfeledtetéshez való jog"). Az adtahordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges. E jog nem érintheti hátrányosan mások jogait és szabadságait.

8.7. A tiltakozáshoz való jog

A GDPR 21. cikke alapján az érintett jogosult az Adatkezelőtől a rá vonatkozó személyes adat kezelése ellen tiltakozni az alábbiak szerint:

(1) Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak közérdekből, közhatalmi jogosítvány gyakorlása érdekében vagy az adatkezelő (harmadik fél) jogos érdekében történő kezelése ellen, ideértve az ezen alapuló profilalkotást is. Ebben az esetben az Adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az Adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

(2) Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

(3) A tiltakozáshoz való jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

(4) Az információs társadalommal összefüggő szolgáltatások igénybevételéhez kapcsolódóan és a 2002/58/EK irányelvtől eltérve az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

(5) Ha a személyes adatok kezelésére tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

8.8. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Ez a jogosultság nem alkalmazandó abban az esetben, ha a döntés:

- az érintett és a Szervezet közötti szerződés megkötése vagy teljesítése érdekében szükséges;

- meghozatalát a Szervezetre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy
- az érintett kifejezett hozzájárulásán alapul.

8.9. Jogorvoslati jog

Az érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a Rendeletet. Az a felügyeleti hatóság, amelyhez a panaszt benyújtották, köteles tájékoztatni az ügyfelet a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről, ideértve azt is, hogy az ügyfél jogosult bírósági jogorvoslattal élni.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Postacím: 1363 Budapest, Pf.: 9.

Cím: 1055 Budapest, Falk Miksa utca 9-11.

Telefon: +36 (1) 391-1400

Fax: +36 (1) 391-1410

E-mail: ugyfelszolgalat (kukac) naih.hu

Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben. Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden érintett jogosult a hatékony bírósági jogorvoslatra, ha az illetékes felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

A rendelkezésre álló közigazgatási vagy nem bírósági útra tartozó jogorvoslatok – köztük a felügyeleti hatóságnál történő panasztételhez való jog – sérelme nélkül, minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak e rendeletnek nem megfelelő kezelése következtében megsértették az e rendelet szerinti jogait. Az adatkezelővel vagy az adatfeldolgozóval szembeni eljárást az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt kell megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is, kivéve, ha az adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.

9. ZÁRÓ RENDELKEZÉSEK

A jelen Szabályzat 2021. május 28.. napján lép hatályba.

A Szabályzat tartalmának megismerése és előírásainak megtartása a Szervezet munkavállalóinak munkaköri kötelezettsége, a Szervezet szerződő partnereinek pedig a rájuk vonatkozó szerződés előírásainak függvényében szerződéses kötelezettsége.

A mellékletek bármelyikében bekövetkező változás nem vonja maga után a jelen Szabályzat módosításának kötelezettségét.

10. MELLÉKLETEK

1. számú melléklet: Titoktartási nyilatkozat
2. számú melléklet: Adatvédelmi tájékoztató munkavállaló részére
3. számú melléklet: Hozzájáruló nyilatkozat fotó és videofelvétel készítéséhez
4. számú melléklet: Válaszlevél minták beérkezett CV-kre
5. számú melléklet: Adatvédelmi érdekmérlegelési teszt
6. számú melléklet: Adatvédelmi hatásvizsgálat elkészítéséhez útmutató
7. számú melléklet: Adatvédelmi incidens nyilvántartó

Kelt: Veszprém, 2021. május 28. napján

Markovits Aliz
vezérigazgató

Veszprém-Balaton 2023 Zrt.
8200 Veszprém, Óváros tér 26.
Cégj.sz.: 19-10-500277
Adószám: 23701142-2-19
2.