Iktatószám: PA-SZAB-0006/2023

A PANNON EGYETEMÉRT ALAPÍTVÁNY

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA[1]

[1] Elfogadta a Kuratórium a 88/2023. (09.01.) számú határozatával

TARTALOMJEGYZÉK

I. Általános rendelkezések 3
II. Fogalmak 4
III. Az adatkezelésért felelős vezető 4
IV. Az adatvédelmi tisztviselő 4
V. Személyes adatok kezelésének általános szabályai 5
VI. Az adatvédelmi hatásvizsgálat 6
VII. Az adatvédelmi nyilvántartás 7
VIII. Az érintettek tájékoztatása 7
IX. Az érintetti jogok gyakorlása 8
X. Adatvédelmi incidenssel kapcsolatos eljárás 9
XI. Az adatkezelés biztonságára vonatkozó szabályok 10
XII. Az adatok törlése 10
XIII. Egyes adatkezelésekre vonatkozó különös szabályok 11
XIII.1) Önéletrajzok, álláspályázatok megőrzése 11
XIII.2) Alapítványi eszközök használatának ellenőrzése 11
XIV. Egyéb rendelkezések 12

A Pannon Egyetemért Alapítvány (székhely: 8200 Veszprém, Egyetem utca 10.; nyilvántartási szám: 19-01-0001867; a továbbiakban: Alapítvány), mint adatkezelő az Európai Parlament és a Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló (EU) 2016/679 rendelete (általános adatvédelmi rendelet, a továbbiakban: GDPR vagy általános adatvédelmi rendelet), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alapján az adatkezelés rendjére az alábbi Adatvédelmi és Adatbiztonsági Szabályzatot (a továbbiakban: Szabályzat) alkotja:

I. Általános rendelkezések

1. A jelen Szabályzat célja, hogy a szervezeti folyamatok, technikai intézkedések és felelősségi szabályok meghatározása révén az Alapítvány működésében a személyes adatok kezelésére vonatkozó jogszabályok, így különösen az általános adatvédelmi rendelet rendelkezései érvényre jussanak.

2. Az Alapítvány a személyes adatok kezelése során e Szabályzatban foglaltak szerint jár el. Az Alapítvány gondoskodik arról, hogy alkalmazottai és azok a személyek, akik az Alapítvány nevében eljárnak, a jelen Szabályzatot megismerjék.

3. A jelen Szabályzatot alkalmazni kell a személyes adatok elektronizált (az általános adatvédelmi rendelet szerint automatizált, azaz elektronikus eszköz útján megvalósuló) és manuális (papír alapú) kezelésére is. Nem kell alkalmazni e Szabályzatot azokra az adatkezelési műveletekre, amelyek nem személyes adatokra vonatkoznak.

4. Az Alapítvány biztosítja, hogy adatkezelési műveletei során
   a) minden adatkezelésnek meghatározott, egyértelmű, valós, jogszerű célja van, és ezen célnak az adatkezelés a teljes tartama alatt megfelel;
   b) minden adatkezelést jogszerűen és tisztességesen, az érintett számára átlátható módon végez;
   c) a kezelt személyes adatok köréről tudatos döntés születik, így az Alapítvány csak azokat az adatokat kezeli (tárolja, továbbítja stb.), amelyek az adatkezelési cél eléréséhez elengedhetetlenül szükségesek és alkalmasak;
   d) a személyes adat kezelése a cél eléréséhez szükséges ideig tart;
   e) az érintett megfelelő, érthető és könnyen elérhető tájékoztatást kap az adatai kezeléséről;
   f) az érintett érvényesíteni tudja az őt megillető jogokat;
   g) a személyes adatok pontosak, és szükség esetén naprakészek;
   h) a személyes adatok védelmére megfelelő technikai és szervezési intézkedéseket vezet be a jogosulatlan vagy jogellenes adatkezelés, a véletlen elvesztés és megsemmisülés megakadályozása érdekében, és
   i) a személyes adatokat (is) tartalmazó adathordozókkal kapcsolatosan végrehajtott minden tevékenységet dokumentál annak érdekében, hogy a személyes adatok útja és azok fellelhetőségének helye pontosan megállapítható legyen.

5. Amennyiben egy adatról nem eldönthető annak személyes adat jellege, illetve különleges személyes adat jellege, úgy azt az azzal kapcsolatos belső döntésig úgy kell tekinteni, mintha ezen minősége/jellege fennállna. Az adat személyes adatként vagy különleges személyes adatként való minősítéséről az Alapítvány operatív igazgatója (továbbiakban: operatív igazgató) – az adatvédelmi tisztviselő véleményét bekérve – dönt.

6. A személyes adatok kezelésében közreműködő alkalmazottak kötelesek a személyes adatok védelmére vonatkozó jogszabályok és a jelen Szabályzat rendelkezéseit megismerni és maradéktalanul betartani. Az adatvédelmi szabályok megsértői – a vonatkozó jogszabályok rendelkezéseinek megfelelően – munkajogi, szabálysértési, polgári jogi és büntetőjogi felelősséggel tartoznak.

7. A jelen Szabályzat hatálya a személyes adatok védelmére vonatkozó rendelkezések tekintetében nem terjed ki az Alapítvány fenntartásában álló intézményekre, az Alapítvány tulajdonában álló gazdasági társaságokra, az alapítvány részvételével működő vagy az Alapítvány működéséhez kapcsolódó bármely önálló jogalanyisággal rendelkező szervezetre (a továbbiakban szervezet), azonban az Alapítvány ezen szervezetek fenntartójaként, tulajdonosaként, résztvevő tagjaként, illetve együttműködő partnereként segíti és elvárja, hogy ezen szervezetek saját adatvédelmi rendszerüket jelen szabályzatban meghatározott adatvédelmi elvek szerint alakítsák ki.

II. Fogalmak

1. A jelen Szabályzatban alkalmazásában használt fogalmak – a II.2. pontban meghatározott kivételekkel – megegyeznek az általános adatvédelmi rendelet 4. cikkében meghatározott fogalommeghatározásokkal.
2. A II.1. pontban foglaltakon felül a jelen Szabályzat alkalmazásában foglalkoztatott az a személy, aki az Alapítvánnyal munkaviszonyban vagy foglalkoztatásra irányuló egyéb jogviszonyban áll.

III. Az adatkezelésért felelős vezető

1. Az Alapítványt, mint adatkezelőt, illetve adatfeldolgozót terhelő kötelezettségek teljesítéséért, illetve az ahhoz szükséges döntések előkészítéséről az operatív igazgató (a továbbiakban: adatkezelésért felelős vezető) gondoskodik az Alapítvány szervezeti egységeinek hatáskörébe tartozó tevékenységek megvalósítása során.
2. Az adatkezelésért felelős vezető feladata különösen:
   a) a döntéshez az adatkezelés szükségességére, céljára és időtartamára vonatkozó javaslat előkészítése,
   b) az adatvédelmi kockázatelemzés, illetve hatásvizsgálat elkészítése,
   c) az adatkezelés rendszeres felülvizsgálata,
   d) az adatkezelés jogszerűségét alátámasztó körülmények dokumentálása (így különösen hozzájárulás, érdekmérlegelés),
   e) ha az adatkezelésbe harmadik fél bevonása válik szükségessé, úgya szükséges adatfeldolgozói szerződés vagy közös adatkezelői szerződés előkészítése,
   f) érintettek tájékoztatásának előkészítése,
   g) incidens bekövetkezése esetén az incidens értékelése és az annak nyomán szükséges intézkedések meghatározása.

IV. Az adatvédelmi tisztviselő

1. Az Alapítvány az általános adatvédelmi rendelet 37-39. cikke szerint kijelölt független adatvédelmi tisztviselőt alkalmaz, aki adatvédelmi feladatai ellátásával kapcsolatban nem utasítható és ebben a minőségében közvetlenül az operatív igazgató felügyelete alá tartozik, és az operatív igazgatónak tartozik beszámolási kötelezettséggel.
2. Az adatvédelmi tisztviselő segíti az operatív igazgatót és az Alapítvány alkalmazottait az adatvédelmi kérdésekben, így különösen:
   a) naprakész tájékoztatást és szakmai tanácsot ad az általános adatvédelmi rendelet, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezések szerinti kötelezettségekkel kapcsolatban az adatkezelési műveleteket végrehajtó munkatársaknak;
   b) figyelemmel kíséri és ellenőrzi az általános adatvédelmi rendeletnek, az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, valamint az Alapítvány személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését;
   c) részt vesz és koordinálja az adatkezelési műveletekben érintett munkavállalók tudatosság-növelését és képzését;
   d) részt vesz és figyelemmel kíséri az információbiztonsági, adatbiztonsági ellenőrzéseket és a kapcsolódó auditokat;
   e) elősegíti az érintettet megillető jogok gyakorlását, részt vesz az érintett panaszainak kivizsgálásában, és kezdeményezi a panasz orvoslásához szükséges intézkedések megtételét az Alapítványnál;
   f) együttműködik a NAIH-al, és felé kapcsolattartó pontként szolgál;
   g) figyelemmel kíséri és szakmai tanáccsal segíti a kockázatelemzés, illetve adatvédelmi hatásvizsgálat, és az adatvédelmi incidens bekövetkezése esetén előírt eljárás lefolytatását, ellenőrzi az ezekhez kapcsolódó kötelezettségek teljesítését, valamint részt vesz ezen eljárások és az alkalmazott módszerek továbbfejlesztésében;

h) kapcsolatot tart a külső hatóságokkal, szervezetekkel adatvédelmet érintő kérdésekben, megadja részükre a szükséges felvilágosítást, külső vizsgálatok esetén együttműködik a vizsgálatot lefolytató hatóságokkal;

i) évente beszámol a operatív igazgatónak a tevékenységéről, az Alapítvány személyes adatokat érintő folyamatairól, és az adatvédelmi kötelezettségek teljesítésének állásáról;

j) vezeti az Alapítvány adatvédelmi és incidens-nyilvántartását.

3. Az adatvédelmi tisztviselőt be kell vonni valamennyi, személyes adatok kezelését érintő döntés előkészítésébe; ezért minden szervezeti egység vezetője felelősséggel tartozik. Az adatvédelmi tisztviselő részére hozzáférést kell biztosítani mindazon információkhoz és adatokhoz, amelyek az adatvédelmi feladatai ellátásához szükségesek.

4. Az adatvédelmi tisztviselő jogosult:
   a) minden, a jelen Szabályzat hatálya alá tartozó adatkezelést vizsgálni és minden olyan helyiségbe belépni, ahol adatkezelés folyik,
   b) tájékoztatást, felvilágosítást kérni minden, a jelen Szabályzat hatálya alá tartozó adatkezelésről,
   c) tanácskozási és jóváhagyási joggal részt venni minden olyan fórumon, ahol a hatáskörébe tartozó témák szerepelnek a napirenden.

5. Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódhasson. Feladatai ellátásához jogosult betekinteni a kezelt adatokba.

V. Személyes adatok kezelésének általános szabályai

1. Személyes adatok az Alapítványnál az alábbi feltételek együttes teljesülése esetén kezelhetők:
   a) az adatkezelés jogalapja az általános adatvédelmi rendelet 6. cikk (1) bekezdésének valamely pontját teljesíti, így:

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

      ab) 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;

      ac) az adatkezelés az Alapítványra vonatkozó jogi kötelezettség teljesítéséhez szükséges;

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

      ae) az adatkezelés közérdekű vagy az Alapítványra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

      af) az adatkezelés az Alapítvány vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek;

   b) az adatkezelés szükségességét az operatív igazgató jóváhagyta;

   c) az adatkezelésre vonatkozóan az adatvédelmi kockázatelemzés, és amennyiben szükséges, úgy a hatásvizsgálat elkészült – ha pedig az adatvédelmi hatásvizsgálat alapján az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában is valószínűsíthetően magas kockázattal jár, úgy a NAIH-al való konzultáció megtörtént, és az adtakezelést a NAIH nem tiltotta meg, illetve az általa előírt feltételeket az Alapítvány teljesítette;

   d) az adatkezelés az Alapítvány adatvédelmi nyilvántartásában rögzítésre került, vagy – az adatkezelés megkezdését követően – haladéktalanul rögzítésre kerül.

2. Különleges adatok kezelése esetén az V.1 pontban írt feltételek teljesítésén túl szükséges az is, hogy az adatkezelés megfeleljen az általános adatvédelmi rendelet 9. cikk (2) bekezdésének valamely pontjában foglaltaknak is.

3. Ha a személyes adatok kezelése az adatgyűjtés eredeti céljától eltérő célból válik szükségessé, és e célok egymással összeegyeztethetők, az adatkezelési művelet elvégzéséhez nem kell új jogalapot megjelölni.

   A célok összeegyeztethetőségéről való döntés során figyelembe kell venni
   - a személyes adatok gyűjtésének körülményeit,
   - az érintett és az Alapítvány közötti kapcsolatot (pl. van-e egyenlőtlenség),
   - a személyes adatok jellegét (különleges adatok-e),
   - hogy a további adatkezelés az érintettre milyen következménnyel járna, és
   - megfelelő garanciák állnak-e rendelkezésre (pl. titkosítás, álnevesítés).

   Nem kell külön mérlegelni a célok összeegyeztethetőségét, ha a további adatkezeléshez az érintett hozzájárult, vagy ha azt uniós vagy nemzeti jog írja elő. A közérdekű archiválás, tudományos vagy történelmi kutatás, vagy statisztikai célból folytatott további adatkezelés jogszerűnek tekinthető.

   Eltérő célból való további adatkezelés megkezdése előtt a célok összeegyeztethetőségéről való döntésről és a figyelembe vett szempontokról emlékeztetőt kell készíteni; az érintettet továbbá tájékoztatni kell az eltérő célról.

4. Minden olyan adatkezelés esetén, amelyben az adatkezelés célját és eszközeit nem kizárólag az Alapítvány határozza meg, úgy az adatkezelés további feltétele, hogy az Alapítvány a többi adatkezelővel az általános adatvédelmi rendelet 26. cikke szerinti megállapodást megkösse.

5. Ha az Alapítvány adatfeldolgozóként jár el, vagy az adatkezelés során adatfelgozót (al-adatfeldolgozót) kíván igénybe venni, és az adatfeldolgozói feladatokról nem – vagy nem teljeskörűen – rendelkezik jogszabály, az adatfeldolgozói feladatok ellátásáról szerződést kell kötni az általános adatvédelmi rendelet 28. cikke (3) bekezdése szerinti tartalommal.

VI. Az adatvédelmi hatásvizsgálat

1. Az adatkezelés előtt adatvédelmi hatásvizsgálatot kell készíteni, ha
   a) a kockázatelemzés eredménye szerint az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve,
   b) az adatkezelés megfelel az általános adatvédelmi rendelet 35. cikk (3) bekezdésében írt feltételeknek, vagy
   c) az adatkezelés szerepel a NAIH által az általános adatvédelmi rendelet 35. cikk (4) bekezdés alapján kiadott jegyzékben.

2. A kockázatelemzés, illetve adatvédelmi hatásvizsgálat lefolytatásába az adatvédelmi tisztviselőt be kell vonni, aki szakmai tanácsokkal segíti azok lefolytatását.

3. Az adatvédelmi hatásvizsgálat alapján javaslatot kell tenni különösen
   a) az adathoz való hozzáférés (pl. személyi, időbeli) korlátaira,
   b) az adattovábbítás szabályaira (kinek, milyen célból, milyen feltételekkel),
   c) az adatkezeléssel összefüggésben végrehajtandó egyéb technikai és szervezési intézkedésekre (pl. az adatot tartalmazó file-ok vagy dokumentumok őrzési helyének kijelölésére, az adat tárolására szolgáló eszközök használatával kapcsolatos jelszókezelési szabályokra, a felhasználásnak a Alapítvány székhelyére való korlátozására, titkosításra stb.).

   E javaslatokról az operatív igazgató a hatásvizsgálati lapok jóváhagyásával dönt.

4. Az operatív igazgató által jóváhagyott hatásvizsgálati lapokat elektronikus formában kell elmenteni C:/NextCloud/*PEA Adatvédelem*, amelyekhez az operatív igazgató és az adatvédelmi tisztviselő férhet hozzá.

5. Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés a kockázat mérséklése céljából – az VI.3 pont szerinti vagy más – tervezett intézkedések ellenére valószínűsíthetően továbbra is magas kockázattal járna az érintettekre nézve, az Alapítvány köteles előzetes konzultációt kezdeményezni a NAIH-nál.

Az ehhez szükséges kérelmet és mellékleteit a hatásvizsgálatot lefolytató adatkezelésért felelős vezető és az adatvédelmi tisztviselő közösen készíti elő. Az előzetes konzultáció lefolytatásáig az adatkezelés nem kezdhető meg.

6. Ha az Alapítvány adatfeldolgozó, az adatvédelmi hatásvizsgálatot azonban nem kell lefolytatni. Az adatfeldolgozáshoz kapcsolódó adatkezelés hatásvizsgálatának elvégzése az adatkezelő felelősségi körébe tartozik. Az Alapítvány köteles együttműködni az adatkezelővel e feladatainak ellátása érdekében.

VII. Az adatvédelmi nyilvántartás

1. Az adatkezelés és az adatfeldolgozás megkezdését, módosítását és megszüntetését be kell jelenteni az adatvédelmi tisztviselőnek, aki – haladéktalanul – gondoskodik annak bejegyzéséről, illetve a változások átvezetéséről az adatvédelmi nyilvántartásában. A nyilvántartást – kérésre – a NAIH rendelkezésére kell bocsátani.

2. Az adatvédelmi nyilvántartásban szereplő adatkezelések felülvizsgálatát indokolt esetben, de legalább minden év januárjában el kell végezni. Ennek során ellenőrizni kell az adatkezelések célját, a korábban elvégzett érdekmérlegelési teszteket, a kockázatelemzés és adatvédelmi hatásvizsgálat megállapításait. Az adatvédelmi nyilvántartás felülvizsgálatát az adatvédelmi tisztviselő koordinálja. A felülvizsgálat megtörténtét követően a nyilvántartás naprakész adatait be kell mutatni az operatív igazgatónak , aki a nyilvántartás adatait – egyetértése esetén – jóváhagyja.

VIII. Az érintettek tájékoztatása

1. Az Alapítvány az adatkezelés körülményeiről tájékoztatja az érintettet. Ha az Alapítvány adatfeldolgozó, az adatfeldolgozói szerződés eltérő rendelkezésének hiányában az érintett tájékoztatásáról az adatkezelő gondoskodik (nem az Alapítvány).

   Az érintett tájékoztatása kiterjed az alábbiakra:
   a) az Alapítvány, mint adatkezelő (és képviselőjének) kiléte és elérhetősége,
   b) az adatvédelmi tisztviselő elérhetősége, ha ilyen működik az Alapítványnál;
   c) a személyes adatokat az Alapítvány milyen forrásból szerezte meg, ha azokat nem közvetlenül az érintett bocsátja az Alapítvány rendelkezésére,
   d) az adatkezelés tervezett célja és jogalapja (jogos érdeken alapuló adatkezelés esetén a jogos érdek megnevezése),
   e) a személyes adatok kategóriái,
   f) a személyes adatok címzettje, illetve aki számára a személyes adat továbbításra kerül, vagy számára az megismerhető lesz,
   g) harmadik országba vagy nemzetközi szervezet részére való adattovábbítás esetén ennek ténye, továbbá az adattovábbítás jogszerűségének körülményei,
   h) a személyes adatok tárolásának időtartama, vagy ezen időtartam meghatározásának szempontjai,
   i) az érintett joga a hozzáféréshez, az adat helyesbítéséhez és törléséhez, az adatkezelés korlátozásához, az adatkezelés elleni tiltakozáshoz, és az adathordozhatósághoz,
   j) az érintett hozzájárulásán alapuló adatkezelés esetén a hozzájárulás visszavonásához való jog (amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét), és ennek feltételei,
   k) hogy az adat szolgáltatása szerződésen vagy jogszabályon alapul-e, hogy az adat megadása az adott szerződés megkötésének előfeltétele-e, továbbá, hogy az érintett köteles-e megadni a személyes adatait, és milyen következményekkel jár az adatok megadásának elmaradása,
   l) profilalkotás esetén az automatizált döntéshozatal ténye, annak logikája, következményei,
   m) a NAIH-hoz panasz benyújtásának és a bírósági igényérvényesítés joga.

2. A tájékoztatást az érintett részére a személyes adatai gyűjtésével egyidejűleg kell megadni. Ha az adatokat az Alapítvány nem az érintettől szerzi meg, a tájékoztatásról
   a) legkésőbb 1 hónapon belül,
   b) kapcsolattartási célból szerzett adatok esetén az első kapcsolatfelvétel alkalmával,
   c) ha az adatokat harmadik személyekkel is közlik, akkor az első közléskor
   kell gondoskodni.

3. A tájékoztatást tömör, átlátható, világos, közérthető és könnyen hozzáférhető formában kell nyújtani, amelynek nyelvezetét és formáját a tájékoztató célcsoportjára figyelemmel kell kialakítani.

4. A tájékoztatást írásban (elektronikus úton vagy papíron) kell megadni. Az érintett kérésére kivételesen szóbeli tájékoztatás is nyújtható (telefonon vagy személyesen); ebben az esetben a tájékoztatás megtörténtéről – a későbbi igazolhatóság érdekében – írásbeli emlékeztetőt kell készíteni.

5. Nem kell tájékoztatást nyújtani az általános adatvédelmi rendelet 13. cikk (4) bekezdésében és a 14. cikk (5) bekezdésében írt esetekben. Az adatkezelésért felelős vezető az adatkezelési tevékenység megkezdése előtt felméri, hogy az adatkezelésre vonatkozóan az Alapítvány köteles-e tájékoztatást nyújtani az érintettek számára. A tájékoztatás előkészítéséhez és teljesítéséhez az adatvédelmi tisztviselő segítséget nyújt.

IX. Az érintetti jogok gyakorlása

1. Az érintettet a saját személyes adataira vonatkozó adatkezelések tekintetében megilleti
   a) a hozzáféréshez és az adatkezelés részleteire vonatkozó tájékoztatáshoz való jog,
   b) a pontatlan vagy hiányos adatok helyesbítéséhez való jog,
   c) az adat törléséhez való jog,
   d) az adatkezelés korlátozásához való jog,
   e) az adathordozhatósághoz való jog,
   f) a tiltakozáshoz való jog,
   g) a NAIH-nál panasz előterjesztéséhez való jog,
   h) a bírósági igényérvényesítéshez való jog.

2. Az érintettnek a személyes adatok kezelésére vonatkozó, az általános adatvédelmi rendelet 13-22. cikkeiben foglalt jogok érvényesítésére irányuló kérelmei intézéséről és az érintett részére szóló válasz előkészítéséről az adatkezelésért felelős vezető gondoskodik. A kérelem kivizsgálásába az adatvédelmi tisztviselőt be kell vonni, az érintettnek szóló válasz tervezetét – jóváhagyás előtt – be kell mutatni az adatvédelmi tisztviselő részére.

3. A szóban vagy telefonon előterjesztett kérelemről az érintettől írásbeli megerősítést kell kérni. Ha ez nem lehetséges, akkor a kérelemről írásbeli emlékeztetőt kell készíteni.

   A kérelem beérkezésekor meg kell vizsgálni, hogy a kérelmet az érintett nyújtotta-e be. Ha az Alapítvány rendelkezésére álló adatok alapján nem egyértelmű, hogy a kérelem az érintett természetes személytől származik (például, ha a kérelem addig ismeretlen email-címről érkezik), tőle a személyazonosság igazolásához további információk kérhetők.

   Ennek érdekében a kérelmezőtől csak olyan adat kérhető, amely az Alapítvány számára elengedhetetlenül szükséges és alkalmas annak eldöntéséhez, hogy a kérelmet az érintett nyújtotta-e be.

4. Az érintett kérelmét haladéktalanul érdemben meg kell vizsgálni, ennek során ellenőrizni kell, hogy az Alapítvány kezeli-e az érintett adatait, azokat adatkezelőként vagy adatfeldolgozóként kezeli-e, mi az adatkezelés jogalapja, és mi az adatkezelés időtartama. Az érintett azonosításáig, illetve a kérelemről való döntésig az adatkezelés korlátozása elrendelhető, ha a kérelem az adat pontosságát vitatja.

5. Az érintettet mihamarabb, de legkésőbb 1 hónapon belül – írásban, vagy ha a kérelem elektronikus úton érkezett, elektronikus úton – tájékoztatni kell
   a) a megtett intézkedésekről, vagy
   b) az intézkedések elmaradásának okairól (a NAIH-hoz vagy bírósághoz való fordulás lehetőségéről szóló tájékoztatással együtt).

   Ez a határidő különösen indokolt esetben (figyelemmel a kérelmek számára, illetve összetettségére) további 2 hónappal meghosszabbítható; erről az érintettet legkésőbb az említett 1 hónapos határidőben tájékoztatni kell.

6. Ha a kérelem alapján az adatkezelést módosítani, illetve a személyes adatot törölni kell, úgy erről értesíteni kell az adatvédelmi tisztviselőt, aki a változásokat haladéktalanul átvezeti az adatvédelmi nyilvántartásban. A személyes adat módosításának és törlésének megtörténtéről lehetőség szerint valamennyi címzettet értesíteni kell, akivel azt korábban közölték.

7. Az érintett kérelmeinek intézését díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, a kért tájékoztatás vagy intézkedés teljesítésével járó adminisztratív költségek (pl. személyi jellegű költségek, másolat, adathordozó költségei stb.) felszámíthatók, indokolt esetben az intézkedés megtagadható. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének okairól írásban emlékeztetőt kell készíteni.

8. Ha az Alapítvány adatfeldolgozó, az adatfeldolgozással kapcsolatban közvetlenül az érintettnek nem nyújthat tájékoztatást, és az érintetti kérelmeket közvetlenül nem intézheti, kivéve, ha az adatfeldolgozói szerződés vagy az adatkezelő írásbeli utasítása ettől eltérően rendelkezik. Ha az érintett az Alapítványnál terjeszti elő a kérelmét, úgy az érintett azonosítását nem kell elvégezni, hanem a kérelmet az adatkezelésért felelős vezető köteles haladéktalanul továbbítani az adatkezelő számára. Az érintett kérelméről és annak továbbításáról az adatvédelmi tisztviselőt tájékoztatni kell. Az Alapítvány köteles együttműködni az adatkezelővel az érintett kérelmének intézése során.

9. Az Alapítvány az érintettet megillető jogok teljesítéséről nyilvántartást vezet, amely tartalmazza:
   a) az érintett kérelmének időpontját,
   b) a kérelemre adott válasz időpontját,
   c) a teljesítés/elutasítás időpontját,
   d) elutasítás esetén az elutasítás indokát.

X. Adatvédelmi incidenssel kapcsolatos eljárás

1. Aki adatvédelmi incidens megtörténtéről szerez tudomást, azt haladéktalanul köteles jelezni az operatív igazgatónak vagy az adatvédelmi tisztviselőnek.

2. Az adatkezelésért felelős vezető - az adatvédelmi tisztviselő bevonásával - gondoskodik a személyes adatra vonatkozó incidens kivizsgálásáról, az incidenssel kapcsolatos kockázatok értékeléséről, valamint – szükség szerint – az incidens NAIH részére való bejelentésével és az érintettek tájékoztatásával kapcsolatos dokumentáció előkészítéséről. Az incidens kivizsgálása során meg kell határozni azokat a technikai és szervezési intézkedéseket, amelyek a további incidensek elkerülését szolgálják. Az incidens kivizsgálására irányuló eljárás lefolytatásába az adatvédelmi tisztviselőt be kell vonni.

3. Az incidens kivizsgálásának eredményéről az operatív igazgatót tájékoztatni kell, aki dönt az incidenssel kapcsolatos további intézkedésekről.

4. Ha a kockázatértékelés alapján az incidens az érintett(ek) jogaira és szabadságaira nézve valószínűsíthetően kockázatot jelent, azt haladéktalanul, de legkésőbb – az incidens bekövetkeztétől vagy az arról való tudomásszerzéstől számított – 72 órán belül az általános adatvédelmi rendelet 33. cikke szerinti tartalommal be kell jelenteni a NAIH-nak. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát. Ha ez a kockázat valószínűsíthetően magas, a NAIH mellett az érintett(ek)et is értesíteni kell az általános adatvédelmi rendelet 34. cikkében foglaltak szerint.

5. Az adatvédelmi incidenst az adatvédelmi tisztviselő bevezeti az incidens- nyilvántartásba. Az adatvédelmi incidenst akkor is rögzíteni kell a nyilvántartásban, ha a NAIH-nak való bejelentése, illetve az érintettek tájékoztatása azzal kapcsolatban nem indokolt.

6. Az incidens értékelésével kapcsolatos dokumentumokat elektronikus formában kell elmenteni C:/NextCloud/*PEA Adatvédelem*, amelyekhez az operatív igazgató és az adatvédelmi tisztviselő férhet hozzá.

7. Ha az adatvédelmi incidens az Alapítvány adatfeldolgozási feladatainak ellátása során következett be, akkor azt – az arról való tudomásszerzést követően haladéktalanul – jelezni kell az adatkezelőnek.

   Ebben az esetben az Alapítványnak az incidens kockázatértékelését nem kell elvégeznie, az incidenst a NAIH részére nem kell bejelentenie, és arról az érintetteket sem kell tájékoztatnia, mert ezekről az adatkezelő gondoskodik. Az Alapítvány köteles együttműködni az adatkezelővel ezen feladatainak teljesítése során.

8. Az Alapítvány – az adatvédelmi tisztviselő útján – az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza:
   a) az érintett személyes adatok körét,
   b) az adatvédelmi incidenssel érintettek körét és számát,

c) az adatvédelmi incidens időpontját, körülményeit, hatásait,
d) az elhárítására megtett intézkedéseket, valamint
e) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

XI. Az adatkezelés biztonságára vonatkozó szabályok

1. Az adatok elvesztése, megsemmisülése, károsodása és az azokhoz való jogosulatlan hozzáférés megelőzése és megakadályozása érdekében szükséges biztonsági intézkedéseket az adatkezelés (adatfeldolgozás) megkezdése előtt – a kockázatelemzés során – az adatkezelés jellemzőihez és a személyes adatok jellegéhez mérten kell meghatározni, és azokat – az adatokat érintő incidens bekövetkezésének hiányában is – rendszeresen felül kell vizsgálni.

   Az adatvédelmi tisztviselő ellenőrzi az adatbiztonsági előírások meglétét és betartását.

2. A személyes adatot tartalmazó papír alapú dokumentum biztonságának garantálása érdekében elrendelhető különösen a dokumentumokról lista készítése, a dokumentumok előírt helyen, illetve elzártan tartása, a dokumentumok felhasználásának bejelentéshez vagy jóváhagyáshoz kötése, a dokumentumokhoz hozzáférésre jogosultak körének meghatározása.

3. Személyes adatot tartalmazó papír alapú dokumentum csak zárt borítékban, vagy dokumentum-továbbításra alkalmas, zárt eszközben továbbítható.

4. A munkavállalók és a tisztségviselők kötelesek az általuk nyomtatott, fénymásolt személyes adatokat tartalmazó dokumentumokat a közös használatú (hálózati) nyomtatóról és fénymásolóról haladéktalanul magukhoz venni.

5. A számítógépeken végrehajtott adatkezelési műveletek során a képernyőt úgy kell beállítani, hogy a személyes adatokat csak az arra jogosultak láthassák.

6. Elektronikus formában tárolt személyes adatok, vagy személyes adatokat tartalmazó dokumentumok kizárólag (erős) jelszóval védett számítógépen, valamint az Alapítvány által használt felhő-, és közös munkavégzést lehetővé tevő (jogosultságkezeléssel biztosított) szolgáltatásokban kezelhetők.

7. Az operatív igazgató kifejezett utasítása hiányában az elektronikus formában tárolt személyes adatok, vagy személyes adatokat tartalmazó dokumentumok, adatbázisok külső tárhelyre vagy levelezőrendszerre történő továbbítása, illetve más, harmadik személy által hozzáférhető eszközökön való használata, megnyitása, tárolása tilos.

8. Az adatok visszaállíthatóságának érdekében a személyes adatokat tartalmazó elektronikus dokumentumokról vagy adatbázisokról rendszeresen biztonsági mentést kell készíteni. A biztonsági mentések (vagy ilyen dokumentumokat, illetve adatbázisokat is tartalmazó biztonsági mentések) megfelelő titkosítás mellett is kizárólag olyan környezetben tárolhatók, amelyek magas szinten támogatják az adatkezeléssel kapcsolatos garanciák megtartását, valamint nem jelentenek kockázatot az adatok biztonságára vonatkozóan.

9. Az adatkezelésért felelős vezető az Alapítvány munkafolyamatait úgy szervezi meg, hogy személyes adathoz csak olyan munkatárs és csak annyi ideig férhessen hozzá, akinek az az adat a feladatai ellátásához elengedhetetlenül szükséges.

XII. Az adatok törlése

1. A személyes adatokat törölni kell, ha
   a) az adatkezelésre meghatározott időtartam eltelt,
   b) az adatkezelés célja megvalósult vagy a cél személyes adatok kezelése nélkül is elérhetővé vált,
   c) az érintett kéri,
   d) adatfeldolgozás esetén arra az adatkezelő az Alapítványt írásban utasítja,
   e) arra az Alapítványt jogszabály, bírósági vagy hatósági határozat kötelezi.

2. Az előző pontban foglaltaktól eltérően nem törölhető olyan adat, amely az Alapítvány szerződéses vagy jogszabályi kötelezettségeinek teljesítése érdekében szükséges lehet, vagy amely megtartása az Alapítvány gazdasági működésével összefüggésben jogszabály alapján kötelező.

3. Az adatok törléséhez előzetesen be kell szerezni az operatív igazgató jóváhagyását. Ez nem vonatkozik azokra az automatizált adattörlésekre, amelyek elektronikus adatbázisokat vagy dokumentumokat érintenek, és amelyekkel kapcsolatban a törlési rutinokat az operatív igazgató előzetesen jóváhagyta.

4. Ha az V.1 pont *ac)* vagy *ae)* alpontjában írt jogalapon folyatott kötelező adatkezelés időtartamára vagy szükségességének rendszeres felülvizsgálatára nincs előírás (törvényben, önkormányzati rendeletben, uniós jogban), akkor – az adatkezelés megkezdésétől számított – legalább 3 évente felül kell vizsgálni, hogy az adott személyes adat az adatkezelés céljának megvalósulásához szükséges-e vagy annak törléséről kell gondoskodni. A felülvizsgálat elvégzéséről jegyzőkönyvet kell készíteni, amelynek tartalmaznia kell az adatkezelés további szükségességét alátámasztó indokokat. A jegyzőkönyvet 10 évig meg kell őrizni, és kérésre a NAIH rendelkezésére kell bocsátani.

5. A személyes adatok törlése során úgy kell eljárni, hogy a törölt adat a továbbiakban ne legyen megismerhető és visszaállítható. Ennek érdekében a személyes adatot tartalmazó
   a) papír alapú dokumentumot teljes egészében meg kell semmisíteni (pl. iratmegsemmisítővel), vagy ha ez nem indokolt, a konkrét személyes adatot kell olvashatatlanná tenni;
   b) elektronikus dokumentumot teljes egészében törölni kell, vagy ha az nem indokolt, abból a konkrét személyes adatot kell eltávolítani úgy, hogy a dokumentum eredeti, személyes adatot is tartalmazó változata ne legyen helyreállítható.

6. A személyes adatok törlését valamennyi elektronikus dokumentumban végre kell hajtani, így azokat a biztonsági mentésekből is törölni kell, vagy olyan visszaállítási protokollt kell biztosítani, amely a kérdéses file-okat nem állítja vissza, és a biztonsági másolatok tartalmát nem teszi elérhetővé. A papír alapú dokumentumról készített elektronikus másolatokat az új, törölt adatot nem tartalmazó másolattal kell helyettesíteni.

7. A törlés megfelelőségéért az adat törlését végrehajtó munkatárs felelős.

XIII. Egyes adatkezelésekre vonatkozó különös szabályok

XIII.1) Önéletrajzok, álláspályázatok megőrzése

1. Az Alapítvány álláshirdetésére érkezett önéletrajzok és egyéb dokumentumok személyes adatait, valamint az állás betöltésével kapcsolatos döntés érdekében az Alapítványnál keletkezett személyes adatokat a meghirdetett állás betöltése esetén a próbaidő leteltét követő 7 napon belül törölni kell. Ha a meghirdetett munkakört nem sikerült betölteni, az említett adatokat a pályázat beérkezésétől számított 90 napon belül törölni kell.

2. Az előző pontban foglaltaktól eltérően nem kell törölni az álláspályázatokat, ha a megtartáshoz a pályázó kifejezett, egyértelmű és önkéntes nyilatkozatával hozzájárul annak érdekében, hogy a pályázata további munkakörökre való jelentkezésként figyelembe vételre kerüljön. A pályázó hozzájárulását a törlési határidő leteltét megelőzően kell beszerezni. A pályázatok adatai azonban legkésőbb az Alapítványhoz érkezéstől számított 1 év elteltével ebben az esetben is törlésre kerülnek.

XIII.2) Alapítványi eszközök használatának ellenőrzése

1. Az Alapítvány tulajdonában álló eszközökön (különösen számítógép, pendrive stb.) tilos magáncélú személyes adatot tárolni, illetve azokat véglegesen törölni kell legkésőbb akkor, amikor az eszközöket az Alapítvány részére visszaszolgáltatják.

2. A munkavégzés céljára biztosított számítógépek, notebookok stb. magáncélú használatát – beleértve a munkavállalók internethasználatát is – az Alapítvány akkor ellenőrizheti, ha azokkal kapcsolatban gyanú merül fel
   a) jogsértő tartalom kezelésére,
   b) adatvédelmi incidens megtörténtére,
   c) az eszköz károsodását eredményező vagy azt kockáztató használatra.

3. Az ellenőrzést az operatív igazgató által kijelölt személy végzi el. Az ellenőrzésen az eszközt használó munkavállaló részt vehet, őt az ellenőrzés megkezdése előtt tájékoztatni kell az ellenőrzés okáról. Az Alapítvány a munkavállaló személyes adatait csak annyiban ismerheti meg, amennyiben az a fenti célokkal összefüggésben közvetlenül és feltétlenül szükséges. Az ellenőrzésről jegyzőkönyvet kell készíteni.

XIV. Egyéb rendelkezések

1. Akinek a munkája során személyes adat kezelésével kapcsolatos kérdés merül fel, így például bizonytalan az adatkezelést vagy egy adat személyes adatnak minősülését illetően, valamint ha az adatkezelési szabályok megsértését észleli, annak tisztázása érdekében haladéktalanul köteles megkeresni az adatkezelésért felelős vezetőt vagy az adatvédelmi tisztviselőt, aki a jelzés alapján megteszi a szükséges intézkedéseket a biztonságos, az érintettek jogait és szabadságait biztosító adatkezelés feltételeinek kialakítása érdekében.
2. Az adatkezeléssel kapcsolatos nyilatkozatokat és utasításokat írásban kell megtenni. Ha az eset összes körülményére tekintettel sürgős szóbeli közlés indokolt, úgy azt utóbb, a közlés szóbeliségére okot adó körülmény elmúlását követően haladéktalanul írásba kell foglalni. Az e-mailben, smsben és egyéb üzenetküldő alkalmazásban, illetve szolgáltatással történt közlés az Alapítványon belül írásbelinek minősül, ha az a szükséges ideig visszakövethetően változatlan formában rendelkezésre áll.
3. Az adatvédelemmel kapcsolatos működés során mindenkor a legteljesebb mértékben törekedni kell arra, hogy a jelen Szabályzatnak és a jogszabályi elvárásoknak való megfelelés igazolható legyen, amely vonatkozik különösen:
   a) az érintett adatkezeléshez történt hozzájárulására,
   b) a jogos érdek alapján történő adatkezelés érdekmérlegelési tesztjének elvégzésére,
   c) az érintett panaszaira és kérelmeire, különösen az adatkezelés részleteihez való hozzáférésre, az egyes adatok törlésére, helyesbítésére, továbbítására, illetve az adatkezelés korlátozására, vagy azzal kapcsolatos tiltakozására irányuló kérelmeinek intézésére,
   d) az adatvédelmi incidensekről szóló érintetti értesítésre,
   e) az adatvédelmi és incidens-nyilvántartásra,
   f) adatfeldolgozói tevékenységre vonatkozó adatkezelői utasításra.

   Ezekben az esetekben az írásbeli (vagy annak minősülő) forma sürgős esetekben sem mellőzhető.
4. Harmadik személyektől nem fogadható el a teljesítés, ha az olyan személyes adatot tartalmaz, melynek jogszerű kezelhetősége az Alapítvány számára nem biztosított. Ezen rendelkezést a harmadik személyekkel kötött szerződéses megállapodásban rögzíteni kell.
5. A jelen Szabályzatot szükség esetén, de legalább kétévente felül kell vizsgálni.
6. A jelen Szabályzat a kiadásának napján lép hatályba. Jelen Szabályzatot a kuratórium a 88/2023. (09.01) számú határozattal fogadta el.

Veszprém, 2023. 09. 01.

Dr. Birkner Zoltán
kuratóriumi elnök