



3700 Kazincbarcika
Rákóczi tér 9.

Adatvédelmi és incidenskezelési szabályzat

Dokumentum kontroll

Változások

Verzió	Kiadás dátuma	Kiadás célja / módosítás lényege
01.	2025. 12. 16.	Egressy Béni Városi Könyvtár adatkezelési tevékenységeivel kapcsolatos szervezési, adminisztratív, logikai és fizikai védelmi intézkedési kötelezettségeinek meghatározása

Kiadás

Készült	2 eredeti példányban
---------	----------------------



3700 Kazincbarcika
Rákóczi tér 9.

TARTALOMJEGYZÉK

Dokumentum kontroll	1
1.	4
2.	4
3.	5
4.	8
5.	9
5.1.	9
5.2.	10
5.3.	10
5.4.	10
5.5.	11
6.	13
7.	13
7.1.	13
7.2.	14
7.3.	15
7.4.	16
8.	17
8.1.	17
8.2.	17
9.	18
10.	19
10.1.	19
10.2.	19
10.3.	20
10.4.	20
ADATVÉDELMI INCIDENS KEZELÉSE	21
10.5.	21
10.6.	21
10.7.	22

10.8. 23

10.9. 23

11. 23

11.1. 24

11.2. 24

11.3. 25

11.4. 25

11.5. 26

11.6. 26

11.7. 27

12. 27

13. 28

1. melléklet: Szerződésekben használandó adatvédelmi, titoktartási, kapcsolattartási klauzulák 28

2. melléklet: Adatfeldolgozói szerződés minta 31

3. melléklet: Titoktartási nyilatkozat minta 34

4. melléklet: Adatkezelési tevékenység nyilvántartó lap - bevezetés 35

5. melléklet- Érdekmérlegelési teszt minta 39

6. 43

7. 44

8. 48

9. 49

1. Általános rendelkezések

Az Egressy Béni Városi Könyvtár (a továbbiakban: EBVK vagy Adatkezelő, székhelye: 3700 Kazincbarcika, Rákóczi tér 9., adószáma: 15353287-2-05, adatvédelmi tisztviselő: ETK Szolgáltató Zrt., adatvédelmi tisztviselő elérhetősége: dpo.kazincbarcika@etk-rt.hu) Kazincbarcika Város Önkormányzata (a továbbiakban: Fenntartó) által irányított és fenntartott, önállóan működő költségvetési szerv, amelynek fő tevékenysége nyilvános könyvtár működtetése, könyvtári és szabadidős szolgáltatások nyújtása.

Az EBVK az adatkezelési tevékenységgel járó folyamatainak hatékony és ésszerű tervezése és szervezése, dokumentálása és nyilvántartása, az alkalmazottak feladat- és jogköreinek meghatározása, az érintettek adatvédelemmel kapcsolatos jogainak biztosítása, valamint az adatvédelmi incidensek kezelésével kapcsolatos eljárásrend kialakítása céljából az alábbi Adatvédelmi és Incidenskezelési Szabályzatot (a továbbiakban: szabályzat) alkotja.

Jelen rendelkezéseket az EBVK egyéb szabályzatainak előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és a bármely más, jelen szabályzat hatályba lépése előtt hatályba lépett szabályzat előírásai között, úgy a jelen rendelkezések az irányadók.

Jelen szabályzat az alábbi jogszabályokban meghatározottakkal együtt értelmezendő. A szabályzatban a jogszabályok és az adatvédelmi felügyeletet ellátó hatóság az alábbi rövidítésekkel szerepelnek:

GDPR	az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről
Infotv.	az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság

2. A szabályzat célja és hatálya

A szabályzat meghatározza az EBVK szervezetén belüli mindazon szervezési és technikai intézkedéseket, azok kialakítását és alkalmazását, folyamatos ellenőrzését, valamint szükség esetén azok korrekcióját, amelyekkel az adatvédelem alapelveinek, a jogszerű adatkezelés feltételeinek, az adatbiztonság követelményeinek érvényesülése megvalósítható.

Adatkezelő az adatok biztonsági állapotának lehetséges sérülése esetén kötelezően elvégzendő vizsgálatra, a vizsgálat eredménye alapján lefolytatandó eljárásokra jelen szabályzatban cselekvési rendet határoz meg annak érdekében, hogy az adatvédelmi incidensek minden esetben azonos, magas színvonalon kerüljenek felderítésre, valamint a lehetséges kockázatok a lehető leghamarabb és leghatékonyabb módszerekkel csökkenthetőek legyenek, az EBVK tevékenysége pedig megfeleljen a GDPR-ban meghatározott elvárásoknak és transzparenciának.

A szabályzat tárgyi hatálya kiterjed az EBVK valamennyi olyan folyamatára, amely során a GDPR 4. cikk 1. pontja szerinti személyes adat kezelése megvalósul.

Jelen szabályzat személyi hatálya kiterjed az Adatkezelő irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyekre (a munkavégzésre irányuló jogviszony jellegétől

függetlenül), és azon természetes személyekre (a továbbiakban: érintett), akik személyes adatát feldolgozzák, továbbá azon érintettek, akik jogait vagy jogos érdekeit az EBVK adatkezelési tevékenysége érinti. Az EBVK alkalmazottai kötelesek a 9. melléklet szerinti dokumentumok és jognyilatkozatok kitöltésére, változás esetén az EBVK vezetőjének értesítésére.

AZ EBVK megbízásából személyes adatok kezelését vagy feldolgozását végzőkkel a GDPR 28. cikkének megfelelő tartalommal adatfeldolgozási szerződést (2. melléklet) kell kötni, amelyben rendelkezni kell arról, hogy az EBVK által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen szabályzat rendelkezéseit (figyelembe véve a 1. mellékletben meghatározott adatvédelmi bekezdések, kiegészítések tartalmát).

AZ EBVK adatkezelést végző alkalmazottai és az EBVK megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottai kötelesek a megismert személyes adatokat üzleti titokként, magántitokként megőrizni, bizalmasan kezelni.

A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek Titoktartási nyilatkozatot tenni (3. melléklet).

3. Fogalmak

Adatállomány: az Infotv. 3. § 21.pontja szerinti adatok („az egy nyilvántartásban kezelt adatok összessége”);

Adatfeldolgozás: az Infotv. 3. § 17. pont szerinti tevékenység („az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége”);

Adatfeldolgozó: a GDPR 6. cikk 8. pontja szerinti személy vagy szervezet („az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel”);

Adatkezelés: GDPR 4. cikk 2. pontjában meghatározott tevékenység („a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés”);

Adatkezelő: GDPR 4. cikk 7. pontjában meghatározott személy vagy szervezet („az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja”);

Adatkezelés korlátozásához való jog: a GDPR 18. cikk. (1) bekezdés szerinti érintetti jog („Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

- a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
- b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

- c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- d) az érintett a 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.”);

Adatmegsemmisítés: az Infotv. 3. § 16. pont szerinti tevékenység („az adatot tartalmazó adathordozó teljes fizikai megsemmisítése”);

Adattovábbítás: Infotv. 3. § 11. pontjában meghatározott tevékenység („az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele”);

Adattörlés: Infotv. 3. § 13. pont szerinti tevékenység („az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges”);

Adatvédelmi incidens: az adatok biztonságának sérülése a GDPR 6. cikk 12. pont szerint („a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi”);

Álnevesítés: a GDPR 6. cikk 5. pontja szerinti tevékenység („a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni”);

Az érintett hozzájárulása: GDPR 4. cikk 11. szerinti jognyilatkozat („az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez”)

Címzett: a GDPR 6. cikk 9. pontja szerinti személy vagy szervezet („az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak”);

EGT-állam: az Infotv. 3. § 23. pontja szerinti államok („az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez”);

Érintett: GDPR 4. cikk 1. pont szerinti személy („azonosított vagy azonosítható természetes személy”);

Érintett jogai: a GDPR 15-21. cikkében szabályozott jogok, azaz

- tájékoztatás joga,
- hozzáférési jog,
- helyesbítéshez való jog,
- törléshez való jog,
- adatkezelés korlátozhatóságához való jog,
- adathordozhatósághoz való jog,

- tiltakozáshoz való jog;

Felügyeleti hatóság: egy tagállam által a GDPR 51. cikknek megfelelően létrehozott független közhatalmi szerv. Az Infotv. 38. § (2a) bekezdés alapján a GDPR-ban a felügyeleti hatóság részére megállapított feladat- és hatásköröket a Magyarország joghatósága alá tartozó jogalanyok tekintetében az általános adatvédelmi rendeletben, valamint az Infotv-ben meghatározottak szerint a NAIH gyakorolja;

Fenntartó: Kazincbarcika Város Önkormányzata Polgármesteri Hivatal

Harmadik fél: a GDPR 4. cikk 10. pontja szerinti személy vagy szervezet („az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak”);

Harmadik ország: az Infotv. 3. § 24. pontja szerinti államok („minden olyan állam, amely nem EGT-állam”);

Képviselő: a GDPR 6. cikk 17. pontja szerinti személy vagy szervezet („az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában”);

Nyilvánosságra hozatal: az Infotv. 3. § 12. pont szerinti közzététel („az adat bárki számára történő hozzáférhetővé tétele”);

Nyilvántartási rendszer: a GDPR 6. cikk 6. pontja szerinti rendszer („a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális, vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető”);

Profilalkotás: a GDPR 6. cikk 4. pontja szerinti tevékenység („személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előre jelzésére használják”);

Releváns és megalapozott kifogás: a GDPR 6. cikk 24. pontja szerinti joggyakorlás („a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve, hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét”);

Személyes adat: GDPR 4. cikk 1. pont szerinti információ („azonosított vagy azonosítható természetes személyre [„érintett”] vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható”);

Személyes adat különleges kategóriái: GDPR 9. cikk 1. szerinti információ („személyes adat különleges kategóriái: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek

egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok”);

Tiltakozás: GDPR 21. cikk (1) bekezdésben meghatározott joggyakorlás („az érintett jogosult arra, hogy saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a GDPR 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is”).

4. Az adatkezelés alapelvei, jogszerűsége

Az EBVK felelős a személyes adatok kezelésére vonatkozó, a GDPR 5. cikk (1) bekezdésében meghatározott alapelvek betartásáért. Az EBVK-nak képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek betartásának igazolására a GDPR 5. cikk (2) bekezdésének megfelelően.

A megfelelés igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettől származó nyilatkozatok (pl. hozzájáruló nyilatkozatok, az adatkezelési tájékoztató megismerését igazoló dokumentumok), továbbá a személyes adatokat tartalmazó (elektronikus vagy papír alapú) dokumentumok szervezeten belüli vagy azon kívüli mozgásának megfelelő dokumentálásával történik.

Az EBVK – a GDPR 30. cikkének megfelelően – nyilvántartást vezet az általa végzett adatkezelésekről (a továbbiakban: adatkezelési tevékenységek nyilvántartása).

A megfelelés igazolása adatvédelmi incidens esetén különösen az incidenssel érintettek körének, az incidenssel érintett személyes adatok körének, az incidens kezelése során tett intézkedéseket megalapozó körülmények és a döntések dokumentálásával történik. Az EBVK – a GDPR 33. cikkének megfelelően – nyilvántartást vezet a bekövetkezett incidensekkel kapcsolatos tényekről és intézkedésekről (adatkezelési incidensek nyilvántartás).

Az EBVK a megfelelés igazolásához az érintetti joggyakorlás teljesítésének körülményeiről nyilvántartást vezet. Érintetti joggyakorlásra vonatkozó megkeresés esetén különösen az adatigénylés tárgyát, dátumát, az érintett személyes adatok körét, az adatszolgáltatásra vonatkozó körülményeket, a megkeresésre adott mindennemű kommunikációt tartja nyilván az Adatkezelő (Érintetti joggyakorlás nyilvántartása).

Az EBVK köteles a személyes adatok kezelésének jogszerűségét biztosítani (GDPR 6. cikk). Személyes adatok kezelése akkor jogszerű, ha a GDPR szerinti jogalapja meghatározható [GDPR 6. cikk (1)], személyes adatok különleges kategóriáinak minősülő adatok esetén pedig az EBVK rendelkezik az általános adatkezelésre vonatkozó tiltás [GDPR 9. cikk (1)] alól a GDPR 9. cikk (2) bekezdése szerinti felmentéssel.

Az EBVK a jogszerűség megalapozottságát, folyamatos fennállását az adatkezelés minden fázisában ellenőrzi, meghatározott időnként felülvizsgálja, és az egyes adatkezelési tevékenységek nyilvántartásában dokumentálja.

Az EBVK nevében adatkezelést végző alkalmazottak kártérítési, szabálysértési- és büntetőjogi felelősséggel tartoznak a személyes adatok jogszerű kezeléséért.

5. Az adatvédelmi tevékenység szervezete

Az adatvédelmi tevékenység irányításában és ellátásában az EBVK vezetője, az adatvédelmi feladatok ellátásában az EBVK vezetője által kijelölt munkavállaló, továbbá a Fenntartó jogi, illetve informatikai feladatokat ellátó munkatársai az alábbiak szerint vesznek részt:

5.1. Az EBVK vezetője

Az EBVK vezetője

- gondoskodik az adatvédelmi irányítási rendszer működtetéséhez szükséges anyagi-, tárgyi-, emberi erőforrás biztosításáról az éves költségvetési tervben meghatározott keretek között;
- a szervezet egyéb szabályzatai és belső rendelkezései kapcsán kiemelt figyelmet fordít a jelen szabályzat és az adatvédelemmel kapcsolatos ágazati jogszabályok érvényesülésére;
- felelős azért, hogy az EBVK személyes adatot tartalmazó dokumentumainak kezelése kapcsán érvényesüljenek a jelen szabályzatban meghatározott elvek, jogok és kötelezettségek;
- kijelöli az adatvédelmi tevékenység irányításában és ellátásában résztvevő személyeket, meghatározza a feladatokat, illetve az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogköröket és szinteket;
- biztosítja, hogy a Fenntartó jogi szakterülete minden személyes adat kezelésével járó beszerzésről, szerződéskötésről tudomással rendelkezzen;
- gondoskodik az adatvédelmi és incidenskezelési, valamint az információbiztonsági szabályzat kiadásáról, betartásáról és betartatásáról;
- intézkedik az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszüntetéséről, szükség szerint a felelősségrevonás kezdeményezéséről;
- gondoskodik a jelen szabályzatban meghatározott kötelezettségek megszegésének szankcionálásáról;
- megbízza az EBVK Adatvédelmi Tisztviselőjét, és az Adatvédelmi Tisztviselő nevét és elérhetőségét bejelenti a NAIH-nak;
- az Adatvédelmi Tisztviselővel, szükség esetén a Fenntartó jogi szakterületével és az informatikai fejlesztést és rendszerüzemeltetést végző szervezettel együttműködve gondoskodik az adatvédelmi és információbiztonsági előírások megismertetéséről, rendszeres oktatásáról a 4. mellékletben foglaltaknak megfelelően;
- ellenjegyzí az adatvédelmi tárgyú kiadmányokat;
- gondoskodik arról, hogy a 9. melléklet szerinti dokumentumok és jognyilatkozatok a munkavállalók felvétele, foglalkoztatása és a munkaviszony megszűnése esetén kitöltésre és a munkavállalók személyi anyagának részeként megőrzésre kerüljenek;
- kiemelt figyelmet fordít arra, hogy szóban, az érintett azonosítása nélkül személyes adatot senki ne közöljön a megkeresőkkel;
- gondoskodik az érintetti joggyakorlások, incidensbejelentések kivizsgálásának koordinálásáról, az Adatvédelmi Tisztviselő értesítéséről;
- biztosítja, hogy az Adatvédelmi Tisztviselő véleményét kikérjék az EBVK adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során;

- biztosítja, hogy a sajtó képviselőivel történő kapcsolattartás során az EBVK által kezelt személyes adatok tekintetében az adatvédelmi és titoktartási kötelezettség érvényesüljön;
- gondoskodik arról, hogy adatvédelmi incidens esetén – az Adatvédelmi Tisztviselő közreműködésével és javaslata alapján – kiadott sajtóközlemény a GDPR szerinti cél elérésére alkalmas legyen.

5.2. Az EBVK vezetője által kijelölt munkavállaló

Az EBVK vezetője által kijelölt munkavállaló:

- gondoskodik a papír alapú dokumentumok iratkezelése során jelen szabályzatban meghatározottak érvényesüléséről;
- felelős az EBVK által végzett adatkezelési tevékenységekkel kapcsolatosan meghatározott folyamatok, és jelen szabályzatban meghatározott elvek gyakorlati alkalmazásáért az Adatvédelmi Tisztviselő szükség szerinti közreműködésével;
- elvégzi az alkalmazottakkal kapcsolatos nyilvántartások vezetését, a tájékoztatások átadását, jognyilatkozatok begyűjtését, iratok tárolását, selejtezését;
- betartja és betartatja az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírásokat;
- gondoskodik arról, hogy az EBVK felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek;
- gondoskodik arról, hogy az EBVK alkalmazottai az adatkezelés meghatározott feltételeinek megfelelően járjanak el (GDPR 32. cikk (4) bek.);
- kiemelt figyelmet fordít arra, hogy a napi feladatellátáshoz használt adatbázisokhoz, nyilvántartásokhoz semmilyen körülmények között ne férjen hozzá illetéktelen személy, valamint arra, hogy a megőrzési idő lejáratakor az adatállományok törlése dokumentáltan megtörténjen;
- a napi feladatellátás során feltárt, informatikai rendszerek működéséből eredő lehetséges adatvédelmi kockázatokat az EBVK vezetője és az Adatvédelmi Tisztviselő felé írásban jelezze.

5.3. A Fenntartó jogi szakterületének feladata

A Fenntartó jogi szakterülete az EBVK vezetőjének kezdeményezésére:

- szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében;
- biztosítja az EBVK képviseletét az érintett által az EBVK ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve az EBVK által a NAIH határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.

5.4. Informatikai fejlesztést és rendszerüzemeltetést végző szervezet feladata

Az informatikai fejlesztést és rendszerüzemeltetést végző szervezet:

- ellátja az informatikai fejlesztéseknél és beszerzéseknél a beépített adatvédelem kontrolljai meglétének biztosításával, az adatminőség biztosításával, az informatikai biztonság kockázatarányos szintjét biztosító jogosultsági és naplózási rendszer kialakításának

megfelelőségével, a biztonságos szoftverfejlesztés alapelveinek érvényesítésével kapcsolatos feladatokat;

- az informatikai rendszerek üzemeltetése területén ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását;
- ellátja a hatáskörébe tartozó információbiztonsági feladatokat, valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és -kezelési tevékenység támogatását;
- az EBVK vezetőjével együttműködve gondoskodik az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról,
- új informatikai rendszer bevezetése, informatikai rendszerrel kapcsolatos változások esetén tájékoztatja az EBVK vezetőjét a tervezett rendszerről, változásokról, intézkedésekről;
- informatikai incidens észlelése esetén haladéktalanul értesíti az EBVK vezetőjét vagy az általa kijelölt munkatársat és az Adatvédelmi Tisztviselőt, biztosítva, hogy a személyes adatokkal kapcsolatos érintettség vizsgálatát elvégezhesse;
- adatvédelmi incidens észlelésekor a kivizsgálási, kockázat csökkentési, értékelési folyamatban aktívan közreműködik a 11. fejezet rendelkezéseinek megfelelően.

5.5. Az Adatvédelmi Tisztviselő

Az EBVK adatvédelmi tevékenységében közreműködő Adatvédelmi Tisztviselőt az EBVK vezetője bízza meg vagy nevezi ki. Adatvédelmi Tisztviselőnek olyan személy vagy szervezet bízható meg vagy nevezhető ki, aki vagy amelynek a feladatot ellátó munkatársa rendelkezik:

- jogi végzettséggel, vagy informatikai főiskolai (BSc) vagy egyetemi (MSc) szintű végzettséggel;
- az európai és hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével;
- alapvető adatvédelmi és informatikai folyamatok ismeretével;
- legalább 2 év adatvédelmi területen szerzett gyakorlattal.

Az Adatvédelmi Tisztviselő megbízása vagy kinevezése mellett az EBVK adatvédelmi tanácsadási feladattal egyéb, jogi vagy természetes személy szakértőt is megbízhat.

Az Adatvédelmi Tisztviselő szakmai tanácsadói feladatot lát, e feladatkörében utasítást nem fogadhat el, az EBVK vagy a Fenntartó munkavállalója esetén szakmai álláspontja miatt – ide nem értve a szakszerűtlen, gondatlan feladatellátást – nem szankcionálható. Jelen szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag az EBVK vezetőjének tartozik felelősséggel.

Az EBVK elősegíti az Adatvédelmi Tisztviselő megfelelő szakmai feladatellátását. Ennek érdekében az EBVK biztosítja az Adatvédelmi Tisztviselő részére megküldött információk teljeskörűségét, az adatvédelmi kérdés kapcsán vizsgált személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést. Amennyiben az Adatvédelmi tisztviselő az EBVK vagy a Fenntartó munkavállalója, részére az EBVK vagy a Fenntartó biztosítja a szakértői szintű ismereteinek fenntartásaihoz szükséges forrást, továbbá elegendő időt feladatai ellátásához. Az Adatkezelő a felügyeleti hatósággal történő együttműködés során az Adatvédelmi Tisztviselő útján – és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

Az Adatvédelmi Tisztviselő véleményét – a jelen szabályzat rendelkezései szerint – ki kell kérni az adatkezelést érintő döntések, szerződések és belső szabályzatok tervezetéről.

Az Adatvédelmi Tisztviselőt tisztsége fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott, közérdekű vagy közérdekből nem nyilvános adatnak nem minősülő információk kapcsán.

Nem lehet Adatvédelmi Tisztviselő az a természetes személy, aki az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen az EBVK vezetője, vagy az adatkezelésért felelős, illetve adatkezelést végző munkatársa, valamint az EBVK informatikai rendszere üzemeltetéséért, fejlesztéséért felelős vezető beosztású munkavállaló.

Az Adatvédelmi Tisztviselő - amennyiben munkavállalóként látja el a feladatkört - az adatvédelmi tisztviselői feladatokon kívül az EBVK döntése alapján más munkakörhöz kötődő feladatokat is elláthat, amennyiben azok nem eredményeznek összeférhetetlenséget.

Az Adatvédelmi Tisztviselő nevét és elérhetőségeit az EBVK honlapján és székhelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. Az EBVK továbbá közli az Adatvédelmi Tisztviselő nevét és elérhetőségét a NAIH-al.

Az Adatvédelmi Tisztviselő feladatai:

- segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- ellenőrzi a GDPR, az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen szabályzat, továbbá az EBVK egyéb belső szabályzatai rendelkezéseinek a megtartását;
- legalább 2 évente belső adatvédelmi ellenőrzési eljárást folytat le minden szakterületen;
- kivizsgálja – szükség szerint az érintett szakterületek bevonásával – a neki címzett panaszokat, jogszertlenség észlelése esetén annak megszüntetésére, korrekciós intézkedés megtételére hívja fel az adatkezelést végzőt vagy az adatfeldolgozót;
- elkészíti, és időszakosan felülvizsgálja, szükség esetén aktualizálja az Adatvédelmi és incidenskezelési szabályzatot;
- gondoskodik az adatvédelmi ismeretek oktatásáról;
- személyes adatot is kezelő, új informatikai rendszer vagy alkalmazás belső fejlesztéssel történő bevezetése során elvégzi az adatvédelmi hatásvizsgálatot;
- az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat;
- vezeti az Adatkezelési Tevékenységek Nyilvántartást;
- éves összefoglaló jelentést készít a szervezet adatvédelmi helyzetéről az EBVK vezetőjének;
- kapcsolatot tart és – szükség szerint az érintett szakterület munkatársainak bevonásával – együttműködik a NAIH-al;
- a NAIH kérésére adatszolgáltatást teljesít;
- a szervezet által kötött szerződések esetében elvégzi a partner pozíciójának meghatározását (pl. adatfeldolgozó, közös adatkezelő, önálló adatkezelő) és a szükséges nyilvántartási feladatokat (adatfeldolgozói megállapodás előkészítése, az adatkezelési tájékoztatók, az adatkezelési tevékenységek nyilvántartása frissítése).

6. Adatvédelmi oktatás

Az Adatvédelmi Tisztviselő gondoskodik az adatvédelmi tudatosság növelése céljából tartandó adatvédelmi és incidenskezelési oktatás megszervezéséről, illetve megtartásáról.

Az oktatások során általános, betekintő jellegű adatvédelmi ismereteket, a szervezeti egységek napi tevékenységi körébe tartozó adatkezelések kapcsán pedig folyamatismertetést, az adatvédelem gyakorlati érvényesülését (pl. értelmezések, esetek), valamint az adatvédelmi incidensekkel kapcsolatos oktatást tart. Az adatvédelmi incidensek kapcsán ismerteti a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit elemzi, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást ad, illetve az ismereteket ellenőrzi.

Az adatvédelmi és incidenskezelési oktatáson való részvétel minden EBVK által munkaviszonyban foglalkoztatott személy részére kötelező.

7. Adatkezelési tevékenység

Az adatkezelési tevékenységek fázisai:

- adatkezelési tevékenység bevezetése,
- adatkezelési tevékenység aktív alkalmazása,
- adatkezelési tevékenység megszüntetése.

7.1. Általános szabályok

Az egyes adatkezelési fázisokban jelen, 7. fejezet szerinti folyamatok alkalmazása szükséges az adatkezelés alapelveinek hatékony érvényesüléséhez.

Minden folyamatot dokumentálni kell a 4. melléklet szerinti adatkezelési tevékenység nyilvántartó lap nyomtatványon. A végleges dokumentumok szakmai megfelelőségéért az adatkezelés létrehozását kezdeményező (a nyomtatványt kitöltő) szakterület, az adatvédelmi megfelelőségéért az Adatvédelmi Tisztviselő a felelős. Abban az esetben, ha bármely szakterület eltér a megfogalmazott szakmai, adatvédelmi vagy információbiztonsági állásfoglalásoktól, az eltérésért, illetve a végleges dokumentumért az eltérő szakterületi vezető tartozik felelősséggel.

Az adatkezelési tevékenységgel kapcsolatos információkat tartalmazó nyilvántartó lapot – a kitöltést követően – az EBKV vezetője vagy az általa kijelölt munkatárs véleményezésre megküldi az Adatvédelmi Tisztviselőnek, és szükség szerint a Fenntartó jogi szakterületének, amely indokolt esetben további szakterületek véleményét is kérheti. A véleményeket a Fenntartó jogi szakterülete összesíti és véglegesíti, szükség esetén a véleményezőkkal való konzultáció után. A vélemények, előkészítő dokumentumok megőrzéséről az EBVK vezetője az adatkezelési tevékenységek nyilvántartásával egy helyen gondoskodik.

Amennyiben az adatkezeléssel kapcsolatos feltételek kidolgozásában a résztvevők között véleményeltérés van, az Adatvédelmi Tisztviselő – szükség szerint az adatkezelést végző szakterület vezetőivel és a véleményezőkkal való konzultáció után – javaslatot tesz a lehetséges megoldásra. Az adatkezeléssel kapcsolatos információk nyilvántartásba vétele, a változás átvezetése kizárólag akkor hajtható végre, ha a konzultációs eljárásban minden résztvevő számára elfogadható megállapodás született az adatkezeléssel kapcsolatban.

Az Adatvédelmi Tisztviselő véleményét az adatkezelésről szóló döntést kezdeményező előterjesztésben ismertetni kell.

Új adatkezelési tevékenység bevezetése, meglévő adatkezelési tevékenység módosítása vagy megszüntetése kizárólag az adatkezelési tevékenység nyilvántartó lapon dokumentált vezetői jóváhagyást követően történhet.

7.2. Új adatkezelési tevékenység bevezetése

Jogszabályban elrendelt vagy az EBVK döntése alapján létrehozandó, személyes adatokat kezelő, új adatkezelés (nyilvántartás, informatikai alkalmazás stb.) bevezetése esetén (ideértve a meglévő nyilvántartási rendszer adatainak új célú felhasználásával, vagy a meglévő nyilvántartási rendszerbe új típusú adatok felvételével, vagy új feltételek [pl. tárolás, harmadik személynek továbbítás stb.] kialakításával járó adatkezelési tevékenységet is) bevezetése során az alábbi folyamat alkalmazása szükséges.

7.2.1. Új adatkezelés bevezetése

Új adatkezelés bevezetése során az adatkezelési tevékenységet végző szervezeti egységnek az Adatvédelmi Tisztviselővel együttműködve meg kell határozni:

- az adatkezelési tevékenység tervezett folyamatát;
- az EBVK adatkezelésben betöltött szerepét (adatkezelőként, más adatkezelővel együtt közös adatkezelőként, adatfeldolgozóként végzi a műveleteket);
- az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így az adatok felvételének, módosításának, törlésének rendjét;
- meglévő nyilvántartásban szereplő új típusú adatok felvétele, vagy a meglévő adatok új célú felhasználása esetén meg kell határozni, hogy az új adatkezelési cél összeegyeztethető-e az adatkezelés eredeti céljával, és így annak jogalapja szolgálhat-e a tervezett új célú adatkezelés jogalapjául [GDPR 6. cikk (4) bek.];
- az adatkezelés lényeges körülményeit érintően:
 - meg kell határozni az adatkezelés célját, jogalapját, szükség szerint feltüntetve a jogalapot alátámasztó jogszabályt, jogos érdeket, szerződést, létfontosságú érdeket, a kezelendő adatkategóriákat, a lehetséges érintettek kategóriáit, valamint a személyes adatok megőrzési idejét;
 - vizsgálni kell, hogy a tervezett adatgyűjtés a célhoz kötött adatkezelés és az adattakarékosság elvének megfelelő -e;
 - meg kell határozni az adatkezelési tevékenység során szükséges adatszolgáltatási kötelezettségeket;
 - meg kell jelölni a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendjét, azoknak a munkavállalóknak, egyéb címzetteknek a körét, akik részére a kezelendő személyes adatok továbbíthatók;
 - vizsgálni kell, hogy történik-e EGT térségen kívülre adattovábbítás, ha igen, melyik országba, milyen feltételekkel;
 - vizsgálni kell az egyéb, az adatkezelés bevezetéséhez eldöntendő feltételek teljesíthetőségét, fennállását;
- az adatkezeléssel járó folyamatokra vonatkozó, és a gyakorlatban alkalmazott általános adatbiztonsági intézkedéseket, kiemelten a személyes adatok sértetlenségével, bizalmasságuk

megőrzésével és az üzletmenet-folytonossággal kapcsolatos kontrollokat (pl. változáskezelés, rendelkezésre állás, jogosultságkezelés, adatretjő eljárások, incidenskezelés támogatása);

- a beépített adatvédelem elvének érvényesítésére alkalmazott technikai megoldásokat az informatikai szakterület közreműködésével;
- az informatikai szakterület közreműködésével azt, hogy az adatkezelés minden fázisa során biztosítható-e az események, változások automatikus dokumentálása (naplózás), amennyiben ez biztosítható, ezek milyen szabályrendszer alapján kerüljenek alkalmazásra;
- amennyiben az adatkezelés során az Érintett jognyilatkozatot tesz, ennek tárolása visszakereshető formában hogyan valósul meg;
- az adatkezelés automatizált döntéshozatali módszerrel történik-e, illetve profilalkotási módszer alkalmazására sor kerül-e (GDPR 22. cikk (1) bekezdés).

7.2.2. Az Adatvédelmi Tisztviselő feladata új adatkezelés esetén:

Az új adatkezelés legfontosabb körülményeinek tisztázását, valamint az új adatkezelés bevezetésének jóváhagyását követően az Adatvédelmi Tisztviselő

- előkészíti az adatkezelési tájékoztatókat, érdekmérlegelési tesztet, továbbá nyilvántartásba veszi az új adatkezelési tevékenységet;
- előkészíti az érintett hozzájárulásán alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját, szerződés teljesítése jogalap esetén a szerződésben rögzítendő, adatkezelésre vonatkozó szakaszokat;
- felméri, hogy egyéb kapcsolódó nyomtatványon, tájékoztató dokumentumban szükséges-e az új adatkezeléssel kapcsolatos tájékoztató módosítása, vagy az elkészült tájékoztató dokumentumok közzététele;
- gondoskodik arról, hogy az új adatkezelésről készített tájékoztatás az EBVK honlapján vagy - ha az új adatkezelési tevékenység bevezetése kizárólag az EBVK munkavállalóit érinti - a helyben szokásos módon az EBVK közlétegye;
- egyedi esetben, szükség szerint előterjesztést tesz az EBVK vezetőjének arról, hogy a személyes adatok harmadik országba továbbíthatók-e.

Amennyiben az új adatkezelés bevezetése elektronikus információs rendszert érint, az informatikai szakterületet is be kell vonni a folyamatba.

Az új adatkezelés bevezetésének igényét megfogalmazó szervezeti egység vezetője az egyéb szakterületek bevonásáról szükség szerint gondoskodik.

Az új adatkezelés feltételeinek kidolgozásában érintett szakterületek és szervezeti egységek vezetői kötelesek egymással és az Adatvédelmi Tisztviselővel együttműködni.

Az új adatkezelés bevezetésének koordinálásáról az Adatvédelmi Tisztviselő gondoskodik.

7.3. Adatkezelési tevékenységek ellátása (aktív szakasz)

7.3.1. Az adatkezelésért felelős szervezeti egység a feladatkörébe tartozó kérdésekben:

- képviseli az adatkezelőt az adatfeldolgozó felé vagy – közös adatkezelés esetén – a többi adatkezelő felé (amennyiben releváns);

- figyelemmel kíséri az adatkezelés feltételeinek folyamatos fennállását (beleértve az adatkezelés jogszerűségéhez szükséges tájékoztatások megadását, nyilatkozatok beszerzését stb.) és szükség esetén megteszi vagy kezdeményezi az adatkezelés feltételeinek módosítása iránti intézkedéseket (beleértve az Adatvédelmi Tisztviselő értesítését is);
- az adathordozók tekintetében köteles gondoskodni a fizikai védelmi mechanizmusok alkalmazásáról (zárható szekrényekben tárolás, iratkezelési szabályzatban meghatározottak követése, fizikai adathordozók védelme stb.);
- az elektronikus információs rendszerek használata tekintetében köteles gondoskodni az adatbiztonsági intézkedések megtételéről, támogatásáról (közreműködés a jogosultsági rendszer napra készen tartásában, jelszópolitika érvényesítése stb.).

7.3.2. Az Adatvédelmi Tisztviselő feladatai az adatkezelési tevékenység aktív szakaszában:

- a hozzájáruláson alapuló adatkezelések esetében ellenőrzi, hogy az érintett az adatkezelési hozzájárulását szabályosan adta-e meg (GDPR 7. cikk (1) bek.);
- gondoskodik arról, hogy legalább az érintettel való első kapcsolatfelvételnél az adatkezelési tájékoztató vagy annak online elérhetősége az érintettek részére rendelkezésre álljon;
- rendszeres időközönként, de legalább évente áttekinti az adatvédelmi hatásvizsgálatban azonosított kockázatok alakulását, elvégzi az adatvédelmi hatásvizsgálatok utóellenőrzését (GDPR 35. cikk (11) bek.),
- az adatkezelés feltételeinek módosítása esetén kapcsolatot tart az érintett szervezeti egységekkel, intézkedik az adatkezelési tevékenység nyilvántartó lapjának kitöltésére, továbbá a változásokat rögzíti az adatkezelési tevékenységek nyilvántartásába.

7.3.3. Változás az adatkezelési tevékenységben az aktív szakaszban

Amennyiben az adatkezelési tevékenység aktív szakaszában szükséges valamilyen adatkezelési feltétel módosítása (pl. meglévő adatkezelés új célja, új adatkör, új megőrzési idő miatt), az EBVK az Adatvédelmi Tisztviselő koordinációjával ismételten megteszi a 7.3 pont szerinti intézkedéseket, és azokat dokumentálja az adatkezelési tevékenység nyilvántartó lapon.

7.4. Adatkezelés megszüntetésével kapcsolatos feladatok

Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult, vagy megszűnt), vagy jogszabályi változások miatt, illetve az adatvédelmi felügyeleti hatóság vagy bíróság döntése értelmében a személyes adatok kezelését meg kell szüntetni, az adatkezelést végző szakterület – az Adatvédelmi Tisztviselő az érintett szakterületek véleményének kikérése után – az adatkezelési tevékenység nyilvántartó lapon javaslatot tesz az EBVK vezetőjének:

- az adatkezelés egészének vagy egyes adatfajták nyilvántartásának megszüntetésére (ezzel együtt az adatok archiválására vagy álnevesítésére a megőrzési idő leteltéig),
- nyilvántartási rendszer egésze vagy egyes adatfajták, illetve adatok törlésére, vagy anonimizálására.

Adatkezelési tevékenység részleges vagy teljes megszüntetésekor az Adatvédelmi Tisztviselő koordinálásával az együttműködő szakterületeknek:

- fel kell mérni az adatkezelési tevékenység részleges vagy teljes megszüntetésével járó következményeket,

- az Adatkezelési Tevékenységek Nyilvántartásából az adatkezelést vagy az egyes adatfajtákat törölni kell,
- az adatokat az informatikai rendszerekben archiválni, vagy álnevesíteni kell, illetve
- az informatikai rendszerekből törölni vagy anonimizálni kell, a papír alapú nyilvántartásban kezelt adatokat pedig selejtezni kell,
- jogszabály eltérő rendelkezése hiányában értesítenie kell az érintetteket és mindazokat, akik az anonimizált vagy törölt adatokat korábban megkapták.

8. Érdekmérlegelés

8.1. Általános rendelkezések

Amennyiben az adatkezelési tevékenység végzése az EBVK, vagy harmadik fél jogos érdekére alapozható [GDPR 6. cikk (1) bekezdés f) pontja], az adatkezelési folyamat akkor és annyiban lesz jogszerű, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

Az adatkezelés jogszerűségének vizsgálatához a tevékenység bevezetésekor az Adatvédelmi Tisztviselő az érintett szakterületek aktív közreműködésével elvéggez egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és írásban megfelelően alátámasztja, összegzi. Minden egyes, jogos érdeken alapuló adatkezelési tevékenységhez külön érdekmérlegelési tesztet kell elvégezni.

Az érdekmérlegelési teszt során az EBVK azonosítja jogos érdekét az adatkezeléshez, valamint a súlyozás ellenpontját képező érintett alapjogokat és érdekeket mérlegeli. Az egymással ellentétes jogok és érdekek súlyozásának feltételét mindig az adott eset sajátos körülményeire való tekintettel vizsgálja. Az EBVK a mérlegelés során figyelembe veszi különösen a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabálysértés súlyosságát stb.

Az érdekmérlegelési teszt részeként a szükségesség és arányosság vizsgálatát is elvégzi az EBVK. A kezelhető adatok jellege és mennyisége nem haladhatja meg a jogszerű érdekek érvényesítése céljából szükséges mértéket. Az arányosság vizsgálata a célok és a megválasztott eszközök közötti kapcsolat értékelését foglalja magában. A választott eszközök a szükségesség mértékét nem haladhatják meg, azonban az eszközöknek is alkalmasnak kell lenniük a meghatározott cél elérésére.

Az érdekmérlegelés elvégzése alapján az EBVK megállapítja, hogy kezelhető-e a személyes adat.

A teszt lényegéről az érintettek tájékoztatást kapnak az adatkezelési tájékoztatóban, amelyben röviden ismertetni kell, hogy az EBVK adatkezeléshez fűződő jogos érdeke miért erősebb az érintett jogainál, illetve érdekeinél. Az EBVK tájékoztatja az érintetteket az alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről.

8.2. Érdekmérlegelési teszt elkészítésének folyamata

AZ EBVK a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése, megvizsgálja, hogy rendelkezésre állnak-e olyan alternatív folyamatok, adatok, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.

Amennyiben a tervezett célhoz elengedhetetlen a személyes adatok kezelése, továbbá a GDPR 6. cikk (1) bekezdés a)-e) pontjaiban említett adatkezelési jogalapok egyike sem alkalmas az adatkezelés megalapozásához, az EBVK elvégzi az érdekmérlegelési tesztet, amelyben

- körütekintően és részletesen meghatározza az adatkezeléssel összefüggő jogos érdekét;
- meghatározza az adatkezelés lényeges körülményeit (cél, kezelt adatok köre, adatkezelés folyamata stb.);
- meghatározza, hogy az adatkezelés az érintettek mely jogait és szabadságait érinti, illetve mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket az érintettek felhozhatnak az adatkezeléssel szemben);
- elvégzi a jogos érdekeinek és az érintettek alapjogainak, vélelmezett érdekeinek összevetését, és ez alapján megállapítja, hogy a személyes adat kezelhető-e. Az EBVK meghatározza, hogy miért arányos az érintetti jogok korlátozása, illetve az érinti várakozásoktól eltérés a jogos érdekeivel, milyen érdeksérelemmel járhat a jogkorlátozás hiánya;
- meghatározza, hogy az információs egyensúly hiánya ellenére mely garanciák biztosíthatják az érintett jogainak és szabadságainak védelmét, valamint az érintett érdekeinek érvényesülését.

Az érdekmérlegelési tesztet írásban kell elkészíteni, az 5. számú melléklet szerinti nyomtatványon.

9. Hatásvizsgálat

Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelést megelőzően adatvédelmi hatásvizsgálatot kell végezni. Olyan, egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokat jelentenek, egyetlen adatvédelmi hatásvizsgálat (a továbbiakban: hatásvizsgálat) keretei között is értékelhetők.

A hatásvizsgálat elvégzésének szükségességéről az Adatvédelmi Tisztviselő állást foglal, és az érintett szakterületek bevonásával elkészíti a hatásvizsgálatot. A hatásvizsgálat megállapításait írásban kell rögzíteni.

Ha az Adatvédelmi Tisztviselő úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal az érintettek jogaira és szabadságaira, úgy meg kell indokolnia és dokumentumokkal igazolnia a mellőzés okait. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a NAIH által közzétett jegyzékben (https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf) szereplő tevékenységek esetén kötelező elvégezni.

A fenti eseteken túl minden olyan bevezetésre kerülő – különösen az új technológiákat alkalmazó – adatkezelés esetén hatásvizsgálatot kell végezni, mely adatkezelés az érintettekre tekintettel jelentős joghatással bír/a természetes személyt jelentős mértékben érinti.

A hatásvizsgálat elvégzése során EBVK a NAIH honlapján közzétett szoftvert alkalmazza, a hatásvizsgálatot abban végzi el (<https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html>)

A hatásvizsgálat megállapításait az adatkezelési tevékenység nyilvántartó lapjához hozzá kell csatolni és a hatásvizsgálatban tett megállapításoknak megfelelően kell kialakítani az adatkezelést.

A hatásvizsgálatot legalább évente felül kell vizsgálni, szükség esetén újra el kell végezni.

10. Adatbiztonsági szabályok

10.1. Fizikai védelem

A papír alapon kezelt személyes adatok biztonsága érdekében az EBVK az alábbi intézkedéseket alkalmazza:

- a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi szempontból biztosított, lehetőleg zárható helyiségben helyezi el;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá, a folyamat lezárását követően az iratokat irattárba kell helyezni;
- az EBVK adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat, papír alapú adathordozókat elzárja, vagy az irodát bezárja, a kulcsot a vagyonőrök részére leadja;
- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó adatbiztonsági szabályokat alkalmazza az EBVK,
- a papír alapú dokumentumokat az iratkezelési szabályoknak megfelelően kezeli.

Amennyiben a papír alapon tárolt személyes adat kezelésének célja megvalósult, úgy az EBVK vezetője az illetékes szakterület bevonásával intézkedik az irat selejtezéséről és megsemmisítéséről. Az adatkezelésért felelős szervezeti egység a megsemmisítésben közreműködő szervezeti egység bevonásával állítja össze a megsemmisítendő iratsomagot. A megsemmisítésen az EBVK vezetője által kijelölt háromtagú megsemmisítési bizottság vesz részt. A megsemmisítési bizottság legalább egy tagját az EBVK delegálja. A megsemmisítésről jelen szabályzat 6. mellékletében lévő nyomtatványt kell kitölteni.

Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére (ide nem értve az adattörlést) a papíralapú dokumentumokra vonatkozó megsemmisítési szabályok az irányadók.

Az EBVK valamennyi adatkezelése tervezésekor, bevezetésekor vizsgálja az alkalmazandó fizikai védelmi intézkedéseket is.

10.2. Logikai védelem

A számítógépen, illetve informatikai hálózaton tárolt személyes adatok biztonsága érdekében az EBVK, illetve az informatikai fejlesztésért és üzemeltetésért felelős szervezet külön szabályzatban rögzíti:

- a fejlesztési folyamatai során kötelezően alkalmazandó szempontrendszerait (beépített adatvédelem és információbiztonság elveinek alkalmazása),
- az informatikai eszközkezelés életciklusait,
- a jogosultság, és hozzáférésmenedzsment folyamatait,
- a mentési és archiválási rendjét,
- a naplózási rendjét,
- a külső adathordozói védelmének rendjét,
- a kötelezően alkalmazandó határvédelmi megoldásokat

- az adattárolók, szerverek biztonsága (fizikai, logikai, adminisztratív) céljából alkalmazott egyéb intézkedéseit.

Az EBVK valamennyi adatkezelése tervezésekor, bevezetésekor vizsgálja az alkalmazandó logikai védelmi intézkedéseket is.

10.3. Álnevesítés, anonimizálás

Az anonimizálás a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik. Ilyen esetben tehát az adat elveszti személyes adat jellegét. Amennyiben az adat az anonimizálás után visszaállítható (az adat és a természetes személy közötti kapcsolat helyreállítható) az Adatkezelőnél vagy az informatikai fejlesztésért és üzemeltetésért felelős szervezetnél közvetlenül rendelkezésre álló kulcs használatával, nem tekinthető úgy, hogy az adat elvesztette személyes adat jellegét, ezért azok kezelésére az adatvédelmi szabályok továbbra is érvényesek.

Amennyiben a személyes adatot egy vagy több algoritmus szerint képzett karaktersorral váltják fel az azonosítás elfedéséhez, álnevesítés történik. Álnevesített adatok tekintetében a feloldáshoz (az azonosítás újbóli elvégzéséhez) szükséges információt az EBVK logikailag elkülönülten tárolja, valamint technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot csak meghatározott körülmények között lehessen újra hozzákapcsolni. A fejlesztési, üzemeltetési folyamatok során minden esetben vizsgálni kell ennek a lehetőségét, és ha ez a lehetséges kockázatokkal arányos költség ellenében megvalósítható, álnevesített tárolási eljárást kell alkalmazni.

Az anonimizált adatok kezelését az EBVK a statisztikai célra gyűjtendő adatok, az álnevesített adatok kezelését az informatikai fejlesztés, tesztelés, karbantartás alatt álló rendszerek esetében a tesztadatok tekintetében végzi.

Az EBVK valamennyi adatkezelése tervezésekor, bevezetésekor vizsgálja az anonimizálás és álnevesítés alkalmazásának eseteit is.

10.4. Beépített adatvédelem

Az informatikai fejlesztési, folyamatszervezési feladatok ellátása során már a tervezési fázisban törekedni kell az adatvédelem elveinek érvényesülésére. Ennek érdekében át kell gondolni, hogyan valósítható meg:

- a személyes adatok kezelésének adatkezelési célhoz igazodó, minimálisra csökkentése,
- a személyes adatok álnevesítése vagy anonimizálása,
- a személyes adatok kezelésének és a kapcsolódó szervezeti funkciók átláthatósága,
- a törlési kötelezettség maradéktalan teljesítése – lehetőleg az adatok álnevesítése által, így megelőzve az alkalmazásban kezelt egyéb adatok rendelkezésre állásának biztosítására vonatkozó kötelezettség sérülését,
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritása, rendelkezésre állása és ellenálló képessége,
- fizikai vagy műszaki incidens esetén az arra való képesség, hogy a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állása kellő időben visszaállítható legyen;

- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelése, felmérése és értékelése rendszeres időközönként megtörténjen,
- a hozzáférési jog közvetlen gyakorlásának lehetősége kialakításra kerüljön.

Az EBVK és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az EBVK utasításának megfelelően kezelhessék az adatokat.

Adatvédelmi incidens kezelése

10.5. Adatvédelmi incidens észlelése és jelentése

Az EBVK minden foglalkoztatottja – beleértve az egyéb jogviszonyban foglalkoztatott személyeket is – köteles az EBVK tevékenysége során bekövetkezett (adatvédelmi) incidenst vagy annak gyanúját haladéktalanul jelenteni az EBVK vezetőjének és az Adatvédelmi Tisztviselőnek. A bejelentést nem szabad késleltetni információgyűjtésre hivatkozással.

Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni az EBVK tulajdonát képező informatikai eszközön (pl. adathordozón, mobiltelefonon, laptopon, egyéb számítástechnikai eszközön) kezelt személyes adatokra függetlenül attól, hogy a munkavégzés helye az adatvédelmi incidens észlelésének időpontjában hol van. Az adatvédelmi incidensre vonatkozó szabályokat az EBVK birtokában lévő papíralapú adathordozón lévő adatokra is alkalmazni kell.

A bejelentésnek tartalmaznia kell a bejelentő nevét, telefonszámát, beosztását, szervezeti egységének megnevezését, valamint az incidens tárgyát, rövid leírását és azt, hogy az incidens érinti-e az EBVK valamelyik informatikai rendszerét. A bejelentés megtehető szabadszöveges formában, vagy az Incidens kivizsgáló lap (7. melléklet) nyomtatványon. Telefonon tett bejelentés esetén a bejelentést követően a bejelentőnek ki kell töltenie a 7. melléklet szerinti nyomtatványt, és el kell juttatnia az Adatvédelmi Tisztviselőnek, aki a vizsgálat további szakaszaiban véglegesíti az Incidens kivizsgáló lap tartalmát.

Amennyiben az adatvédelmi incidens érinti az EBVK informatikai rendszerét is, akkor a bejelentést az az adott információs rendszer működtetéséért, fejlesztéséért felelős informatikai szakterületnek is meg kell küldeni.

Amennyiben a fentiek szerint megadandó információk valamelyike a bejelentésekor még nem áll rendelkezésre, a hiányzó információkat később, a részletes kivizsgálás keretében kell rögzíteni.

A bejelentés Adatvédelmi Tisztviselőhöz történő beérkezését követően az Adatvédelmi Tisztviselő haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését.

10.6. Adatvédelmi incidens kivizsgálása, értékelése

Az Adatvédelmi Tisztviselő – informatikai rendszert érintő incidens esetén az adott információs rendszer működtetéséért, fejlesztéséért felelős informatikai szakterülettel együttműködve – megvizsgálja a bejelentést, és amennyiben szükséges, a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az Adatvédelmi Tisztviselő felhívására – amennyiben a szabadszavas, illetve a telefonos bejelentésben vagy a 7. pont szerinti nyomtatványon nem szerepel – a bejelentő köteles megadni:

- az adatvédelmi incidens bekövetkezésének időpontját és helyét,
- az adatvédelmi incidens egyéb körülményeit,
- az adatvédelmi incidens által érintett adatok körét, mennyiségét,

- az adatvédelmi incidenssel érintett személyek körét és számát,
- az adatvédelmi incidens várható hatásait,
- az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett intézkedések felsorolását.

A bejelentő az adatszolgáltatást a felhívást követően haladéktalanul, de legkésőbb 8 órán belül teljesíti az Adatvédelmi Tisztviselő részére.

Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel, az Adatvédelmi Tisztviselő az adott információs rendszer működtetéséért, fejlesztéséért felelős informatikai szakterülettel, valamint egyéb, a vizsgálat lefolytatásához szükséges munkatársak bevonásával lefolytatja a vizsgálatot.

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

A vizsgálat eredményeként az Adatvédelmi Tisztviselő javaslatot tesz az EBVK vezetőjének és szükség szerint az informatikai üzemeltetését felelős szervezeti egységnek az incidenskezeléshez szükséges intézkedések megtételére.

A javaslat alapján a megvalósítandó, további intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület véleményének figyelembevételével – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében az adott információs rendszer üzemeltetéséért vagy fejlesztéséért felelős informatikai szakterülettel együttműködve – az EBVK vezetője dönt.

A vizsgálatot legkésőbb a bejelentés EBVK vezetőjéhez, illetve az Adatvédelmi Tisztviselőhöz történő érkezésétől számított 72 órán belül be kell fejezni. Amennyiben ezen időszak alatt az adatvédelmi incidens körülményei nem tárhatók fel teljes egészükben, a vizsgálatot addig kell folytatni, amíg a vizsgálatot megnyugtatóan le lehet zárni. Az adatvédelmi incidens vizsgálatának meghosszabbítása legfeljebb 30 napig tarthat.

10.7. Az adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidensekről az EBVK a 8. melléklet szerinti nyilvántartást vezet.

Az adatvédelmi incidensek nyilvántartása tartalmazza:

- a bejelentő megnevezését
- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az elhárítására megtett intézkedéseket és
- egyéb jogszabályban előírt adatokat.

Az adatvédelmi incidensek nyilvántartása pontos vezetéséről, aktualizálásáról az EBVK vezetője által kijelölt személy gondoskodik.

10.8. Az adatvédelmi incidens bejelentése a NAIH részére

Az Adatvédelmi Tisztviselő az adatvédelmi incidenst az arról való tudomásszerzést követően haladéktalanul, de legkésőbb az adatvédelmi incidens bekövetkezésétől számított 72 órán belül bejelenti a NAIH részére, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár magas kockázattal a természetes személyek jogaira és szabadságaira nézve. Az adatvédelmi incidens bejelentése szakaszosan is történhet.

Ha az adatvédelmi incidens bejelentése nem történik meg határidőben, az Adatvédelmi Tisztviselő köteles ennek okát igazolni a NAIH részére.

A NAIH-nak történő bejelentésnek tartalmaznia kell:

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

10.9. Az érintettek tájékoztatása az adatvédelmi incidensről

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az Adatvédelmi Tisztviselő az EBVK vezetőjének jóváhagyásával haladéktalanul értesíti az érintetteket.

Nem kell az érintetteket tájékoztatni:

- ha az EBVK olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét;
- ha az adatvédelmi incidens bekövetkezését követően az EBVK olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázatból eredő hátrányos következmények az érintettek nézve valószínűsíthetően nem valósulnak meg;
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton, vagy a Fenntartó bevonásával sajtó útján is megtörténhet.

11. Az érintettek jogainak érvényesítése

Az EBVK köteles gondoskodni az érintetti jogok gyakorlásának biztosításáról. Az érintetti jogok gyakorlásának teljesítési határideje a kérelem, kérdés beérkezését követő legfeljebb egy hónap. Indokolt esetben ez a határidő további két hónappal meghosszabbítható, amelyről az érintettet a határidő meghosszabbításának indokát tartalmazó értesítésben tájékoztatni kell.

Az érintetti jogok gyakorlására írásbeli bejelentést követően van lehetőség az EBVK hivatalos elektronikus elérhetőségein (az egressykonyvtar@gmail.com vagy az 1. pontban jelölt elérhetőségen).

Az EBVK Adatvédelmi Tisztviselője a hozzá beérkezett kérelemről, illetve az adatkezelés elleni tiltakozásról köteles a beérkezéstől számított 10 napon belül értesíteni az adatkezelés szempontjából feladat- és hatáskörrel rendelkező szervezeti egység vezetőjét, és részére megküldeni szakmai álláspontját a kérelem teljesíthetőségéről, a teljesítés módjáról.

A feladat- és hatáskörrel rendelkező szervezeti egység vezetője véleményegyezőség hiányában egyeztet az Adatvédelmi Tisztviselővel, majd a közösen kialakított álláspontjuk alapján az Adatvédelmi Tisztviselő előkészíti az érkezésétől számított legkésőbb 25 napon belül az Érintett részére kiadmányozandó, közérthető írásbeli válaszát. A választervezetet kiadmányozás előtt az Adatvédelmi Tisztviselő egyezteti az EBVK vezetőjével, aki kiadmányozza az iratot.

11.1. Tájékoztatáshoz való jog (GDPR 13. és 14. cikk)

Az Adatkezelő tömör, érthető és könnyen hozzáférhető formában köteles tájékoztatni az érintettet az adatkezelés tényéről, céljáról, jogalapjáról és körülményeiről a GDPR 13-14. cikkében meghatározottak szerint.

Az EBVK a tájékoztatási kötelezettségének első sorban honlapján közzétett adatkezelési tájékoztatók útján tesz eleget. Az EBVK az adatfelvételkor, első kapcsolatfelvételkor haladéktalanul, az adatok harmadik féltől való megszerzése esetén az attól számított legfeljebb 30 napon belül tájékoztatja az érintetteket az adatkezelés körülményeiről. EBVK a honlapján közzétett adatkezelési tájékoztatóin kívül más formában nem tájékoztatja az érintetteket az adatkezelés lényeges körülményeiről, ha az adatkezelést kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog.

Az adatkezelési tájékoztató legalább az alábbi információkat tartalmazza:

- tájékoztatást az Adatkezelő kilétéről, elérhetőségeiről, Adatvédelmi Tisztviselője elérhetőségeiről,
- tájékoztatást az adatkezelés céljáról, jogalapjáról, az adatkezelő vagy harmadik fél jogalapot teremtő jogos érdekeiről,
- tájékoztatást a személyes adatok címzettjeiről, illetve a címzettek kategóriáiról, EGT országon kívüli adattovábbítás esetén annak körülményeiről,
- tájékoztatást az adatmegőrzésre kitűzött időtartamról,
- tájékoztatást az érintetti joggyakorlási lehetőségekről, jogorvoslati lehetőségekről, hozzájárulás visszavonásának korlátlan lehetőségéről,
- tájékoztatást arról, hogy milyen jogi kötelezettségen alapul az adatkezelés, vagy szerződés feltétele-e, adatkezelés hiányának következményei e két esetben,
- tájékoztatást arról, hogy automatizált döntéshozatalt, profilalkotást végez-e az adatkezelő, ha igen, ennek körülményeiről.

11.2. Hozzáférési jog (GDPR 15. cikk)

Az érintett jogosult az EBVK-től információt kérni arra vonatkozóan, hogy vele kapcsolatban végez-e adatkezelési tevékenységet.

Hozzáférési jog gyakorlása esetén az érintett minden esetben legalább a természetes személyazonosító adatainak megadására köteles, valamint rendelkeznie kell arról, hogy milyen csatornán kívánja a hozzáférési joga gyakorlására kapott válasziratot kézhez venni. Az EBVK kizárólag a megadott adatok alapján végzi el keresését, és annak eredményéről tájékoztatja az érintettet.

Amennyiben az EBVK végez az érintettel kapcsolatban adatkezelési tevékenységet, az érintettnek lehetősége van a róla, illetve vele összefüggésben kezelt információkhoz való hozzáféréshez, valamint amennyiben tagállami törvény nem rendelkezik eltérően, kérése nem lehetetlen, vagy nem érinti hátrányosan mások jogait és szabadságait, jogosult az EBVK kezelésében lévő adatairól elektronikus vagy egyéb formátumú másolatot kérni, ami évente egyszer térítésmentes. Amennyiben az érintett további másolatokat igényelne, az EBVK jogosult az indokolt költségek fedezésére térítési díjat felszámítani.

Az Adatvédelmi tisztviselő a szervezeti egységek vezetőitől információt kér, hogy az általuk kezelt nyilvántartásokban az érintett által megadott adatok, illetve kért információk fellelhetőek-e. Ha van folyamatban adatkezelési tevékenység az érintettre vonatkozóan, a szervezeti egységek vezetője az adatbekérő nyomtatvány kitöltésével, 5 munkanapon belül tájékoztatja az Adatvédelmi Tisztviselőt, és szükség esetén csatolja az adatokról készített elektronikus másolatot is.

11.3. Helyesbítéshez való jog (GDPR 16. cikk)

A valóságnak nem megfelelő adatot az EBVK – amennyiben a szükséges adatok és az azokat bizonyító okiratok rendelkezésre állnak – helyesbíti, illetve a GDPR. 17. cikkében meghatározott okok fennállása esetén törli. Nem gyakorolható ez az érintetti jog azokra a személyes adatokra, amelyekre ezt jogszabály kizárja (pl. beadvány hitelességének megőrzése).

Bármely érintett kérheti az Adatkezelőtől a rá vonatkozó adatainak módosítását (javítását vagy kiegészítését). Az érintett kérelmére a helyesbítésről haladéktalanul intézkedni kell, amelynek megtörténtéről az érintett által megadott elérhetőségre tájékoztatást kell küldeni.

Helyesbítési jog gyakorlása esetén az Adatvédelmi Tisztviselő lefolytatja a hozzáférési jog gyakorlásánál ismertett eljárást, felméri a kapcsolódó nyilvántartásokat, megvizsgálja a kérelem teljesíthetőségének feltételeit. Amennyiben az igény teljesíthető, jelzi a nyilvántartást kezelő szakterület részére a helyesbítés végrehajthatóságát. A szervezeti egységek legfeljebb 3 munkanapon belül köteles gondoskodni a helyesbítés dokumentált végrehajtásáról.

11.4. Törléshez való jog (GDPR 17. cikk)

A személyes adatot törölni kell, ha

- az adatkezelés jogellenes, így különösen, ha az adatkezelés az 4. pont szerinti alapelvekkel ellentétes, vagy
- az adatkezelés célja teljesült vagy megszűnt, vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához, vagy
- az adatkezelés törvényben, nemzetközi szerződésben vagy az Európai Unió kötelező jogi aktusában meghatározott időtartama eltelt, vagy
- az adatkezelés jogalapja megszűnt és az adatok kezelésének nincs másik jogalapja,
- az érintett az adatkezeléshez adott hozzájárulását visszavonja vagy a személyes adatainak törlését kéri;
- az adatok törlését jogszabály, az Európai Unió jogi aktusa, a hatóság vagy a bíróság elrendelte.

A személyes adatok nem törölhetők a GDPR 17. cikkében vagy jogszabályban meghatározott feltételek fennállása esetén (pl. ha azok a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából, jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez, vagy közérdekű archiválás céljából szükségesek).

Törlési kérelem esetén az Adatvédelmi Tisztviselő felméri a vonatkozó adatkezeléseket, és megvizsgálja a kérelem teljesíthetőségének feltételeit. Amennyiben a törlés teljesíthető, jelzi a szakrendszert kezelő szakterület vezetőjének, aki köteles legfeljebb 3 munkanapon belül intézkedni a törlés dokumentált végrehajtásáról.

11.5. Az adatkezelés korlátozásához való jog (GDPR 18. cikk)

Az érintett jogosult arra, hogy kérésére az EBVK korlátozza az adatkezelést, amennyiben az alábbi feltételek valamelyike áll fenn:

- az érintett vitatja a személyes adatok pontosságát,
- az adatkezelés jogellenes és az érintett ellenzi az adatok törlését, ehelyett kéri azok felhasználásának korlátozását,
- az EBVK-nek már nincs szüksége a személyes adatokra az adatkezelés céljából, azonban az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett tiltakozik az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy EBVK jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A korlátozott kezelésű személyes adatokkal csak az érintett hozzájárulásával, jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve valamely tagállam által meghatározott fontos közérdekből végezhető a tároláson kívül egyéb adatkezelési művelet.

A személyes adat kezelése korlátozásának kérése esetén az Adatvédelmi Tisztviselő felméri az érintett adatkezeléseket, és megvizsgálja a kérelem teljesíthetőségének feltételeit. Amennyiben az igény teljesíthető, jelzi a nyilvántartást kezelő szakterület vezetője részére, hogy a személyes adattal az ismételt értesítésig a tároláson kívül egyéb adatkezelési művelet nem végezhető. Abban az esetben, ha az adatkezelés korlátozásának időtartama vélhetően meghaladja a személyes adat megőrzésére kijelölt időt, külön figyelmet kell fordítani arra, hogy a korlátozás alá eső személyes adatokat az azt kezelő rendszer automatikusan ne törölje vagy anonimizálja, papír alapú adatkezelés esetén az adathordozó selejtezésére ne kerüljön sor addig, amíg az adatkezelés korlátozásának időtartama el nem telik.

A személyes adatok korlátozásával kapcsolatos vizsgálatot (ideértve a jogi igények érvényesítéséhez vagy védelméhez szükséges bírósági eljárás lefolytatását is) követően az Adatvédelmi tisztviselő értesíti a kapcsolódó nyilvántartást kezelő szervezeti egység vezetőjét a korlátozás feloldásáról, és a korlátozás alól feloldott személyes adat további kezeléséről vagy törléséről.

A korlátozás alá eső személyes adatot tartalmazó nyilvántartást kezelő szervezeti egység vezetője haladéktalanul, legfeljebb 1 munkanapon belül gondoskodik az adatkezelés korlátozásának dokumentált végrehajtásáról. Az Adatvédelmi Tisztviselő értesítését követően legfeljebb 3 munkanapon belül el kell végezni a személyes adat korlátozás alóli feloldását és – ha az értesítés ezt tartalmazza – törlését.

11.6. Adathordozhatósághoz való jog (GDPR 20. cikk)

Ha az adatkezelés az érintett hozzájárulásán alapul, vagy szerződés kötéséhez, illetve teljesítéséhez szükséges, és az adatkezelés automatizált módon történik, az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formában megkapja, továbbá jogosult arra, hogy kérésére az EBVK ezeket az adatokat egy másik adatkezelőnek továbbítsa.

Adathordozási kérés esetén az Adatvédelmi Tisztviselő felméri az érintett adatkezeléseket, és megvizsgálja a kérelem teljesíthetőségének feltételeit. Amennyiben az igény teljesíthető, jelzi a hordozni kért személyes adatot tartalmazó informatikai rendszer üzemeltetéséért felelős szervezeti egység részére az elektronikus másolat elkészítésének igényét. Az érintett számára átadandó, hordozható másolatot legfeljebb 15 munkanapon belül kell elkészíteni.

11.7. Tiltakozáshoz való jog (GDPR 21. cikk)

Az érintett tiltakozhat személyes adatának kezelése ellen,

- ha a személyes adatok kezelése vagy továbbítása közérdekű feladatellátáshoz kapcsolódó, vagy közhatalmi jogosultságok érvényesítéséhez szükséges jogalapon vagy
- az EBVK vagy harmadik személy jogos érdekének érvényesítéséhez szükséges jogalapon történik; vagy
- ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint
- törvényben meghatározott egyéb esetben.

Az Adatvédelmi Tisztviselő az adatkezelés elleni tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja.

Ha az Adatvédelmi Tisztviselő az érintett tiltakozásának megalapozottságát megállapítja, haladéktalanul értesíti az illetékes szervezeti egység vezetőjét, hogy intézkedjen az adott érintett vonatkozásában az adatkezelés – beleértve a további adatfelvételt és adattovábbítást is – megszüntetéséről, továbbá értesítse az összes olyan címzettet, akinek részére a tiltakozással érintett személyes adatot korábban továbbította.

12. Adattovábbítások, adatfeldolgozói és közös adatkezelői jogviszony kezelése

Az EBVK minden szerződéskötés előtt megállapítja a másik szerződő fél státuszát (adatkezelő, közös adatkezelő vagy adatfeldolgozó).

Ha személyes adatokat is megismer a szerződő fél a szerződés teljesítése során, akkor vagy

- önálló adatkezelők közötti adattovábbításról,
- adatfeldolgozói, vagy
- közös adatkezelői jogviszonyról van szó.

Az 5. fejezetben meghatározott felelős megvizsgálja, hogy szükség van-e külön adatfeldolgozói vagy közös adatkezelési megállapodás megkötésére, vagy a meglévő szerződés kiegészítésére, módosítására. Amennyiben a Szervezet közös adatkezelői jogviszonyt létesít egy vagy több partnerrel, közös adatkezelői megállapodást kell kötni, amely megfelel a GDPR 26. cikk feltételeinek.

Meg kell vizsgálni továbbá, hogy személyes adat harmadik országba történő továbbításának szükségessége felmerül-e, ideértve harmadik országbeli adatfeldolgozó igénybevételét is.

Adatfeldolgozó igénybevétele esetén lehetőség szerint 2. mellékletben szereplő Adatfeldolgozói megállapodás iratmintát kell alkalmazni.

13. Záró rendelkezések

Jelen szabályzattal érintett munkavállalóknak a szabályzat rendelkezéseit meg kell ismerniük és annak tényét az aláíróíven igazolniuk kell.

A jelen szabályzat 2025. napján lép hatályba.

Jelen szabályzat rendelkezéseit alkalmazni kell a hatálybalépésekor már folyamatban lévő adatkezelési tevékenységekre, érintetti joggyakorlásokra és incidenskezelési folyamatra is.

Budapest, 2025.

1. melléklet: Szerződésekben használandó adatvédelmi, titoktartási, kapcsolattartási klauzulák

ADATVÉDELEM

[kitöltendő] jelen szerződésben személyes adatok kezelésével is járó szakértői feladatok ellátására vállalt kötelezettséget, amely feladatok végrehajtása során adatfeldolgozóként adatkezelési tevékenységet végez jelen [kitöltendő] részére a Szerződés [kitöltendő]. mellékletében meghatározott feltételeknek megfelelően. Az adatfeldolgozói megállapodás a Szerződés elválaszthatatlan része.

TITOKTARTÁS

Jelen [kitöltendő] fejezetben foglalt titoktartási rendelkezések alkalmazását jogszabály kizárhatja, korlátozhatja. A Szerződés megszűnése nem érinti a Felek titoktartási kötelezettségét.

A Szerződés aláírásával Felek feltétlen és visszavonhatatlan kötelezettséget vállalnak arra, hogy a Szerződés végrehajtása során tudomásukra jutott minden adatot, információt időbeli korlátozás nélkül, a 2018. évi LIV. törvénynek megfelelően, külön minősítési eljárás nélkül is üzleti titokként kezelnek. Felek az átadott mindennemű információt kizárólag a Szerződés keretei között használhatják, kizárólag azoknak a szintén titoktartási kötelezettség hatálya alatt álló személyeknek hozhatják tudomására, akiknek azt a Szerződésben meghatározott célok elérése érdekében tudniuk kell. Felek az információt ugyanolyan gondossággal kötelesek kezelni, mint amellyel a hasonló információk titkosságát és bizalmas jellegét saját szervezetükön belül védik. Az üzleti titok az átadó fél tulajdonában marad és a fogadó félnek történő átadás (tudomásra hozás) csak korlátozott engedélyt ad Feleknek, vagy bármely velük a Szerződéssel kapcsolatban jogviszonyban álló harmadik személynek a fenti információ felhasználására.

Felek rögzítik, hogy a titoktartási kötelezettség megsértését súlyos szerződésszegésnek tekintik. Ilyen esetekben Felek azonnali hatállyal jogosult a Szerződés megszüntetésére.

KAPCSOLATTARTÓ SZEMÉLYEK

A Felek a Szerződés teljesítéséhez szükséges kapcsolattartás céljából a szerződéskötéssel egyidejűleg kötelesek az illetékes képviselőiket kijelölni a [kitöltendő] mellékletként csatolt nyilatkozat kitöltésével és érintetti nyilatkozatok beszerzésével. A Felek kötelesek a saját Kapcsolattartóik személyes adataiban bekövetkezett változásról a másik Felet haladéktalanul tájékoztatni, új kapcsolattartó kijelölésekor a nyilatkozatot az érintettel ismertetni, kitöltve a másik Fél rendelkezésére bocsátani. A Felek kötelesek a másik fél Kapcsolattartójának személyes adatait véglegesen és helyreállíthatatlanul törölni/megsemmisíteni, amennyiben az azok kezelésére vonatkozó jogalap és/vagy az adatkezelési cél megszűnik.

A Felek rögzítik, hogy egymás között minden nyilatkozatot elektronikus úton (emailben), írásban, szükség szerint tértivevényes levélben kell megküldeni, amely akkor tekinthető jogszerűen kézbesítettnek, ha azt a képviselőre jogosult vagy a kapcsolattartó személyek részére a mellékletben megjelölt email címre, vagy postai címre kézbesítették. Az értesítés akkor válik hatályossá, amikor azt a címzett igazoltan átvette. Az e-mail útján történő kézbesítés esetén a nyilatkozat vagy értesítés akkor válik joghatályossá, amikor a címzett azt igazoltan kézhez vette, arról automatikus, vagy kifejezett visszaigazolás érkezett.

Kapcsolattartók megjelölése és adatkezelési tájékoztató

EBVK részéről biztosított kapcsolattartók nyilatkozata

Értesítések fogadására és küldésére jogosult személy(ek)

- **név:** [kitöltendő]
- email cím: [kitöltendő]
- telefonszám: [kitöltendő]
- betöltött pozíció: [kitöltendő]

Megértettem, hogy jelen [kitöltendő] szerződés kapcsán [kitöltendő] szakértőként, a Felek között létrejött jognyilatkozatok és egyéb dokumentumok, utasítások érvényességének szükség szerinti igazolásához, az ezzel kapcsolatos esetleges jogérvényesítés megvalósíthatóságához, a kapcsolatfelvételhez és kapcsolattartáshoz, továbbá a szerződéssel kapcsolatos általános adminisztrációk elvégzéséhez személyes adataim [kitöltendő], mint Adatkezelő adatkezelésébe kerülnek.

[kitöltendő] jogaimat ismertette, Adatkezelő adatkezeléssel kapcsolatos tájékoztatóját [hivatkozás annak elérhetőségére, vagy adatkezelés lényeges körülményeinek ismertetése] megismertem, a benne foglaltakat megértettem, és elfogadom.

Kelt: Budapest, [kitöltendő]

XY

[kitöltendő] részéről biztosított kapcsolattartók

Értesítés fogadására és küldésére jogosult személyek

- **név:** [kitöltendő]
- email cím: [kitöltendő]
- telefonszám: [kitöltendő]
- betöltött pozíció: [kitöltendő]

Megértettem, hogy jelen [kitöltendő] szerződés kapcsán kapcsolattartóként, a Felek között létrejött jognyilatkozatok és egyéb dokumentumok, utasítások érvényességének szükség szerinti igazolásához, az ezzel kapcsolatos esetleges jogérvényesítés megvalósíthatóságához, a kapcsolatfelvételhez és kapcsolattartáshoz, továbbá a szerződéssel kapcsolatos általános adminisztrációk elvégzéséhez személyes adataim [kitöltendő], mint Adatkezelő adatkezelésébe kerülnek a felelősségre vonhatóság elévülésének idejéig, de legfeljebb a szerződés teljesülését követő 5 évig. Adataim nem kerülnek továbbításra harmadik fél részére.



3700 Kazincbarcika
Rákóczi tér 9.

EBVK tájékoztató, hogy jogaimmal kapcsolatos bővebb információt az alábbi elérhetőségen talállok:

.....

Adatkezelő adatkezeléssel kapcsolatos tájékoztatóját megismertem, a benne foglaltakat megértettem, és elfogadom.

Kelt: Budapest, [kitöltendő]

2. melléklet: Adatfeldolgozói szerződés minta

Adatfeldolgozói megállapodás

mely létrejött

[Kitöltendő] (székhely:[kitöltendő]; adószám:[kitöltendő];képviseli:[kitöltendő]) mint Megbízó és Adatkezelő (továbbiakban: [kitöltendő] vagy Adatkezelő), és

[Kitöltendő] (székhely: [kitöltendő], adószám: [kitöltendő], mint megbízó, képviseli: [kitöltendő]) mint [kitöltendő] és Adatfeldolgozó (továbbiakban: [kitöltendő] vagy Adatfeldolgozó),

együttesen Felek között az alábbiakban meghatározott helyen, időben és tartalommal.

1. Adatkezelési tevékenység leírása, érintett adatok köre

[Szerződéses tevékenység leírása]

Adatfeldolgozó feladata:

[kitöltendő]

[kitöltendő]

[kitöltendő]

2. A Felek jogai és kötelezettségei

2.1 Adatfeldolgozó az 1. pontban meghatározott adatfeldolgozási tevékenység ellátására vállal kötelezettséget. Az adatfeldolgozási tevékenység elvégzéséért külön díjazás Adatfeldolgozót nem illeti meg.

2.2 Adatfeldolgozó az adatokkal kapcsolatos érdemi döntést nem hozhat, kizárólag az Adatkezelő által a jelen megállapodásban meghatározottak szerinti feladatok elvégzésére jogosult és a tudomására jutott személyes adatokat kizárólag az Adatkezelő írásbeli utasításai szerint kezelheti. Adatfeldolgozó a feladatellátása során az Adatkezelő nevében és annak megbízásából, továbbá rendelkezésének megfelelően (utasítási jog) végzi a tevékenységét. Adatkezelő nevében utasítási jogkörrel rendelkező személy az EBVK vezetője, valamint a szerződésben kapcsolattartóként megjelölt személy. Írásbeli utasítást az Adatfeldolgozó 1. pontba megjelölt elérhetőségére köteles címezni Adatkezelő.

2.3 Feladata ellátása céljából Adatkezelő [adatmegosztás módja kitöltendő] megosztja Adatfeldolgozóval az üzleti titkot és személyes adatot is tartalmazó állományt. Az átadott adatokat Adatfeldolgozó nem jogosult továbbítani, megosztani további címzettekkel, [ide nem értve az 1.2 pontban meghatározott célból igénybe veendő további adatfeldolgozót és adattovábbítást], adatok bizalmasságának megőrzéséért jelen megállapodás hatályától független, időben korlátlan titoktartási kötelezettség terheli. Az adatokkal kizárólag az 1.2 pontban meghatározott műveletek elvégzésére jogosult.

2.4 Adatfeldolgozó tudomásul veszi, hogy amennyiben az Európai Unió 2016/679 rendeletének (a továbbiakban: GDPR) rendelkezéseit sértve maga határozza meg az adatkezelés céljait és eszközeit, akkor őt az adott adatkezelés tekintetében adatkezelőnek kell tekinteni, és teljes körűen viselni köteles az adatkezelői minőséggel kapcsolatos jogokat és kötelezettségeket, jelen megállapodás megszegésének jogi következményeit.

2.5 Adatkezelő kizárólag a mellékletben megjelölt további adatfeldolgozó igénybevételére jogosítja az Adatfeldolgozót. Adatfeldolgozó részére az 1.2 pontban meghatározott adatkörben, és adatkezelési célból, adatkezelési műveletek elvégzésére továbbítható adat.

2.6 Adatfeldolgozó köteles a személyes adatokat érintő bármely incidensről (különösen a kezelt személyes adatokhoz való illetéktelen hozzáférésről, a jogosulatlan megváltoztatásról vagy a hozzáférhetetlenné válásról) a tudomásszerzését követően haladéktalanul (legkésőbb 8 órán belül) írásban tájékoztatni (adatvédelmi kérdésekben alkalmazott elérhetőségére küldött elektronikus levél formájában) Adatkezelőt annak érdekében, hogy a GDPR-ban meghatározott – incidensek kezelésével járó – kötelezettségeit teljesíteni tudja, továbbá köteles Adatkezelőt segíteni az esetleges adatvédelmi vizsgálat lefolytatásával összefüggő feladatai ellátásában.

2.7 Az adatfeldolgozási tevékenység során Adatfeldolgozó megfelelő technikai és szervezési intézkedések útján garantálja a kezelt személyes adatok biztonságát, azok bizalmas jellegének biztosítását, valamint integritását és rendelkezésre állását. Adatfeldolgozó különösen az alábbi technikai és szervezési intézkedéseket hajtja végre annak érdekében, hogy a megfelelő szintű adatbiztonságot garantálja:

- biztosítja, hogy a nevében eljáró személyek titoktartási kötelezettség hatálya alatt álljanak;
- [kitöltendő]
- [kitöltendő]
- [kitöltendő]

2.8 Adatkezelő jogosult ellenőrizni Adatfeldolgozónál a szerződés szerinti tevékenység végrehajtását és a megtett védelmi intézkedéseket a hatékonyság és biztonság érdekében.

2.9 Adatfeldolgozó az Adatkezelő megkeresésére a hatásvizsgálat elkészítésében vagy módosításában is adatszolgáltatási támogatást biztosít az Adatkezelőnek.

3. Érintetti joggyakorlás

Az adatkezelés jellegének figyelembevételével az érintetti joggyakorlások esetén kizárólag Adatkezelő jogosult az érintettek kérelmének megválaszolására, ehhez szükség szerint kérheti Adatfeldolgozó közreműködését, aki a kérés érkeztetését követő 10 munkanapon belül Adatkezelő rendelkezésére áll.

4. Kártérítési felelősség meghatározása

4.1 Adatfeldolgozó kijelenti, hogy amennyiben a jelen szerződésben, továbbá a GDPR-ban, valamint a vonatkozó ágazati jogszabályokban foglalt, adatvédelemmel összefüggő bármely kötelezettségét neki felróható módon megszegi, az ebből eredő vagyoni, illetve nem vagyoni károkat köteles teljes mértékben megtéríteni, beleértve az Adatfeldolgozó magatartásából eredően az Adatkezelő terhére kirótt adatvédelmi bírságokat is.

4.2 Felek kötelezettséget vállalnak arra, hogy minden olyan körülményről tájékoztatják egymást, amely a szerződés teljesítését, illetve a másik Fél jogos érdekét érinti. A bejelentési kötelezettség elmulasztásából eredő károkért a mulasztó Fél teljes kárfelelősséggel tartozik.

5. Adatfeldolgozói megállapodás hatálya, módosítása, megszűnése

5.1 Jelen megállapodás a Felel általi aláírással lép hatályba, és a szerződésben meghatározott tevékenység elvégzéséig tartó ideig jogosítja és kötelezi a Feleket a benne foglaltakra. Jelen szerződés megszűnésével egyidejűleg Adatfeldolgozó minden még birtokában lévő személyes adatot és készített másolatot az Adatkezelő rendelkezésének megfelelően töröl úgy, hogy azok fizikai és logikai helyreállítása a továbbiakban nem lehetséges.

5.2 A jelen megállapodásban nem szabályozott kérdésekben a GDPR, Infotv., a Ptk., továbbá a vonatkozó ágazati jogszabályok rendelkezései irányadók.

5.3 Jelen szerződést a Felek, mint akaratukkal mindenben megegyezőt helyben hagyólag írták alá.

Budapest, [kitöltendő]

[kitöltendő]

képviseli: [kitöltendő]

Adatkezelő

[kitöltendő]

képviseli: [kitöltendő]

Adatfeldolgozó

3. melléklet: Titoktartási nyilatkozat minta

TITOKTARTÁSI NYILATKOZAT

Alulírott név: [kitöltendő] születési idő, hely: [kitöltendő], a [kitöltendő] (székhely: [kitöltendő]; adószám: [kitöltendő]) munkavállalójaként/ egyéb közreműködőjeként nyilatkozom az alábbiakról:

Jelen nyilatkozat tétellel kötelezem magam, hogy az előttem [jogviszony specifikusan kitöltendő] az Egressy Béni Városi Könyvtár (továbbiakban, mint „EBVK”) által feltárt, és a jövőben feltárando információkat, így különösen üzleti titkokat, [jogviszony specifikusan kitöltendő], és bármilyen egyéb információt az üzleti titokról szóló 2018. évi LIV. törvényben foglaltaknak megfelelően, üzleti titokként vagy magántitokként kezelek, a tevékenységem során a hatályos jogszabályoknak, az EBVK utasításainak megfelelően járok el.

Tudomásul veszem, hogy amennyiben az információt a hatályos jogszabályoknak nem megfelelő módon (különösen ideértve üzleti titokra és magántitokra vonatkozó titoktartási kötelezettség megszegésével), az EBVK utasításaival nem egyező módon, vagy EBVK részemre biztosított szabályzataiban foglaltakat nem figyelembe véve kezelem, teljeskörűen terhel a magatartásomból eredő kár- és büntetőjogi felelősség.

Tudomásul veszem továbbá, hogy titoktartási kötelezettségem alól - az engedélyben meghatározott információk erejéig - csak jogszabály rendelkezése alapján, vagy az EBVK írásbeli engedélyével mentesülhetek.

Tudomásul veszem továbbá, hogy jelen nyilatkozatban szabályozott titoktartási kötelezettség időbeli hatálya korlátlan. Megértettem, hogy a jelen nyilatkozatban foglalt kötelezettség megszegése esetén szakmai, polgári jogi és – szándékosság esetén – büntetőjogi felelősséggel tartozom.

Budapest, [kitöltendő]

.....

Aláírás

A jelen nyilatkozat aláírásával tudomásul veszem és megértettem, hogy a fent megadott személyes adataimat az EBVK, mint Adatkezelő, a vonatkozó adatvédelmi szabályoknak megfelelő az Adatkezelő tulajdonhoz és üzleti titkainak, nyilvántartásaiban kezelt személyes adatok védelméhez fűződő jogos érdeke alapján kezeli, és megőrzi a felelősségre vonhatóság elévülésének idejéig. Megértettem, hogy adataim továbbításra nem kerülnek, jogaimmal kapcsolatos bővebb tájékoztatást az alábbi elérhetőségen talállok:

4. melléklet: Adatkezelési tevékenység nyilvántartó lap - bevezetés

[Adatkezelési tevékenység sorszáma]	[Adatkezelés megnevezése]	
Adatkezelésért felelős szervezeti egység:		
Bevezetés oka:		
Bevezetés dátuma:		
Adatkezelés tervezett folyamata:		
Érintettek köre:		
Kezelendő adatok köre, adatkezelési cél adatkörönként		
Adatkezelés jogalapja:		
Jogalap indoklása:		
Adatok forrása		
Hogyan történik az adatok felvétele, tárolása?		
Érintett szakrendszerek		
Lehetséges kockázatok		
Alkalmazott adatbiztonsági intézkedések leírása		
Adattovábbítás történik? Ha igen, hova?		
EGT országon kívüli adattovábbítás esetén megfelelőségi határozat, vagy megfelelő garancia		
Adatfeldolgozó igénybevétele		
Adatfeldolgozói megállapodás		
Adatkezelésről tájékoztatás módja		



3700 Kazincbarcika
Rákóczi tér 9.

Adatkezelés tervezett időtartama	
----------------------------------	--

Adatkezelési tevékenység nyilvántartó lap - módosítás

[Adatkezelési tevékenység sorszáma]	[Adatkezelés megnevezése]
Módosítás sorszáma	
Adatkezelésért felelős szervezeti egység:	
Módosítás oka:	
Módosítás dátuma:	
Adatkezelés tervezett folyamata a módosítást követően	
Érintettek köre a módosítást követően:	
Kezelendő adatok köre, adatkezelési cél adatkörönként- a módosítást követően:	
Adatkezelés jogalapja a módosítást követően:	
Jogalap indoklása a módosítást követően:	
Adatok forrása a módosítást követően:	
Hogyan történik az adatok felvétele, tárolása a módosítást követően?	
Érintett szakrendszerek a módosítást követően:	
Lehetséges kockázatok	
Alkalmazott adatbiztonsági intézkedések leírása a módosítást követően	
Adattovábbítás történik? Ha igen, hova?	
EGT országon kívüli adattovábbítás esetén megfelelőségi határozat, vagy megfelelő garancia	
Adatfeldolgozó igénybevétele a módosítást követően	
Adatfeldolgozói megállapodás a módosítást követően	



3700 Kazincbarcika
Rákóczi tér 9.

Adatkezelésről tájékoztatás módja a módosítást követően	
Adatkezelés tervezett időtartama	

Adatkezelési tevékenység nyilvántartó lap – adatkezelés kivezetése

[Adatkezelési tevékenység sorszáma]	[Adatkezelés megnevezése]
Kivezetésért felelős szervezeti egység:	
Kivezetés oka:	
Kivezetés dátuma:	
Adatkezelés kivezetését követően archívként megőrzendő?	
Érintettek köre	
Kivezetendő adatok köre	
Hogyan történik az archív adatok tárolása?	
Érintett szakrendszer	
Lehetséges kockázat	
Alkalmazott adatbiztonsági intézkedések leírása	
Adattovábbítás történik? Ha igen, hova?	
Adatfeldolgozó igénybevétele a módosítást követően	
Adatfeldolgozói megállapodás	
Adatkezelés kivezetéséről hogyan történik az Érintettek tájékoztatása	

5. melléklet- Érdekmérlegelési teszt minta

[Tervezett adatkezelés megnevezése]	
Adatkezelés tervezett célja	
Adatkezelés tervezett időtartama	
Kezelendő adatok tervezett köre	
Adatfeldolgozás tervezett folyamata	
Adatkezelés szükséges?	
Létezik alternatív mód az adatkezelés cél elérésére?	
1. Adatkezelő jogszerű érdekeinek értékelése	
Védendő alapvető jogok felsorolása (EJEE, Alapjogi Charta, Alaptörvény)	
Közérdek, közösségi érdek	
Egyéb jogos érdek	
Az érdekek jogszerűségének jogi és kulturális /társadalmi elismerése	
Adatkörök korlátozása	
Adattárolás időtartamának korlátozása	
Álnevesítési vagy anonimizálási technikák	
Aggregált adatok	
Tiltakozási jog biztosítása	
Törlési kérés mérlegelés nélküli teljesítése	
Egyéb adatbiztonsági intézkedés	
Egyéb szervezési intézkedés	
2. Érintettre gyakorolt hatás	
Adatkezelés lehetséges következményei	
Kockázat bekövetkezésének lehetősége	
Kockázat súlyossága	
Érintettek potenciális száma	
Felek státusza	
Érintett ésszerű elvárása	
3. Érdekek egyensúlya megállapítható?	
Igen	Nem
4. Amennyiben nem, további biztosítékok meghatározása	
Adatkörök korlátozása	

Adattárolás időtartamának korlátozása	
Álnevesítési vagy anonimizálási technikák	
Aggregált adatok	
Tiltakozási jog biztosítása	
Törlési kérés mérlegelés nélküli teljesítése	
Egyéb adatbiztonsági intézkedés	
Egyéb szervezési intézkedés	
5. Érdekek egyensúlya megállapítható a biztosítékok alkalmazását követően?	
Igen	Nem

6. melléklet: Adatmegsemmisítési jegyzőkönyv minta

Jegyzőkönyv irat/adatmegsemmisítésről

Irat/Adatmegsemmisítési bizottság tagjai

(1) Munkavállaló neve:

Születési hely, idő:

Munkakör:

(2) Munkavállaló neve:

Születési hely, idő:

Munkakör:

(3) Munkavállaló neve:

Születési hely, idő:

Munkakör:

DPO

A megsemmisítés tárgya, adathordozó típusa és száma:

[kitöltendő]

A megsemmisítés módszere

[kitöltendő]

A megsemmisítés oka

[kitöltendő]

Adatmegsemmisítés helye és ideje

[kitöltendő]

[kitöltendő]

Az adatok megsemmisítését jóváhagyom:

Igazgató

Aláírással igazolom, hogy az adatok törlése a jegyzőkönyvben rögzítetteknek megfelelően megtörtént.

Kelt: Budapest, [kitöltendő]

Név

Név

Név

7. melléklet- Incidens kivizsgáló lap

Jegyzőkönyv lehetséges adatvédelmi incidens kivizsgálásáról

Jelen jegyzőkönyv a [kitöltendő éééé.hh.nn-én óó:pp-kor] történt az [kitöltendő] rendszerrel kapcsolatos [kitöltendő] üzemzavar/bejelentés [kitöltendő] által észlelt lehetséges incidens (továbbiakban: lehetséges incidens vagy esemény) kivizsgálásával kapcsolatos részletes információkat tartalmazza.

Adatkezelő:	
Cím:	

1. ESEMÉNY KIVIZSGÁLÁSA ELŐTT ISMERT KÖRÜLMÉNYEK

Vizsgálat tárgya:	
Esemény rövid leírása:	
Eseményt észlelő személy:	
Az esemény felfedezésének helye:	
Az esemény felfedezésének ideje:	
Egyéb észleléssel kapcsolatos körülmény:	
A lehetséges incidens bekövetkezésének helye:	
A lehetséges incidens bekövetkezésének ideje	
Adatkezelő mikor értesült az eseményről?	

2. VIZSGÁLAT SORÁN FELTÁRTAK

Vizsgálat helye és ideje	
Esemény melyik adatkezelési tevékenységhez kapcsolódik?	
Esemény kapcsolódik informatikai rendszerhez? Ha igen, melyik rendszerhez?	
Az esemény kapcsán biztosan érintett / részt vevő személyek (név, titulus, szerep az eseményben (pl rendszergazda, munkavállaló, bejelentő, észlelő stb.)	
Esemény érint személyes adatokat?	
Esemény érinti személyes adatok különösen védett kategóriáját (9. cikk (1) bekezdés)	
Rendelkezésre álló és vizsgált bizonyítékok	
Vizsgálat tapasztalata	



Az esemény lehetséges bekövetkezésének körülményei

Megállapítható személyes adatok véletlen vagy jogellenes **megsemmisítése?**

Megállapítható személyes adatok véletlen vagy jogellenes **elvesztése?**

Megállapítható személyes adatok véletlen vagy jogellenes **megváltoztatása?**

Megállapítható személyes adatok véletlen vagy jogellenes **közlése?**

Megállapítható személyes adatok véletlen vagy jogellenes **hozzáférés?**

amennyiben igen/nem

ADATVÉDELMI INCIDENS TÖRTÉNT?

további szakaszok kitöltése kizárólag akkor szükséges, ha adatvédelmi incidens történt, egyébként a 4. blokk végéig törölhető

3. KÁRKOCKÁZATOK FELMÉRÉSE, KÁRENYHÍTÉS

Egyedi vagy tömeges érintettség vélelmezhető?

Egyedi érintettség esetén érintettek

Tömeges érintettség esetén érintetti kategória

Az incidens bekövetkezését elősegítő tényezők

Visszaállíthatók a megsemmisült, megváltoztatott adatok mentésből?

Van reális esély az elveszetett adatok megtalálására?

Van lehetőség az adatok törlésére, az illetéktelenül tudomást szerzővel titoktartási megállapodás megkötésére további illetéktelen közlések megelőzése céljából?	
Van lehetőség a hozzáférés megszüntetésére?	
Illetéktelen hozzáférés esetén értelmezhetőek voltak az adatok a hozzáférőnek?	
Van olyan logikai intézkedés (pl. jelszócsere) amivel megelőzhetőek a további károk?	
Van olyan fizikai intézkedés (pl. zárcsere) amivel megelőzhetőek a további károk?	
Van olyan adminisztratív intézkedés (pl. közlemény közzététele, törlési nyilatkozat bekérése, titoktartási megállapodás megkötése) amivel megelőzhetőek a további károk?	
Milyen lehetséges hátrányok érhetik az érintetteket az incidens hatására?	
Az incidens kapcsán végrehajtott intézkedések	
TOVÁBBI SZÜKSÉGES KÁRENYHÍTÉS - CSELEKVÉSI TERV	
Továbbra is fennáll bármilyen kockázat az érintettekre nézve?	
ha igen, az adatvédelmi incidens jelentése szükséges a Hatóságnak.	
A fennálló kockázat magas kockázatnak minősíthető az érintettre nézve?	
ha igen, az érintettel meg kell próbálni felvenni a kapcsolatot, vagy közlemény formájában szükséges tájékoztatni az érintetti kört a lehetséges kockázatról	
Egyéb megállapítások, szükséges intézkedések	
További szükséges intézkedések (pl. feljelentés megtétele)	
Mellékletek	



3700 Kazincbarcika
Rákóczi tér 9.

Kelt: Budapest, [kitöltendő]

Esemény kivizsgálásában részt vevő személyek:

Név: Pozíció:

Név: Pozíció:

Név: Pozíció:

Név: Pozíció:



3700 Kazincbarcika
Rákóczi tér 9.

8. melléklet: Adatvédelmi incidens nyilvántartás

Sorszám	Az adatvédelmi incidens rövid megnevezése	Az adatvédelmi incidensről való tudomásszerzés időpontja	Az adatvédelmi incidens bekövetkezésének napja (mikor történt)	A bejelentő megnevezése (adatfeldolgozó, munkavállaló, stb.)	Az incidens körülményeinek, a tények leírása	Kik az érintettek, akiknek az adatait az incidens érte	Milyen személyes adatok érintettek az incidenssel	Érintett információs rendszer	Az incidens okának leírása	Az incidens hatásai (valószínű kockázatok, következmények)	Az orvoslásra tett intézkedések listája/leírása, valamint annak hatása	Az incidensről a hatóság, illetve az érintettek tájékoztatásra kerültek-e, amennyiben nem, úgy ennek indoka és magyarázata



3700 Kazincbarcika
Rákóczi tér 9.

9. melléklet: Munkaviszony létesítése, foglalkoztatás fennállása és munkaviszony megszűnése kapcsán kitöltendő dokumentumok és jognyilatkozatok