A MOSOLY ALAPÍTVÁNY

ADATVÉDELMI SZABÁLYZATA

Közzététel napja: 2019.12.05.

Jóváhagyta és kiadmányozta:

…….
Gallai Zsuzsanna
ügyvezető

1. A SZABÁLYZAT CÉLJA ÉS HATÁLYA

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 Mosoly Alapítvány (a továbbiakban: Adatkezelő vagy Alapítvány) által kezelt személyes adatok védelme, továbbá azok jogosulatlan felhasználásnak megakadályozása érdekében az adatvédelemi előírások és az adatbiztonsági követelmények érvényesüléséhez szükséges szabályokat és az Alapítvány által vezetett nyilvántartások működésének rendjét.

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

2. AZ ADATKEZELÉS ELVEI

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

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

2.2. Célhoz kötöttség elve [GDPR 5. cikk (1) b)]: az Alapítvány 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 az Alapítvány 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 az Alapítvány törli.

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

2.4. Pontosság elve [GDPR 5. cikk (1) d)]: az Alapítvány 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.

2.5. Korlátozott tárolhatóság elve [GDPR 5. cikk (1) e)]: az Alapítvány 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 az Alapítvány.

2.6. Integritás és bizalmasság elve [GDPR 5. cikk (1) f)]: azz Alapítvány 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.

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

3. AZ ADATKEZELÉS JOGALAPJA

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

3.2. Az Alapítvány 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.

3.3. A személyes adatok különleges kategóriáiba tartozó személyes adatot főszabály szerint az Alapítvány csak terápiás tevékenysége során, a szükséges mértékig kezel.

3.4. Az adatkezelés lehetséges jogalapjai személyes adatok esetében

- 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 Alapítványra vonatkozó jogi kötelezettség teljesítéséhez szükséges.
- Az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.
- Az adatkezelés az Alapítvány vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

3.5. 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. Az Alapítvány 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.

3.6. Az Alapítvány 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. Az Alapítvány ennek úgy tesz eleget, hogy elsődlegesen az írásban szerzi be az érintett hozzájárulását, amelyet így az írásbeliséggel tud igazolni.

3.7. Az Alapítvány 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.).

3.8. Az Alapítvány 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 az Alapítvány. Az Alapítvány a visszavonás tényét az adatkezelés során rögzíti, az adatot a továbbiakban nem kezeli, az adat helyét „a hozzájárulás visszavonva” jelzéssel jelöli meg.

3.9. Az Alapítvány természetes személy létfontosságú érdekére hivatkozó jogalappal akkor végez adatkezelést, ha az adott adatkezelés egyéb jogalappal nem végezhető. Az Alapítvány működése során tipikusan a kórházi terápiás foglalkozásokon résztvevő gyermekek adatainak kezelése tartozik ebbe a körbe.

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

4. Az adatkezelés szabályai

4.1. Alapvetések

4.1.1. Az Alapítvány 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.
Az Alapítvány csak úgy folytat adatkezelést, hogy az minden szakaszában megfelel az adatkezelési célnak.

4.1.2. Az Alapítvány 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.

4.1.3. Az Alapítvány munkaszervezési, fizikai, informatikai és jogosultságkezelési eszközökkel gondoskodik arról, hogy illetéktelen személyek a személyes adatokat ne ismerhessék meg.

4.2. A személyes adatokkal kapcsolatos titoktartási szabályok

4.2.1. Az Alapítvány munkatársai és az adatkezelésben résztvevő - annak valamely műveletét végző - adatfeldolgozók kötelesek az adatkezelés során megismert személyes adatokat titokként megőrizni.

4.2.2. 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.

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

4.2.4. Ha az Alapítvány valamely munkatársa a Szabályzatot megszegi, az Alapítvány és közte lévő jogviszony jellegétől függően felelősséggel tartozik.

4.3. A személyes adatok megsemmisítése

4.3.1. Abban az esetben, ha az Alapítvány az általa kezelt személyes adatokat az adatkezelés szabályai alapján a továbbiakban nem kezelheti, köteles a személyes adatokat tartalmazó adathordozót megsemmisíteni, a megsemmisítés tényét pedig megfelelően dokumentálni.

5. AZ ÉRINTETTEK JOGAI

5.1. Az érintett tájékoztatása az adat felvételéhez kapcsolódóan

5.1.1. Abban az esetben, amennyiben az adatkezelés során a személyes adatokat az Alapítvány közvetlenül az érintettől szerzi meg, úgy a személyes adatok megszerzésének időpontjában az alábbiakról tájékoztatja az érintettet:

- az Alapítvány pontos megnevezése, elérhetőségei,
- az Alapítvány adatvédelmi tisztviselőjének neve és elérhetőségei,
- az adatkezelés célja,
- az adatkezelés jogalapja,
- amennyiben az adatkezelés célja a jogos érdek érvényesítése, úgy az Alapítvány vagy a harmadik fél jogos érdekének megnevezése,
- amennyiben az Alapítvány 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.

5.1.2. Amennyiben az Alapítvány a személyes adatot nem közvetlenül az érintettől szerzi meg, úgy az 5.1.1. 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 Alapítvány általi megszerzésének időpontja,
- amennyiben az Alapítvány 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.

5.1.3. Amennyiben az Alapítvány az adatkezelése során az adatot nem közvetlenül az érintettől szerzi meg, az érintettet az 5.1.2. pontban foglaltakról az alábbi időpontban tájékoztatja:

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

5.1.4. A fenti 5.1.1. és 5.1.3. 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 Alapítványra 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.

5.2. Az érintett jogainak érvényesítése

5.2.1. A GDPR 15-21. cikkei szerint az érintett az alábbi jogérvényesítési lehetőségekkel élhet az Alapítvány 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.

5.2.2. Az Alapítvány annak érdekében, hogy az érintettek a jogaikkal élhessenek, részletesen meghatározza az érintetti joggyakorlással kapcsolatos jogokat, kötelezettségeket és eljárási szabályokat.

5.2.3. Az Alapítvány 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.

5.2.4. Az Alapítvány 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 az Alapítvány erre felhatalmazott munkatársa a tájékoztatást szóban is megadhatja.

5.2.5. Az Alapítvány az érintett számára tájékoztatást csak és kizárólag abban az esetben nyújt, ha az Alapítvány erre felhatalmazott munkatársa meggyőződött az érintett személyazonosságáról. Az Alapítvány nem fogadja el a személyazonosítás telefonos úton történő egyetlen formáját sem, így az érintett telefonon nem kezdeményezheti jogainak érvényesítését. Amennyiben a személyazonosság igazolása nem történik meg, az Alapítvány az érintetti joggyakorlási kérelmet elutasítja, és egyben tájékoztatja az érintettet jogai gyakorlásának módjáról.

5.2.6. Az Alapítvány 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 az adatvédelmi tájékoztatóban meghatározott személy számára megteszi
- az írásba foglalt igény az Alapítvány hivatalos címére vagy az erre a célra megadott email címére megérkezik.

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

5.2.7. Az Alapítvány a jelen pontban foglaltak szerinti tájékoztatást és intézkedéseket díjmentesen végzi.

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

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

- az adatkezelés célja vagy céljai,
- az érintett személyes adatok kategóriái,
- azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat az Alapítvány 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.

5.3.2. Az Alapítvány a fenti tájékoztatás során az adatkezelés tárgyát képező személyes adatok másolatát az érintett kérelmére az érintett rendelkezésére bocsátja.

5.3.3. Az 5.2.5. pontban foglaltak miatt az Alapítvány egyetlen munkatársa sem ad tájékoztatást az Alapítvány által kezelt konkrét személyes adatról telefonos úton.

5.4. Az érintett helyesbítéshez való joga

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

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

5.4.3. Az Alapítvány 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.

5.5. Az érintett törléshez való joga

5.5.1. Az Alapítvány 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 az Alapítvány 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.
- Az Alapítvány tudomására jut, hogy a személyes adat kezelése jogellenes.
- Uniós vagy hatályos magyar jogban előírt jogi kötelezettség úgy teljesíthető, ha a Alapítvány 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.

5.5.2. A személyes adatot az Alapítvány olyan módon törli, hogy helyreállítása többé ne legyen lehetséges.

5.5.3. Amennyiben az érintett olyan személyes adatot kíván töröltetni, amely hiányában az érintett és az Alapítvány közötti jogviszony nem tartható fenn, a jogviszony megszűnik. Erről azonban a törlés előtt az Alapítvány 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.

5.5.4. 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,
- az Alapítvány 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.

5.5.5. Az Alapítvány 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.

5.6. Az adatkezelés korlátozásához fűződő érintetti jog

5.6.1. Az érintett kérelmezheti az Alapítványnál a rá vonatkozóan tárolt személyes adatok megjelölését jövőbeli kezelésük korlátozása céljából.

5.6.2. Az Alapítvány 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 az Alapítvány ellenőrzi a személyes adatok pontosságát,
- az adatkezelés jogellenes, de az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,
- bár az Alapítványnak 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 az Alapítvány jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

5.6.3. Amennyiben a személyes adat kezelését az Alapítvány 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.

5.6.4. Amennyiben az adatkezelés korlátozását az Alapítvány 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.

5.6.5. Az Alapítvány 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.

5.7. Tiltakozás a személyes adat kezelése ellen

5.7.1. 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.

5.7.2. Az Alapítvány 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 az Alapítvány a vizsgálata során megállapítja, hogy a fenti feltételek egyike sem érvényesül, a tiltakozással érintett személyes adatot nem kezeli tovább.

5.8. Az adathordozhatósághoz való érintetti jog gyakorlása

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

5.8.2. Az Alapítvány a 6.8.1. szerinti megfelelést elsősorban .xml, .csv vagy .doc formátumban teljesíti a kérelemmel érintett személyes adatok jellegétől függően.

5.8.3. Az érintett kérelmezheti továbbá az Alapítványtól, hogy az általa kezelt személyes adatokat egy másik, az érintett által egyértelműen megjelölt adatkezelőnek továbbítsa.

5.8.4. 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.

5.9. Jogorvoslat

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

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

6. AZ ALAPÍTVÁNY ADATVÉDELMI RENDSZERE

6.1. Általános rendelkezések

6.1.1. Az Alapítvány ügyvezetője az Alapítvány sajátosságainak figyelembe vételével e Szabályzatban határozza meg az adatvédelmi előírások megvalósításához szükséges feladat- és hatásköröket.

6.1.2. Az Alapítvány minden adatkezelése felett a felügyeletet elsődlegesen az adatvédelmi tisztviselő látja el.

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

6.1.4. A Szabályzatban előírtak betartatásáért az Alapítvány minden munkatársa felelős.
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.

6.2. Az adatvédelmi tisztviselőre vonatkozó szabályok

6.2.1. Az adatvédelmi tisztviselő az ügyvezető közvetlen felügyeletével irányítja és ellenőrzi az Alapítvány adatvédelmi és adatbiztonsági rendszerét.

6.2.2. 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 az Alapítvány munkavállalója lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait.

6.2.3. Adatvédelmi tisztviselővé az ügyvezető 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.

6.2.4. Az Alapítvány 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.

6.2.5. Az adatvédelmi tisztviselő az információs önrendelkezési jog biztosítása során közvetlenül csak az Alapítvány kuratóriumának és ügyvezetőjének tartozik beszámolási kötelezettséggel. Az Alapítvány kuratóriuma és ügyvezetője a beszámoltatási jogot írásban delegálhatja.

6.3. Hatáskörök az adatvédelemmel kapcsolatosan

6.3.1. A kuratórium

- felelős az Alapítvány által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért,
- belső adatvédelmi vizsgálatot rendelhet el.

6.3.2. Az ügyvezető

- felelős az érintettek jogainak gyakorlásához szükséges 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 az Alapítvány adatvédelemmel kapcsolatos belső szabályzatait,
- különösen súlyos törvénysértés esetén a munkajogi konzekvenciákat alkalmaz a személyes adatot jogszabálysértő módon kezelő munkavállaló ellen.

6.3.3. 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 ügyvezető részére az Alapítvány 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 az Alapítványt 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 az Alapítvány munkatársai számára adatvédelmi kérdésekben,
- véleményezi az Alapítvány által kiadandó szabályzatok azon részeit, amelyek adatvédelmi kérdést érintenek,
- ellátja a jogszabályok által ráruházott adatvédelemmel kapcsolatos feladatokat.

6.3.4. A szervezeti egységek 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.

6.3.5. 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 felelőssel a személyes adatok kezelését érintő ügyekben;
- a tudomásukra jutott adatkezeléssel kapcsolatos jogsértésekről haladéktalanul tájékoztatják az ügyvezetőt és az adatvédelmi felelőst.

6.4. Munkavállalók, önkéntesek, megbízottak felelőssége

6.4.1. Az Alapítvány önkéntesei és megbízottai polgári jogi és büntetőjogi, az Alapítvány munkavállalói ezen felül munkajogi felelősséggel is tartoznak a munkájuk során végzett adatkezelési műveletek jogszerűségéért és a jelen Szabályzatban foglaltak betartásáért.

6.4.2. Vétkes kötelezettségszegésnek minősül amennyiben a munkavállaló, illetve az önkéntes vagy megbízott nem tartja be a jelen szabályzatban, illetve a személyes adatok kezelésére vonatkozó jogszabályokban foglalt kötelezettségeit. A munkavállalóval szemben ilyen esetben a munkaszerződésében írt hátrányos jogkövetkezmények alkalmazhatóak.

6.4.3. A munkavállaló a jelen szabályzatban, valamint a jogszabályokban foglalt személyes adatok kezelésére vonatkozó kötelezettségének megszegésével okozott kárt köteles megtéríteni, ha nem úgy járt el, ahogy az adott helyzetben általában elvárható.
A kártérítés mértéke nem haladhatja meg a munkavállaló négyhavi távolléti díjának összegét. Szándékos vagy súlyosan gondatlan károkozás esetén a teljes kárt kell megtéríteni.
Nem kell megtéríteni azt a kárt, amelynek bekövetkezése a károkozás idején nem volt előrelátható, vagy amelyet a munkáltató vétkes magatartása okozott, vagy amely abból származott, hogy a munkáltató kárenyhítési kötelezettségének nem tett eleget.

7. ADATBIZTONSÁGI SZABÁLYOK

7.1. Az Alapítvány, illetőleg tevékenységi körében az Alapítvány 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.

7.2. Az Alapítvány 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.

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

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

7.5. A papíralapon kezelt személyes adatok biztonsága érdekében az Alapítvány, összhangban az iratkezelésre vonatkozó belső szabályzatok 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;
- az Alapítvány 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;

- az Alapítvány 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 az Alapítvány.

7.6. A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében az Alapítvány összhangban az informatikai biztonságra vonatkozó belső szabályzatok 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 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,
- Külső – karbantartó vagy fejlesztő – cég alkalmazottja folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet,
- Az elektronikusan kezelt személyes adatok kizárólag olyan esetben nyomtathatók ki, amikor ez kifejezetten szükséges valamilyen jog gyakorlásához vagy kötelezettség teljesítéséhez.

8. ADATVÉDELMI INCIDENS KEZELÉSE

8.1. Adatvédelmi incidens észlelése és jelentése

8.1.1 Az Alapítvány 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 az Alapítvány informatikai rendszerét vagy sem.

8.1.2. Az adatvédelmi incidens adatvédelmi tisztviselőnek való jelentésének bizonyítható módon kell megtörténnie, ezért az Alapítvány 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.

8.1.3. Amennyiben az adatvédelmi incidens érinti az Alapítvány informatikai rendszerét is, akkor az adatvédelmi tisztviselő az adatvédelmi incidens kivizsgálásába bevonja az Alapítvány érintett programozó alvállalkozóját illetve az erre kijelölt munkavállalót is.

8.1.4. 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.

8.2. Adatvédelmi incidens kivizsgálása

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

8.2.2. 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.

8.2.3. 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.

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

8.2.5. 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 tájékoztatja az ügyvezetőt.

8.3. Adatvédelmi incidens értékelése

8.3.1. Az Alapítvány 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.

8.3.2. Az Alapítvány 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.

8.3.3. Az Alapítvány 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.

8.3.4. Az incidenst az Alapítvány „1. kategória: valószínűsíthetően kockázattal nem járó incidens”-nek minősíti, ha:

- a 8.3.3. pontban felsorolt feltételek közül legfeljebb kettő áll fenn és
- a Alapítvány képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

8.3.5. Az incidenst az Alapítvány „2. kategória: valószínűsíthetően alacsony kockázattal járó incidens”-nek minősíti, ha:

- a 8.3.3. pontban felsorolt feltételek közül egy áll fenn és
- az Alapítvány 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.

8.3.6. Az incidens az Alapítvány „3. kategória: valószínűsíthetően magas kockázattal járó incidens”-nek minősíti, ha:

- a 8.3.3. pontban felsorolt feltételek közül legalább kettő áll fenn és
- az Alapítvány 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.

8.3.7. Abban az esetben, ha a kockázat besorolására a NAIH vagy az Európai Adatvédelmi Testület útmutatást ad ki, az Alapítvány a 8.3. pontot felülvizsgálja.

8.4. Adatvédelmi incidens bejelentése a NAIH-nak

8.4.1. Amennyiben az Alapítvány a 8.3.5. 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 az Alapítvány tudomására jutott, az adatvédelmi incidenst bejelenti a NAIH-nak.

8.4.2. 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.

8.5. Az érintettek tájékoztatása az adatvédelmi incidensről

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

8.5.2. Az érintettek írásban elektronikus vagy postai úton kell tájékoztatni, amely kizárólag akkor mellőzhető, ha az érintett elérhetősége ismeretlen.

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

8.6. Helyesbítő-megelőző intézkedések bevezetése

8.6.1. A 8.2. pont szerinti vizsgálat eredménye, valamint az incidens kivizsgálásába bevont szervezeti egységek észrevételi, javaslatai alapján az adatvédelmi tisztviselő javaslatot tesz az ügyvezetőnek helyesbítő és/vagy megelőző intézkedések bevezetésére a hasonló adatvédelmi incidensek megelőzése érdekében.

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

8.7. Az adatvédelmi incidens nyilvántartása

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

8.7.2. 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.

9. ADATVÉDELMI OKTATÁS

9.1. Az adatvédelmi tisztviselő évente legalább egy alkalommal oktatást tart az adatvédelmi tudatosság emelése érdekében, amelyen kötelesek részt venni az Alapítvány 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.

9.2. Az adatvédelmi tisztviselő rendkívüli oktatást tart – amennyiben az indokolt – az alábbi esetekben:

- adatvédelmi incidens megtörténte,
- marasztalással záruló NAIH-eljárás lefolytatása az Alapítvánnyal szemben.
- adatvédelmi bírság kiszabása bármely hasonló tevékenységet végző civil szervezettel szemben, ha eltérő gyakorlatot igényel az Alapítvány adatvédelmi rendszerében.

10. ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA

10.1. Az Alapítvány minden általa végzett adatkezelési tevékenységről – elektronikusan - nyilvántartást vezet.

10.2. Az adatkezelési tevékenységek nyilvántartása a következő információkat tartalmazza:

- az Alapítvány neve és elérhetősége,
- az Alapítvány 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 az Alapítvány közli vagy várhatóan közölni fogja,
    - a különböző adatkategóriák törlésére előirányzott határidők, ha lehetséges,
    - adatbiztonsági technikai és szervezési intézkedések általános leírása, ha lehetséges.

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

10.4. Az adatkezelési nyilvántartás naprakészsége biztosítása érdekében az Alapítványi 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.

10.5. Az adatvédelmi tisztviselő a 10.4. szerinti bejelentés alapján:

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

11. ADATFELDOLGOZÓKRA VONATKOZÓ SZABÁLYOK

11.1. Az Alapítvány 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.

11.2. Az Alapítvány minden adatfeldolgozójával adatfeldolgozói írásbeli szerződést köt, amely legalább az alábbi kérdéseket tisztázza:

- az adatkezelés, amelybe az Alapítvány az adatfeldolgozót bevonta,
- az adatfeldolgozó által ellátott adatkezelői tevékenység
- az adatfeldolgozás időtartama, jellege és célja,
- az adatfeldolgozásra átadott adatok típusa,
- az adatfeldolgozással érintett érintettek kategóriái,
- az adatkezelő jogai és kötelezettségei,
- az adatfeldolgozó jogai és kötelezettségei.

11.3. Az Alapítvány 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 az Alapítványt 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 az Alapítványt és együttműködik az adatvédelmi incidens kezelésében,
- az adatfeldolgozási szolgáltatásának nyújtásának befejezését követően az Alapítvány döntése alapján minden személyes adatot töröl vagy visszajuttat az Alapítványnak, valamint a személyes adatokról készült másolatokat ezzel egyidőben megsemmisíti vagy törli,
- lehetővé teszi és elősegíti, hogy a Alapítvány ellenőrizhesse az adatvédelmi szabályok megvalósulását,
- vezeti a GDPR 30. cikk (2) bekezdése szerinti adatfeldolgozói nyilvántartást.

11.4. Az adatvédelmi tisztviselő gondoskodik arról, hogy az Alapítvány rendelkezésére álljon a GDPR-nak megfelelő tartalmú adatfeldolgozási szerződésminta. Az adatfeldolgozási szerződéseket

azok megkötése előtt a vonatkozó belső szabályzatban írtak szerint az adatvédelmi tisztviselővel előzetesen véleményeztetni kell.

12. ADATVÉDELMI HATÁSVIZSGÁLAT

12.1. Az adatvédelmi hatásvizsgálat-köteles adatkezelések

12.1.1. Ha a Szabályzat hatályba lépését követően az Alapítvány új adatkezelést kíván rendszerébe bevezetni, úgy jelen 12. pont szerint köteles megvizsgálni, hogy az adatkezelés megkezdése előtt köteles-e adatvédelmi hatásvizsgálatot lefolytatni.

12.1.2. Az Alapítvány 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 12.1.3. pontba sorolt feltételek közül az adatkezelésre legalább három szempont igaz.

12.1.3. Az Alapítvány 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.

12.1.4. Abban az esetben, ha az Alapítvány 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 Alapítvány felülvizsgálja.

12.2. Az adatvédelmi hatásvizsgálat lefolytatása

12.2.1. 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 az Alapítvány 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.

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

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

13. ZÁRÓ RENDELKEZÉSEK

13.1. Jelen szabályzat jóváhagyásának napján lép hatályba.

13.2. A szabályzat gazdája

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

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

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

13.3. A Szabályzat rendelkezéseit az Alapítvány 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.

13.4. 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: Adatvédelmi incidens jelentő lap - minta

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

1. sz. melléklet

MOSOLY ALAPÍTVÁNY

ADATVÉDELEMMEL KAPCSOLATOS ESEMÉNY BEJELENTŐ

Az EU 2016/679 számú Általános Adatvédelmi Rendelete (GDPR) szerint 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.
Ha a MOSOLY ALAPÍTVÁNY adatkezelésével kapcsolatban ilyet észlel, kérjük azt jelezze!

Bejelentő elérhetőségei	Kérjük adja meg elérhetőségeit, hogy szükség esetén további tájékoztatást tudjunk kérni Öntől!

Név:	
Email cím:	
Telefonszám:	

Érintettség	Kérjük jelezze érintettségét!

érintett vagyok ☐ alkalmazott vagyok ☐ adatfeldolgozó vagyok ☐ egyik sem ☐

Észlelt esemény	Kérjük minél részletesebben írja le az eseményt!

Időpontja:	
Helye:	
Esemény leírása:	

Dátum: …… Aláírás: ……

☺	Köszönjük, hogy a kitöltéssel segítette a MOSOLY ALAPÍTVÁNY munkáját!

!	Kérjük adja át ezt a bejelentő lapot az Alapítvány bármelyik dolgozójának vagy küldje el a dpo@mosolyalapítvany.hu email címre!

MOSOLY ALAPÍTVÁNY
Adatvédelmi incidens nyilvántartása

Azonosítószám: 201.../...../.....

I. Incidens leírása

Incidens megnevezése	Incidens időpontja, időtartama	Incidens bekövetkezésének a helye (helyszín vagy rendszer)	Az incidensben érintettek köre	Az incidensben érintett személyes adatok köre, száma	Incidens oka

II. Incidens kezelése

Az Incidens hatása	Az incidens elhárítására megtett intézkedések, és azok időpontja	A hátrányos következmények enyhítését célzó intézkedések rövid leírása	Bejegyzés lezárásának időpontja	lezáró neve	aláírása