A
Mosonmagyaróvári Kulturális Egyesület
ADATKEZELÉSI SZABÁLYZATA

Ezen Adatkezelési Szabályzatot elfogadta a Mosonmagyaróvári Kulturális Egyesület Elnöksége a 2026. ……án tartott ülésén ??/2026 (??.??) Elnökségi határozattal.

1. A szabályzat célja
2. A szabályzat hatálya
3. Az adatkezelés elvei
4. Az adatkezelés jogalapja
4.1. A jogalapra vonatkozó általános rendelkezések
4.2. Az adatkezelés lehetséges jogalapjai személyes adatok esetében
4.3. Körülmények, amelyek esetén a Szervezet személyes adatok különleges kategóriáiba tartozó adatokat kezelhet
4.4. A hozzájárulásra, mint jogalapra vonatkozó különleges szabályok
4.5. A szerződéses jogviszonyra, mint jogalapra vonatkozó különleges szabályok
4.6. A jogi kötelezettségre, mint vonatkozó különleges szabályok
4.7. A létfontosságú érdekre, mint jogalapra vonatkozó különleges szabályok
4.8. A jogos érdekre, mint jogalapra vonatkozó különleges szabályok
5. Az adatkezelés szabályai
5.1. Alapvetések
5.2. A személyes adatokkal kapcsolatos titoktartási szabályok
5.3. A személyes adatok megsemmisítése
6. Az érintettek jogai
6.1. Az érintett tájékoztatása az adat felvételéhez kapcsolódóan
6.2. Az érintett jogainak érvényesítése
6.3. Az érintett tájékoztatása a rá vonatkozó adatkezelésről („hozzáférés”)
6.4. Az érintett helyesbítéshez való joga
6.5. Az érintett törléshez való joga
6.6. Az adatkezelés korlátozásához fűződő érintetti jog
6.7. Tiltakozás a személyes adat kezelése ellen
6.8. Az adathordozhatósághoz való érintetti jog gyakorlása
6.9. Jogorvoslat
7. A Szervezet adatvédelmi rendszere
7.1. Általános rendelkezések
7.2. Az adatvédelmi tisztviselőre vonatkozó szabályok
7.3. Hatáskörök az adatvédelemmel kapcsolatosan
8. Adatbiztonsági szabályok
9. Adatvédelmi incidens kezelése
9.1. Adatvédelmi incidens észlelése és jelentése
9.2. Adatvédelmi incidens kivizsgálása
9.3. Adatvédelmi incidens értékelése
9.4. Adatvédelmi incidens bejelentése a NAIH-nak
9.5. Az érintettek tájékoztatása az adatvédelmi incidensről
9.6. Helyesbítő-megelőző intézkedések bevezetése
9.7. Az adatvédelmi incidens nyilvántartása
10. Adatvédelmi oktatás
11. Adatkezelési tevékenységek nyilvántartása
12. Adatfeldolgozókra vonatkozó szabályok
13. Adatvédelmi hatásvizsgálat
13.1. Az adatvédelmi hatásvizsgálat-köteles adatkezelések
13.2. Az adatvédelmi hatásvizsgálat lefolytatása
14. Záró rendelkezések

1. A SZABÁLYZAT CÉLJA

1.1. A szabályzat célja, hogy az EU 2016/679 számú Általános Adatvédelmi Rendeletének (a továbbiakban: GDPR) 33. és 34. cikkében meghatározottakkal, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) és a személyes adatok kezelését érintő egyéb magyar jogszabályokkal valamint a 29-es cikk szerint létrehozott Adatvédelmi Munkacsoport WP250 sz. iránymutatásával összhangban meghatározza a Mosonmagyaróvári Kulturális Egyesület (9200 Mosonmagyaróvár, Pacsirta u. 14.) (a továbbiakban: Adatkezelő, vagy Szervezet) által kezelt személyes adatok védelme, továbbá azok jogosulatlan felhasználásnak megakadályozása érdekében az adatvédelemi előírások és az adatbiztonsági követelmények érvényesüléséhez szükséges szabályokat és a Szervezetben vezetett nyilvántartások működésének rendjét.

1.2. Jelen szabályzat a Szervezet kezelésében lévő személyes adatok tekintetében a legfontosabb adatvédelmi szabályokat tartalmazza, különös tekintettel a GDPR által az adatkezelővel szemben támasztott követelményekre és a GDPR III. fejezetében meghatározott érinteti jogok érvényesülésének biztosítására.

1.3. A Szabályzattal a Szervezet biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést, azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.

1.4. Jelen szabályzatot a Szervezet egyéb – különösen az adatkezelés és adatbiztonság vonatkozásában rendelkezéseket tartalmazó – szabályzataival és eljárásrendjeivel összhangban kell értelmezni és alkalmazni.

2. A SZABÁLYZAT HATÁLYA

2.1. Szervezeti hatály
Jelen szabályzat szervezeti hatálya kiterjed a Szervezet minden szervezeti egységére.

2.2. Személyi hatály
Jelen szabályzat személyi hatálya kiterjed a Szervezet által foglalkoztatott munkavállalókra, valamint olyan természetes személyekre és a jogi személyek, jogi személyiséggel nem rendelkező szervezetek minden olyan természetes személy alkalmazottaira, akik a Szervezet szolgáltatásaival, illetve tevékenységével és a Szervezet informatikai rendszereivel jogviszonyba, vagy más kapcsolatba kerülnek.

2.3. Tárgyi hatály
Ezt a szabályzatot kell alkalmazni minden olyan adatkezelésére és adatfeldolgozására, amely természetes személy személyes adataira vonatkozik, beleértve az adatkezelés minden elemét, függetlenül attól, hogy az elektronikusan vagy papír alapon történik.

3. AZ ADATKEZELÉS ELVEI

A Szervezet az adatkezelés során az alábbi alapelvek alapján szervezi folyamatait:

3.1. Jogszerűség, tisztességes eljárás és átláthatóság elve [GDPR 5. cikk (1) a)]: A Szervezet személyes adatot csak jogszerűen és a tisztességesen kezel, az adatkezelést az érintett számára átlátható módon végzi, többek között jelen Szabályzat nyilvánosságra hozatalával, végzi.

3.2. Célhoz kötöttség elve [GDPR 5. cikk (1) b)]: a Szervezet minden esetben, ha személyes adatot kezel, az adat felvétele előtt meghatározza a személyes adat kezelésének célját, amely így előre meghatározott, egyértelmű és jogszerű. Személyes adatot a Szervezet az előre meghatározott céllal össze nem egyeztethető módon nem kezel. Amennyiben teljesült az adatkezelés célja és jogszabály nem írja elő kötelezően az adat további kezelését, úgy a személyes adatot a Szervezet törli.

3.3. Adattakarékosság elve [GDPR 5. cikk (1) c)]: a Szervezet az adatkezelés során csak olyan személyes adatot kezel, amely a cél eléréséhez megfelelő és releváns, a Szervezet az adatkezelést csak a cél eléréséhez szükséges minimum adatmennyiségre korlátozza.

3.4. Pontosság elve [GDPR 5. cikk (1) d)]: a Szervezet törekszik rá, hogy az általa kezelt személyes adatok pontosak és naprakészek legyenek és a jelen Szabályzatba foglalt módon törekszik rá, hogy a pontatlan személyes adatokat haladéktalanul törölje, vagy – az érintett kérelmére vagy tudomására jutása esetén hivatalból – helyesbítse.

3.5. Korlátozott tárolhatóság elve [GDPR 5. cikk (1) e)]: a Szervezet személyes adatot csak úgy tárol, hogy a személyes adat érintettje csak az adatkezelés céljának eléréséig azonosítható az adatkezelés során, a személyes adatok ennél hosszabb ideig történő tárolását csak jogszabály kötelező előírása alapján végzi a Szervezet.

3.6. Integritás és bizalmasság elve [GDPR 5. cikk (1) f)]: a Szervezet az adatkezelési folyamatait úgy tervezi és hajtja végre, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítja a személyes adatok megfelelő biztonságát, így különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet.

3.7. Elszámoltathatóság elve [GDPR 5. cikk (2)]: a Szervezet az adatkezelési folyamatait úgy tervezi és hajtja végre, hogy az adatkezelés bármely pillanatában képes legyen a jelen pontba foglalt elveknek való megfelelést igazolni.

4. AZ ADATKEZELÉS JOGALAPJA

4.1. A jogalapra vonatkozó általános rendelkezések

4.1.1. Az adatkezelés jogalapját a Szervezet minden adatkezelési folyamatnál meghatározza. Az adatkezelésre jogalapot csak a GDPR 6. cikk (1) és 9. cikk (2) bekezdésekben rögzítettek szerint határoz meg a Szervezet.

4.1.2. A Szervezet az adatkezelési rendszerét úgy alakítja ki, hogy minden személyes adatra vonatkozóan bizonyítani tudja, hogy mikor, milyen formában történt a személyes adat felvétele és milyen tájékoztatást kapott az érintett a személyes adat felvételekor.

4.1.3. A személyes adatok különleges kategóriáiba tartozó személyes adatot főszabály szerint a Szervezet nem kezel, kivéve abban az esetben, amennyiben bizonyítani tudja a 4.3. pontba foglalt valamely körülmény fennállását.

4.2. Az adatkezelés lehetséges jogalapjai személyes adatok esetében

4.2.1. Az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez.

4.2.2. 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.

4.2.3. Az adatkezelés a Szervezetre vonatkozó jogi kötelezettség teljesítéséhez szükséges.

4.2.4. Az adatkezelés az érintett, vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

4.2.5. Az adatkezelés közérdekű, vagy a Szervezetre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

4.2.6. Az adatkezelés a Szervezet, vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

4.3. Körülmények, amelyek esetén a Szervezet személyes adatok különleges kategóriáiba tartozó adatokat kezelhet

4.3.1. Az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy a hatályos magyar jog úgy rendelkezik, hogy 4.1.3. pontban foglalt tilalom az érintett hozzájárulásával sem oldható fel.

4.3.2. Az adatkezelés a Szervezetnek, 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 hatályos magyar jog lehetővé teszi.

4.3.3. 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.

4.3.4. Az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott.

4.3.5. Az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

4.3.6. Az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy a hatályos magyar 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.

4.3.7. 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 hatályos magyar jog alapján vagy egészségügyi

szakemberrel kötött szerződés értelmében, amennyiben az adatkezelés adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, akire szakmai titoktartási kötelezettség hatálya alatt áll.

4.3.8. Az adatkezelés a népegészségügy területét érintő közérdekből szükséges.

4.3.9. Az adatkezelés közérdekű archiválás, tudományos és történelmi kutatási, vagy statisztikai célból szükséges olyan uniós, vagy hatályos magyar 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.

4.4. A hozzájárulásra, mint jogalapra vonatkozó különleges szabályok

4.4.1. Amennyiben az adatkezelés az érintett hozzájárulásán alapszik, úgy az érintett a hozzájárulását bármilyen bizonyítható módon megadhatja, így írásban (nyilatkozaton, dokumentumon), szóban és ráutaló magatartással is.
A Szervezet nem tesz különbséget a hozzájárulások között azok formáját tekintve, a hozzájárulások formái egyenértékűek, de fenntartja magának a jogot, hogy egyes adatkezelések esetén a hozzájárulás egyes formáit kizárja.

4.4.2. A Szervezet minden adatkezelési folyamatát úgy határozza meg jelen szabályzat kiadásakor és minden, a későbbiekben bevezetendő adatkezelés esetén, hogy amennyiben annak jogalapja az érintett hozzájárulása, úgy képes legyen annak bizonyítására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. A Szervezet ennek úgy tesz eleget, hogy elsődlegesen az írásban szerzi be az érintett hozzájárulását, amelyet így az írásbeliséggel tud igazolni.

4.4.3. Amennyiben a Szervezet a ráutaló magatartást, vagy a szóbeliséget is elfogadja a hozzájárulás jogalapjául, úgy az adatkezelés minden körülményét megvizsgálja és dokumentálja, hogy utóbb is igazolni tudja a hozzájárulást.

4.4.4. A Szervezet az adatkezelései során lehetőség szerint minden egyes személyes adatnál feltünteti, hogy a hozzájárulás mikor érkezett, milyen formában történt (írásban/szóban/ráutaló magatartással), milyen cselekmény eredménye, ha ez értelmezhető (például: feliratkozás/jelentkezés/kapcsolatfelvétel/stb.).

4.4.5. A Szervezet biztosítja a jogot arra is, hogy az érintett ugyanúgy, ahogy a hozzájárulást megadta, a hozzájárulását visszavonja. A ráutaló magatartással megtett hozzájárulás visszavonását csak írásban fogadja el a Szervezet.

4.4.6. A Szervezet a visszavonás tényét az adatkezelés során rögzíti, az adatot a továbbiakban nem kezeli, de az adat helyét „a hozzájárulás visszavonva” jelzéssel jelöli meg. A megjelölés tartalmazza hozzájárulás visszavonására vonatkozó, a 4.4.4. pont szerinti értelemszerű adatokat.

4.5. A szerződéses jogviszonyra, mint jogalapra vonatkozó különleges szabályok

4.5.1. Ha az adatkezelés jogalapja a Szervezettel írásban kötött szerződés megkötését megelőzően lépések tétele vagy teljesítése, úgy a szerződésnek minimálisan tartalmaznia kell az arra való utalást, hogy az adatkezelés a jelen Szabályzat szerint történik és arra a konkrét adatkezelési folyamatleírásra való hivatkozást, amely a konkrét adatkezelést rögzíti.

4.5.2. A szerződéses jogviszonyra hivatkozó jogalap csak akkor alkalmazható, ha az szerződés egyik szerződő fele az érintett.

4.6. A jogi kötelezettségre, mint vonatkozó különleges szabályok

4.6.1. Amennyiben az adatkezelés jogalapja a 7.2.3. pont szerinti jogi kötelezettség, úgy e jogi kötelezettséget csak és kizárólag az Európai Unió, vagy Magyarország hatályos és alkalmazandó jogszabályának kell megállapítania.

4.6.2. Amennyiben a Szervezet az adatkezelése során a jogalapként a jogi kötelezettséget határozza meg, úgy az adatkezelési nyilvántartásban a jogi kötelezettséget előíró jogszabályi rendelkezést a jogszabályra és a jogszabályi helyre történő pontos hivatkozással kell megjelölni.

4.7. A létfontosságú érdekre, mint jogalapra vonatkozó különleges szabályok

4.7.1. A Szervezet természetes személy létfontosságú érdekére hivatkozó jogalappal akkor végez adatkezelést, ha az adott adatkezelés egyéb jogalappal nem végezhető.

4.7.2. Az elszámoltathatóság elve miatt a Szervezet az adatkezelés megkezdése köteles megvizsgálni, hogy a személyes adat kezelése megvalósítható-e bármely más jogalappal.
Ugyancsak az elszámoltathatóság elvéből fakadóan a Szervezetnek tudnia kell bizonyítania a létfontosságú érdek fennállását.

4.8. A jogos érdekre, mint jogalapra vonatkozó különleges szabályok

4.8.1. A jogos érdekre hivatkozó jogalapot a szükségesség-arányosság elve alapján alkalmazza a Szervezet, ha az adatkezeléssel elérendő cél más jogalappal nem megvalósítható és az érintett magánszférájának korlátozása arányban áll az elérendő céllal.

4.8.2. A Szervezet a jogos érdekre hivatkozó jogalappal végzett adatkezelés megkezdése előtt az érintettek magánszférájának, érdekeinek és alapvető jogainak biztosítása érdekében érdekmérlegelési tesztet végez el.

Az érdekmérlegelési teszt célja az adatkezelő, vagy egy harmadik fél jogos érdekeinek és az érintett érdekeinek illetve alapvető jogainak és szabadságainak összevetése annak eldöntése érdekében, hogy jogos érdekre hivatkozó jogalappal elvégezhető-e a tervezett adatkezelés. A jogos érdekre történő hivatkozásnál érdekmérlegelési teszt elvégzésével kell összevetni, illetve az érintettet tájékoztatni kell arról, hogy az adatkezelés az adatkezelő jogos érdekén alapul.

Az érdekmérlegelési tesztnek ki kell terjednie:

- a kezelni kívánt személyes adatok körének meghatározására,
- annak a személynek a meghatározása, akinek a jogos érdekében az adatkezelés szükséges,
- a jogos érdek lehető legpontosabb meghatározására,
- az adatkezelés céljának meghatározására,
- annak vizsgálatára, hogy az adatkezelés feltétlenül szükséges-e a feltárt jogos érdek érvényesítéséhez,
- a jogos érdek és az érintetti alapjogi korlátozás összevetésére.

4.8.3. Amennyiben az érdekmérlegelési teszt eredményeként a Szervezet megállapítja, hogy az adatkezeléssel érintett jogos érdekkel szemben elsőbbséget élveznek az érintett érdekei és alapvető jogai, a jogos érdekre hivatkozó jogalapot nem alkalmazza.

5. Az adatkezelés szabályai

5.1. Alapvetések

5.1.1. A Szervezet kizárólag a hatályos jogszabályok rendelkezései alapján végez adatkezelést.

5.1.2. A Szervezet személyes adatot csak és kizárólag a GDPR 6. cikkébe, a személyes adatok különleges kategóriáiba tartozó személyes adatot csak és kizárólag a GDPR 9. cikk (2) bekezdésében foglalt jogalapokkal, jog gyakorlása vagy kötelezettség teljesítés érdekében kezel.

5.1.3. A konkrét adatkezelési folyamattal érintett jogosultság, vagy kötelezettség keletkezhet a Szervezet, az érintett, vagy harmadik fél oldalán is.

5.1.4. A Szervezet kezelésében lévő személyes adat az adatkezelés során mindaddig megőrzi személyes adat minőségét, amíg belőle az érintett azonosított, vagy azonosítható. A Szervezet akkor tekint egy adatot személyes adatnak, amennyiben rendelkezik azzal a technikai feltétellel, amely segítségével képes az adatból azonosítani az érintettet.

5.1.5. A Szervezet csak úgy folytat adatkezelést, hogy az minden szakaszában megfelel az adatkezelési célnak.

5.1.6. A Szervezet minden esetben előzetes tájékoztatást nyújt az érintettek részére az adatkezelés céljáról, az adatkezelés jogalapjáról, valamint az adatkezeléssel kapcsolatos, a GDPR 13-14. cikkében meghatározott tényekről.

5.1.7. A Szervezet munkaszervezési, fizikai, informatikai és jogosultságkezelési eszközökkel gondoskodik arról, hogy illetéktelen személyek a személyes adatokat ne ismerhessék meg.

5.2. A személyes adatokkal kapcsolatos titoktartási szabályok

5.2.1. A Szervezet munkatársai és az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek munkatársai és megbízottjai (alvállalkozói) kötelesek az adatkezelés során megismert személyes adatokat titokként megőrizni.

5.2.2. A személyes adatok egyetlen része, vagy töredéke sem tehető közzé, nem bocsátható rendelkezésre, vagy nem tárható fel semmilyen módon harmadik személy előtt, kivéve ha a személyes adat közérdekből nyilvános adatként történő nyilvánosságra hozatalát jogszabály írja elő.

5.2.3. A Szervezet munkatársai kötelesek megtenni azokat az intézkedéseket, amelyek kizárják, hogy a szóban elhangzott, papíralapon vagy elektronikus formátumban rögzített személyes adatot bármely harmadik személy jogosulatlanul megismerje.

5.2.4. Személyes adatról papíralapú, vagy elektronikus másolat csak abban az esetben készíthető, ha azt az adatkezelés folyamata szükségessé teszi, vagy jogszabály előírja.

5.2.5. Ha a Szervezet valamely munkatársa a Szabályzatot megszegi, a Szervezet és közte lévő jogviszony jellegétől függően felelősséggel tartozik.

5.2.6. Ha a Szabályzatot a Szervezettel munkaviszonyban álló személy szegi meg és ezzel kárt okoz, úgy a munkaviszony ellátásra vonatkozó általános (a mindenkori munka törvénykönyvéről szóló, a Szabályzat kiadásakor a munka törvénykönyvéről szóló 2012. évi I. törvény) vagy speciális jogszabály munkaviszonyból származó kötelezettségének megszegésével okozott kárra vonatkozó szabályok szerint felel.

5.2.7. Ha a Szabályzatot a Szervezettel egyéb jogviszonyban álló személy szegi meg és ezzel kárt okoz, úgy a mindenkori polgári törvénykönyv (a Szabályzat kiadásakor a Polgári Törvénykönyvről szóló 2013. évi V. törvény) károkozásért való felelősségre vonatkozó szabályok szerint felel.

5.3. A személyes adatok megsemmisítése

5.3.1. Abban az esetben, ha a Szervezet az általa kezelt személyes adatokat az adatkezelés szabályai alapján a továbbiakban nem kezelheti, köteles a személyes adatokat tartalmazó adathordozót megsemmisíteni, a megsemmisítés tényéről pedig jelen Szabályzat 1. sz. melléklete szerinti megsemmisítési jegyzőkönyvet felvenni.

5.3.2. A megsemmisítési jegyzőkönyv tartalmazza az alábbiakat:
- az adatmegsemmisítésért felelős munkavállaló azonosító adatait,
- a megsemmisítést engedélyező személy azonosító adatait,
- a megsemmisítés tárgya,
- az adathordozók száma legalább megközelítőlegesen,
- a megsemmisítéssel érintett adatkezelési folyamat megnevezése,
- az adatmegsemmisítés módja,
- a megsemmisítés időpont, helyszíne,
- a megsemmisítést ténylegesen lefolytató, illetve azon jelen lévők neve és aláírása (minimum három fő).

5.3.3. A Szervezet az Adatmegsemmisítési jegyzőkönyvet iratkezelési szabályzata szerint tárolja.

6. AZ ÉRINTETTEK JOGAI

6.1. Az érintett tájékoztatása az adat felvételéhez kapcsolódóan

6.1.1. Abban az esetben, amennyiben az adatkezelés során a személyes adatokat a Szervezet közvetlenül az érintettől szerzi meg, úgy a személyes adatok megszerzésének időpontjában az alábbiakról tájékoztatja az érintettet:
- a Szervezet pontos megnevezése, elérhetőségei,
- a Szervezet adatvédelmi tisztviselőjének neve és elérhetőségei,
- az adatkezelés célja,
- az adatkezelés jogalapja,
- amennyiben az adatkezelés célja a jogos érdek érvényesítése, úgy a Szervezet, vagy a harmadik fél jogos érdekének megnevezése,
- amennyiben a Szervezet a személyes adatokat az adatkezelés során harmadik fél számára átadja, a személyes adatok címzettjei, illetve a címzettek kategóriái.

- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- a hozzáférési jog gyakorlásának szabályai,
- a helyesbítési jog gyakorlásának szabályai,
- a törlési jog gyakorlásának szabályai,
- az adatkezelés korlátozására irányuló jog gyakorlásának szabályai,
- a tiltakozási jog gyakorlásának szabályai,
- az adathordozhatósághoz való jog gyakorlásának szabályai,
- a hozzájárulás visszavonására irányuló jog gyakorlásának szabályai, amennyiben az adatkezelés jogalapja az érintett hozzájárulása,
- a Nemzeti Adatvédelmi és Információszabadság Hatósághoz címzett panasz benyújtásának jogáról;
- annak ténye, hogy a személyes adat kezelése szolgáltatása jogszabályon, szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele és az érintett köteles-e a személyes adatokat megadni, valamint a lehetséges következmények, amennyiben az érintett személyes adatait nem adja meg,
- az automatizált döntéshozatal ténye, valamint legalább az ennek során alkalmazott logika és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

6.1.2. Amennyiben a Szervezet a személyes adatot nem közvetlenül az érintettől szerzi meg, úgy az 6.1.1. pontban foglaltatok túl az alábbiakról tájékoztatja az érintettet:

- a kezelt személyes adatok kategóriái,
- a személyes adat forrása,
- amennyiben az adatok harmadik forrásból való gyűjtését jogszabály írja elő, úgy a konkrét jogszabályi hely megjelölése,
- a személyes adat Szervezet általi megszerzésének időpontja,
- amennyiben a Szervezet által folytatott ügyben van szükség a személyes adatokra, úgy a konkrét ügy ügyszámmal vagy egyéb módon történő megjelölése,
- annak ténye, hogy a személyes adat nyilvánosan hozzáférhető forrásból származik-e.

6.1.3. Amennyiben a Szervezet az adatkezelése során az adatot nem közvetlenül az érintettől szerzi meg, az érintettet a 6.1.2. pontban foglaltakról az alábbi időpontban tájékoztatja:

- a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül,
- ha a Szervezet a személyes adatokat az érintettel való kapcsolattartás céljára használja, az érintettel való első kapcsolatfelvétel alkalmával vagy
- ha a Szervezet az adatokat várhatóan más címzettel is közli, legkésőbb a személyes adatok első alkalommal való közlésekor.

6.1.4. A fenti 6.1.1. és 6.1.3. pontokba foglaltakat nem kell alkalmazni, amennyiben:

- az érintett már rendelkezik az ezen pontokba foglalt információkkal,
- a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne,
- az adat megszerzését, vagy közlését kifejezetten előírja a Szervezetre alkalmazandó uniós, vagy a hatályos magyar jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről is rendelkezik vagy
- a személyes adatoknak valamely uniós, vagy a hatályos magyar jogban előírt szakmai titoktartási kötelezettség alapján bizalmasnak kell maradnia.

6.2. Az érintett jogainak érvényesítése

6.2.1. A GDPR 15-21. cikkei szerint az érintett az alábbi jogérvényesítési lehetőségekkel élhet a Szervezet adatkezelései során:

- az érintett kérheti az 5.3. pont szerint tájékoztatását személyes adatai kezeléséről,
- az érintett kérheti az 5.4. pont szerint személyes adatainak helyesbítését,
- az érintett kérheti az 5.5. pont szerint személyes adatainak törlését,
- az érintett kérheti az 5.6. pont szerint személyes adatai kezelésének korlátozását,
- az érintett az 5.7. pont szerint tiltakozhat személyes adatai kezelése ellen,
- az érintett élhet az 5.8. pont szerinti adathordozhatósághoz való jogával.

6.2.2. A Szervezet annak érdekében, hogy az érintettek a jogaikkal élhessenek, részletesen meghatározza az érintetti joggyakorlással kapcsolatos jogokat, kötelezettségeket és eljárási szabályokat.

6.2.3. A Szervezet minden esetben törekszik arra, hogy az általa az érintettnek adott tájékoztatás minden esetben a GDPR által meghatározott szabályok teljesítése mellett is a lehetőségekhez mérten tömör, átlátható, érthető, könnyen hozzáférhető, világos és közérthető legyen.

6.2.4. A Szervezet az érintettnek adott minden tájékoztatást főszabály szerint írásban tesz meg, ideértve az elektronikus utat is.
Amennyiben az érintett kéri a szóbeli tájékoztatást, úgy személyazonossága igazolását követően a Szervezet erre felhatalmazott munkatársa a tájékoztatást szóban is megadhatja.

6.2.5. A Szervezet az érintett számára tájékoztatást csak és kizárólag abban az esetben nyújt, ha a Szervezet erre felhatalmazott munkatársa meggyőződött az érintett személyazonosságáról.
Az érintett személyazonosságáról való meggyőződésnek számít, ha a Szervezet erre felhatalmazott munkatársa előtt:

- az érintett személyazonosságát a hatályos magyar jog szerinti személyazonosság igazolására alkalmas okmány bemutatásával (így különösen, de nem kizárólagosan személyazonosító igazolvánnyal, útlevéllel, vezetői engedéllyel) igazolja,
- az érintett személyazonosságát az Európai Unió joga szerint személyazonosság igazolására alkalmas okmány bemutatásával igazolja,
- az érintett kérelme a Szervezet előtt már korábbi ügyből ismert, az érintetthez köthető e-mail címről érkezik,
- az érintett kérelme a Szervezet által biztosított, zárt, a megfelelő személyazonosítás megtörténte után használható csatornán érkezik.

6.2.6. A Szervezet nem fogadja el a személyazonosítás telefonos úton történő egyetlen formáját sem, így az érintett telefonon nem kezdeményezheti a 6.2.1. pontba foglalt jogainak érvényesítését.

6.2.7. Amennyiben a személyazonosság igazolása a 6.2.5. pont szerint nem történik meg, a Szervezet az érintetti joggyakorlási kérelmet elutasítja, és egyben tájékoztatja az érintettet jogai gyakorlásának módjáról.

6.2.8. A Szervezet az érintettet a kérelem beérkezésétől számított egy hónapon belül tájékoztatja a jogaikkal kapcsolatos - megfelelően közölt nyilatkozatba foglalt - kérelem esetén.
Megfelelő közlésnek, illetve beérkezésnek az számít, ha az igényt az érintett:

- szóban személyesen személyazonosítást követően a szervezet ügyfélszolgálatán vagy az adatvédelmi tájékoztatóban meghatározott személy számára megteszi
- az írásba foglalt igény a Szervezet hivatalos címére, vagy az erre a célra megadott email címére megérkezik.

A nem a fenti megfelelő módok valamelyikén közölt igényt a Szervezet nem veszi figyelembe.

6.2.9. A 6.2.8. pontba foglalt határidőt a Szervezet maximum további két hónappal meghosszabbítja, ha a kérelem összetettsége, vagy az aktuálisan kezelt kérelmek száma azt indokolja. A határidő meghosszabbításáról a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül, elektronikus úton tájékoztatja az érintettet.

6.2.10. A Szervezet a jelen pontban foglaltak szerinti tájékoztatást és intézkedéseket díjmentesen végzi.

6.2.11. A 6.2. pontba foglaltak szerinti tájékoztatás és intézkedés megtételéréért a Szervezet adatvédelmi tisztviselője felelős a szakterületek által szolgáltatott adatok alapján.
Az írásbeli tájékoztatók mintáit az adatvédelmi tisztviselő az elnökkel (ha a két tisztséget ugyanaz a személy tölti be, akkor az elnökségi üléssel) előzetesen jóváhagyja.

6.2.12. A tájékoztatásra vonatkozó adatok birtokában lévő szakterület köteles az adatvédelmi tisztviselővel együttműködni, számára előzetesen írásban minden információt, adatot megadni a tájékoztatás teljesítéséhez.

6.3. Az érintett tájékoztatása a rá vonatkozó adatkezelésről („hozzáférés”)

6.3.1. Amennyiben az érintett a GDPR 15. cikke szerinti hozzáférési jogával kíván élni, úgy a Szervezet az alábbiakról tájékoztatja:

- az adatkezelés célja, vagy céljai,
- az érintett személyes adatok kategóriái,
- azon címzettek, vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat a Szervezet már közölte, vagy a jövőben közölni fogja,
- a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- a helyesbítési jog gyakorlásának szabályai,
- a törlési jog gyakorlásának szabályai,
- az adatkezelés korlátozására irányuló jog gyakorlásának szabályai,
- a tiltakozási jog gyakorlásának szabályai,
- a Nemzeti Adatvédelmi és Információszabadság Hatósághoz való panasz benyújtásának joga,
- ha a személyes adatok forrás nem az érintett, a forrásra vonatkozó minden elérhető információ,
- amennyiben az adatkezelés automatizált döntéshozatalon alapszik, úgy ennek ténye, valamint az alkalmazott logikára és arra vonatkozó érthető információk.

6.3.2. A Szervezet a fenti tájékoztatás során az adatkezelés tárgyát képező személyes adatok másolatát az érintett kérelmére az érintett rendelkezésére bocsátja.

6.3.3. A 6.2.5. pontban foglaltak miatt a Szervezet egyetlen munkatársa sem ad tájékoztatást a Szervezet által kezelt konkrét személyes adatról telefonos úton.

6.4. Az érintett helyesbítéshez való joga

6.4.1. Amennyiben az érintett személyes adatának helyesbítését kéri és nem áll rendelkezésre a személyes adat, amelyre a már kezelt adatot helyesbíteni kell, hiánypótlásra hívja fel a Szervezet az érintettet.

6.4.2. Amennyiben az érintett személyes adatának helyesbítését kéri és a személyes adat rendelkezésre áll, a Szervezet a személyes adatot helyesbíti és azzal egyidőben írásban tájékoztatja az érintettet a helyesbítés tényéről és időpontjáról.

6.4.3. A Szervezet minden olyan címzettet tájékoztat a helyesbítésről akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

6.5. Az érintett törléshez való joga

6.5.1. A Szervezet az általa kezelt személyes adatot késeledelem nélkül törli, amennyiben az alábbi feltételek egyike megvalósul:

- A személyes adatok már nincs szükség abból a célból, amelyből azt a Szervezet kezeli.
- Az adatkezelés jogalapja az érintetti hozzájárulása és ezt a hozzájárulását az érintett a megfelelően közölt nyilatkozattal visszavonja.
- Az érintett megfelelően közölt nyilatkozattal tiltakozik az adatkezelés ellen.
- A Szervezet tudomására jut, hogy a személyes adat kezelése jogellenes.
- Uniós, vagy hatályos magyar jogban előírt jogi kötelezettség úgy teljesíthető, ha a Szervezet a személyes adatot törli.
- A személyes adat kezelése közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában történt, a hozzájárulást maga a 16. életévét már betöltött gyermek, vagy 16. életévét be nem töltött gyermek feletti szülői felügyeletet gyakorló adta meg és ezt a hozzájárulását az érintett (vagy amennyiben ennek időpontjában 16. életévét továbbra sem töltötte be, úgy a felette szülői felügyeletet gyakorló személy) a megfelelően közölt nyilatkozattal visszavonja.

6.5.2. A személyes adatot a Szervezet olyan módon törli, hogy helyreállítása többé ne legyen lehetséges.

6.5.3. Amennyiben az érintett olyan személyes adatot kíván töröltetni, amely hiányában az érintett és a Szervezet közötti jogviszony nem tartható fenn, a jogviszony megszűnik. Erről azonban a törlés előtt a Szervezet tájékoztatja az érintettet és amennyiben törlési kérelmét fenntartja, a törlés megtörténik. A törlési kérelem fenntartásának minősül, ha a tájékoztatás kézbesítésétől számított 3 napon belül az érintett törlési kérelmét nem vonja vissza.

6.5.4. A személyes adat törlésére az alábbi szabályok közül a felsorolásban előbb szereplő szabályt kell alkalmazni. Amennyiben az alkalmazandó szabály az adott személyes adatra nézve nem értelmezhető, a felsorolásban soron következő szabályt kell alkalmazni:

- a személyes adat kezelésének megszüntetésére vonatkozó kötelező jogszabályi előírás;
- a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet a személyes adatot hordozó papíralapú dokumentum megsemmisítésére vonatkozó előírás,
- a Szervezet iratkezelési szabályzatának a személyes adatot hordozó papíralapú dokumentum megsemmisítésére vonatkozó előírás,
- a Szabályzat konkrét adatkezelésre vonatkozó, adattörlési vagy adatmegsemmisítési GDPR szerinti adattörlési vagy adatmegsemmisítési szabálya.

6.5.5. A Szervezet minden olyan címzettet tájékoztat a törlésről akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

6.6. Az adatkezelés korlátozásához fűződő érintetti jog

6.6.1. Az érintett kérelmezheti a Szervezetnél a rá vonatkozóan tárolt személyes adatok megjelölését jövőbeli kezelésük korlátozása céljából.

6.6.2. A Szervezet az érintett kérelmére akkor korlátozza az adatkezelést, amennyiben az alábbi feltételek egyike fennáll:

- az érintett kérelmében vitatja a rá vonatkozó személyes adatok pontosságát, ebben az esetben a korlátozás arra az időtartamra vonatkozik, ameddig a Szervezet ellenőrzi a személyes adatok pontosságát,
- az adatkezelés jogellenes, de az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,
- bár a Szervezetnek az adatkezelés megkezdése előtt meghatározott cél eléréséhez már nincs szüksége a személyes adat kezelésére, de az érintett kérelmében igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett az 5.7. pont alapján tiltakozik a közérdekű feladat végrehajtására, vagy jogos érdekre hivatkozó jogalappal kezelt személyes adat kezelése ellen, ebben az esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Szervezet jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

6.6.3. Amennyiben a személyes adat kezelését a Szervezet korlátozza, az ilyen személyes adatot a korlátozás időtartama során - a tárolás kivételével - csak az érintett hozzájárulásával vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve a valamely tagállam fontos közérdekéből lehet kezelni.

6.6.4. Amennyiben az adatkezelés korlátozását a Szervezet feloldja, a korlátozás feloldását megelőzően a korlátozás feloldásának tényéről írásban tájékoztatja azt az érintettet, akinek a kérésére a korlátozás megtörtént, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

6.6.5. A Szervezet minden olyan címzettet tájékoztat az adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

6.7. Tiltakozás a személyes adat kezelése ellen

6.7.1. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a közérdekű feladat végrehajtására, vagy jogos érdekre hivatkozó jogalapon alapuló kezelése ellen.

6.7.2. A Szervezet a megfelelően közölt nyilatkozattal történt tiltakozás esetén megvizsgálja, 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.
Amennyiben a Szervezet a vizsgálata során megállapítja, hogy a fenti feltételek egyike sem érvényesül, a tiltakozással érintett személyes adatot nem kezeli tovább.

6.8. Az adathordozhatósághoz való érintetti jog gyakorlása

6.8.1. Amennyiben az adatkezelés jogalapja az érintett hozzájárulása, úgy az érintett jogosult arra, hogy az általa a Szervezet részére átadott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja.

6.8.2. A Szervezet a 6.8.1. szerinti megfelelést elsősorban .xml, .csv vagy .doc formátumban teljesíti a kérelemmel érintett személyes adatok jellegétől függően.

6.8.3. Az érintett kérelmezheti továbbá a Szervezettől, hogy az általa kezelt személyes adatokat egy másik, az érintett által egyértelműen megjelölt adatkezelőnek továbbítsa.

6.8.4. E pontba foglalt jog nem illeti meg az érintettet, ha az adatkezelés közérdekű, vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges, valamint ha ez a jog hátrányosan érintené mások jogait és szabadságait.

6.9. Jogorvoslat

6.9.1. Az érintett a GDPR 77. cikk (1) bekezdése alapján a Szervezet adatkezelési eljárásával kapcsolatos panasszal a NAIH-hoz fordulhat.

6.9.2. Az érintett a GDPR 79. cikk (1) bekezdése szerint a Szervezet adatkezelési eljárásával kapcsolatos jogsértés miatt a lakóhelye vagy tartózkodási helye szerinti törvényszékhez fordulhat.

7. A SZERVEZET ADATVÉDELMI RENDSZERE

7.1. Általános rendelkezések

7.1.1. A Szervezet elnöke a Szervezet sajátosságainak figyelembe vételével e Szabályzatban határozza meg az adatvédelmi előírások megvalósításához szükséges feladat- és hatásköröket.

7.1.2. A Szervezet minden adatkezelése felett a felügyeletet elsődlegesen az adatvédelmi tisztviselő látja el.

7.1.3. Az adatvédelmi tisztviselő Szabályzat szerinti feladatainak ellátásához szükséges mértékben a szervezeti egységek vezetői kötelesek kijelölni a szervezeti egység adatkezelési feladataiért felelős egy, vagy több személyt, aki e tevékenysége ellátása során közvetlenül az adatvédelmi tisztviselővel tartja a kapcsolat, neki köteles jelenteni.

7.1.4. A Szabályzatban előírtak betartatásáért a Szervezet minden munkatársa felelős.

7.1.5. Mindenki köteles gondoskodni 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.

7.2. Az adatvédelmi tisztviselőre vonatkozó szabályok

7.2.1. Az adatvédelmi tisztviselő a jogi tanácsadó közvetlen felügyeletével irányítja és ellenőrzi a Szervezet adatvédelmi és adatbiztonsági rendszerét.

7.2.2. Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a feladatok ellátására való alkalmasság alapján kell kijelölni. Az adatvédelmi tisztviselő a Szervezet munkavállalója lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait.

7.2.3. Adatvédelmi tisztviselővé az elnök a GDPR 37. cikk (5) előírásai alapján olyan személyt nevez ki, aki megfelelő adatvédelmi szakmai rátermettséggel, valamint az adatvédelmi jog és gyakorlat szakértői szintű ismeretével rendelkezik.

7.2.4. A Szervezet a feladatai ellátásához biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint deklarálja, hogy az adatvédelmi tisztviselő az információs önrendelkezési jog biztosítása érdekében végzett feladatai ellátása során utasításokat senkitől sem köteles elfogadni, ezen feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható.

7.2.5. Az adatvédelmi tisztviselő az információs önrendelkezési jog biztosítása során közvetlenül csak a Szervezet elnökének tartozik beszámolási kötelezettséggel. A Szervezet elnöke a beszámoltatási jogot írásban delegálhatja.

7.3. Hatáskörök az adatvédelemmel kapcsolatosan

7.3.1. Az elnök

- felelős az érintettek jogainak gyakorlásához szükséges feltételek biztosításáért,
- 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,
- belső adatvédelmi vizsgálatot rendelhet el,
- kiadja a Szervezet adatvédelemmel kapcsolatos belső szabályzatait,
- különösen súlyos törvénysértés esetén a munkajogi szabályok alapján fegyelmi eljárást indít a személyes adatot jogszabálysértő módon kezelő személy ellen.
- feladatait a jogi igazgatónak delegálhatja.

7.3.2. Az adatvédelmi tisztviselő

- segítséget nyújt az érintettek jogainak biztosításában;
- kezeli az adatvédelmi nyilvántartást és szükség esetén módosítja vagy – új folyamat esetén – kiegészíti azt;
- minden év január 15-ig jelentést készít az elnök részére a Szervezet adatvédelmi feladatainak végrehajtásáról,
- jogosult a Szabályzat betartását bármely szervezeti egységnél ellenőrizni,
- ellenőrzi a GDPR és az adatkezelésre vonatkozó más jogszabályok, valamint a Szabályzat rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását és az ellenőrzés tapasztalatairól tájékoztatja az ügyvezetőt,
- segítséget nyújt a szervezeti egységek számára az adattovábbítási nyilvántartások vezetésében,
- figyelemmel kíséri az adatvédelemmel kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi a Szabályzat módosítását,

- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat GDPR 35. cikk szerinti elvégzését,
- együttműködik a NAIH-hal, az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele,
- általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg,
- kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés vagy annak veszélyének észlelése esetén annak megszüntetésére hívja fel a Szervezetet, vagy az adatfeldolgozót,
- javaslatot tesz a szükséges intézkedésekre az ellenőrzési tapasztalatai és az adatvédelmi előírások megszegéséről készült jegyzőkönyvek alapján,
- felügyeli a külső szervezetektől érkező személyes adatokat érintő megkeresések teljesítését,
- gondoskodik az adatvédelmi ismeretek oktatásáról,
- közreműködik, valamint segítséget nyújt az adatkezeléssel kapcsolatos döntések meghozatalában,
- szükség esetén felvilágosítást nyújt a Szervezet munkatársai számára adatvédelmi kérdésekben,
- véleményezi a Szervezet által kiadandó szabályzatok azon részeit, amelyek adatvédelmi kérdést érintenek,
- ellátja a jogszabályok által ráruházott adatvédelemmel kapcsolatos feladatokat.

7.3.3. A szervezeti egység vezetői
- kötelesek biztosítani és ellenőrizni a vezetésük alá tartozó szervezeti egységnél az adatkezelésre vonatkozó jogszabályok és a Szabályzatban foglaltak betartását,
- intézkednek a külső szervezetektől érkező és a hatáskörükbe tartozó személyes adatokat érintő megkeresések teljesítéséért,
- szabályellenes adatkezelés esetén haladéktalanul intézkednek annak megszüntetéséről, és arról haladéktalanul értesítik az adatvédelmi tisztviselőt,
- kötelesek gondoskodni arról, hogy a Szabályzat előírásait és változásait az általuk irányított munkatársak feladatköreiknek megfelelő részletességgel megismerjék.

7.3.4. Az adatkezelésben érintett munkatársak
- kötelesek a Szabályzat előírásai szerint kezelni a személyes adatokat;
- felelősek feladatkörükben eljárva a személyes adatok a Szabályzat szerinti feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos és követhető dokumentálásáért;
- amennyiben szükséges, előzetesen egyeztetnek a felettesükkel és az adatvédelmi tisztviselővel a személyes adatok kezelését érintő ügyekben;
- a tudomásukra jutott adatkezeléssel kapcsolatos jogsértésekről haladéktalanul tájékoztatják a felettesüket.

7.3.5. Amennyiben az adatvédelmi tisztviselő feladatkörét az elnök látja el, úgy a 7.3.1. pontban gyakorolt hatásköröket az elnökség látja el.

8. ADATBIZTONSÁGI SZABÁLYOK

8.1. A Szervezet, illetőleg tevékenységi körében a Szervezet által megbízott adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a GDPR, valamint a Szabályzat érvényre juttatásához szükségesek.

8.2. A Szervezet az adatbiztonsági folyamatait úgy alakítja ki, hogy azok a személyes adatokat megvédjék a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás, vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

8.3. Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az Infotv., valamint az adatkezelésre vonatkozó külön törvények keretei között a Szervezet határozza meg. Az általa adott utasítások jogszerűségéért a Szervezet felel.

8.4. Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag a Szervezet rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat a Szervezet rendelkezései szerint köteles tárolni és megőrizni.

8.5. A papíralapon kezelt személyes adatok biztonsága érdekében a Szervezet, összhangban a hatályos Iratkezelési 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 személyes adatokat tartalmazó 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 munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;
- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza a Szervezet.

8.6. A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Szervezet összhangban a hatályos Informatikai Biztonsági Szabályzat előírásaival, az alábbi intézkedéseket alkalmazza:

- A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítja, hogy a nyilvántartásokban tárolt adatok - kivéve ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők,
- megfelelő technikai megoldással biztosítja, a jogosulatlan adatbevitel és hozzáférés megakadályozását, részletes, biztonságos és ellenőrizhető hozzáférés-kezelési protokollt alakít ki,
- megfelelő technikai megoldással biztosítja annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az adatfeldolgozó rendszerekbe,
- megfelelő technikai megoldással biztosítja, annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
- megfelelő technikai megoldással biztosítja a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és azt, hogy a feldolgozás során fellépő hibákról jelentés készüljön;
- Az adathordozó eszközök elhelyezésére csak olyan helyiséget jelöl ki, amely elegendő biztonságot nyújt az illetéktelen, vagy erőszakos behatolás, tűz, vagy természeti csapás ellen.
- Az adatállományok kezelése úgy kerül megszervezésre, hogy részleges, vagy teljes megsemmisülés esetén tartalmuk rekonstruálható legyen. Az adatállományok kezelése során a munkaközi mentés eszközével is élni kell. Az adatállományokról másolatot kell készíteni,

hogy az eredeti megsemmisülése, sérülése esetén az adatok továbbra is rendelkezésre álljanak.

9. ADATVÉDELMI INCIDENS KEZELÉSE

9.1. Adatvédelmi incidens észlelése és jelentése

9.1.1 A Szervezet minden munkatársa köteles a tudomására jutott adatvédelmi incidenst haladéktalanul jelenteni az adatvédelmi tisztviselőnek. A jelentésnek legalább az alábbi adatokat tartalmaznia kell:

- az adatvédelmi incidenst észlelő személy neve,
- amennyiben az adatvédelmi incidens észlelő és jelentő személy nem azonos, úgy az adatvédelmi incidenst jelentő személy nevét,
- az adatvédelmi incidens rövid leírását, valamint
- annak tényét, hogy az észlelt adatvédelmi incidens érinti-e a Szervezet informatikai rendszerét vagy sem.

9.1.2. Az adatvédelmi incidens adatvédelmi tisztviselőnek való jelentésének bizonyítható módon kell megtörténnie, ezért a Szervezet az adatvédelmi incidensek jelentésére formanyomtatványt rendszeresít (1. sz. melléklet). A jelentést a formanyomtatvány megfelelő kitöltésével, dátumozásával, aláírásával és iktatásával, belső levélként kell megküldeni az adatvédelmi tisztviselőnek. Amennyiben elháríthatatlan okból kifolyólag az adatvédelmi incidenst észlelő, vagy jelentő személy nem tudja írásban megtenni a jelentés, és ezért szóban tesz jelentést az adatvédelmi tisztviselőnek, úgy az adatvédelmi tisztviselő köteles erről jegyzőkönyvet felvenni, amelynek tartalmaznia kell a legalább az előző pont szerinti információkat. Az akadály megszűnését követően haladéktalanul az adatvédelmi incidenst észlelő, vagy jelentő személy köteles a bejelentést írásban is megerősíteni, azaz a kitöltött formanyomtatványt utólag megküldeni az adatvédelmi tisztviselőnek.

9.1.3. Amennyiben az adatvédelmi incidens érinti a Szervezet informatikai rendszerét is, akkor az adatvédelmi tisztviselő az adatvédelmi incidens kivizsgálásába bevonja a Szervezet informatikai részlegének erre kijelölt munkavállalóját is.

9.1.4. A bejelentés érkezését követően az adatvédelmi tisztviselő – az érintett szervezeti egységek bevonásával – haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését. A kivizsgálásban és értékelésben valamennyi érintett szervezeti egység együttműködni köteles.

9.2. Adatvédelmi incidens kivizsgálása

9.2.1. Az adatvédelmi tisztviselő megvizsgálja a jelentést és amennyiben szükséges, a bejelentőtől, illetve az érintett szervezeti egységek vezetői, munkatársaitól további adatokat kér az incidensre vonatkozóan.

9.2.2. Az adatvédelmi tisztviselő az alábbi információkat (amennyiben azok a jelentésből nem derülnek ki) lehetőségéhez mérten köteles felderíteni:

- az adatvédelmi incidens bekövetkezésének időpontja és helye,
- az adatvédelmi incidens által érintett adatok köre,
- az adatvédelmi incidenssel érintett személyek köre és száma.

9.2.3. Ezen adatokból az adatvédelmi tisztviselő összegzést készít az adatvédelmi incidens várható hatásairól és cselekvési tervet készít a következményeinek enyhítése érdekében, az érintett szakterületek szakmai véleményei és javaslatai figyelembe vételével.

9.2.4. Az adatvédelmi tisztviselő jogosult munkájába bevonni az adatvédelmi incidenssel érintett szervezeti egységek vezetőit és munkatársait, akik kötelesek együttműködni az adatvédelmi tisztviselővel.

9.2.5. A vizsgálatot legkésőbb az adatvédelmi tisztviselőhöz érkezéstől számított 48 órán belül be kell fejezni. A vizsgálat eredményéről és a tervezett további feladatokról az adatvédelmi tisztviselő – a jogi szakértő útján – tájékoztatja az elnököt, vagy az általa kijelölt személyt.

9.3. Adatvédelmi incidens értékelése

9.3.1. A Szervezet az adatvédelmi incidenseket három kategóriába sorolja:
- 1. kategória: valószínűsíthetően kockázattal nem járó incidens
- 2. kategória: valószínűsíthetően alacsony kockázattal járó incidens
- 3. kategória: valószínűsíthetően magas kockázattal járó incidens.

9.3.2. A Szervezet az adatvédelmi incidenst az alábbi szempontok szerint értékeli:
- az incidens típusa (bizalmassági, integritási vagy elérhetőségi),
- a személyes adatok jellege (személyes adat/különleges kategória),
- a személyes adatok száma,
- az érintett személyek száma,
- az érintett természetes személyek kategóriái,
- az érintett természetes személyek azonosíthatósága,
- a természetes személyre nézve fennálló következmények valószínűsége és súlyossága;
- az érintett adatkezelés jogalapja.

9.3.3. A Szervezet az incidens értékelése során az alábbi konkrét szempontokat különös súllyal veszi figyelembe:
- az incidensben érintett adatok között találhatóak a személyes adatok különleges kategóriáiba eső adatok,
- az incidensben érintett személyes adatok száma meghaladja a 100 darabot,
- az incidensben érintett természetes személyek között találhatóak 16. életévüket be nem töltött természetes személyek,
- az incidensben érintett természetes személyek száma meghaladja a 100 főt,
- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre (így különösen lakcím, telefonszám, e-mail cím)
- az incidensben érintett adatkezelés jogalapja a GDPR 6 cikk (1) bekezdés d) pont szerinti jogalap,
- az incidensben érintett adatkezelés jogalapja GDPR 6 cikk (1) bekezdés e) pont szerinti jogalap,
- az incidensben érintett adatkezelés jogalapja GDPR 6 cikk (1) bekezdés f) pont szerinti jogalap,
- a személyes adatok alkalmasak az érintett természetes személy személyazonosságának ellopására vagy a személyazonosságával való visszaélésre,
- az incidensben érintett személyes adatok alkalmasak arra, hogy pénzügyi veszteséget okozzanak az érintettjüknek.

9.3.4. Az incidenst a Szervezet „1. kategória: valószínűsíthetően kockázattal nem járó incidens”-nek minősíti, ha:

- a 9.3.3. pontban felsorolt feltételek közül legfeljebb kettő áll fenn és
- a Szervezet képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

9.3.5. Az incidenst a Szervezet „2. kategória: valószínűsíthetően alacsony kockázattal járó incidens”-nek minősíti, ha:

- a 9.3.3. pontban felsorolt feltételek közül egy áll fenn és
- a Szervezet nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

9.3.6. Az incidens a Szervezet „3. kategória: valószínűsíthetően magas kockázattal járó incidens”-nek minősíti, ha:

- a 9.3.3. pontban felsorolt feltételek közül legalább kettő áll fenn és
- a Szervezet nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

9.3.7. Abban az esetben, ha a kockázat besorolására a NAIH vagy az Európai Adatvédelmi Testület útmutatást ad ki, a Szervezet a 9.3. pontot felülvizsgálja.

9.4. Adatvédelmi incidens bejelentése a NAIH-nak

9.4.1. Amennyiben a Szervezet a 9.3.5. szerint 2. kategóriába vagy 3. kategóriába tartozónak minősíti, úgy az adatvédelmi tisztviselő az értékelés megtörténtét követően, de legkésőbb 72 órával azután, hogy az adatvédelmi incidens a Szervezet tudomására jutott, az adatvédelmi incidenst bejelenti a NAIH-nak.

9.4.2. A NAIH-nak történő bejelentésnek tartalmaznia kell:

- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelmi tisztviselő nevét és elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

9.5. Az érintettek tájékoztatása az adatvédelmi incidensről

9.5.1. Amennyiben az adatvédelmi incidens veszélyességének súlyossága valószínűsíthetően magas kockázattal jár az érintett személyek jogaira nézve, a Szervezet a kockázati értékelés elvégzését követően azonnal tájékoztatja az adatvédelmi incidensben érintetteket.

9.5.2. Az érintettet írásban elektronikusan, vagy postai úton kell tájékoztatni, amely kizárólag akkor mellőzhető, ha az érintett elérhetősége ismeretlen.

9.5.6. Az érintetteket úgy kell tájékoztatni minden esetben, hogy annak ténye, tartalma és a tájékoztatott érintetti kör bizonyítható legyen.

9.6. Helyesbítő-megelőző intézkedések bevezetése

9.6.1. A 9.2. pont szerinti vizsgálat eredménye, valamint az incidens kivizsgálásába bevont szakterületek észrevételi, javaslatai alapján az adatvédelmi tisztviselő javaslatot tesz az elnöknek helyesbítő és/vagy megelőző intézkedések bevezetésére a hasonló adatvédelmi incidensek megelőzése érdekében.

9.6.2. A javasolt helyesbítő és/vagy megelőző intézkedések bevezetéséről az elnök dönt, az adatvédelmi incidenssel érintett szervezeti egységek vezetőinek véleménye alapján.

9.7. Az adatvédelmi incidens nyilvántartása

9.7.1. Az adatvédelmi incidensről az adatvédelmi tisztviselő nyilvántartást vezet a Szabályzat 2. sz. melléklete szerinti nyilvántartó-minta alkalmazásával.

9.7.2. A nyilvántartás tartalmazza:
- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit,
- az adatvédelmi incidens hatásait,
- az elhárítására megtett intézkedéseket,
- az adatvédelmi incidens kivizsgálásának hatására bevezetett helyesbítő-megelőző intézkedéseket.

10. ADATVÉDELMI OKTATÁS

10.1. Az adatvédelmi tisztviselő évente legalább egy alkalommal oktatást tart az adatvédelmi tudatosság emelése érdekében, amelyen kötelesek részt venni a Szervezet kijelölt munkatársai.

Az adatvédelmi oktatásnak legalább az alábbi témákra kell kiterjednie:
- az előző oktatás óta eltelt időszak tapasztalatai az adatvédelem területén
- amennyiben az előző oktatás óta módosult a Szabályzat, a módosítással kapcsolatos legfontosabb tudnivalók,
- az esetlegesen megtörtént adatvédelmi incidens bemutatása, értékelése, a helyesbítő-megelőző intézkedések ismertetése,
- az adatvédelem területén történt általános változások, jogszabály módosítások, Magyarországon és az Európai Unióban, különös tekintettel a hatóságok bírságolási gyakorlatára.

10.2. Az adatvédelmi tisztviselő rendkívüli oktatást tart – amennyiben az indokolt – az alábbi esetekben:
- adatvédelmi incidens megtörténte,
- marasztalással záruló NAIH-eljárás lefolytatása a Szervezettel szemben.
- adatvédelmi bírság kiszabása bármely magyarországi személyszállítási szolgáltatást végző Szervezettel, de elsősorban közlekedési központtal szemben, ha eltérő gyakorlatot igényel a Szervezet adatvédelmi rendszerében.

11. ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA

11.1. A Szervezet minden általa végzett adatkezelési tevékenységről – elektronikusan - nyilvántartást vezet.

11.2. Az adatkezelési tevékenységek nyilvántartása a következő információkat tartalmazza:

- a Szervezet neve és elérhetősége,
- a Szervezet adatvédelmi tisztviselőjének neve és elérhetősége;
- az adatbiztonságra vonatkozó technikai és szervezési intézkedések általános leírása jelen Szabályzat, vagy egyéb, technikai és szervezési intézkedéseket tartalmazó egyéb belső szabályzat vonatkozó pontjára való utalással;
- adatkezelésenként:
    - adatkezelés céljai;
    - az érintettek kategóriái
    - a személyes adatok kategóriái
    - olyan címzettek kategóriái, akikkel a személyes adatokat a Szervezet közli vagy várhatóan közölni fogja,
    - a különböző adatkategóriák törlésére előirányzott határidők, ha lehetséges,
    - adatbiztonsági technikai és szervezési intézkedések általános leírása, ha lehetséges.

11.3. Az adatkezelési nyilvántartást az adatvédelmi tisztviselő tartja naprakészen és módosítja szükség esetén.

11.4. Az adatkezelési nyilvántartás naprakészsége biztosítása érdekében a szervezeti egységek kötelesek minden, az általuk végzett adatkezelési folyamatban bekövetkező változást (módosítás, megszűnés stb.) vagy általuk tervezett új adatkezelési műveletet a tervezett változás vagy a bevezetés előtt legkésőbb 5 munkanappal írásban bejelenteni azt az adatvédelmi tisztviselőnek.

11.5. Az adatvédelmi tisztviselő a 11.4. szerinti bejelentés alapján:

- az érintett adatkezelésre vonatkozó adatokat az adatkezelési tevékenységek nyilvántartásában korrigálja,
- szükség esetén adatvédelmi hatásvizsgálat lefolytatását kezdeményezi.

12. ADATFELDOLGOZÓKRA VONATKOZÓ SZABÁLYOK

12.1. A Szervezet csak és kizárólag olyan adatfeldolgozót vesz igénybe bármely adatkezelési folyamata során, aki, vagy amely megfelelő garanciákat nyújt az adatkezelés GDPR követelményeinek való megfeleléséről és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtásáról.

12.2. A Szervezet minden adatfeldolgozójával adatfeldolgozói írásbeli szerződést köt, amely legalább az alábbi kérdéseket tisztázza:

- az adatkezelés, amelybe a Szervezet az adatfeldolgozót bevonta,
- az adatfeldolgozó által ellátott adatkezelői tevékenység
- az adatfeldolgozás időtartamát, jellegét és célját,
- az adatfeldolgozásra átadott adatok típusa,
- az adatfeldolgozással érintett érintettek kategóriái,
- az adatkezelő jogai és kötelezettségei,

- az adatfeldolgozó jogai és kötelezettségei.

12.3. A Szervezet csak olyan adatfeldolgozóval köt szerződést adatfeldolgozói feladatra, aki az adatfeldolgozói szerződésben vállalja, hogy:

- a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli,
- az általa személyes adatok feldolgozásában résztvevő személyek titoktartási kötelezettséget vállalnak, vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak,
- biztosítja a GDPR 32. cikk szerinti adatbiztonsági szabályokat,
- adatkezelő előzetesen írásban tett eseti, vagy általános felhatalmazása nélkül további adatfeldolgozót nem vesz igénybe,
- az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti a Szervezetet abban, hogy teljesíteni tudja kötelezettségét az érintett 8. pontban foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében,
- adatvédelmi incidens esetén az incidens tudomására jutása pillanatában azonnal értesíti a Szervezetet és együttműködik az adatvédelmi incidens 12. pont szerinti kezelésében,
- az adatfeldolgozási szolgáltatásának nyújtásának befejezését követően a Szervezet döntése alapján minden személyes adatot töröl, vagy visszajuttat a Szervezetnek, valamint a személyes adatokról készült másolatokat ezzel egyidőben megsemmisíti, vagy törli,
- lehetővé teszi és elősegíti, hogy a Szervezet ellenőrizhesse az adatvédelmi szabályok megvalósulását,
- vezeti a GDPR 30. cikk (2) bekezdése szerinti adatfeldolgozói nyilvántartást.

12.4. A jogi szakértő gondoskodik arról, hogy a Szervezet rendelkezésére álljon a GDPR-nak megfelelő tartalmú adatfeldolgozási szerződésminta. Az adatfeldolgozási szerződéseket azok megkötése előtt a vonatkozó belső szabályzatban írtak szerint a jogi szakértő előzetesen véleményeztetni kell.

13. ADATVÉDELMI HATÁSVIZSGÁLAT

13.1. Az adatvédelmi hatásvizsgálat-köteles adatkezelések

13.1.1. Ha a Szabályzat hatályba lépését követően a Szervezet új adatkezelést kíván rendszerébe bevezetni, úgy jelen 16. pont szerint köteles megvizsgálni, hogy az adatkezelés megkezdése előtt köteles-e adatvédelmi hatásvizsgálatot lefolytatni.

13.1.2. A Szervezet adatvédelmi hatásvizsgálatot köteles lefolytatni, ha az alábbi feltételek legalább egyike fennáll:

- az adatkezelés 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,
- az adatkezelés érintett adatok legalább 1000 darab, a személyes adatok különleges kategóriáiba eső adat kezelését valósítja meg,
- az adatkezelés nyilvános helyek nagymértékű, módszeres megfigyelését valósítja meg,
- a 13.1.3. pontba sorolt feltételek közül az adatkezelésre legalább három szempont igaz.

13.1.3. A Szervezet a bevezetendő új adatkezelés hatásvizsgálat-kötelességét az alábbi szempontok alapján ítéli meg:

- az adatkezelésben érintett személyes adatok száma várhatóan meghaladja az 1000 darabot,

- az adatkezelésben érintett természetes személyek között találhatóak 16. életévüket be nem töltött természetes személyek,
- az adatkezelésben érintett természetes személyek száma várhatóan meghaladja az 1000 főt,
- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre (így különösen lakcím, telefonszám, e-mail cím)
- az adatkezelés jogalapja a GDPR 6 cikk (1) bekezdés d) pont szerinti jogalap,
- az adatkezelés jogalapja a GDPR 6 cikk (1) bekezdés e) pont szerinti jogalap,
- az adatkezelés jogalapja a GDPR 6 cikk (1) bekezdés f) pont szerinti jogalap,
- az adatkezelésben érintett személyes adatok alkalmasak az érintett természetes személy személyazonosságának ellopására, vagy a személyazonosságával való visszaélésre,
- az adatkezelésben érintett személyes adatok alkalmasak arra, hogy pénzügyi veszteséget okozzanak az érintettjüknek.

13.1.4. Abban az esetben, ha a Szervezet felügyeleti hatósága összeállítja és nyilvánosságra hozza az adatkezelések olyan típusainak a jegyzékét, amelyekre hatásvizsgálatot kell, vagy nem kell végezni, úgy a 16.1. pontot a Szervezet felülvizsgálja.

13.2. Az adatvédelmi hatásvizsgálat lefolytatása

13.2.1. Az adatvédelmi hatásvizsgálatnak ki kell terjednie:
- a tervezett adatkezelési művelet módszeres leírására és az adatkezelés céljainak ismertetésére,
- ha a tervezett adatkezelés jogalapja a jogos érdekre hivatkozó jogalap, akkor a Szervezet által érvényesíteni kívánt jogos érdekre,
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára,
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára és
- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

13.2.2. A hatásvizsgálatot az adatkezelést bevezetni kívánó szervezeti egység vezetője, vagy az általa ezzel megbízott munkavállaló az adatvédelmi tisztviselő szakmai tanácsának kikérésével köteles elvégezni.

13.2.3. Az adatvédelmi tisztviselő az adatkezelés bevezetését követő hat hónap elteltével köteles megvizsgálni, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

14. ZÁRÓ RENDELKEZÉSEK

14.1. Jelen szabályzat jóváhagyásának napján lép hatályba.

14.2. A szabályzat gazdája

14.2.1. Jelen szabályzat és mellékleteinek elkészítéséért, érvényes állapotban tartásáért és fejlesztéséért az Adatvédelmi tisztviselő felelős.

14.2.2. Jelen szabályzatot legalább évente, vagy jogszabályi változásokat, illetve jelentős szervezeti változásokat követően át kell vizsgálni és aktualizálni kell.

14.2.3. A GDPR változása és/vagy a magyarországi vonatkozó jogszabályok változása esetén a szabályzat aktualizálását teljes körűen és késedelem nélkül el kell végezni.

14.3. A Szabályzat rendelkezéseit a Szervezet többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen Szabályzat és a bármely más, jelen Szabályzat hatálybalépése előtt hatályba lépett szabályzat, utasítás előírásai között, úgy abban az esetben a Szabályzat rendelkezései az irányadóak.

14.4. Amennyiben ellentmondás áll fent jelen Szabályzat és a bármely más, jelen Szabályzat hatálybalépése utána hatályba lépő szabályzat, vagy utasítás előírásai között, úgy csak abban az esetben nem e Szabályzat rendelkezései az irányadóak, ha a később hatályba lépő szabályzat vagy utasítás arról kifejezetten rendelkezik.

Mellékletek:

1. sz. melléklet: Adatmegsemmisítési jegyzőkönyv - minta

2. sz. melléklet: Adatvédelmi incidens jelentő lap - minta

3. sz. melléklet: Adatvédelmi incidens-nyilvántartó lap – minta

Nagy Sándor
elnök

1. sz. melléklet

Adatmegsemmisítési jegyzőkönyv - minta

Iktató szám: ……../20……

ADATMEGSEMMISÍTÉSI JEGYZŐKÖNYV

(Az adatmegsemmisítésért felelős munkavállaló tölti ki!)

Az adatmegsemmisítésért felelős munkavállaló

neve:

beosztása:

törzsszáma:

szervezeti egysége:

A megsemmisítést engedélyezte:

Az adatmegsemmisítéskor jelen lévő háromtagú bizottság tagjai:

1. *(1. bizottsági tag: adatmegsemmisítésért felelős munkavállaló - neve, beosztása)*

2. *(2. bizottsági tag neve beosztása)*

3. *(3. bizottsági tag neve, beosztása)*

Az adatmegsemmisítés helye és időpontja (dátum-óra-perc):

A megsemmisítés tárgya, az adathordozók (megközelítőleges) száma:

(pl.: 2008. január 1-jétől nem használható számlák, számlatömbök; 2014. évben érkezett önéletrajzok stb)

A megsemmisítéssel érintett adatkezelési folyamat megnevezése:

Az adatmegsemmisítés módja

- ❑ iratmegsemmisítő gép
- ❑ égetés
- ❑ zúzás
- ❑ darálás
- ❑ egyéb:

……	……	……
1. bizottsági tag aláírása	2. bizottsági tag aláírása	3. bizottsági tag aláírása

(adatmegsemmisítésért felelős munkavállaló)

2. sz. melléklet

Adatvédelmi incidens jelentő lap - minta

Iktató szám: ……../20……

ADATVÉDELMI INCIDENS JELENTŐ LAP

(lehetőleg az adatvédelmi incidenst észlelő munkatárs töltse ki!)

Az adatvédelmi incidenst bejelentő személy neve: ……,

beosztása: ……, törzsszáma: ……,

szervezeti egysége: ……..

Az adatvédelmi incidens adatai:

- mikor észlelte az adatvédelmi incidenst?: ……. év ….. hó …. nap … óra ….. perc

- hol észlelte az incidens bekövetkezését?: ……..

- hogyan észlelte az incidens bekövetkezését?:

……

……..

- az incidens bekövetkezésének ideje (amennyiben ismeri): ……. év ….. hó …. nap ….. perc vagy: ……. év ….. hó …. nap … óra ….. perc és ……. év ….. hó …. nap … óra ….. perc közötti időszakban

- az incidens rövid leírása:

……

……

……

- Az Ön tudomása szerint milyen személyes adatok érintettek az incidensben?

……

……

- Az észlelt adatvédelmi incidens érinti-e a Szervezet informatikai rendszerét (bármely adatbázisát, levelező rendszerét, személyes adatokat tartalmazó elektronikus dokumentumait, stb.)? IGEN /NEM

Amennyiben az incidens a Szervezet informatikai rendszerét, illetve eszközeit (telefon, mobil telefon, számítógép, stb.) érinti, azt köteles haladéktalanul bejelenteni az Szervezet informatikai vezetőjének is!

Az informatikai vezető értesítése megtörtént-e? IGEN / NEM

Kelt: Mosonmagyaróvár, 20…… év ……. hó …… nap …… perc

……

bejelentő aláírása

3. sz. melléklet

Adatvédelmi incidens-nyilvántartó lap - Minta

……../20…../AVINC

(Értelemszerűen iktatva, például 1/2018/AVINC, azaz a 2018-as év 1-es számú incidense.)

ADATVÉDELMI INCIDENS-NYILVÁNTARTÓ LAP

(Adatvédelmi tisztviselő tölti ki!)

Az adatvédelmi incidens időpontja: ***(****incidens kezdetének dátumától (nap-óra-perc) az incidens végleges elhárításának dátumáig (nap-óra-perc)*

Az adatvédelmi incidens tudomásra jutásának időpontja:

Az adatvédelmi incidenssel érintett szervezeti egység(ek):

Az adatvédelmi incidens észlelésének releváns körülményei:

Az adatvédelmi incidenssel érintett személyes adatok köre:

Az adatvédelmi incidenssel érintettek köre és száma:

Az adatvédelmi incidens körülményeinek leírása:

Az adatvédelmi incidens hatásai:

Az adatvédelmi incidens elhárítására tett intézkedések leírása:

Kelt: Mosonmagyaróvár, 20 ……. év ……. hó …… nap

……

adatvédelmi tisztviselő