

ADATVÉDELMI SZABÁLYZAT



Szentendrei Árvácska Állatvédő Egyesület
Szentendre

ÉRVÉNYES: 2023. május 1-től visszavonásig

Tartalomjegyzék

1.	Bevezetés	3
2.	Adatkezelő, Adatvédelmi tisztviselő	3
3.	Fogalom meghatározás	3
4.	A szabályzat célja	3
5.	Az adatkezelés alapelvei	4
6.	Az adatkezelések jogalapjai	5
7.	Az Alapítványok adatkezeléssel érintett főbb tevékenységei	6
8.	Adatfeldolgozás	6
9.	Adattovábbítás	7
10.	Adatkezeléssel kapcsolatos belső szabályok	7
10.1.	Adatvédelmi incidensek kezelése	7
10.1.1.	Információbiztonsági incidensek	7
10.2.	Igazolványok fénymásolása	12
10.3.	Az adatkezeléssel érintett jogok biztosítása	12
10.4.	Az Alapítvány informatikai eszközeinek használata	12
10.5.	Elektronikus levelezőrendszerrel kapcsolatos szabályok	13
10.5.1.	Email fiókkal kapcsolatos teendők a munkavállaló kilépése esetén	14
10.6.	Adatbiztonsági intézkedések szervezeten belül	14
10.7.	Otthoni munkavégzés (Home Office) esetén követendő alapvető adatbiztonsági szabályok	15
11.	Jogorvoslati lehetőségek	16
12.	Egyéb rendelkezések	17

Verziószám	Készítette	Elfogadta	Dátum	Módosítások részletezése
1.0	Cseke András ev.		2023.április	Első verzió

1. BEVEZETÉS

Jelen belső szabályzat célja, hogy rögzítse a Szentendrei Árvácska Állatvédő Egyesület, adatkezeléssel kapcsolatos alapvető tevékenységeit és eljárásait, szabályait.

Amikor a szabályzatban Adatkezelőről, vagy Alapítványról, esik szó, az alatt minden esetben a Szentendrei Árvácska Állatvédő Egyesületet kell érteni.

Az Alapítvány személyes adatkezelés során tiszteletben tartják az érintettek személyhez fűződő jogait, ezért adatkezelése során az alábbi szabályzatban foglaltak értelmében jár el. Az Adatkezelő a Szabályzatnak az időközben módosulandó jogszabályi háttérrel és egyéb belső szabállyal való összehangolása miatti megváltoztatására a jogot fenntartja.

Az adatvédelmi szabályzat mindenkor hatályos változata elérhető az Alapítvány székhelyén.

2. ADATKEZELŐ, ADATVÉDELMI TISZTVISELŐ

A szabályzat szempontjából adatkezelőnek minősül:

Szentendrei Árvácska Állatvédő Egyesület
Nyilvántartási szám: 13 02 0002313

Adatvédelmi kapcsolattartó elérhetősége:

Email: szentendre@arvacska.hu

Az Alapítvány saját belső döntése alapján nem jelöl ki adatvédelmi tisztviselőt, mert tevékenysége nem esik abba a kategóriába, ahol ezen pozíció kijelölése kötelező.

Az adatvédelmi kapcsolattartó ettől függetlenül bármilyen, adatvédelemmel kapcsolatos ügyben kereshető, és az ő feladata eldönteni, hogy külső tanácsadó segítségét igénybe kell-e venni vagy sem.

3. FOGALOM MEGHATÁROZÁS

Jelen szabályzatban használatos adatkezeléssel kapcsolatos fogalmak jelentése elérhető a Nemzeti Adatvédelmi és Információbiztonság Hatóság (a továbbiakban NAIH vagy Hatóság) weboldalán <https://www.naih.hu/adatvedelmi-szotar.html>

4. A SZABÁLYZAT CÉLJA

A jelen szabályzat elsődleges célja, hogy az Adatkezelővel kapcsolatba kerülő természetes személyek adatainak kezelésére vonatkozó alapvető elveket és rendelkezéseket, intézkedési gyakorlatokat meghatározza, annak érdekében, hogy a természetes személyek magánszférája védelemben részesüljön a vonatkozó törvényi előírásoknak és hatósági állásfoglalásoknak megfelelően, valamint további célja annak biztosítása, hogy az Adatkezelő mindenben megfeleljen a hatályos jogszabályok adatvédelemmel kapcsolatos rendelkezéseinek, így különösen, de nem kizárólagosan

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. Törvény
- 2016/679/EU Rendelet (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK Rendelet hatályon kívül helyezéséről
- 2013. évi V. tv. a Polgári Törvénykönyvről - 2012. évi I. tv a Munka Törvénykönyvéről - 2012. évi C. tv. a Büntető Törvénykönyvről - 2003. évi C. tv. az Elektronikus Hírközlésről - 2013. évi CLXV. tv. a Panaszokról és a Közérdekű bejelentésekről
- 2000. évi C. törvény a számvitelről
- A Polgári Törvénykönyvről szóló 2013. évi V. törvény,

- Az adózás rendjéről szóló 2017. évi CL. törvény és végrehajtására kiadott jogszabályok,
- Mt. - A munka törvénykönyvéről szóló 2012. évi I. törvény

Az Adatkezelő tehát kiemelten fontosnak tartja, egyben elkötelezett az iránt, hogy az érintett által rendelkezésre bocsátott személyes adatokat védelemben részesítse, és az érintettek információs önrendelkezési jogát tiszteletben tartsa. E körben a vonatkozó hatályos jogszabályoknak teljeskörűen eleget téve járul hozzá az érintett személyes adatok biztonságos, jogszerű kezeléséhez.

5. AZ ADATKEZELÉS ALAPELVEI

Jelen szabályzat rendelkezése, valamint az Adatkezelő gyakorlata nem lehet ellentétes az adatkezelési elvekkel.

Az adatkezelés törvényi szabályozása következő adatkezelési elveket alkalmazza, amely elvek kötelező rendelkezések és iránymutatásul szolgálnak olyan kérdésekben, amelyeket a jelen szabályzat nem tárgyal.

Jogszerűség, tisztességes eljárás, átláthatóság A személyes adatok kezelése csak jogszerűen történhet. A személyes adatokat tisztességesen és az érintett által átlátható módon kell kezelni. Az adatkezeléssel kapcsolatos információkat pontos, átlátható, érthető és könnyen hozzáférhető formában, egyszerű és érthető nyelvezettel kell megadni.

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

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

Pontosság A vállalkozásoknak tudniuk kell igazolni, hogy az általuk kezelt személyes adatok pontosak és naprakészek. A pontatlan adatokat haladéktalanul törölni vagy helyesbíteni kell. A vállalkozások kötelesek az adatok aktualizálására rutinszerű eljárásokat bevezetni.

Korlátozott tárolhatóság A személyes adatok érintettek azonosítását lehetővé tevő formában történő tárolása az adatkezelés céljának eléréséhez szükséges ideig lehetséges. Továbbá be kell tartani a jogszabályban előírt határidőket is. Vizsgálni kell azt is, hogy az álnevesítésnek vagy anonimizálásnak helye van-e. Az álnevesítés esetében az adatok más információkkal való összekapcsolás nélkül nem rendelkezhetők hozzá az érintetthez. Ennek biztosítására megfelelő technikai és szervezeti intézkedéseket kell bevezetni.

Integritás, bizalmi jelleg Biztosítani kell, az adatok jogosulatlan és jogellenes kezelésének, véletlen elvesztésének, megsemmisülésének, illetve károsodásának megelőzését. Ezért elsősorban IT és szervezeti vonatkozásban (pl.: hozzáférési és jogosultsági eljárásrendek, kódolás) kell megfelelő intézkedéseket foganatosítani, figyelembe véve különösen a 32. cikk (az adatkezelés biztonsága) és 35. cikk (adatvédelmi hatásvizsgálat) rendelkezéseit. Az adatvédelmi incidenseket, azaz a személyes adatok sérelmét, ha fennáll a kockázata annak, hogy az érintettek jogai sérülnek, a 33. cikk értelmében az adatvédelmi hatóságnak be kell jelenteni. Adott esetben – ha a kockázat magas – az érintett személy közvetlenül is értesítendő.

Elszámolhatóság Az elszámoltathatóság alapelveként értelmében a vállalkozásoknak az előzőekben bemutatott alapelveknek való megfelelést tudniuk kell dokumentumokkal alátámasztva igazolni.

6. AZ ADATKEZELÉSEK JOGALAPJAI

Az Adatkezelő kizárólag GDPR rendelet által definiált jogalapok alapján kezel személyes adatokat, melyek a következők lehetnek:

- a) **személyes hozzájárulás:** Amennyiben a személyes adatok kezeléséhez az érintett hozzájárulása szükséges azt Az Alapítvány minden esetben beszerzi írásban, vagy elektronikus formában.

A hozzájárulás önkéntességét biztosítani kell. A GDPR értelmében a hozzájárulás „az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez”.

Hozzájárulásnak minősül az is, ha az érintett Az Alapítvány honlapjának megtekintése során bejelöl egy erre létrehozott négyzetet, amely az adott összefüggésben az érintett önkéntes, tájékoztatáson alapuló hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi. A hallgatás, az előre bejelölt négyzet, előre aláhúzott válasz vagy a nem cselekvés nem minősül hozzájárulásnak.

Az Alapítványnak bármikor igazolnia kell tudni azt, hogy az adatkezelési művelethez az érintett Hozzájárult (elszámoltathatóság elve).

- b) **szereződés teljesítéséhez szükséges jogalap:** 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. Alapítvány nem kötheti szerződés megkötését, teljesítését olyan személyes adatok szolgáltatása feltételül, amelyek nem szükségesek a szerződés teljesítéséhez.

A szerződés előkészítése során, a tervezet kidolgozásakor, véleményezésre megküldése során személyes adat feltüntetésére csak az azonosításhoz szükséges mértékben kerülhet sor.

A szerződésben csak a szerződés érvényességéhez és a teljesítéséhez szükséges személyes adatok kezelhetők.

A szerződésekben külön adatvédelmi záradékot kell feltüntetni, amiben rögzíteni kell a papír alapú, illetve az elektronikus védelmi intézkedéseket a szerződésben szereplő személyes adatok védelmé érdekében.

Az Alapítvány a szerződést kötő partnerét tájékoztatja jelen szabályzatban meghatározott, szerződéskötéshez kapcsolódóan lényeges adatkezelési, adatvédelmi feltételekről.

- c) **jogi kötelezettség teljesítése:** A jogi kötelezettségen alapuló adatkezelés szabályaira – adatkezelés célja, kezelhető adatok köre, tárolás időtartama, címzettek – a vonatkozó jogszabályok rendelkezései irányadók.

A jogi kötelezettség teljesítésén alapuló adatkezelés az érintett hozzájárulásától független. Az érintettel az adatkezelés megkezdése előtt ez esetben közölni kell, hogy az adatkezelés kötelező, továbbá az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a rá vonatkozó jogi kötelezettség alapján kezeli, illetve arról, hogy kik ismerhetik meg az

adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Kötelező adatkezelés esetén a tájékoztatás megtörténhet az előbbi információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

- d) **az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges adatkezelés:** Ezen jogalap a természetes személy életének védelme vagy más kiemelten fontos érdek védelme, veszély megelőzése érdekében alkalmazható. Olyan atipikus helyzetekben alkalmazható, amikor más jogalap nem megfelelő. A létfontosságú érdek, mint jogalap a 9. cikk szerinti tilalom alól is kivételt képez (pl. egészségügyi adat ezen jogalapon történő kezelése esetén), figyelemmel a 9. cikk (2) bekezdés c) pontjára ("az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképzetlensége folytán nem képes a hozzájárulását megadni"). Kivételessége okán ez a jogalap csak szűken értelmezve alkalmazható.

- e) **közhatalmi jogosítvány gyakorlásának keretében végzett feladat:** Az Alapítvány ezen jogalap alapján személyes adatokat nem kezelhet
- f) **Jogos érdek érvényesítés:** Az adatkezelő vagy valamely harmadik fél jogos érdeke teremthet jogalapot az adatkezelésre, feltéve, hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget az adatkezelő (vagy harmadik fél) jogos érdekével szemben, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait.
- Az ilyen jogos érdekről lehet szó például olyankor, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll. A jogos érdek fennállásának megállapításához mindenképpen körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számíthatnak további adatkezelésre. Személyes adatoknak a csalások megelőzése céljából feltétlenül szükséges kezelése szintén az érintett adatkezelő jogos érdekének minősül. **Jogos érdekérvényesítés esetén minden esetben el kell végezni az érdekmérlegelési tesztet, mellyel Az Alapítvány bizonyítja, hogy jogos üzleti érdeke fűződik az adott adatkezeléshez.**

7. AZ ALAPÍTVÁNY ADATKEZELÉSSSEL ÉRINTETT FŐBB TEVÉKENYSÉGEI

A Szentendrei Árvácska Állatvédő Egyesület az alább felsorolt tevékenységek kapcsán végez személyes adatkezelést:

- a) Munkahelyi adatkezelés során, a munkaviszony létesítéséhez, megtartásához és megszüntetéséhez szükséges a kollégák személyes adatainak kezelése.
- b) Ügyfelek, örökbefogadók, támogatók kiszolgálása során szükséges az érintettek személyes adatainak kezelése
- c) Szerződött partnerek (alvállalkozók, beszállítók) szerződésben rögzített személyes adatainak kezelése során
- d) Személy- és vagyonvédelmi okokból üzemeltetett kamerarendszer által végzett képrögzítés során

A fenti tevékenységek során történő adatkezelések részleteiről érintettek tájékoztatása külön dokumentumokban történik.

8. ADATFELDOLGOZÁS

Az Alapítványok bizonyos tevékenységei során adatfeldolgozók szolgáltatásait veszi igénybe.

Az adatfeldolgozás általános feltételei

- Az Alapítvány az adatfeldolgozási tevékenységre írásbeli szerződést köt.
- Az általános szerződési feltétel tartalmát a másik féllel a szerződéskötést megelőzően meg kell ismertetni, és azt a másik félnek el kell fogadnia.
- Amennyiben az adatfeldolgozó ÁSZF (Általános Szerződési Feltételek) dokumentumában megtalálható az adatfeldolgozással kapcsolatos szabályok, akkor új szerződést nem szükséges kötni.

Az adatfeldolgozó számára az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az Adatkezelő felel. Az adatfeldolgozó tevékenységi körén belül, valamint az Adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért. Az Adatfeldolgozókról Az Alapítvány nyilvántartást vezet. **Az adatfeldolgozók nyilvántartása jelen szabályzat mellékletében történik.**

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

9. ADATTOVÁBBÍTÁS

Az adatkezelők a személyes adatokat nem adják tovább, illetve nem teszi hozzáférhetővé az általa kezelt, őrzött személyes adatokat, kivéve:

- a) amennyiben az adattovábbítást jogszabály írja elő (pl. statisztikai adatgyűjtés; munkáltatót terhelő adatszolgáltatási kötelezettség stb.) és az adattovábbítás címzettjeként bíróság, hatóság vagy egyéb állami szerv Az Alapítvány felé hivatalos megkeresését eljuttatja. Ilyen esetben Az Alapítvány a meghatározott terjedelemben, a megkeresés teljesítéséhez szükséges mértékben biztosítja az általa tárolt személyes adatok továbbítását.
- b) amennyiben az adattovábbításhoz az érintett kifejezett hozzájárulását adta, és ha az adatkezelés feltételei és garanciái minden egyes továbbítandó személyes adatra nézve teljesülnek. Ebben az esetben köteles tájékoztatni az érintettet:
 - a. az adattovábbítás címzettjének, valamint képviselőjének nevééről, elérhetőségéről;
 - b. arról, hogy az adattovábbítással kapcsolatos tájékoztatás ismeréséhez és az adattovábbításhoz hozzájárul;
 - c. az adattovábbítás pontos céljáról, konkrét terjedelméről;
 - d. a személyes adat jogosultját megillető jogokról;
 - e. a Hatóságnak címzett panasz, vagy bírósági jogorvoslat előterjesztésének lehetőségéről.

10. ADATKEZELÉSEL KAPCSOLATOS BELSŐ SZABÁLYOK

10.1. ADATVÉDELMI INCIDENSEK KEZELÉSE, AZ EZZEL KAPCSOLATOS ELJÁRÁS, SZABÁLYOK

Az esetlegesen bekövetkező adatvédelmi incidens kezelésére az alábbi eljárásrendet kell alkalmazni.

FONTOS: Adatvédelmi, információbiztonsági incidens gyanúja esetén mindenképp javasolt szakember segítségével kivizsgálni azt!

Tipikus adatvédelmi, információbiztonsági incidensek lehetnek az alábbiak, melyeket minden esetben szükséges kivizsgálni

- Elhagyott laptop, mobiltelefon
- Irodai vagy akár otthoni betörés (home office esetén)
- Nem megfelelő iratselejtezés (kukába kerülnek a papírok megsemmisítés nélkül)
- Hacker támadás
- Rossz helyre küldött email vagy levél, mely tartalmat személyes adatokat
- Rosszul beállított megosztás miatt bizalmas adatokhoz hozzáférhetnek illetéktelenek.

10.1.1. INFORMÁCIÓBIZTONSÁGI INCIDENSEK

Az információbiztonsági incidensek olyan nem kívánt vagy nem várt, egyedi vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel veszélyeztetik az üzleti tevékenységet és fenyegetik az információbiztonságot.

Információbiztonsági incidensek jellemző előfordulásai:

- A szolgáltatás, a berendezés vagy az eszközök elvesztése;
- A rendszer hibás működése vagy túlterhelések (DDos-támadás);
- Emberi hibák;
- Szabályzatoknak vagy irányelveknek való nem-, vagy hiányos megfelelés;
- A fizikai biztonsági rendelkezések megsértése;
- A rendszert érintő előre nem ellenőrzött változások;
- A szoftver vagy hardver hibás működése;
- Hozzáférési sértések.
- Rosszindulatú kód;
- Nem teljes vagy nem pontatlan működési adatokból eredő hibák;
- A bizalmasság és sértetlenség megsértése;
- Az információrendszerekkel való visszaélés

10.1.2. SZEMÉLYES ADATOKAT ÉRINTŐ (ADATVÉDELMI) INCIDENSEK

Adatvédelmi incidensnek minősül a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését, az azokhoz való jogosulatlan hozzáférést vagy a jogosultak számára a hozzáférhetetlenné férést eredményezi.

Személyes adatok kezelésében érintett adatvédelmi incidensnek általános példái:

- Személyes adatok akár papíralapú dokumentumon, akár bármilyen elektronikus hordozható eszközön, adathordozón vagy egyéb informatikai rendszeren, például email forgalomban, felhő alapú tárterületen vagy egyéb azonnali üzenetküldő alkalmazással (Facebook, Instagram, Viber, Twitter, WhatsApp stb.) történő nem az adatkezelés céljával és érintetteivel összeegyeztethető továbbítása.

- Illetéktelen hozzáférések személyes adatokat kezelő informatikai rendszerhez vagy alkalmazáshoz. Általános esete például jelenlegi vagy volt alkalmazott véletlen vagy tudatos közreműködése által, vagy biztonsági rések kihasználásával történő illetéktelen hozzáférés, törlés, megváltoztatás, illetve eltulajdonítás-másolás.

- Személyes adatokat tartalmazó adatbázis részének vagy egészének sérülése vagy elvesztése. Általános példa az adathordozók elvesztése, vagy olyan eszközök meghibásodása, vagy vírusfertőzése, melyen személyes adatok kezelése folyik rendszeres biztonsági mentés nélkül.

- Az informatikai rendszer részének vagy egészének hozzáférési rendjének előre nem várt változása, mely következményeként a rendelkezésreállítás sérül. Ennek kiváltó okai legtöbbször az eszközök meghibásodása, valamint vírus vagy egyéb rosszindulatú szoftvertámadás.

Minden ilyen behatás esetén, melyben előre nem tervezett módon módosul a személyes adatok bizalmassága, sértetlensége vagy rendelkezésre állása köteles Az Alapítvány az esetet kivizsgálni, az incidensnyilvántartásban rögzíteni és a bejelentés szükségességéről dokumentált értékelést és döntést hozni a jelen szabályzat megkötéseinek értelmében.

10.1.3. FELELŐSSÉGI KÖRÖK

Az adatvédelmet sértő események megelőzése és kezelése vállalat vezetőjének felelőssége és feladata. Minden szervezeti egység vezetője felelős a feladatkörébe tartozó szakterületen észlelt adatvédelmet sértő esemény ismételt előfordulásának megelőzéséhez szükséges intézkedések megtételéért, a bekövetkezett esemény feltárásáért, szükség esetén annak dokumentálásáért, továbbá indokolt esetben a felelősségre vonással és a hiányosságok megszüntetésével kapcsolatos intézkedések kezdeményezéséért és megvalósításuk ellenőrzéséért

Az értékelésnek ki kell térni különösen az alábbiakra:

- a) az incidens bekövetkezésének időpontja és helye,
- b) az incidens leírása, körülménye, hatásai,
- c) az incidens során kompromittálódott adatok köre, számossága,
- d) a kompromittálódott adatokkal érintett személyek köre,

- e) az incidens elhárítása érdekében tett intézkedések leírása,
- f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírása.

Az adatvédelmi incidensekről nyilvántartást kell vezetni, melynek tartalmaznia kell az alábbiakat:

- a) az érintett személyes adatok körét,
- b) az adatvédelmi incidenssel érintettek körét és számát,
- c) az adatvédelmi incidens időpontját,
- d) az adatvédelmi incidens körülményeit, hatásait,
- e) az adatvédelmi incidens orvoslására megtett intézkedéseket,
- f) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat 5 évig meg kell őrizni.

10.1.4. ELJÁRÁSREND ADATVÉDELMI INCIDENS ESETÉN

- 1) Adatvédelmi tisztviselőt haladéktalanul értesíteni kell.
- 2) Adatvédelmi incidens észlelésekor az azt észlelő személy köteles haladéktalanul részletes tájékoztatásban részesíteni közvetlen felettesét, aki erről késedelem nélkül köteles tájékoztatni az adatvédelemi döntéshozatalért felelős vezetőt. Amennyiben nincs erre kijelölt személy, vagy adatvédelmi tisztviselő, úgy a felelős cégvezetőt kell tájékoztatni az incidens bekövetkeztéről.
- 3) Az adatvédelemért felelős vezetőnek amennyiben az incidens jellege és körülményei indokolják (a szabályzat folytatásában lefektetett elvek szerint történő értékelését követően) eleget kell tennie jelentéstételi kötelezettségeinek úgy a hatóság, mint az incidensben érintett természetes személyek irányába egyaránt. Jelen szabályzat 2. számú melléklete tartalmazza az incidens dokumentálásához kötelezően összegyűjtendő adatokat.
- 4) Amennyiben a kezelt adatok relációjában Az Alapítvány adatfeldolgozónak minősül, úgy az észlelést követően a lehető leghamarabb, indokolatlan késedelem nélkül köteles - dokumentált formában - értesíteni annak bekövetkeztéről a felelős adatkezelőt, vagy az adatfeldolgozói láncolatban felette álló adatfeldolgozót.
- 5) Amennyiben, mint adatfeldolgozó észleli az incidenst azt köteles jelenteni az adatkezelő irányába és ezt követően pedig köteles a törvényes keretek adta minden rendelkezésére álló lehetőséggel élve támogatni az adatkezelőt annak kivizsgálásában és enyhítésében.
- 6) Amennyiben Az Alapítvány, mint adatkezelő szenved el az adatvédelmi incidenst, úgy amennyiben az incidens körülményei ezt indokoltá teszik az észlelést (bejelentést) követően a lehető leghamarább, indokolatlan késedelem nélkül, de legkésőbb 72 órán belül az incidenst jelenteni kell a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH).
- 7) Minden incidenst dokumentálni szükséges, attól függetlenül, hogy bejelentési kötelezettséggel bír e vagy sem. A dokumentációnak a következő adatokat szükséges tartalmaznia:
- 8) Az adatvédelmi incidens jellegét, beleértve az érintettek kategóriáit és hozzávetőleges számát, a lehető legpontosabban, amit a rendelkezésre álló technológia és szaktudás birtokában elérhető Az Alapítvány számára.
- 9) Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kontaktszemély nevét, email címét és telefonszámát.
- 10) Az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- 11) Az incidens okozta lehetséges károk orvoslására tett vagy tenni kívánt lépéseket, mellyel célja az adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az adatvédelemért felelős vezető, illetve amennyiben az incidens informatikai eszközzel kapcsolatba hozható, akkor az adatvédelemért felelős vezető és az informatikáért felelős munkatárs, vagy megbízott szolgáltató feladatai a továbbiak:

- Az adatvédelmi incidens rögzítése, bejelentése, az incidenssel kapcsolatos további adatok, információk begyűjtése.
- Adatvédelmi incidens lehetséges hatásának és következményeinek felmérése Az Alapítvány, illetve az érintettek jogai szempontjából.
- A megtámadott információs rendszer és/vagy hálózat leválasztásának lehetővé tétele ezzel megszakítva a támadás / fertőzés terjedését.

- Az üzleti szempontból kritikus szolgáltatások, rendszerek helyes működésének biztosítása.
- A kapcsolódó folyamatok / tevékenységek felelőseinek értesítése az incidensről.
- Az incidens hatását, és az incidenskezelés módját, lépéseit meghatározó szakértői team összehívása. Feladatuk az incidenssel kapcsolatos minden információ felderítése, bizonyítékok további gyűjtése, majd a szükséges technikai és szervezési intézkedések meghatározása és fogantatása.
- A feltárt eredmények dokumentálása az Adatvédelmi incidensek nyilvántartásában.
- Az adatvédelmi incidens kiértékelésének eredményéről tájékoztatni kell a hatóságot.

10.1.5. TÁJÉKOZTATÁSI KÖTELEZETTSÉGEK

Annak megállapítását követően, hogy adatvédelmi incidens történt, a Rendelet két fél tájékoztatását írja elő. Ezek a következők:

1. Felügyeleti hatóság
2. Érintettek

Az incidenst „a természetes személyek jogaira és szabadságaira” gyakorolt kockázat értékelésétől függően kell jelenteni, ezért annak bekövetkezte esetén mindig szükségszerű elvégezni az abban rejlő kockázatok értékelést.

Az Adatkezelő továbbá köteles dokumentált formában rögzíteni, hogy az incidens rendelkezik-e az érintett Hatóság felé bejelentési kötelezettséggel, tekintetbe véve a szabályzat folytatásában rögzített bejelentéselbírálási eljárás kritikus kérdéseit.

FELÜGYELETI HATÓSÁG

A Rendelet alapján Adatkezelőnek a Nemzeti Adatvédelmi és Információszabadság Hatósággal szükséges felvennie a kapcsolatot személyes adatok kezelését érintő adatbiztonsági kérdésekben, melyet a következő elérhetőségein tehet meg:

Hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság

Web: www.naih.hu

Incidensbejelentő rendszer <http://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html>

AZ ÉRINTETT TÁJÉKOZTATÁSA AZ ADATVÉDELMI INCIDENSRŐL

Amennyiben Az Alapítvány a kezelt személyes adatok vonatkozásában, mint Adatkezelő vesz részt, és a bekövetkezett adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve, az adatkezelő indokolatlan késedelem nélkül, világos, közérthető, az érintettek számára értelmezhető megfogalmazásban (például külföldi érintettek esetében a magyar nyelvű tájékoztatás nem elégséges) tájékoztatni köteles az érintettet az adatvédelmi incidens őt érintő minden részletéről.

Ezen tájékoztatónak minimum a következő adatokat kell tartalmaznia:

- Az adatvédelmi incidens jellegét,
- Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb munkatárs nevét és elérhetőségeit,
- Az adatvédelmi incidensből eredően lehetséges következményeket,
- Az adatkezelő által az adatvédelmi incidens orvoslására tett vagy előirányzott intézkedéseket, beleértve adott esetben az incidensből eredő kárenyhítést célzó lépéseket.

DÖNTÉS ARRÓL, HOGY KELL-E ÉRTESSÍTENI A FELÜGYELETI HATÓSÁGOT

A Rendelet kimondja, hogy az adatkezelési incidenst be kell jelenteni a felügyeleti hatóságnak, „kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve”.

Ennek alapján Adatkezelő köteles értékelni az adatvédelmi incidens által jelentett kockázat szintjét és mértékét, mielőtt dönt arról, hogy tesz-e bejelentést.

A kockázatértékelés körében többek között az alábbi szempontokat érdemes figyelembe venni:

- az incidens jellege;
- az incidenssel érintett személyes adatok természete, érzékenysége és mennyisége;
- egyéb, relevánsnak tekintett tényezők (ideértve különösen, de nem kizárólagosan az incidens hatásának értékelését).

A fenti kockázatértékelés elvégzésére, a bejelentéssel kapcsolatos döntés végrehajtása, a megfelelő dokumentáció elkészítése, és az érintettek felé kapcsolattartás és a részükről felmerülő további kérdések megválaszolása és ügyek intézésére Adatkezelő vezetője felelőst nevez ki.

A kockázatértékelés módját, az indokolást és a következtetéseket dokumentálni kell, és azt a felső vezetésnek kell az aláírásával ellátnia. A kockázatértékelés eredményének az alábbi következtetések egyikét kell tartalmaznia:

- Az adatvédelmi incidens nem igényel bejelentést
- Az adatvédelmi incidenst csak a felügyeleti hatóságnak kell bejelenteni
- Az adatvédelmi incidenst a felügyeleti hatóságnak és az érintetteknek egyaránt be kell jelenteni

A FELÜGYELETI HATÓSÁGI BEJELENTÉS MÓDJA

Amennyiben a döntés alapján bejelentést kell tenni a felügyeleti hatósághoz, a Rendelet megköveteli, hogy azt „indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott” kell megtenni. Ha jogszerű indok alapján a bejelentést nem teszik meg az előírt határidőn belül, az indokot fel kell tüntetni a bejelentésben.

A bejelentést az illetékes adatvédelmi hatóság felé megfelelően, és biztonságos módon kell megtenni.

DÖNTÉS MEGHOZATALA AZ ÉRINTETTEK TÁJÉKOZTATÁSI KÖTELEZETTSÉGÉRŐL

A Rendelet kimondja, hogy az adatkezelési incidensről tájékoztatni kell az érintettet, „ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”.

A Rendelet akkor nem követeli meg az érintettek tájékoztatását, ha az „aránytalan erőfeszítést tenne szükségessé”. Ilyen esetekben azonban az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni.

AZ ÉRINTETTEK TÁJÉKOZTATÁSÁNAK MÓDJA

Miután döntés született arról, hogy az incidens indokolja az érintettek tájékoztatását, a Rendelet alapján a tájékoztatást indokolatlan késedelem nélkül kell megtenni.

AZ ÉRINTETTEKNEK ADOTT TÁJÉKOZTATÁSBAN „VILÁGOSAN ÉS KÖZÉRTHETŐEN ISMERTETNI KELL AZ ADATVÉDELMI INCIDENS JELLEGÉT” ÉS A KÖVETKEZŐKET:

- a) az incidens részleteiről további tájékoztatást nyújtó kapcsolattartó nevét és elérhetőségét;
- b) az adatvédelmi incidensből eredő, valószínűsíthető következmények leírását; és
- c) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az esetleges hátrányos következmények enyhítését célzó intézkedéseket.

10.2. IGAZOLVÁNYOK FÉNYMÁSOLÁSA

Fő szabályként Az Alapítvány – betartva az adattakarékosság, és a célhoz kötött adatkezelés elvét- nem **másol igazolványokat, és nem tárol semmilyen személyes iratról fénymásolatot**, mely alól kivételt képeznek az olyan tevékenységek, ahol a személyes iratok másolatát jogi kötelezettség teljesítése végett a hatóságoknak szükségük átadni.

Amennyiben bármilyen szolgáltatás nyújtásához az érintett személyazonosságának igazolása szükséges, abban az esetben az igazolvány felmutatásával Az Alapítvány meggyőződik az egyén kilétéről, és szükség esetén annak azonosítóját, valamint az adatkezelési cél megvalósulásához szükséges egyéb adatokat rögzíti.

10.3. AZ ADATKEZELÉSEL ÉRINTETT JOGOK BIZTOSÍTÁSA

Az adatkezeléssel érintetteket számos, a 11.pontban bővebben kifejtett jogok illetik meg, mely jogok biztosítását Az Alapítvány kiemelten fontosnak tartja, így minden érintetti joggyakorlással kapcsolatos megkeresést írásban rögzít, és igyekszik a kérésnek a lehető legrövidebb határidőn belül eleget tenni. Továbbá az üzletvitellel kapcsolatban olyan technikai és szervezési intézkedéseket alkalmaz, melyek biztosítják a jogorvoslat lehetőségét, mint pl:

- Adatkezeléssel kapcsolatos megkeresések esetére jelen szabályzatban elérhetőséget tüntet fel.
- Informatikai rendszeréből -kérés esetén- az érintettre vonatkozó összes személyes adatot törölni, vagy zárolni tudja
- Adatvédelemmel kapcsolatos kérdések, kérések esetén a megfelelő hozzáértő személy tanácsát kikéri.
- Panasz esetén törekszik az érintettel való megegyezésre, vele teljes mértékben együttműködik.

10.4. AZ ALAPÍTVÁNY INFORMATIKAI ESZKÖZEINEK BIZTONSÁGOS HASZNÁLATA

Az Alapítvány jelen szabályzattal előírja, hogy az általa biztosított számítástechnikai vagy elektronikus eszközt így különösen számítógépet, laptopot, tabletet a munkavállaló kizárólag a munkavégzéshez használhatja, ezek magáncélú használatát Az Alapítvány nem engedélyezi, ezen eszközökön a munkavállaló semmilyen személyes adatot, levelezését nem kezelhet és nem tárolhat.

Az elektronikai eszközök időszakos mentéséről gondoskodni kell, megelőzően az érintetteket fel kell hívni, hogy esetleges személyes adataikat távolítsák el az adathordozókról.

Az Alapítvány által biztosított mobil adathordozókon kívül egyéb eszköz nem csatlakoztatható, Az Alapítvány informatikai eszközeihez, jelszavas védelmi ellenőrzéssel biztosítani kell az idegen eszközök használatának kizárását.

Az informatikai eszköz javítására Az Alapítvány rendszergazdája intézkedik, amennyiben ő nem tudja megjavítani, úgy a javítás idején jelen kell lennie, hogy személyes adat jogosulatlanul ne kerülhessen ki az informatikai eszköz adathordozójáról. A harmadik személy által végzett javítás idején akkor lehet az informatikus távol, ha adathordozót (winchestert) nem ad át, vagy a harmadik személy igazolja, hogy az általa folytatott tevékenység a GDPR rendeletnek megfelel, és titoktartási nyilatkozatot tesz.

Az informatikai eszköz selejtezését, értékesítését megelőzően gondoskodni kell az adathordozó fizikai megsemmisítéséről.

A jogviszony megszűnését megelőzően a munkavállaló gondoskodik arról, hogy az esetlegesen informatikai eszközön lévő magáncélú adatait törölje. A jogviszony megszűnését követően a Alapítvány az informatikai eszközön tárolt személyes adatokat megsemmisíti.

A munkavállaló köteles 24 órán belül bejelenteni Az Alapítvány vezetője részére, ha informatikai eszközét elvesztette és közölni, hogy az eszközön megközelítőleg hány, és milyen jellegű

személyes adat volt.

A távmunkavégzés Az Alapítvány által rendelkezésre bocsátott informatikai eszköz felhasználásával engedélyezhető. A távmunkavégzés esetén a munkavállalót tájékoztatni kell Az Alapítvány általi ellenőrzés és az informatikai eszköz használata korlátozásának szabályairól.

Az informatikai eszközök védelméről a rendszergazda gondoskodik, amelynek során megfelelő intézkedéseket tesz annak érdekében, hogy az eszköz elvesztése esetén a tárolt személyes adatokhoz ne lehessen hozzáférni.

10.5. ELEKTRONIKUS LEVELEZŐRENDSZERREL KAPCSOLATOS SZABÁLYOK

A munkavállaló az elektronikus levelezőrendszert magán célra nem használhatja, a fiókban személyes leveleket nem kezelhet.

Az Alapítvány elektronikus levelezőrendszerének informatikai védelméről a rendszergazda gondoskodik.

Az elektronikus levelezőrendszer használata során az érintett munkavállaló köteles megfelelő körültekintéssel eljárni, mind a címzettek megadása, titkos másolatok alkalmazása, mind a dokumentumok csatolása során. Ügyelni kell arra, hogy a címzettek és másolatot kapó személyhez kapcsolódó elektronikus levelezési cím is személyes adat.

Az elektronikus levelezés során törekedni kell a személyes adatok titkosítására.

A dokumentumok tervezeteit személyes adatok feltüntetése nélkül kell egyeztetésre küldeni.

A munkahelyi levelezőrendszer használata kizárólag munkahelyi eszközökön engedélyezett.

A munkáltató jogosult az e-mail fiók tartalmát és használatát rendszeresen ellenőrizni. Az ellenőrzés célja az e-mail fiók használatára vonatkozó munkáltatói rendelkezés betartásának ellenőrzése, továbbá a munkavállalói kötelezettségek teljesítésének ellenőrzése.

Az ellenőrzésre és adatkezelésre a munkáltató vezetője, vagy a munkáltatói jogok gyakorlója jogosult.

Lehetőség szerint biztosítani kell, hogy a munkavállaló jelen lehessen az ellenőrzés során, távollétében két személy jelenlétében jegyzőkönyvet kell felvenni a tapasztalatról.

Az ellenőrzés megkezdése előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre, munkáltató részéről, ki végezheti az ellenőrzést, - milyen szabályok szerint kerülhet sor és mi az eljárás menete, - milyen jogai és jogorvoslati lehetőségei vannak az ellenőrzés eredményével kapcsolatban.

Az ellenőrzés során a fokozatosság elvét kell érvényesíteni, így elsődlegesen levél címéből és tárgyából kell következtetést levonni arra vonatkozóan, hogy az a munkavállaló munkaköri feladatával kapcsolatos, és nem személyes célú. A nem személyes célú e-mailek tartalmát Az Alapítvány korlátozás nélkül vizsgálhatja.

Amennyiben megállapítható, hogy a munkavállaló az elektronikus levelezőrendszert személyes célra használta, fel kell szólítani, hogy a személyes adatokat haladéktalanul törölje.

A munkavállaló távolléte, vagy együttműködésének hiánya esetén a személyes adatokat az ellenőrzéskor a munkáltató törli.

Az elektronikus levelező rendszer jelen szabályzatba ütköző használata miatt Az Alapítvány a munkavállalóval szemben, az Mt. 56. § alapján, a munkaszerződésben rögzített jogkövetkezményeket alkalmazhat.

A munkavállaló az elektronikus levelezőrendszer ellenőrzésével együtt járó adatkezeléssel kapcsolatban jelen szabályzatnak az érintett jogairól szóló részében írt jogokat gyakorolhatják.

A jogviszony megszűnését megelőzően a munkavállaló gondoskodik arról, hogy az esetleges magáncélú leveleit törölje. A jogviszony megszűnését követően Az Alapítvány az elektronikus levelezőrendszerben tárolt személyes adatokat megsemmisíti.

Az a munkavállaló, aki a levelezőrendszer működésében rendellenességet észlel, vagy olyan személyes adat válik számára hozzáférhetővé, amelynek megismerésére nem jogosult, köteles azonnal jelezni a rendszergazda, és Az Alapítvány vezetője felé.

10.5.1. EMAIL FIÓKKAL KAPCSOLATOS TEENDŐK A MUNKAVÁLLALÓ KILÉPÉSE ESETÉN

- Amikor a személyzet egyik tagja elhagyja a céget, lehetőséget kell számára biztosítani a személyes e-mailjei összegyűjtéséhez. Ennek azt megelőzően kell megtörténnie, hogy az érintett ténylegesen távozna a cégtől, ennek végrehajtására és felülvizsgálatára egy megbízható személy kijelölése javasolt. A személyes email-ek összegyűjtésének és átadásának tényét dokumentálni kell.
- A kilépő munkavállalóval közösen a folyamatban lévő ügyekkel kapcsolatos levelezéseket továbbítani kell abba a postafiókba, aki cégen belül tovább viszi az ügyeket.
- Kilépés után Az Alapítványnak aktiválnia kell egy automatikus üzenetet, mely tájékoztatja a levélírókat, hogy az érintett személy már nem dolgozik a cégnél, illetve megadja egy másik illetékes személy elérhetőségét, akihez kérdéseikkel fordulhatnak. A munkavállaló távozásáról tájékoztató automatikus válaszüzenetnek alapesetben egy hónapig üzemelni javasolt, mely szükség esetén 3 hónapig meghosszabbítható.
- Az automatikus válaszüzenet maximális időtartamának (3 hónap) elérése után az e-mail fiókot törölni kell.

10.6. ADATBIZTONSÁGI INTÉZKEDÉSEK SZERVEZETEN BELÜL

Alapítványunk rendelkezik IT biztonsággal kapcsolatos szabályzattal, mely részletesen összefoglalja azokat az intézkedéseket, melyeket többek között a személyes adatok védelme érdekében alkalmazunk.

Az Adatkezelő az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

Az Adatkezelő az adatkezeléshez szükséges informatikai támogatórendszer üzemeltetőivel együtt olyan technikai, szervezési és szervezeti intézkedésekkel gondoskodik az adatok biztonságáról, ami az adatkezeléssel kapcsolatban jelentkező kockázatoknak megfelelő védelmi szintet nyújt.

A papíralapú adatkezelés során az adatkezelő a személyes adatokat tartalmazó dokumentumokat a jogosulatlan hozzáférés és visszaélés ellen az adatokat elzárt, illetéktelenek által nem hozzáférhető helyen tárolja.

Az érintett a hozzájárulását az Adatkezelővel írásban kötött szerződés keretében is megadhatja a szerződésben foglaltak teljesítése céljából. Ebben az esetben a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbítását, esetleges adatfeldolgozók igénybevételét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.

A személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait – ha törvény kivételt nem tesz – az adatkezeléshez fűződő más érdekek, ideértve a közérdekű adatok nyilvánosságát is, nem sérthetik.

Adatok tárolása, selejtezése, felhasználásának, feldolgozásának, továbbításának fizikai, üzemeltetési és technikai biztonsági módozata, a jogszabályoknak megfelelően történik, pontos dokumentálással lekövetve. A fenti tevékenységek naplózása, nyilvántartása a vállalkozás által üzemeltetett informatikai rendszerből nyomon követhető. Az adatok törlése, helyesbítése, zárolásának formája, az ezzel kapcsolatos nyilvántartások Az Alapítvány által használt programok naplózásában rögzítésre kerül.

A magánszemély részére biztosítandó tiltakozási jog biztosításáról való tájékoztatás, ennek megtagadása (jogszabályhelyi hivatkozás alapján), az érintettek azonosításának módjáról való rendelkezést jelen szabályzat tartalmazza.

Adatvédelmi incidens esetén követendő protokoll eljárásban Az Alapítvány adatvédelmi tisztviselőjének tájékoztatását követően a rendszer üzemeltetőjével haladéktalanul fel kell venni a kapcsolatot a további adatvesztés elkerülése érdekében. Az adatvédelmi incidens bekövetkeztét követően elsődleges feladat az érintettek tájékoztatása, az adatvédelmi tisztviselő bevonásával, a megtett intézkedésekről való pontos dokumentáció ismertetése, amennyiben lehetséges, az adatmentés megszervezése a szakértők bevonásával.

Az Alapítvány az adatbiztonság érdekében az az alábbi fizikai kontrollokat alkalmazza:

- a) Mind az elektronikusan, mind pedig papír alapon kezelt adatokhoz való jogosulatlan hozzáférés elkerülése érdekében biztosítja, hogy a kezelt adatokhoz fizikailag ne férhessen hozzá arra jogosulatlan személy; irodák, szerver szobák zárva vannak, és csak megfelelő jogosultsággal történhet azokba belépés

Az Alapítvány az adatbiztonság érdekében az az alábbi logikai kontrollokat alkalmazza:

A megfelelő jogosultsági szintek meghatározásával biztosítja, hogy az általa kezelt adatokhoz kizárólag az arra megfelelő jogosultsággal rendelkezők férjenek hozzá.

Az Alapítvány az adatbiztonság érdekében az az alábbi adminisztratív kontrollokat alkalmazza:

Biztosítja, hogy a személyes adatokhoz való esetleges hozzáférés dokumentációkban nyomon követhető legyen, pld tevékenység logolás; épületbe/irodába való beengedés
Az Alapítványok közös Informatikai biztonsági szabályzattal rendelkeznek.

10.7. OTTHONI MUNKAVÉGZÉS (HOME OFFICE) ESETÉN KÖVETENDŐ ALAPVETŐ ADATBIZTONSÁGI SZABÁLYOK

- Otthoni munkavégzés csak céges eszközzel végezhető
- Otthoni munkavégzés során törekedni kell arra, hogy számítógép monitorját, az esetleges online megbeszéléseken elhangzottakat a velünk együtt lakókon kívül mások lássák, hallják. Publikus helyszínről, pld Internet kávézóból munkavégzés nem megengedett
- Az otthoni hálózatot jelszavas védelemmel kell ellátni
- A számítógépet otthon is védeni kell az illetéktelen hozzáféréstől, pld jelszavas képernyővédő, a lakás ajtaját kulcsa kell zárni, az iratokat mások által nem hozzáférhető helyen tárolni stb.
- Online meeting esetén ajánlott a webkamerás kép háttérét elhomályosítani.

11. JOGORVOSLATI LEHETŐSÉGEK

Az adatkezeléssel érintettek alábbi jogait minden esetben biztosítani kell, és az intézkedésről az érintettet tájékoztatni szükséges. A tájékoztató tartalmazza, hogy fogadták kérését, és mennyi időn belül számíthat válaszra.

- Az érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve –a jogszabályban elrendelt adatkezelések kivételével –törlését vagy zárolását
- Az érintett kérelmére az Adatkezelő tájékoztatást ad az általa kezelt adatokról, az adatkezelés céljáról, jogalapjáról, időtartamáról, adatfeldolgozó adatairól, ha adatfeldolgozót vett igénybe, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá -az érintett személyes adatainak továbbítása esetén -az adattovábbítás jogalapjáról, céljáról és címzettjéről. Az Adatkezelő a valóságnak nem megfelelő személyes adatot helyesbíti, illetve törli az adatot, amennyiben:
 - kezelése jogellenes;
 - az érintett kéri;
 - az hiányos vagy téves -és ez az állapot jogszerűen nem orvosolható -, feltéve, hogy a törlést törvény nem zárja ki.
 - az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt;
 - azt a bíróság vagy a Nemzeti Adatvédelmi és Információszabadság Hatóság elrendelte.
- Az Adatkezelő a helyesbítésről és a törlésről értesíti az érintettet, továbbá mindazokat, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.
- Az érintett tiltakozhat személyes adatának kezelése ellen, ha
 - a személyes adatok kezelése (továbbítása) kizárólag az adatkezelő vagy az adatátvevő jogának vagy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén;
 - a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény kutatás vagy tudományos kutatás céljára történik;
 - a tiltakozás jogának gyakorlását egyébként törvény lehetővé teszi.
- Az Adatkezelő –az adatkezelés egyidejű felfüggesztésével –a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 30 munkanap alatt megvizsgálja, és annak eredményéről a kérelmezőt írásban tájékoztatja. Amennyiben a kérelmező tiltakozása megalapozott, az Adatkezelő az adatkezelést –beleértve a további adatfelvételt és adattovábbítást is –megszünteti, és az adatokat zárolja, valamint a tiltakozásról, illetőleg az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.
- Az érintett kérheti, hogy a rá vonatkozóan kezelt adatokat tagolt, széles körben használt, géppel olvasható formátumban (pl. .doc, .pdf stb.) megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az eredeti adatkezelő.
- Törlés helyett az Adatkezelő zárolja a személyes adatot, ha az érintett ezt kéri, vagy ha a rendelkezésére álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így zárolt személyes adat kizárólag addig kezelhető, ameddig fennáll az az adatkezelési cél, amely a személyes adat törlését kizárta.
- Amennyiben az érintett az Adatkezelő döntésével nem ért egyet, vagy az Adatkezelő az előbbieken hivatkozott határidőt elmulasztja, jogosult –annak közlésétől számított 30 napon belül –bírósághoz fordulni.
- Bírósági jogérvényesítés: Az érintett a jogainak megsértése esetén bírósághoz fordulhat. Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az Adatkezelő köteles bizonyítani.

- Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból kifolyólag bármikor tiltakozzon személyes adatainak meghatározott okból történő kezelése ellen.

Információs önrendelkezési jogának megsértése esetén bejelentéssel, panasszal élhet:

Nemzeti Adatvédelmi és Információszabadság Hatóság

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

Telefon: +36 (1) 3911-400

Fax: +36 (1) 391-1410

<http://www.naih.hu>

e-mail: ugyfelszolgalat@naih.hu

12. EGYÉB RENDELKEZÉSEK

- A szabályzat megállapítására és módosítására Az Alapítvány ügyvezetője jogosult.

Jelen szabályzat 2023.május 1. napjától lép hatályba.

Kelt: Budapest, 2023. május 1.

Szentendrei Árvácska Állatvédő Egyesület

MELLÉKLETEK

1. ADATKEZELŐI NYILVÁNTARTÁS

Jelen dokumentum célja, hogy az Európai Parlament és a Tanács 2016. április 27.-én kiadott, 2018. május 25.-től hatályos, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló (EU) 2016/679 rendelete (GDPR: General Data Protection Regulation – általános adatvédelmi rendelet) 30. cikkének (1) bekezdésében, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (Info tv.) foglalt előírásoknak megfelelően az Adatkezelő, az általa a felelősségébe tartozóan végzett adatkezelési tevékenységekről történő nyilvántartás vezetési kötelezettségének teljesítését biztosítsa.

Az adatkezelői nyilvántartás tartalmazza az Adatkezelő mindenkori, aktuálisan folytatott adatkezeléseiről egyesével a fenti jogszabályi követelményeknek megfelelő információkat.

A nyilvántartás aktualizálásáról és mindenkori hatályos változatának papír alapon történő megőrzéséről Adatkezelő köteles gondoskodni.

Az adatkezelés megnevezése:	Szerződésekben található személyes adatok kezelése
Az adatkezelés célja:	Szerződött partnerekkel való kapcsolattartás, szerződés kötése
Érintettek köre:	A szerződésben szerződő félként megjelölt személyek
Kezelt adatok köre:	A szerződésben megadott adatok: Név, telefonszám, email cím, lakcím, személyi igazolvány szám,
Profilalkotás alkalmazásra kerül-e?	NEM
Adattovábbítás címzettje(i)	Nincs adattovábbítás
Nemzetközi adattovábbítás esetén a továbbított adatok köre:	Nincs nemzetközi adattovábbítás
Az adatkezelési műveletek jogalapja	a) Szerződő fél és képviselő személyes adatainak kezelése során a GDPR rendelet 6. cikk 1. bekezdés b) pontja, azaz szerződés teljesítéséhez szükséges adatkezelés b)
A kezelt személyes adatok törlésének időpontja:	A szerződéseket – azok lejárta után - 5 évig meg kell őrizni, az adatok utána kerülnek törlésre
Adatbiztonsági intézkedések:	Adatvédelmi szabályzatunkban foglaltak szerint
Adatvédelmi incidensek adatai:	
Hozzáférés korlátozás, megtagadás indokai:	

Az adatkezelés megnevezése:	Kapcsolatfelvétel során kezelt személyes adatok
Az adatkezelés célja:	Az Alapítvánnyal kapcsolatba lehet lépni többféle kommunikációs csatornán keresztül, pl email, telefon, személyesen. Telefonon történő megkeresés esetén a beszélgetésről hangfelvétel nem készül. Az adatkezelés célja: Az Alapítvány termékeivel, szolgáltatásaival kapcsolatban érdeklődők kiszolgálása
Érintettek köre:	Az Alapítvánnyal kapcsolatba lépő ügyfelek.

Kezelt adatok köre:	Név, e-mail cím, telefonszám, lakcím, és az üzenet szövegében esetlegesen megadott egyéb személyes adatok.
Profilalkotás alkalmazásra kerül-e?	NEM
Adattovábbítás címzettje(i)	Nincs adattovábbítás
Nemzetközi adattovábbítás esetén a továbbított adatok köre:	Nincs nemzetközi adattovábbítás
Az adatkezelési műveletek jogalapja	Szerződés teljesítéséhez szükséges Alapítványunk úgy tekinti hogy a vele kapcsolatba lépő személyek adatainak kezelése egy később mrgkötendő szerződés miatti előzetes adatkezelés.
A kezelt személyes adatok törlésének időpontja:	Amennyiben az érdeklődő és Az Alapítvány között nem jön létre üzleti kapcsolat, úgy az adatokat megőrizzük, de azt semmilyen célra nem használjuk fel, kizárólag statisztikiai kimutatásokat (pl hány db ajánlatkérés volt) készítünk belőle
Adatbiztonsági intézkedések:	Adatvédelmi szabályzatunkban foglaltak szerint
Adatvédelmi incidensek adatai:	
Hozzáférés korlátozás, megtagadás indokai:	

Az adatkezelés megnevezése:	Munkaviszony létesítése során történő adatkezelés
Az adatkezelés célja:	Munkaviszony létesítése, fenntartása, valamint megszüntetése
Érintettek köre:	Az Alapítvány alkalmazásában álló személyek
Kezelt adatok köre:	teljes név születési név születési hely és idő lakcím állampolgárság anyja neve tartózkodási hely címe adóazonosító jel TAJ-szám személyigazolvány szám bankszámlaszám családi állapot neme végzettséget és nyelvtudást igazoló bizonyítványok adatai magánnyugdíjpénztári tagság önkéntes nyugdíjpénztári tagság önkéntes egészségpénztári tagság jövedelem adatok (bér, szabadság, munkaidőkedvezmény, ügyelet, készenlét) levonások, letiltások beosztás keresőképtelenség kódja munkaviszony kezdete és vége telefonszám (céges) telefonszám (magán) e-mail cím gyermek adatai (név, születési hely és idő, lakcím, TAJ szám, adóazonosító jel, anyja neve, születési anyakönyvi kivonat), házastárs adatai megváltozott munkaképesség igazolására szolgáló dokumentum, orvosi igazolás, adókedvezményekhez kapcsolódó nyilatkozatok, szociális hozzájárulási adókedvezmény igazolás

Profilalkotás alkalmazásra kerül-e?	NEM
Adattovábbítás címzettje(i)	<p>Az illetékes hivatal felé továbbítjuk az egészség-, nyugdíj- és társadalombiztosításhoz, valamint az üzemi balesetkez kapcsolódó adatokat.</p> <p>A Nemzeti Adó és Vámhivatal felé továbbítjuk a bér és járulék adatokat, a kijelentés és bejelentéshez kapcsolódó, valamint, az adókedvezményhez kapcsolódó adatokat.</p> <p>A letiltással kapcsolatos adatokat a letiltást elrendelő felé továbbítjuk. (pl.: bíróság, NAV, végrehajtó).</p>
Nemzetközi adattovábbítás esetén a továbbított adatok köre:	Nincs nemzetközi adattovábbítás
Az adatkezelési műveletek jogalapja	szerződés Szerződés teljesítése a GDPR 6. cikk (1) bekezdés b) pontja alapján; valamint jogi kötelezettség teljesítése a GDPR 6. cikk (1) bekezdés c) pontja alapján
A kezelt személyes adatok törlésének időpontja:	<p>A kilépést követően a személyes adatait archiváljuk, és a mindenkori munkajogi, a számviteli, valamint a társadalombiztosítási jogszabályok által meghatározott ideig tároljuk: A társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény 99/A § alapján – a szolgálati időt, valamint a jövedelmet igazoló dokumentumok megőrzendők:</p> <p>A számvitelről szóló 2000. évi C. törvény 169. § (2) bek. alapján- a számviteli bizonylatok megőrzési ideje 8 év</p> <p>A munka törvénykönyvéről szóló 2012. évi I. törvény 286. § (1) bek. alapján az egyéb dokumentumokat és adatokat 3 évig őrizzük meg</p>
Adatbiztonsági intézkedések:	Adatvédelmi szabályzatunkban foglaltak szerint
Adatvédelmi incidensek adatai:	
Hozzáférés korlátozás, megtagadás indokai:	

Az adatkezelés megnevezése:	Hírlevél küldés során kezelt személyes adatok
Az adatkezelés célja:	reklámot tartalmazó elektronikus e-mail üzenetek küldése az érintett részére, tájékoztatás nyújtása az aktuális információkról, termékekről, akciókról..
Érintettek köre:	A hírlevélre feliratkozó ügyfelek
Kezelt adatok köre:	Név, e-mail cím
Profilalkotás alkalmazásra kerül-e?	NEM
Adattovábbítás címzettje(i)	Nincs adattovábbítás
Nemzetközi	Nincs nemzetközi adattovábbítás

adattovábbítás esetén a továbbított adatok köre:	
Az adatkezelési műveletek jogalapja	az érintett önkéntes, megfelelő tájékoztatáson alapuló, határozott hozzájárulása, melyet a Felhasználó a hírlevélre történő feliratkozást megerősítő checkbox bejelölésével ad meg,
A kezelt személyes adatok törlésének időpontja:	A Tiltakozási jog gyakorlásáig
Adatbiztonsági intézkedések:	Adatvédelmi szabályzatunkban foglaltak szerint
Adatvédelmi incidensek adatai:	
Hozzáférés korlátozás, megtagadás indokai:	

Az adatkezelés megnevezése:	Biztonsági kamerarendszer üzemeltetése során kezelt személyes adatok.
Az adatkezelés célja:	Személy-, épület- és vagyonbiztonság
Érintettek köre:	Az Alapítvány telephelyeire be- és kilépő illetve ott tartózkodó személyek
Kezelt adatok köre:	Azonosításra alkalmas képfelvétel
Profilalkotás alkalmazásra kerül-e?	NEM
Adattovábbítás címzettje(i)	Nincs adattovábbítás
Nemzetközi adattovábbítás esetén a továbbított adatok köre:	Nincs nemzetközi adattovábbítás
Az adatkezelési műveletek jogalapja	Jogos érdek, az, GDPR 6. cikk (1) bekezdés f pontja alapján.
A kezelt személyes adatok törlésének időpontja:	
Adatbiztonsági intézkedések:	Adatvédelmi szabályzatunkban foglaltak szerint
Adatvédelmi incidensek adatai:	
Hozzáférés korlátozás, megtagadás indokai:	

2. ADATFELDOLGOZÓK NYILVÁNTARTÁSA

Adatfeldolgozó	Milyen személyes adatokhoz fér hozzá? Milyen módon használhatja fel az adott személyes adatot (milyen tevékenységet végez az Adatkezelő részére)?	Mennyi ideig tárolhatja az adatokat?
Microsoft Corporation Konrad-Zuse-Str.1 85716 Unterschleißheim Germany	Levelezőrendszerünk szolgáltatója, az email-ek a Microsoft szerverein vannak tárolva. Az elektronikus levelek tartalmát az adatfeldolgozó nem olvassa, kizárólag az infrastruktúra szolgáltatást látja el.	Amíg élő szerződésünk van velük.
ROTAPRESS Bt, 1039 Budapest, Karácsony Sándor u. 32.	Könyveléssel, és bérszámfejtéssel megbízott partnerünk, a kiállított számlák könyvelését végzi, így az azon szereplő személyes adatokhoz hozzáfér, de könyvelésen kívül semmilyen egyéb célra nem használja azokat. Ezen kívül a kollégák bérszámfejtéséhez szükséges személyes adatokat dolgozza fel.	Amíg élő szerződésünk van velük.
Tarhely.eu Kft 1144 Budapest, Ormánság utca 4. X. emelet 241.	Weboldalunk tárhelyszolgáltatója, a weboldalon keresztül küldött személyes adatok az ő szerverein keresztül jutnak el hozzánk.	Amíg élő szerződésünk van velük
TJ Property Group Hungary Kft 1134 Budapest, Váci út 47/B Ü-1	Rendszergazdai feladatokat lát el, így Az Alapítványunk számítógépeihez hozzáfér, de az azon levő személyes adatokkal semmilyen tevékenységet nem végezhet.	Amíg élő szerződésünk van velük
Magyar Posta Zrt. 1138 Budapest, Dunavirág utca 2-6	Küldeményszállítás során igénybe vett adatfeldolgozó, a küldemények kézbesítéséhez szükséges személyes adatokat (név, lakcím, telenfonszám) kezeli	Amíg élő szerződésünk van velük