

ERZSÉBETVÁROSI DOB ÓVODA

Adatvédelmi szabályzat



Az intézmény OM azonosítója:

034358

Kiadta:



Patai Edit
Intézményvezető



A dokumentum jellege: nyilvános
Megtalálható: titkárság, kérésre
betekinthető

Iktatószáma: 15-144/2019-D

Hatályos: a kihirdetés napjától visszavonásig, 2019. március 18.

Módosításokkal egységes szerkezetbe foglalt Készült: 2 eredeti példány

Tartalomjegyzék

1. AZ ADATVÉDELMI SZABÁLYZAT CÉLJA	3
2. ALAPELVEK	3
2.1. JELEN SZABÁLYZAT ELKÉSZÍTÉSEKOR FIGYELEMBE VETT JOGSZABÁLYOK	4
2.2. FOGALMAK	4
2.3. A SZEMÉLYES ADATOK KEZELÉSÉNEK ALAPELVEI	7
2.4. AZ INTÉZMÉNY GYAKORLATÁBAN ELŐFORDULÓ ADATKATEGÓRIÁK	8
2.5. ÉRINTETTEK KATEGÓRIÁI	9
3. A SZABÁLYZAT HATÁLYA	9
4. ADATVÉDELMI KOCKÁZATKEZELÉS	9
5. ADATVÉDELMI INCIDENSKEZELÉS	10
6. AZ INTÉZMÉNYRE, MINT ADATKEZELŐRE VONATKOZÓ SZABÁLYOK	10
7. AZ INTÉZMÉNYRE, MINT ADATFELDOLGOZÓRA VONATKOZÓ SZABÁLYOK	11
8. ADATBIZTONSÁG, AZ ADATOK TÁROLÁSA	12
9. AZ ADATVÉDELMI NYILVÁNTARTÁS	12
10. ADATIGÉNYLÉS, ADATSZOLGÁLTATÁS	13
11. ADATTOVÁBBÍTÁS MEGKERESÉS ALAPJÁN	13
12. KÜLFÖLDRE TÖRTÉNŐ ADATTOVÁBBÍTÁS	14
13. SZERVEZETEN BELÜLI ADATTOVÁBBÍTÁS, ADATKEZELÉSEK ÖSSZEKAPCSOLÁSA	15
14. AZ ADATOK HELYESBÍTÉSE, TÖRLÉSE	15
15. AZ ÉRINTETT JOGAI GYAKORLÁSÁNAK BIZTOSÍTÁSA	16
16. SZEMÉLYES ADATOK NYILVÁNOSSÁGRA HOZATALA	17
17. ADATVÉDELMI TISZTVISELŐ	17
18. EGYES HUMÁNPOLITIKAI SAJÁTOSSÁGOK	18
19. BIZTONSÁGI TERÜLET EGYES ADATVÉDELMI SZABÁLYAI	18
20. ZÁRÓ RENDELKEZÉSEK	19

1. AZ ADATVÉDELMI SZABÁLYZAT CÉLJA

A szabályzat célja a személyes adatok védelméről szóló Európai Parlament és Tanács (EU) 2016/679 számú rendelete (GDPR) való megfelelés biztosítása, összhangban az **Erzsébetvárosi Dob Óvoda** (a továbbiakban: *Intézmény vagy Óvoda*) feladataival és céljaival.

A Szabályzat célja ezen belül, hogy a hatályos jogszabályoknak megfelelően meghatározza az Intézmény tevékenysége során végzett adatkezelési műveletek legfontosabb szabályait, meghatározza a törvényes és jogszerű működéshez szükséges felelősségi rendet, valamint biztosítsa az adatvédelem, továbbá az információvédelmi szabályok és szabványok által támasztott követelmények érvényesülését, valamint megakadályozza az adatokhoz történő jogosulatlan hozzáférést, azok megváltoztatását és jogellenes nyilvánosságra hozatalát.

2. ALAPELVEK

Az Óvoda elkötelezett abban, hogy a saját munkavállalóinak, ügyfeleinek és általában az állampolgárok adatait, a vele kapcsolatba kerülő vállalkozások ügyféladatait a lehető legmagasabb színvonalon, és a hatályos jogszabályi előírásoknak megfelelően kezelje. E cél elérésére adatkezelőként és adatfeldolgozóként egyaránt törekszünk. Az Óvoda a személyes adatok védelme nemcsak a működésünk külső sajátossága, hanem tevékenységünk, szolgáltatásaink egyik legfontosabb, központi eleme.

Jelen Adatvédelmi Szabályzat (a továbbiakban: *Szabályzat*) az Óvoda feladatellátása során kezelt adatokkal és a vezetett és kezelt nyilvántartásokkal kapcsolatos legfontosabb, egyben legfelső szintű adatvédelmi szabályokat tartalmazza, különös tekintettel az adatkezeléssel, adatfeldolgozással, adattovábbítással kapcsolatos tevékenységekre és felelősségre.

Figyelemmel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/45/EK rendelet hatályon kívül helyezéséről szóló, az Európai Parlament és a Tanács (EU) 2016/679 rendeletre (általános adatvédelmi rendelet – továbbiakban: GDPR vagy adatvédelmi rendelet) és az ebből eredő fordított bizonyítási teherre, az adatkezelőnek (Óvoda) az általa végzett adatkezelések során függetlenül az adatkezelői vagy adatfeldolgozói státusztól, minden esetben bizonyítania kell tudni az általa végzett műveletek jogszerűségét és nyomon követhetőségét az adat útja és az adatokon végzett műveletek tekintetében.

A szabályzat előírásait együtt kell alkalmazni az Intézmény egyéb érvényes szabályzataival, különös tekintettel azokra, amikre a későbbiekben tételesen is hivatkozunk.

Az itt leírt rendelkezések

- teljes körűek, azaz a rendszer összes elemére kiterjednek,
- zártak, azaz minden fenyegetést figyelembe vesznek
- folytonosak, azaz a változó körülmények és követelmények mellett is megszakítás nélkül megvalósulnak.

2.1. Jelen szabályzat elkészítésekor figyelembe vett jogszabályok

- Alaptörvény
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.)
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a GDPR-en kívül eső és hatályos kérdések vonatkozásában)
- a munka törvénykönyvéről szóló 2012. évi I. törvény
- a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény
- a Büntető Törvénykönyvről szóló 2012. évi C. törvény
- a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény
- a számvitelről szóló 2000. évi C. törvény
- az adózás rendjéről szóló 2003. évi XCII. törvény
- a polgárok személyes adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

2.2. Fogalmak

- **„adatállomány”**: az egy nyilvántartásban kezelt adatok összessége;
- **„adatfeldolgozás”**: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot adatokon végzik. Az adatfeldolgozás alapja az adatkezelővel fennálló rendezett kapcsolat, ami biztosítja a jogalapot az adatkezeléshez és egyben meghatározza annak kereteit;
- **„adatfeldolgozó”**: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi;
- **„adatfelelős”**: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;
- **„adatkezelés korlátozása”**: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából, valamint ezekre az adatokra a kért korlátozás betartása;
- **„adatkezelő”**: 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;
- **„adatközlő”**: az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatait honlapon vagy más módon közzéteszi;
- **„adatmegjelölés”**: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

- **„adatmegsemmisítés”**: az adatok visszafordíthatatlan – felülírással – törlése vagy az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;
- **„adattovábbítás”**: az adat meghatározott harmadik fél, mint címzett számára történő hozzáférhetővé tétele;
- **„adattörlés”**: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;
- **„adatzárolás”**: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;
- **„adatvédelmi incidens”**: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
- **„anonimizálás”**: olyan technikai eljárás, amely biztosítja az érintett személy vagy céges ügyfél és az adat közötti kapcsolat helyreállítása lehetőségének végleges kizárását, oly módon, hogy adatokat vissza nem állítható módon *elmaszkolja* vagy egyéb módon torzítja. Ezáltal nem lehet egyértelműen az adott személyt (akár természetes, akár jogi személy) beazonosítani;
- **„álnevesítés”**: 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;
- **„biometrikus adat”**: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;
- **„bűnügyi személyes adat”**: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szervezeteknél, továbbá a büntetés-végrehajtási szervezetnél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;
- **„címzett”**: 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 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;
- **„egészségügyi adat”**: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
- **„EGT tagállam”**: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes állam, továbbá az az állam, amelynek állampolgára az Európai Unió tagállama és 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”**: bármely meghatározott, személyes adat alapján azonosított vagy – közvetve vagy közvetlenül – azonosítható természetes személy;
- **„érintett felügyeleti hatóság”**: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:
 - a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
 - b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
 - c) panaszt nyújtottak be az említett felügyeleti hatósághoz;

„érintett hozzájárulása”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
- **„felügyeleti hatóság”**: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv;
- **„genetikai adat”**: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;
- **„harmadik fél”**: 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”**: minden olyan állam, amely nem EGT-állam;
- **„kötelező erejű vállalati szabályok”**: a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;
- **„közérdekből nyilvános adat”**: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;
- **„közérdekű adat”**: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegéről, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;
- **„különleges adat”**: 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;

- **„nemzetközi szervezet”**: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre;
- **„nyilvánosságra hozatal”**: az adat bárki számára történő hozzáférhetővé tétele;
- **„nyilvántartási rendszer”**: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
- **„profilalkotás”**: 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 helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;
- **„releváns és megalapozott kifogás”**: 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 gyakorolt hatását;
- **„személyes adat”**: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ, ahol 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;
- **„személyes adatok határokon átnyúló adatkezelése”**:
 - a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
 - b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;
- **„tiltakozás”**: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;
- **„üzleti titok”**: minden olyan gazdasági tevékenységhez kapcsolódó tény, információ, adat, megoldás, amelynek titokban tartásához az Intézménynek méltányolható érdeke fűződik, minősítése megtörtént, és amelynek titokban maradásához a jogosult a szükséges intézkedéseket megtette. Üzleti titok továbbá a jogszerűen működő üzemmel, illetőleg üzlettel és ezek működésével kapcsolatos olyan adat, amelynek illetéktelen személyek tudomására jutása az üzem, illetőleg az üzlet zavartalan és biztonságos működését, vagy anyagi érdekeit veszélyezteti;

2.3. A személyes adatok kezelésének alapelvei

- **„jogszerűség, tisztességes eljárás és átláthatóság”**: A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;

- **„célhoz kötöttség”**: A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés;
- **„adattakarékosság”**: A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;
- **„pontosság”**: A személyes adatok pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
- **„korlátozott tárolhatóság”**: A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel;
- **„elszámoltathatóság”**: A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”). Az adatkezelő felelős az ennek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására;

2.4. Az Intézmény gyakorlatában előforduló adatkategóriák

- **Hitelesítési adatok**: jelszavak, PIN kódok, édesanyja születéskori neve, stb.
- **Azonosító adatok**: név, felhasználói név, egyedi azonosító (szám), szerv által adott azonosító (szám, kód), arckép, biometrikus adat, édesanyja születéskori neve
- **Demográfiai**: korosztály, fizikai tulajdonságok, jövedelem-kategória vagy besorolás, földrajzi adatok (lakóhely, munkahely)
- **Egészségügyi**: egészségi állapot, drog vagy más tesztadatok, fogyatékoság, családi vagy egyéni egészségügyi előtörténet, egészségügyi vizsgálatok adatai, DNS (DNA), vércsoport, gyógyszerhasználat
- **Fizikai paraméterek**: életkor, magasság, súly, hajszín, bőrszín, biológiai nem, piercing
- **Számlaszámok**: kártyaszám, bankszámlaszám
- **Szakmai**: szakmai előélet, pozíciók, munkaügyi dossziék, referenciák, interjúk, bizonyítványok, kutatási tevékenység (tipikusan egy CV adatai)
- **Bűnügyi**: bűnügyi előélet, büntetlenség vagy büntetett előélet csak mint státusz
- **Családi adatok**: családösszetétel, rokonok, leszármazottak, válás
- **Személyes használatú eszköz adatok (eszköz adatok)**: ip cím, MAC cím, browser-azonosító
- **Kapcsolattartási adatok**: email cím, fizikai cím (posta), telefonszám
- **Helyadatok**: ország, GPS koordináta, szobaszám

2.5. Érintettek kategóriái

Az Intézmény tevékenysége során az alábbi jellemző érintettek kategóriák vannak jelen:

- Az Intézmény ügyfelei, állampolgárok vagy más ország állampolgárai, kiemelten:
 - Kerületi állandó lakosok vagy itt tartózkodók
 - Ezen ügyfelek családtagjai, gyermekei
 - Az óvodába jelentkező és beíratott gyermekek
- Az Intézmény saját dolgozói, bármilyen jogcímen
- Az Intézmény létesítményeinek vendégei
- Szervezetek és vállalkozások képviselői és unkaállalói (rendezvényszervezők, előadók, stb)

3. A SZABÁLYZAT HATÁLYA

Jelen Szabályzat hatálya kiterjed az Intézmény valamennyi, személyes adatok kezelésével, feldolgozásával kapcsolatos tevékenységére.

Jelen szabályzatban foglaltak alkalmazhatók minden EGK tagállamba vagy onnan induló adatkezelési műveletre, de nem vonatkoznak automatikusan EGK-n kívüli, tehát harmadik országot érintő adatkezelésre, amely esetben mindig egyedi elbírálás szükséges a GDPR V. fejezetében foglaltak szerint.

- Területi hatály:

Székhely: 1077 Budapest Dob utca 95.

Telephelyek: 1077 Budapest Dob utca 95.

A fentiekén kívül minden olyan helyszín, ahol az Intézmény munkatársai által saját jogán és saját nevében megjelenik és tevékenységet végez, mint például rendezvények vagy közéleti események.

- Időbeli hatály: jelen Szabályzat a kiadás napjától visszavonásig érvényes.
- Személyi hatály: jelen Szabályzat hatálya kiterjed az Intézménnyel vállalkozói jogviszonyban, munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban álló valamennyi természetes személyre, jogi személyre, és jogi személyiséggel nem rendelkező szervezetre.
- Tárgyi hatály: a Szabályzat hatálya kiterjed a személyes adatok kezelésével, feldolgozásával érintett valamennyi az Intézmény által folytatott tevékenységre.

4. ADATVÉDELMI KOCKÁZATKEZELÉS

- a. Minden egyes adatkezelést alá kell vetni egy kockázatértékelési eljárásnak. A kockázatértékelési eljárás módszere az Intézményen belül egységes elvek mentén történik, az adatvédelmi tisztviselő ajánlásának megfelelően.
- b. A kockázat valószínűségét és súlyosságát az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni. A kockázatot olyan objektív értékelés alapján kell felmérni, amelynek során szükséges megállapítani, hogy az adatkezelési műveletek kockázattal, illetve nagy kockázattal járnak-e.
- c. Tekintve, hogy minden adatkezelés természeténél fogva kockázatos, így két kockázati kategória alkalmazandó. Ezek a „**kockázatos**” (vagy „**alacsony kockázat**”) és a „**magas kockázattal jár**”.

- d. A kockázatértékelés – egyebek mellett – figyelembe veszi az érintettek kategóriáit, az érintettek számát, a végzett adatkezelési műveleteket és az alkalmazott adatkezelési technológiát, ezen belül is annak újszerűségét.
- e. Magas kockázattal jár további mérlegelés nélkül az olyan adatkezelés, ami egészségügyi vagy bűnügyi adatok nagy tömegének feldolgozásával jár vagy olyan módszeres és kiterjedt, akár profilalkotással is járó feldolgozás, ami jogkövetkezésménnyel járhat vagy jelentős hatású döntés alapjául szolgál, illetve nyilvános helyek nagymértékű, módszeres megfigyelése.
- f. A kockázat objektív értékeléséhez a mindenkor követendő eljárást adatvédelmi tisztviselő tartja karban és biztosítja az Intézmény és szervezeti egységei számára.
- g. Ha az adatkezelés a kockázat értékelés alapján magas kockázattal jár, akkor az adatkezelő előzetesen hatásvizsgálatot végez (adatvédelmi hatásvizsgálat vagy DPIA).
- h. Az adatkezelési hatásvizsgálathoz az adatvédelmi tisztviselő tanácsát kötelezően ki kell kérni.

5. ADATVÉDELMI INCIDENSKEZELÉS

- a. Az adatkezelésben vagy adatfeldolgozási tevékenységben érintett munkatárs köteles az általa észlelt adatvédelmi eseményt **az adatvédelmi tisztviselőnek közvetlenül vagy az intézményvezető útján** azonnal bejelenteni.
- b. Az adatvédelmi tisztviselő feladatai incidens esetén az információgyűjtés, helyzetfelmérés és jelentés.
- c. A felmérés során az adatvédelmi tisztviselő információt szerez a következőkről: incidens jellege, érintettek és adatok kategóriái és az érintettek száma, incidensből eredő és valószínűsíthető következmények az érintettek nézvé, a lehetséges intézkedésekről, helyreállítási, kárenyhítési műveletek.
- d. Az adatvédelmi tisztviselő a feltárt eseményeket az összegyűjtött információkkal együtt nyilvántartja.
- e. Az adatvédelmi tisztviselő az incidensről haladéktalanul teljes körű jelentést tesz az Intézményvezetőnek.
- f. Adatfeldolgozó tevékenység során bekövetkezett incidens esetén az adatvédelmi tisztviselő bejelentést tesz az Adatkezelőnek és valamennyi, az esettel kapcsolatban gyűjtött információt átadja az Adatkezelőnek is további intézkedésre.
- g. Ha az incidens mértéke eléri az ehhez szükséges szintet, akkor az adatvédelmi tisztviselő köteles azt jelenteni a Felügyeleti Hatóságnak az incidens felmerülésétől számított 72 órán belül.
- h. Amennyiben az incidens mértéke eléri az ehhez szükséges mértéket, úgy az adatvédelmi tisztviselő előkészíti az incidens és hatásainak nyilvánosságra hozataláról szóló közleményt és javaslatot tesz a közzététel módjára a GDPR vonatkozó rendelkezései szerint.

6. AZ INTÉZMÉNYRE, MINT ADATKEZELŐRE VONATKOZÓ SZABÁLYOK

- a. Az Intézmény adatvédelmi szempontból kettős státuszban jelenik meg. Saját, belső tevékenysége vonatkozásában adatkezelőnek minősül. Az Intézmény által nyújtott szolgáltatások szempontjából az Intézmény adatfeldolgozónak minősül.
- b. Az adatkezelési gyakorlatban megkülönböztetünk belső és külső adatkezelést. A belső, amikor az Intézmény saját működéséhez kapcsolódóan kezelünk adatokat. Ennek jogalapja

- törvényi felhatalmazás vagy önkéntes beleegyezés vagy az adatkezelő, ez esetben az Intézmény jogos érdeke. Külső adatkezelés az Intézményi szolgáltatások teljesítése során az Intézményhez adatfeldolgozásra továbbított személyes adatok kezelése.
- c. Személyes adat akkor kezelhető, ha annak valamennyi feltétele fennáll, az adatkezelési alapelvek teljesülnek.
 - d. Különleges adat akkor kezelhető, ha az adatkezeléshez az érintett írásban hozzájárult és az adatkezelést jogszabály kifejezetten lehetővé teszi.
 - e. Kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.
 - f. Ha a hozzájáruláson alapuló adatkezelés célja az adatkezelővel írásban kötött szerződés végrehajtása, a szerződésnek tartalmaznia kell minden olyan információt, amely a személyes adatok kezelése szempontjából az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, az adatfeldolgozó igénybevételének tényét. A szerződésnek félreérthetetlenül tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.
 - g. Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezése hiányában a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll, további külön korlátozás nélkül, valamint az érintett hozzájárulásának visszavonása után is kezelhető. Ugyanakkor az érintettet az adatkezelésről tájékoztatni kell.
 - h. Az Intézmény adatkezelői és adatfeldolgozói tevékenységéért az érintett és harmadik fél felé az Intézményvezető felel (külső felelősség).
 - i. Az Intézmény adatkezelői és adatfeldolgozói tevékenységének végrehajtásáért a feladattal érintett szervezeti egység vezetője felel (belső felelősség).

7. AZ INTÉZMÉNYRE, MINT ADATFELDOLGOZÓRA VONATKOZÓ SZABÁLYOK

- a. Az Intézmény a szervezetekkel kötött szerződésekben vállalt vagy jogszabály által meghatározott feladatok végrehajtása során adatfeldolgozási tevékenységet végez, adatvédelmi státusza: **adatfeldolgozó**. A személyes adatokkal érintett tevékenysége során az Intézmény jogait és kötelezettségeit a vonatkozó törvények, valamint a szerződéses szervezett, mint adatkezelő határozza meg a szerződés adatkezelésre vonatkozó részében vagy ahhoz csatolt vagy külön rögzített adatkezelési megállapodásban vagy oly módon, hogy megjelöli a saját adatkezelése törvényi alapját.
- b. Az általa adott utasítások jogszerűségéért, valamint a feldolgozandó személyes adatok jogszerű kezeléséért az adatkezelő felel, de az Intézmény is vizsgálja a kapott utasítás jogszerűségét. Ha kétely merül fel, akkor azt az adatkezelővel tisztázni kell.
- c. Jogszabályba ütköző adatkezelői utasítást az Intézmény nem hajthat végre, ezt az adatkezelő felé az adatvédelmi tisztviselő tudtával és beleegyezésével írásban kell közölni.
- d. Az Intézmény, mint adatfeldolgozó az adatkezelést érintően érdemi döntést nem hozhat, azaz kizárólag azokat az adatkezelési műveleteket hajthatja végre, amivel a szerv, az adatkezelő megbízta, vagy amiket jogszabály végrehajtásra hozzá rendel. Az Intézmény a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet.

- e. Az Intézmény, mint adatfeldolgozó a részére átadott személyes adatokat a megbízó szervezettel, mint adatkezelővel – akár önállóan, akár szerződés részeként – kötött adatkezelési megállapodás szerint rendelkezései szerint köteles tárolni és legfeljebb az abban engedélyezett tárolási időig megőrizni.
- f. Az adatfeldolgozásra vonatkozó megállapodás, illetve szerződéses tartalom szakmai jóváhagyása minden esetben (különös tekintettel akkor, amikor az Adatkezelő által szövegezett megállapodásról van szó) az adatvédelmi tisztviselő feladata.
- g. Az Intézmény, mint adatfeldolgozó az adatkezelő szervezet rendelkezése szerint vehet igénybe további adatfeldolgozót. Az adatkezelővel kötött szerződés, valamint a hatályos előírások tartalmának megfelelően kell a további adatfeldolgozóval kapcsolatos megállapodásokban az adatkezelésre vonatkozó előírásokat rögzíteni szükséges.
- h. Adatok elektronikus átadására csak biztonságos módon kerülhet sor. Ezt az adatfeldolgozó tevékenységére vonatkozó szerződéses fejezetben vagy az adatfeldolgozói megbízási szerződésben rögzíteni kell.

8. ADATBIZTONSÁG, AZ ADATOK TÁROLÁSA

- a. Az Intézmény köteles az adatkezelési és feldolgozási műveleteket úgy megtervezni és végrehajtani, hogy a vonatkozó törvények és az adatkezelésre/adatfeldolgozásra vonatkozó egyéb szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.
- b. A személyes adatok kezelése és feldolgozása során az alábbiakat kell biztosítani:
 - i. jogosulatlan adatbevitel/hozzáférés megakadályozását
 - ii. az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatbeviteli rendszer segítségével történő használatának megakadályozását
 - iii. annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli rendszer alkalmazásával mely szerveknek vagy szervezeteknek továbbították, vagy továbbíthatják
 - iv. annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat ki és mikor vitte be az adatfeldolgozó rendszerekbe
 - v. a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát
 - vi. az automatizált feldolgozás során fellépő hibákról jelentés készítését
- a. Egyéb részletszabályok a következő helyeken szabályozottak:
 - i. *Szervezeti Működési szabályzat*
 - ii. *Pedagógiai program*
 - iii. *Házirend*
 - iv. *Munkaköri leírás*
 - v. *Iratkezelési szabályzat*
 - vi. *Közalkalmazotti Szabályzat*
 - vii. *Panaszkezelési Szabályzat*

9. AZ ADATVÉDELMI NYILVÁNTARTÁS

- 1. Az Intézmény, mint adatkezelést végző szervezet a GDPR 30. cikk alapján adatvédelmi nyilvántartás vezetésére kötelezett.

2. Az adatvédelmi nyilvántartás tartalmát az **1. melléklet** szerinti minta tartalmazza. A nyilvántartás vagy a minta szerinti táblázatban, vagy azonos rovszerkezetű nyilvántartó informatikai rendszerben kell megvalósítani.
3. A nyilvántartásba való bejegyzést az adatvédelmi tisztviselő, illetve az intézményi adatvédelmi tisztviselő vagy adatvédelmi kapcsolattartó végzi. Automatikus ügyviteli rendszerben megvalósított munkafolyamat esetén a folyamatban szerepelni kell az adatvédelmi tisztviselő ellenőrző tevékenységének, mint önálló lépésnek, ami a bejegyzést meg kell, hogy előzze.
4. Az adatvédelmi nyilvántartásban változást az erre szolgáló, a **2. mellékletben** bemutatott, vagy ezzel azonos adattartalmú elektronikus „Adatvédelmi változás bejelentővel” lehet megtenni.
5. Főszabály szerint minden új szerződés vagy megrendelés új adatkezelésnek minősül, amennyiben személyes adatok feldolgozására is irányul.
6. Minden adatkezelési műveletet meg kell előznie az adatkezelés nyilvántartásba vételének. Ennek biztosítására új feladat vagy feladattípus végrehajtásakor, új adatforrás alkalmazásakor ellenőrizni kell, hogy az szerepel-e már a nyilvántartásban.
7. Amennyiben kétség merül fel az adatkezeléssel kapcsolatban, úgy a munkatársak az adatkezelési nyilvántartásban ellenőrizhetik az adatkezelés jogszerűségét, megfelelőségét. Az adatvédelmi nyilvántartást ezért a szakterületek számára elérhetővé kell tenni az Intézmény belső hálózatán.

10. ADATIGÉNYLÉS, ADATSZOLGÁLTATÁS

1. Az Intézmény saját adatkezeléseiben lévő adataira irányuló, harmadik személytől érkező adatigényléseket az adatvédelmi tisztviselőhöz kell irányítani.
2. Az adatvédelmi tisztviselő a vonatkozó hatályos jogszabályokban és az Intézmény belső jogi normáiban foglaltak alapján megvizsgálja az adatigénylést, és javaslatot tesz a teljesíthetőségre vonatkozóan.
3. Az adatigénylés teljesítéséről az Intézményvezető dönt.
4. Az Intézménytől, mint adatfeldolgozótól személyes adatot igényelni csak a szerződéses szervezetnek, mint adatkezelőnek van módja, adatkezelési időn belül, a feldolgozásra átadott adatok vonatkozásában, az erre irányuló adatkezelési megállapodásban foglaltaknak megfelelően.
5. Az adatigénylés és annak teljesítése kizárólag írásban történhet.
6. Az adatfeldolgozói tevékenység során kezelt személyes adatokra vonatkozóan az Intézmény adatszolgáltatást nem teljesít harmadik személy részére. Ebben az esetben az adatigénylőt az adatkezelőhöz kell irányítani.
7. Az érintett megkeresése esetén indokolatlan késedelem nélkül egyrészt az érintettet tájékoztatni kell írásos válaszban az Intézmény adatfeldolgozói pozíciójáról, másrészt az adatkezelőt tájékoztatni kell a megkeresésről, amiről az érintett is értesítést kap.

11. ADATTOVÁBBÍTÁS MEGKERESÉS ALAPJÁN

- a. Az Intézményhez közigazgatási szervtől, gazdálkodó szervezettől, vagy magánszemélytől érkező, adatközlésre irányuló megkeresés csak akkor teljesíthető, ha arra jogszabály felhatalmazást ad vagy az érintett erre írásban felhatalmazta az Intézményt, illetve az Intézményvezető döntése szerint a kért adat átadása nem sérti az Intézmény érdekeit.

- b. Az érintett előzetesen is adhat ilyen tartalmú meghatalmazást, amely szólhat valamely időtartamra vagy a megkereséssel élő szervek meghatározott körére.
- c. Az adatigénylés – jogszabály eltérő rendelkezése hiányában – akkor teljesíthető, ha a kérelem tartalmazza:
 - i. a kért adatok kezelésének célját
 - ii. a kért adatkör pontos meghatározását
 - iii. az érintett személy egyértelmű azonosításához szükséges, és arra alkalmas adatokat
- d. Az érintett nyilatkozattételétől függetlenül teljesíteni kell a büntetőügyekben eljáró hatóságoktól – rendőrség, bíróság, ügyészség, NAV – valamint a nemzetbiztonsági szolgálatoktól érkező megkereséseket.
- e. Adattovábbítás
- f. Személyes adat törvény felhatalmazása alapján, vagy akkor továbbítható személynek, ha az adatátadáshoz az érintett bizonyíthatóan hozzájárult és ha az adatkezelés feltételei az adatot átvevő szervezetnél vagy személynél minden egyes adatra nézve teljesülnek.
- g. Az adatok átadása, azaz az adattovábbítás történhet
 - i. papíron
 - ii. digitális adathordozón
 - iii. online
- a. Elektronikus adatátadás csak szabályozott eljárások szerint történhet, hivatalos, csatolt, jogszabályra való hivatkozással megkereséssel.
- b. Az Intézmény adatfeldolgozói tevékenysége során a szervezetek részére az egyedi szerződésekben meghatározott módon – az Intézmény ide vonatkozó egyéb szabályzataival összhangban – történhet az adattovábbítás.
- c. Nem minősül adattovábbításnak:
 - i. egy nyilvántartási rendszeren belül az egymással kapcsolatban lévő szervezeti egységek közötti, adatfeldolgozási célú adatátadás
 - ii. a megbízási szerződés alapján adatfeldolgozás céljára történő adatátadás
 - iii. az érintett saját adatairól történő tájékoztatása

12. KÜLFÖLDRE TÖRTÉNŐ ADATTOVÁBBÍTÁS

- a. Az EGT tagállamaiba történő adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.
- b. Az Intézmény adatkezelőként személyes adatot az EGT tagállamain kívüli országban (harmadik ország) adatkezelést végző személy vagy szervezet részére az alábbi feltételek valamelyikének teljesülése esetén adhat át:
 - i. A GDPR szerint a Bizottság cél országra, szervezetre vagy területre vonatkozó megfelelőségi határozatot adott ki.
 - ii. Adatvédelmi hatóság által elfogadott Kötelező Vállalati Szabályok betartása mellett (GDPR 47. cikk).
 - iii. A Felügyeleti Hatóság külön engedélye nélkül, ha Bizottság általi vizsgálóbizottsági eljárást követő jóváhagyás alapján, jóváhagyott magatartási kódex vagy tanúsítási mechanizmus szerinti adattovábbításnál.

- iv. A Felügyeleti Hatóság engedélyével, szerződés alapján, közhatalmi vagy közfeladatot ellátó szervek közötti közigazgatási megállapodás esetén, ha a jogérvényesítés biztosítható.

13. SZERVEZETEN BELÜLI ADATTOVÁBBÍTÁS, ADATKEZELÉSEK ÖSSZEKAPCSOLÁSA

- a. Szervezetten belüli adattovábbításra az Intézmény adatfeldolgozó tevékenységével összefüggésben, az ügyintézéshez, eljárásokhoz közvetlenül kapcsolódva, a zárt és védett informatikai rendszerben kerülhet sor.
- b. Az egyes termékek előállítása során csak az adott termékhez kapcsolódó adatállomány feldolgozása történhet, különböző ügyfelek termékekhez kapcsolódó adatállományok összekapcsolása tilos. Az egyes adatfeldolgozásra átvett adatállományok között folyamatosan biztosítani kell az elhatárolást.
- c. A szervezetten belüli adattovábbításért, valamint az összekapcsolások megakadályozásáért és az adatok elkülönített tárolásáért a termelési informatika felel, amihez az Informatika platformot biztosít.

14. AZ ADATOK HELYESBÍTÉSE, TÖRLÉSE

- a. Az adatokat törölni – papír alapú nyilvántartás esetén selejtezni és megsemmisíteni szükséges, ha:
 - i. az adatkezelésre jogszabályban előírt határidő letelt
 - ii. az adatkezelés jogszerűtlen volta megállapítást nyert
 - iii. a felhasználási cél teljesítését követően az adatátadó fél kéri
 - iv. az érintett a hozzájárulását írásban visszavonta, kivéve ha törvény lehetővé teszi vagy kifejezetten előírja a további őrzést
 - v. a bíróság jogerős határozattal elrendelte
 - vi. az adatkezelés önkéntes hozzájáruláson alapult és az érintett jogszerűen kéri
 - vii. az adat hiányos (töredék) vagy téves, és ez az állapot jogszerűen nem korrigálható, feltéve, hogy a törlést törvény nem zárja ki
 - viii. az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt.
- b. A törlés nem jelenti feltétlenül a teljes adatállomány visszaállíthatatlan törlését. Amennyiben technikailag lehetséges, az adatállomány egyes részeinek megtartásával is eleget lehet tenni a törlési kötelezettségnek, a megmaradó adatok azonban nem lehetnek kapcsolatba hozhatók természetes személyekkel (pl. összesített, statisztikai adatok).
- c. A törlést dokumentálni kell. A dokumentálás elektronikus úton is történhet.
- d. Az érintett kérelmére az Intézmény, mint adatkezelő az érintett hibásan kezelt személyes adatát helyesbíti.
- e. Ha az Intézmény megállapítja, hogy a közvetlen adatforrás nem az érintett, ennél fogva az adat közvetlenül nem javítható és/vagy helyesbíthető, az érintettet tájékoztatni kell az adatforrásról, ahol a javítást/helyesbítést kezdeményezheti.
- f. Amennyiben az érintett tájékoztatása alapján vagy más módon az Intézmény, mint adatkezelő tudomására jut, hogy a közvetlen adatforrásban az adatok helyesbítése/javítása megtörtént, kezdeményezni kell a helyes adat felvételét, és a hibás adatot archiválni kell.

- g. Ha az adat helyesbítése nem lehetséges, vagy bizonyítást nyer, hogy az Intézmény az adatot törvényi felhatalmazás vagy az érintett hozzájárulása nélkül kezeli, akkor az adatokat törölni, vagy véglegesen zárolni kell.
- h. A helyesbítési, törlési kérelmet érdemben meg kell vizsgálni, és amennyiben az megalapozott, a helyesbítést, törlést teljesíteni kell, függetlenül attól, hogy az érintett tájékoztatható-e az eljárás eredményéről.
- i. A helyesbítésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljából továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára tekintettel az érintett jogos érdekét nem sérti és aránytalan ráfordítással járna
- j. Az Intézmény az adatfeldolgozóként kapott adatokat a vonatkozó szerződésekben foglaltak szerint csak a hivatali eljárás befejezéséig, vagy az adatkezelő által megállapított ideig tárolhatja, ezt követően vagy visszaküldi az adatkezelő szervezetnek, vagy visszaállíthatatlan módon törli azokat.
- k. Az informatikai rendszerben a kialakított és elfogadott protokollok csak az arra feljogosított személy törölhet és/vagy helyesbíthet adatokat.
- l. A törléseket/helyesbítéseket a rendszernek naplózni kell vagy más módon bizonyíthatóvá kell tenni.
- m. A személyes adatokat az ügyviteli, ügykezelő és más szakrendszerekből és adatbázisokból az adatkezelési megállapodásban vagy az adatfeldolgozásra irányuló szerződés megfelelő pontjában rögzítettek szerint kell végrehajtani.
- n. A mentésekből a személyes adatokat, ha nincs a megőrzésüket kifejezetten előíró jogszabály, alapesetben törölni kell. Mentésből adatszolgáltatás nem teljesíthető.
- o. A papír alapú anyagok irattári kezeléséért az az **irattári egység** felel, ami a szervezetben az adott egység számára az irattári tevékenységet ellátja.

15. AZ ÉRINTETT JOGAI GYAKORLÁSÁNAK BIZTOSÍTÁSA

- a. Az érintett az Intézménytől tájékoztatást kérhet a róla szóló adatkezelésekről, amelyet az Intézmény adatkezelőként végez.
- b. Az érintett kérésére az Intézmény tájékoztatást ad:
 - i. az általa kezelt, illetőleg általa feldolgozott adatairól,
 - ii. az adatkezelés céljáról, jogalapjáról,
 - iii. az adatfeldolgozó nevééről, címéről (székhelyéről),
 - iv. az adatkezeléssel összefüggő tevékenységéről,
 - v. kik és milyen célból kapták vagy kapják meg az érintett adatait.
- c. Az Intézmény köteles az érintett részére az általa írásban benyújtott kérelem benyújtásától számított legrövidebb idő alatt, de legfeljebb 30 napon belül írásban, közérthető formában megadni a kért tájékoztatást.
- d. A tájékoztatás csak akkor tagadható meg, ha a kért adatokat törvény az állam külső és belső biztonsága, így különösen honvédelmi, nemzetbiztonsági, bűnüldözési, bűnmegelőzési, állami, önkormányzati, gazdasági vagy pénzügyi érdekből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából, továbbá az érintett vagy mások jogainak védelme érdekében korlátozza.

- e. Ez utóbbi esetben az Intézmény, mint adatkezelő köteles az érintettel a közlés megtagadásának indokát közölni.

16. SZEMÉLYES ADATOK NYILVÁNOSSÁGRA HOZATALA

- a. Az Intézmény adatkezelésében lévő adatok nyilvánosságra hozatala – kivéve, ha azt törvény rendeli el – tilos.
- b. Az Intézmény tevékenységével összefüggő, személyes adatokon is alapuló statisztikai adatok minden esetben közölhetők.
- c. Az Intézmény, mint adatfeldolgozó nem hozhatja nyilvánosságra a szerződéses szervezettől kapott személyes adatokat.
- d. A szerződéses szervezet, mint adatkezelő utasítása és rendelkezése alapján az Intézmény biztosíthatja a nyilvánosságra hozatal feltételeit. Ebben az esetben a nyilvánosságra hozatalért a felelősség az adatkezelőt terheli.

17. ADATVÉDELMI TISZTVISELŐ

- a. Az Intézménynél – a GDPR 37. cikkben foglaltakra is tekintettel – adatvédelmi tisztviselőt lehet kinevezni vagy megbízni. Adatvédelmi tisztviselő lehet megfelelő tapasztalattal rendelkező alkalmazott, de szerződéses külső adatvédelmi szakértő is megbízható. Tisztviselői tevékenységén kívül más feladatokat is elláthat, amennyiben azok nem összeférhetetlenek fő feladatával.
- b. Az Intézmény adatvédelmi tisztviselőt kijelöléséről valamennyi érintett szervezeti egységét értesíti.
- c. Az adatvédelmi tisztviselő a munkatársak, a partner szervezetek és az érintettek számára is közvetlenül elérhető, ezért kapcsolattartási adatait könnyen elérhető módon nyilvánosságra kell hozni minden web oldalon és minden adatvédelemmel foglalkozó szabályozásban.
- d. Az adatvédelmi tisztviselő kinevezését a Felügyeleti Hatóságnál be kell jelenteni.
- e. Az adatkezelési és az adatfeldolgozási tevékenységek során az Intézménynek biztosítania kell, hogy az adatvédelmi tisztviselő minden esetben az adatok védelmével kapcsolatos ügyekbe megfelelő időben (lehetőleg már a tervezés fázisában) és módon bekapcsolódjon.
- f. Az Intézmény támogatja az adatvédelmi tisztviselőt a GDPR 39. cikkben említett feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.
- g. Az Intézmény biztosítja, hogy az adatvédelmi tisztviselő - ebben a feladatkörben -a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el, mely nem jelenti azt, hogy tevékenységétől eltérően döntési jogkörrel rendelkezne. Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja, azonban szándékos vagy gondatlan rossz adatkezelési iránymutatás esetén jogi szankcióval léphet fel vele szemben az adatkezelő.
- h. Az adatvédelmi tisztviselő közvetlenül az Intézményvezetőnek tartozik felelősséggel.
- i. Az adatvédelmi tisztviselő feladatkörében:
 - i. tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

- ii. ellenőrzi és fenntartja az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
- iii. kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
- iv. együttműködik a felügyeleti hatósággal; és
- v. az adatkezeléssel összefüggő ügyekben – ideértve a GDPR 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.
- vi. kötelezően részt vesz az adatvédelmi incidensek kivizsgálásában.

18. EGYES HUMÁNPOLITIKAI SAJÁTOSÁGOK

- a. A munkaviszonnyal kapcsolatos adatok tekintetében az Intézmény adatkezelőnek minősül. Ez esetben vegyes – kötelező és önkéntes hozzájáruláson alapuló – adatkezelés valósul meg az Intézménynél. A kötelezően kezelendő adatok körét a munkaviszonyt szabályozó jogszabályok (MT, SZJA tv, Számviteli tv, egészségbiztosítással kapcsolatos jogszabályok, nyugdíjra vonatkozó szabályozás, KJT. Köznevelési törvény, közigazgatási, köztisztviselői tv.) határozzák meg. Az e jogszabályokban meghatározottakon túli további munkaügyi adatok kezelése az érintett önkéntes hozzájárulásán alapul.
- b. Az adott pozícióra beküldött önéletrajzok kezelése a munkaviszony létrejöttéig az érintett önkéntes hozzájárulásán alapul. Ezt a tényt, továbbá az önéletrajzok megőrzési idejére vonatkozó szabályokat az érintettel az álláspályázatok kiírása, továbbá az állásinterjúk során közölni kell és hozzájárulását írásos formában beszerezni.
- c. Amennyiben az érintettel nem jön létre munkaviszony, az önéletrajzát az állás sikeres betöltése után azonnal törölni kell.
- d. A szabályozást úgy kell kialakítani, hogy az állás sikeres betöltésének a munkaviszony létrejöttét majd a próbaidő sikeres leteltét tekintjük, egyben.
- e. Amennyiben nem adott álláshirdetésre érkezik önéletrajz, úgy az az érintettnek megküldött, vagy az általa a honlapról letöltött és aláírásával elfogadott adatkezelési nyilatkozattal együtt őrizhető meg. A nyilatkozat kiemelt része a megőrzési idő, amit bizonyítható módon be kell tartani.
- f. Volt munkavállalók adatai: csak törvény által meghatározott kötelező megőrzési idők szerint kezelhetők tovább.
- g. Kölcsönzött munkaerő esetében a munkaerő kölcsönző szolgáltató az adatkezelő. Az Intézmény részére továbbított adatok tekintetében adatkezelési megállapodást kell kötni.

19. BIZTONSÁGI TERÜLET EGYES ADATVÉDELMI SZABÁLYAI

- a. A belépő kártyák, biztonsági kamerák és belépő-nyilvántartás (vendéglista) tekintetében az Intézmény adatkezelőnek minősül, az adatkezelés alapja az adatkezelő jogos érdeke valamint a jogszabályi felhatalmazás.
- b. A belépő kártyák használatáról, a biztonsági kamerák működéséről és a kapcsolódó adatkezelésről a munkavállalók teljes körű tájékoztatást kapnak belépéskor valamint adatvédelmi oktatás keretében, mely tájékoztatás tényét elismerik (nyilatkozatban vagy oktatási naplóban történő rögzítéssel).

- c. A belépő kártyák használatának célja a biztonság, más célra, mint például a munkavégzés ellenőrzésére nem használhatók és ezt ekként kell szabályozni.
- d. A belépő-nyilvántartás alapja az Intézmény jogos érdeke. A belépők első belépéskor teljes körű, legalább évente megújított tájékoztatást kapnak és egyidejű önkéntes hozzájárulásukat adják a leírt adatkezeléshez.
- e. A kamerás megfigyelő rendszer működtetésének tényét, valamint azt a tényt, hogy nem csak megfigyelés, hanem képrögzítés is történik, jól látható helyen fel kell tüntetni a megfigyelt terület határán minden egyes bejáratnál.
- f. A kamerás megfigyelő rendszer csak magánterületen, a vagyon- és személyvédelem, valamint a közbiztonság érdekében üzemeltethető. Az élőben közvetített vagy rögzített kép más célra, mint például munkavégzés ellenőrzése, nem használható.
- g. A kamerás megfigyelő rendszer adatainak megőrzési ideje a törvény által engedélyezett őrzési időnél nem lehet hosszabb és ennek részleteit a Biztonsági Szabályzat határozza meg.
- h. A kamerás megfigyelő rendszer használata az intim helyiségekben tilos.
- i. A kamerás megfigyelő rendszer által rögzített adatokba adatvédelmi vagy biztonsági incidens, biztonsági esemény vagy annak gyanúja illetőleg audit esetén bizottság általi betekintés történhet, a Biztonsági Szabályzatban részletezett módon.
- j. A kamerás megfigyelő rendszer és a beléptető rendszer által rögzített adatokból az adatkezelési időn belül adatszolgáltatás az Intézményvezető, mint a szervezet első számú vezetőjének engedélyével teljesíthető, kizárólag törvény által lehetővé tett esetekben.
- k. Az egyes kiszervezett biztonsági tevékenységek esetében, mint az élőerős őrző-védő szolgáltatás az Intézmény a hozzá kirendelt munkaerő tekintetében adatfeldolgozónak minősül. Az adatfeldolgozás részleteit az adatkezelővel, aki a kirendelt munkaerő munkáltatója, adatkezelési megállapodást köt.
- l. Az egyes külső beszállítók állandó belépésre jogosult munkatársairól az Intézmény a megjelenéskor azonosításukat is lehetővé tevő nyilvántartást vezet. Ennek tartalma annyi és csak annyi, ami a belépéskori ellenőrzéshez szükséges.

20. ZÁRÓ RENDELKEZÉSEK

A 2016. december 13-tól hatályos Adatkezelési Szabályzat hatályon kívül helyeződik.
Jelen Adatvédelmi Szabályzat 2019. március 18-án lép hatályba.

