



Budapest Főváros XV. kerületi Önkormányzat

Újpalotai Összevont Óvoda

Iktatószám: 204/2024.

EGYSÉGES SZERKEZETBE FOGLALT ADATKEZELÉSI ÉS ADATBIZTONSÁGI SZABÁLYZAT (V_1)

Érvényes: 2024.12.02 - től

TARTALOMJEGYZÉK

<i>Dokumentum változás követése</i>	<i>5</i>
<i>Fogalomtár.....</i>	<i>6</i>
<i>A szabályzat tárgya és kritériumai</i>	<i>8</i>
<i>A szabályzat célja</i>	<i>9</i>
<i>A szabályzat hatálya.....</i>	<i>10</i>
I. MUNKÁLTATÓI ADATKEZELÉSI SZABÁLYOK	11
1. Az érintett hozzájárulása alapján történő adatkezelés.....	11
2. Adatkezelés jogi kötelezettség teljesítése érdekében	11
3. Adatkezelés munkáltatói „jogos érdek” alapján	12
4. Álláspályázatokhoz kapcsolódó adatkezelések.....	13
5. Munkáltatói e-mail cím és fiók használatához kapcsolódó adatkezelés.....	13
6. Munkavégzés helyére történő be- és kiléptetéssel kapcsolatos adatkezelés	15
7. Munkahelyi elektronikus megfigyelő rendszer adatkezelése.....	16
8. Munkáltatói internet és wifi használatával kapcsolatos adatkezelés.....	16
9. Munkáltatói számítógép, laptop, tablet használatával kapcsolatos adatkezelés ...	17
10. Munkáltató által biztosított mobiltelefon használatának ellenőrzésével kapcsolatos adatkezelés	19
11. Munkáltató által biztosított telefon, autó és egyéb eszköz gps adatainak (földrajzi helyzetének) kezelése	20
12. Alkalmassági vizsgálatokhoz kapcsolódó adatkezelés	21
II. MUNKAVÁLLALÓI ADATBIZTONSÁGI SZABÁLYOK.....	23
1. Biztonságra törekvő viselkedés a munkahelyen	23
2. Számítógépes munkahely biztonságos használata.....	23
3. Hordozható számítógépek biztonságos használata.....	24
3.1. Adatbiztonsági szabályok	24
3.2. Jogosulatlanok általi, információhoz való hozzáférések megakadályozása	25
3.3. Hordozható számítógépek fokozott vírusveszélye kockázatainak csökkentése.....	25
3.4. Intézkedések, ha a hordozható számítógépet már ellopták, vagy elveszítették.....	25
4. Mobil informatikai adathordozók biztonságos használata.....	26
5. Az intézmény informatikai hálózatának (ha van) biztonságos használata	26
6. Jelszó használati szabályok	27
6.1. A jelszó képzése	27
6.2. A jelszavak cseréje	27
6.3. A jelszó titokban tartása	27
6.4. Különleges szabályok helyettesítések/vészhelyzetek esetére	28
7. Munkahelyi elektronikus levelezés biztonságos használata	28

7.1.	E-mailek küldésére vonatkozó irányelvek.....	28
7.2.	Az e-mailek fogadására vonatkozó irányelvek	29
8.	Munkahelyi internet biztonságos használata	29
9.	Vírusvédelmi szabályok	29
9.1.	A központi vírusvédelmi szoftver alkalmazására vonatkozó szabályok.....	29
9.2.	Teendők vírusfertőzés gyanúja vagy biztos felismerése esetén.....	30
III.	IT ÜZEMELTETÉS ADATVÉDELMI SZABÁLYOK.....	31
1.	Az IT szabályok használata	31
2.	A fizikai elhelyezés és az üzemeltetés fizikai biztonsága	31
3.	Jogosultságok menedzselése.....	32
4.	Hálózatbiztonsági szabályok.....	32
4.1.	Belső hálózati szabályok	32
4.2.	Intézmény Wi-Fi használati szabályai	33
4.3.	Távmunka és otthoni munkavégzés.....	33
5.	Informatikai eszközök üzemeltetésének logikai biztonsága.....	34
5.1.	Szerverek	34
5.2.	Személyes adatokat tartalmazó fájl-megosztások és alkalmazások biztonsága.....	34
5.3.	Munkaállomások és perifériák	34
6.	Mentési szabályok	35
7.	Titkosítási szabályok	36
8.	Új informatikai rendszerek tervezésére vonatkozó biztonság (privacy by design) 37	
9.	It üzletmenet-folytonosság és katasztrófa-elhárítás	37
IV.	ÉRINTETTI KÉRELMEK TELJESÍTÉSÉNEK RENDJE.....	39
1.	Az adatkezeléssel érintett magánszemélyek alapvető jogai.....	39
2.	Az érintett magánszemély kérelmének benyújtása.....	41
3.	Az érintetti kérelmek elbírálása	41
4.	Adatvédelmi előírások.....	42
V.	ADATVÉDELMI INCIDENSKEZELÉSI SZABÁLYOK.....	43
	Adatvédelmi incidens fogalma	43
	Adatvédelmi incidens eljárásrendje (PROTOKOLL)	43
1.	Adatvédelmi incidens észlelése	43
2.	Adatvédelmi incidens bizonyítékainak a tárolása.....	43
3.	Adatvédelmi incidens vizsgálata	43
4.	Adatvédelmi incidens bejelentése	44
5.	Adatvédelmi incidens érintettjeinek értesítése	44
6.	Adatvédelmi incidens nyilvántartása	44
	Záró rendelkezések	45
	FÜGGELÉKEK.....	46
1.	sz. függelék (Adatkezelési tájékoztató - munkaerő kiválasztásához és felvételéhez)	
	47	

2.	sz. függelék (Érintetti hozzájárulás magánszemély adatainak a kezeléséhez)	50
3.	sz. függelék (Érintettek számára tájékoztatás és kérelem űrlap)	51
4.	sz. függelék (Válaszlevél sablon az érintetti kérelemhez)	53
5.	sz. függelék (Érintetti kérelmek nyilvántartása)	54
MELLÉKLETEK		55
1.	sz. melléklet (Incidenskezelési eljárásrend folyamata – protokoll)	55
2.	sz. melléklet (Incidens bejelentő lap – NAIH honlapjáról letölthető nyomtatvány)	56

I. DOKUMENTUM VÁLTOZÁS KÖVETÉSE

Verzió-szám	Iktatószám (előzmény)	Dokumentum címe	Változás leírása	Felelős (beosztás)	Hatályba lépés dátuma
V_1	/2018.	Munkáltatói adatkezelési szabályzat	Alapdokumentum	Igazgató	2018.05.25
V_2	254/2020	Munkáltatói adatkezelési szabályzat	Belső ellenőri megállapítások átvezetése	Igazgató	2020.06.30
V_1	/2018.	Munkavállalói adatbiztonsági szabályzat	Alapdokumentum	Igazgató	2018.05.25
V_2	398/2020.	Munkavállalói adatbiztonsági szabályzat	DPO által aktualizált	Igazgató	2020/09.01
V_1	/2018.	IT Üzemeltetés adatbiztonsági szabályzat	Alapdokumentum	Igazgató	2018.05.25
V_2	238/2020	IT Üzemeltetés adatbiztonsági szabályzat	Belső ellenőri megállapítások átvezetése	Igazgató	2020/06.30
V_1	560/2020	Érintetti kérelmek teljesítésének rendje	Alapdokumentum	Igazgató	2021.01.04
V_1	254/2018.	Adatvédelmi incidenskezelési szabályzat	Alapdokumentum	Igazgató	2018.06.18
V_2	269/2020	Adatvédelmi incidenskezelési szabályzat	Belső ellenőri megállapítások átvezetése	Igazgató	2020.06.30
V_1	204/2024.	Egységes szerkezetbe foglalt adatkezelési és adatvédelmi szabályzat	5 GDPR szabályzat egységes szerkezetbe foglalása	Igazgató	2024.12.02

II. FOGALOMTÁR

Sorszám	Fogalom / rövidítés	Meghatározás
1.	Adatkezelő	Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Újpalotai Összevont Óvoda
2.	Adatfeldolgozó	Az, aki a Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Újpalotai Összevont Óvoda megbízásából személyes adatokkal dolgozik.
3.	Alkalmazás	(angol: application, app) egy számítógépes program, ami egy fordítóprogram segítségével készül el egy forráskódból. A számítógépes programok ezen elnevezése elsősorban a Windows operációs és felhasználói rendszerek magyar fordítógárdája munkája nyomán terjedt el.
4.	Általános Adatkezelési Szabályzat	GDPR rendelet - EU Parlament és Tanács 2016/679. sz. rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
5.	Anonimizálás (álnevesítés)	Az éles adatbázisban a természetes személyek minden olyan adatának véletlenszerű, de hasonló típusú adattal történő felülírása, amely alapján a természetes személyek beazonosíthatósága már nem lehetséges. Ugyanakkor az adatbázis jellege és struktúrája megmarad, és így az – esetleges – programhibák beazonosíthatósága megmarad.
6.	Incidens	A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését, az azokhoz való jogosulatlan hozzáférést vagy a jogosultak számára a hozzáférhetetlenné férést eredményezi.
7.	Intézmény	Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Újpalotai Összevont Óvoda
8.	Intézményvezető	Az Intézmény Igazgatója
9.	IT BCP-DRP terv	BCP-DRP terv az információbiztonsági szakmában közismert rövidítése az üzletmenet-folytonossági és katasztrófa-elhárítási terveknek, ami rövidítés az angol megfelelőjük (Business Continuity Plan – Disaster Recovery Plan) rövidítéséből, mint mozaik betűszó adódik.
10.	Fájl	(Angol: File) Adatállomány
11.	Felhasználó	Aki az IT rendszereket, alkalmazásokat az eszközökön keresztül használja.
12.	GDPR	GDPR rendelet - EU Parlament és Tanács 2016/679. sz. rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
13.	GMK	Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Gazdasági Működtetési Központ
14.	HDD	(Angol: H ard D isk D rive) Merevlemez
15.	IP	(Angol: Internet Protocol, rövidítve: IP) az internet (és internetalapú) hálózat egyik alapvető szabványa (avagy protokollja). Ezen protokoll segítségével kommunikálnak egymással az internetre kötött csomópontok (számítógépek, hálózati eszközök, webkamerák stb.). A protokoll

Sorszám	Fogalom / rövidítés	Meghatározás
		meghatározza az egymásnak küldhető üzenetek felépítését, sorrendjét stb.
16.	Kétfaktoros azonosítás	további második azonosítási mód egyidejű alkalmazása
17.	Kliens	Olyan számítógép vagy azon futó program, amelyik hozzáfér egy (távoli) szolgáltatáshoz, amelyet egy számítógép hálózathoz tartozó másik számítógép (a szerver) nyújt
18.	Munkáltató	Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Újpalotai Összevont Óvoda
19.	Munkaszerződés	Kinevezés
20.	Munkavállaló	Közalkalmazott
21.	Munkaszerződés	Kinevezés
22.	NIF	Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat Népegészségügyi és Intézmény Felügyeleti Főosztály
23.	Operációs rendszerek	röviden OS az angol O perating S ystem alapján) nevezzük a számítástechnikában a számítógépeknek azt az alapprogramját, mely közvetlenül kezeli a hardvert, és egy egységes környezetet biztosít a számítógépen futtatandó alkalmazásoknak (például szövegszerkesztők, játékok stb.)
24.	Pendrive	(USB-flash-tároló, USB-kulcs, tollmeghajtó) USB-csatlakozóval egybeépített flash memória.
25.	Perifériák	A fogalmat eredetileg azokra az eszközökre alkalmazták, melyek külsőleg csatlakoztak a gazdagéphez, tipikusan egy számítógépes buszon keresztül, mint például az USB. Tipikus példa a joystick, nyomtató, és lapolvasó.
26.	RAID technológia	Minden RAID szint alapján véve vagy az adatbiztonság növelését vagy az adatátviteli sebesség növelését szolgálja.
27.	Rendszergazda	Informatikai üzemeltetést végző GMK informatikai munkavállalója.
28.	RPO	RPO (Return Point of Objective) az IT rendszer működésének leállása utáni visszaállításkor az az állapot, amire a rendszer vissza tud állni (gyakorlatilag maximálisan mennyi idővel lehet az utolsó elmentett állapot a leállást megelőzően)
29.	RTO	RTO (Return Time of Objective) az IT rendszer működésének leállása utáni időtartam, amin belül az IT rendszer újra üzemképesé válik (gyakorlatilag a megengedett legnagyobb leállási időtartam)
30.	Szerver	(az angol server szóból) vagy kiszolgáló az informatikában olyan (általában nagy teljesítményű) számítógépet vagy szoftvert jelent, ami más számítógépek számára a rajta tárolt vagy előállított adatok felhasználását, a szerver hardver erőforrásainak (például nyomtató, háttértárolók, processzor) kihasználását, illetve más szolgáltatások elérését teszi lehetővé.
31.	Szoftver	Számítógépes alkalmazás (program).
32.	VPN	(angolul V irtual P ivate N etwork) egy nyilvános hálózaton keresztül kiterjeszti a helyi hálózatot.
33.	Windows	a Microsoft Corporation gyártotta operációs rendszerek, illetve az ezekbe épített többfeladatos grafikus felhasználói felületek, valamint bizonyos mobiltechnológiák családja. A „Windows” szó és logó a Microsoft cég védjegye.
34.	Wi-Fi	(WiFi, Wifi vagy wifi), az IEEE által kifejlesztett vezeték nélküli mikrohullámú kommunikációt (WLAN) megvalósító, széleskörűen elterjedt szabvány (IEEE 802.11) népszerű neve.

III. A SZABÁLYZAT TÁRGYA ÉS KRITÉRIUMAI

A szabályozás tárgya: A Budapest Főváros XV. kerületi Rákospalota, Pestújhely, Újpalota Önkormányzat **Újpalotai Összevont Óvoda**, mint adatkezelő (továbbiakban: adatkezelő vagy Intézmény) jelen szabályzatban tájékoztatja az érintett munkavállalókat, hogy jelen szabályzatban tömör és közérthető formában igyekszik leírást adni:

- 1) a munkavállalók által kötelezően betartandó adatbiztonsági szabályokról,
- 2) a munkavállalók által végzett személyes adatkezelésekről, az érintettek jogairól, garanciákról,
- 3) tájékoztatni az érintett magánszemélyeket, hogy az egyes benyújtott kérelmeikhez milyen eljárás kapcsolódik,
- 4) a személyes adatkezelések adatvédelmi incidenskezelési eljárásrendjéről.
- 5) az IT üzemeltetés adatvédelmi szabályairól

Jelen adatkezelési és adatbiztonsági szabályok azokat - általános, számítógépes munkahelyen dolgozó minden munkavállaló által betartandó adatbiztonsági célú szabályokat - foglalják össze, amelyek alapvetőek és szükségesek a papír alapú és elektronikus formátumú adatok – különösen a személyes adatok – kezelésének alapvető biztonságos használatához.

A szabályozás kritériumai: Az adatkezelő és / vagy adatfeldolgozó az adatkezelési tevékenységét úgy végzi és munkavállalóitól elvárja, hogy az feleljen meg az Európai Unió Parlament és Tanács 2016/679. számú **Általános Adatvédelmi Rendeletének**, ismert elnevezéssel: a „**GDPR**”-nek, amely alapvetően szabályozza a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását.

Az Intézmény által kezelt adatok adatbiztonságának kialakításához és fenntartásához – a jelen szabályzat előírásán, betartásán és számonkérésén túlmenően – szükség van még az Informatikai infrastruktúra üzemeltetésének megfelelően biztonságos és szabályozott működtetésére is, amelyre vonatkozó adatbiztonsági alapelveket a rendszergazda számára a mindenkor hatályos „IT Üzemeltetés Adatvédelmi Szabályzata” c. szabályzat tartalmazza.

IV. A SZABÁLYZAT CÉLJA

1. Azoknak a belső szabályoknak és intézkedéseknek a megismertetése a munkavállalókkal, amelyek az érintettek számára a jogi garanciákat, az adatkezelő számára a megfelelést (compliance) biztosítják, és azt utólag igazolni is tudja (elszámoltathatóság) mind az adatvédelmi hatóság, mind az érintett magánszemélyek felé.
2. Az Intézmény általános működésében minden papír alapú adatkezelése és informatikai rendszerhasználata során előírni azokat az alapvető, minden munkavállalóra vonatkozó viselkedési, munkahelyi és informatikai eszközök használatára vonatkozó biztonsági szabályokat, amelyek az alapvető adatok (beleértve a személyes adatok) kezelésének adatbiztonsági feltételeit biztosítják.
3. Az Intézmény általános működésében minden informatikai rendszerhasználat során előírni azokat az alapvető, az informatikai rendszerek biztonságos üzemeltetésére vonatkozó biztonsági szabályokat, amelyek az alapvető adatok (elsősorban a személyes adatok szempontjából történő) kezelésének adatbiztonsági feltételeit biztosítják. Az Intézmény által kezelt személyes adatok adatbiztonságának kialakításához és fenntartásához – a jelen szabályzat előírásán, betartásán és számonkérésén túlmenően – szükség van még az informatikai infrastruktúrának az azt használó munkatársak általi biztonságos használatára is.
4. Az érintett magánszemélyek könnyen és akár előzetesen tudjanak tájékozódni jogaikról és az eljárás menetéről.
5. Azoknak a belső szabályoknak és intézkedéseknek a megismertetése a munkavállalókkal, amelyek az adatkezelő (vagy adatfeldolgozó) által a bekövetkezett adatvédelmi incidensek esetén végrehajtandók az incidensek hatásának csökkentésére, bekövetkezési okának feltárására és további incidensek elkerülésére, valamint az incidensek által leállított folyamatok minél előbbi újraindítására.

Jelen Szabályzat az „Általános Adatkezelési Rendelet - GDPR” alapelveinek és előírásainak betartása mellett érvényes, és tartalmazza azoknak az alapelveknek a megvalósítását a külső-belső érintettek, vagyis a magánszemélyek és a munkavállalók esetére is.

V. A SZABÁLYZAT HATÁLYA

Jelen Szabályzat **hatálya** kiterjed az Intézmény minden közalkalmazottjára (továbbiakban: munkavállalóra) és szerződéses alvállalkozójára, akik az Intézmény informatikai infrastruktúrájához hozzáférnek, azt használják, illetve az Intézmény folyamataiban, tevékenységeiben részt vesznek, az adatkezelő számára (adatokkal történő) műveleteket, feladatokat látnak el. Az egyes munkáltatói tevékenységekben a munkavállalók személyes adatai esetileg különböző jogalapok alapján kerülnek kezelésre, így: jogi kötelezettség vagy kinevezés (munkaszerződés) teljesítése, illetve munkáltatói jogos érdek alapján.

A közalkalmazottat foglalkoztató Intézmény (továbbiakban: Munkáltató) vállalja, hogy a munkaviszonyhoz kapcsolódóan adatfeldolgozók részére átadott adatok és a folytatott adatkezelési műveletekre vonatkozóan az adatfeldolgozókkal betartatja a GDPR előírásait.

Továbbá a szabályzat **hatálya** kiterjed

- az Intézmény informatikai rendszerét üzemeltető rendszergazdára vagy rendszergazdai csoportra, függetlenül hogy az az Intézmény alkalmazottja vagy külső szolgáltató. (Külső szolgáltató a GMK, ezért jelen szabályzat alkalmazását az Együttműködési megállapodáson keresztül kell előírni, odafigyelve a jelen szabályzatban előírtak betartásának ellenőrzésére is.)
- az Adatkezelő és/vagy Adatfeldolgozó minden (belső és külső) munkavállalójára, mint az adatvédelmi esemény vagy incidens észlelésekor szolgálati jelentéstételi úton az azonnali jelentési kötelezettség betartására;
- az Adatkezelő vagy Adatfeldolgozó adatvédelemért felelős vezetője számára az incidenskezelési folyamatban meghatározott feladatai végrehajtására;
- az incidenskezelés szakmai elemzésében és megoldásában, kezelésében részt vevő szakértői team tagjaira feladataik végrehajtásában.

VI. MUNKÁLTATÓI ADATKEZELÉSI SZABÁLYOK

1. Az érintett hozzájárulása alapján történő adatkezelés

Az Általános Adatkezelési Rendelet - GDPR „3. Az érintett hozzájárulása alapján történő adatkezelés” c. fejezetben kimondott szabályok itt is érvényesek. Ezeken túlmenően:

1. Az uralkodó joggyakorlat alapján munkaviszonyban a munkavállaló hozzájárulása nem lehet önkéntes, mert egyfajta egyensúlytalanság, hatalmi viszony áll fent a munkáltató javára.

2. Adatkezelés jogi kötelezettség teljesítése érdekében

Az Általános Adatkezelési Rendelet - GDPR „4. Adatkezelés jogi kötelezettség teljesítése érdekében” c. fejezetben kimondott szabályok itt is érvényesek. Ezeken túlmenően:

1. Az adatokat megismerő személyi kör: a munkáltatóra vonatkozóra vonatkozó jogi kötelezettség teljesítését végző belső és külső (GMK) szervezeti egység azon munkatársai, akik a konkrét feladatot végzik.
2. Adatkezelés munkaviszony létesítése, teljesítése és kapcsolódó nyilvántartási kötelezettségeknek való megfelelés érdekében történik.
 - 2.1. A munkavállalóktól kizárólag olyan személyes adatok szerezhetők be és tarthatók nyilván, amelyek munkaviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve az adó- és társadalombiztosítási kötelezettségek teljesítéséhez szükségesek, s a munkavállaló személyhez fűződő jogait nem sértik.
 - 2.2. A munkavállaló kezelt személyes adatainak körét az Intézmény mindenkor hatályos Adatkezelési és adatvédelmi szabályzata tartalmazza.
 - 2.3. A személyes adatok címzettjei: az adatkezelő munkáltató vezetője, munkáltatói jogkör gyakorlója, a munkaügyi feladatokat ellátó munkavállalói és adatfeldolgozói, így különösen az adatkezelő adózási, bérszámfejtési, társadalombiztosítási (kifizetői) tevékenységét ellátó munkavállalói, közreműködői és adatfeldolgozói.
 - 2.4. A személyes adatok tárolásának időtartama: a jogi kötelezettséget előíró jogszabályban meghatározott időtartam.
 - 2.5. Betegsége és szakszervezeti tagságára vonatkozó adatokat az adatkezelő munkáltató csak a Közalkalmazottak Jogállásáról szóló mindenkor hatályos törvény (továbbiakban: Kjt.) és a Munka Törvénykönyvben meghatározott jog, vagy kötelezettség teljesítése céljából kezel.
3. Munkavállalók munkahelyi alkalmassági vizsgálataival kapcsolatos adatkezelések

- 3.1. A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály, mint jogi kötelezettséget előíró szabály határoz meg, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.
- 3.2. A vizsgálat előtt munkáltató érthetően és részletesen tájékoztatja a munkavállalókat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik. Amennyiben nem jogszabály írja elő a vizsgálatot, úgy jogos érdek alapján történő adatkezelés lehetősége merülhet fel.
- Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor a munkáltató tájékoztatja a munkavállalókat a jogszabály címéről és a pontos jogszabályhelyről is.
- 3.3. A kezelhető személyes adatok köre: a munkaköri alkalmasság tényének vagy hiányának megállapítása.
- Nem kezelhető a munkáltató részéről semmilyen szakmai (orvosi, pszichológiai) tesztlapra, kérdéssorra adott válasz és az azokból levonható következtetés.
- 3.4. A személyes adatok kezelésének célja: munkaviszony létesítése, fenntartása, munkaköri feladat ellátása.
- 3.5. A személyes adatok címzettjei, illetve a címzettek kategóriái: Az alkalmassági vizsgálat eredményét a vizsgálatot érintett munkavállaló, illetve a vizsgálatot végző szakember ismerhetik meg. A munkáltató vezetője, munkáltatói jogkör gyakorlója számára csak az az információ adható át, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez.
- A fentiekben felüli vizsgálati eredményt, illetve annak részletes dokumentáltságát a munkáltató nem ismerheti meg.
- 3.6. A személyes adatok kezelésének időtartama: a munkaviszony fennállásának időtartama, illetve azon túl a munkaügyi követelések elévülési ideje, amennyiben a vizsgálatnak van vonatkozása a követeléshez. Ennek hiányában a munkaviszony fennálltának időtartamáig történhet az adatkezelés.
- 3.7. Adattárolás helye, módja: papír alapon a munkavállaló munkaügyi dossziéjában, illetve elektronikusan a munkáltató által használt szoftverek adatbázisaiban.

3. Adatkezelés munkáltatói „jogos érdek” alapján

1. A munkáltatónak a munkavállalóval fennálló munkaviszonya alatt, illetve azt megelőzően és azt követően is fűződhet érdeke személyes adatok kezeléséhez. Az esetek jelentős részében az adatkezelések jogalapja nem az egyébként kapcsolódó jogi kötelezettségek teljesítése, hanem az ún. munkáltatói jogos

érdeken alapuló adatkezelés, amelyekhez érdekmérlegelési teszt elvégzése szükséges.

2. Munkáltató az adatkezelés célját minden esetben világosan és egyértelműen határozza meg. A munkavállalóktól kért adatok köre, velük szemben alkalmazott vizsgálatok csak olyan esetekre vonatkozhat, amikor az lényeges tájékoztatást ad a munkaviszony létesítése, fenntartása, megszüntetése szempontjából.
3. Munkáltató kifejezetten figyel a szükségesség-arányosság elvére, az alkalmazott eszköz alkalmas az adatkezelési cél elérésére, csak szükséges mértékű adatkezeléssel jár, az ellenőrzés csak a munkavégzéssel összefüggésben történik. Munkáltató különösen figyel arra, hogy a munkavállalókat a munkahelyen is megilleti a magánélethez való jog, amelyeknek tipikus színterei: ebédlő, öltöző, pihenő- dohányzó helyiség, mosdók.
4. A munkáltatói ellenőrzések soha nem irányulnak a munkavállalók emberi méltóságának a sérelmére, így a munkavállalók megfélemlítésére, megalázására, zaklatására, zavarására.
5. A jogos érdek jogalap szerinti adatkezelések főbb esetei:
 - nem jogszabályi előírásen alapuló alkalmassági vizsgálatok, készség- és képesség felmerések,
 - álláspályázatokhoz kapcsolódó adatkezelések
 - munkáltatói e-mail fiók és cím használata
 - be- és kiléptető rendszerek adatkezelése
 - elektronikus megfigyelő rendszer által végzett adatkezelés
 - munkahelyi internet, wifi használata
 - munkáltatói laptop, számítógép használata
 - munkáltatói telefon használata

4. Álláspályázatokhoz kapcsolódó adatkezelések

1. Munkáltató álláspályázat meghirdetése esetén előzetes tájékoztatás keretén belül biztosítja saját adatkezelő voltának és elérhetőségének a megismerhetőségét. Az Adatkezelési tájékoztatót – Álláspályáztatás és munkaerő kiválasztáshoz az **1. sz. függelék** tartalmazza, amelyet az Intézmény honlapjára az Adatvédelem oldalra fel kell tölteni.
2. Munkáltató csak olyan személyes adatok megismerhetőségére tart igényt, amelyek lényegesek az adott munkakörrel kapcsolatban.

5. Munkáltatói e-mail cím és fiók használatához kapcsolódó adatkezelés

Fontos tisztázni, hogy az Intézmény saját működéséhez üzleti partnereket is vesz igénybe (pl: GMK végzi a gazdasági, működtetési, informatikai és közétkeztetési feladatokat – együttműködési megállapodás keretében). A közétkeztetés igénybeviteléhez a gyermekek, illetve szüleik az igénybevevők (továbbiakban: ügyfelek), akik pénzügyi és más egyéb szolgáltatási tevékenységeket hárítanak az Intézményre. Számos külső (továbbiakban: partner) cég végez az Intézmény

működéséhez szükséges beszállítói tevékenységet (pl: beszerzések-, közbeszerzések nyertesei , szerződött és megbízott partnerek, stb.), amelyek nem minden munkavállalója járult hozzá a személyes adatok nyilvánosságra hozatalához, ezért körültekintően kell eljárni.

1. Munkáltató partner kapcsolatainak személyes adatainak titokban tartása, illetve a munkavégzés ellenőrzése céljából ellenőrzi a munkavállalók munkáltató által biztosított e-mail fiókjának tartalmát, az abban végbemenő kimenő és beérkező adatforgalmat.
2. A munkáltató adatkezelés jogalapja: munkáltató jogos érdeke, s ez alapján munkáltató elvégezte az érdekmérlegelési tesztet, mely a munkavállalóval megismertetésre kerül.
3. Munkáltató tiltja az általa biztosított e-mail fiókban a magáncélú levelezést, azt a munkavállaló csak munkavégzésére használhatja fel.
4. Munkáltató külön felhívja a munkavállaló figyelmét, hogy amennyiben a tiltás ellenére is magáncélra is használja a munkavállaló az e-mail fiókot, úgy esetlegesen védett személyes adataihoz, vagy az abból származó következtetésekhez való hozzáférés kockázatának teszi ki magát. Az ellenőrzés során talált, nem a munkavégzéshez kapcsolódó e-mail törlésére a munkáltató felhívja a munkavállalót, aki a levél törlését haladéktalanul köteles elvégezni.
5. Munkáltató az ellenőrzés során betartja a fokozatosság elvét és lépcsőzetes ellenőrzési rendszert dolgozott ki. Az e-mail fiók tartalmáról biztonsági másolat nem készül.
6. Az e-mail fiók ellenőrzésének az első lépése: az e-mail címzettjének/küldőjének és a levél tárgyának az ellenőrzése. Amennyiben ennyiből megállapítható, hogy a levél tartalmának megnyitása személyes adathoz való hozzáférést eredményezhet, úgy munkáltató nem nyitja meg a levelet. Amennyiben nem valószínűsíthető a személyes adathoz való hozzáférés, úgy munkáltató jogosult az e-mailt megnyitni és áttanulmányozni, különös tekintettel a levél csatolmányaira. Amennyiben munkáltató mégis személyes adatra bukkan, úgy azt nem jogosult megismerni.
7. Munkáltató az e-mail fiók ellenőrzése során minden esetben biztosítja a munkavállaló jelenlétét, amennyiben ez mégsem lehetséges (pl. betegség, baleset, szabadság), úgy munkáltató képviselője csak tanú jelenlétében végzi el az ellenőrzést.
8. A munkáltató tájékoztatja a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról:
 - az ellenőrzés célja: (pl. annak ellenőrzése, hogy nem került-e ki személyes adat)
 - az ellenőrzést a munkáltató részéről végző jogosult személy: Intézményvezető, belső ellenőr, és az Intézményvezető által írásban ezzel megbízott személy.

- eljárási szabályok, lépések: munkavállaló tájékoztatása az ellenőrzésről, e-mail fiókba való munkavállalói belépés, ellenőrző személy szemrevételezi az e-mailek címzettjeit, tárgymezőket, egyeztetés munkavállalóval, hogy melyek a személyes adatokkal érintett levelek, ellenőrzési jegyzőkönyv megírása, aláírása)
 - munkavállaló tájékoztatása a jogorvoslati jogokról.
9. Munkáltató tájékoztatja a munkavállalót, hogy munkahelyi levelezés megfigyelése nem jogsértő munkáltató részéről, ebben a tárgyban az Emberi Jogok Európai Bíróságának is született ítélete.
10. Adatkezelés időtartama, címzettek, adatok tárolásának helye és módja: a munkáltatói tiltás szerint nem kerül sor személyes adatok kezelésére.

6. Munkavégzés helyére történő be- és kilépéssel kapcsolatos adatkezelés

1. Munkáltató az Intézményben lévő gyermekek védelme, illetve a munkavégzés ellenőrzése céljából szabályozza és ellenőrzi a munkavállalók be- és kilépését a munkáltatói ingatlanokba, a munkavégzés helyére.
2. A munkáltató adatkezelés jogalapja: munkáltató jogos érdeke, s ez alapján munkáltató elvégezte az érdekmérlegelési tesztet, mely a munkavállalóval megismertetésre kerül.
3. Munkáltató minden egyes munkakörre vonatkozóan szabályozza a munkakezdés- és befejezés időpontját, adott helyiségbe és területre való belépés jogát, tilalmát és ezek betartásának ellenőrzése kapcsán kezeli ezeket az adatokat.
4. Munkáltató az ellenőrzés során betartja a fokozatosság elvét és lépcsőzetes ellenőrzési rendszert dolgozott ki. A fenti adatokat tartalmazó adatbázisról biztonsági másolat nem készül.
5. Az adatok ellenőrzésének menete: a munkáltató a rendelkezésre álló adatokból szűrőpróbaszerűen ellenőrzi a szabályok betartását.
6. Munkáltató az ellenőrzés során minden esetben biztosítja a munkavállaló jelenlétét, amennyiben ez mégsem lehetséges (pl. betegség, baleset, szabadság), úgy munkáltató képviselője csak tanú jelenlétében végzi el az ellenőrzést.
7. A munkáltató tájékoztatja a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról:
 - az ellenőrzés célja: (pl. annak ellenőrzése, hogy a munkavállaló beérkezik-e a munkaidő megkezdésére)
 - az ellenőrzést a munkáltató részéről végző jogosult személy: Intézményvezető, belső ellenőr, és az Intézményvezető által írásban ezzel megbízott személy.

- eljárási szabályok, lépések: munkavállaló tájékoztatása ellenőrzésről, adatbázis megnyitása, ellenőrző személy szemrevételezi a kijelölt adatokat, tárgymezőket, egyeztetés munkavállalóval, ellenőrzési jegyzőkönyv megírása, aláírása)
- munkavállaló tájékoztatása a jogorvoslati jogokról.

8. Az adatkezelés időtartama: 2 hónap

9. Az adatkezeléssel érintett adatkör: munkahelyre történő be- és kilépések időpontja, adott helyiségekbe való be- és kilépés időpontjai.

10. Az adatok címzettjei: munkáltató munkaügyi ellenőrzési tevékenységét ellátó munkatársai.

11. Adattárolás helye, módja: papír alapon az ellenőrzési jegyzőkönyvekben, illetve elektronikusan a munkáltató által esetlegesen használt adott szoftver adatbázisában.

7. Munkahelyi elektronikus megfigyelő rendszer adatkezelése

1. Munkáltató személy- és vagyonvédelmi célból alkalmazhat kamerákat, ún. elektronikus megfigyelő rendszert. Az adatkezelésnek kizárólag ez a célja, nem a munkavállalók munkavégzésének általános ellenőrzése és a munkahelyi viselkedés befolyásolása.
2. Munkáltató nem alkalmaz kamerát, megfigyelést olyan helyiségben, ahol az az emberi méltóságot sértheti, így különösen öltözőkben, zuhanyzóknak, illemhelyiségekben, orvosi szobában, pihenőhelyen.
3. Munkáltató kizárólag a saját tulajdonában vagy használatában álló helyiségeket, épület részeket figyel meg, kamera látószöge közterületre nem irányul.
4. A kamerák alkalmazását, az elektronikus megfigyelő rendszerek által végzett személyes adatkezelést a mindenkor hatályos *Kamera adatkezelési szabályzat* tartalmazza, amely az Intézmény munkavállalói számára elérhetőek.

8. Munkáltatói internet és wifi használatával kapcsolatos adatkezelés

1. Munkáltató döntése alapján munkavállaló csak a munkavégzésével kapcsolatban használhatja a munkáltató által biztosított wifi hálózati elérést, illetve csak a munkavégzéssel kapcsolatos honlapok megtekintésére van lehetőség.
2. Munkáltató a munkaidőben történő magán célú internethasználatot tiltja.
3. Munkáltató nem rögzíti a munkavállaló által meglátogatott honlapok elérhetőségét és egyéb internet használatból levonható következtetéseket, de alkalomszerűen azonnali megtekintéssel ellenőrizheti, hogy a munkavállaló milyen honlapon tartózkodik.

4. Munkáltató az informatikai rendszerének védelme, vírusoktól és egyéb káros programoktól való védekezése és a munkavállaló munkavégzésének ellenőrzése céljából ellenőrzi a munkavállaló tevékenységét.
5. A munkáltató adatkezelés jogalapja: munkáltató jogos érdeke, s ez alapján munkáltató elvégezte az érdekmérlegelési tesztet, mely a munkavállalóval megismertetésre kerül.
6. Munkáltató külön felhívja a munkavállaló figyelmét, hogy amennyiben a tiltás ellenére magáncélra (is) használja a wifi hálózatot/internetet, úgy annak munkaügyi következményei lehetnek a munkavállaló számára, illetve munkáltató akaratán kívül hozzáférhet személyes adatokhoz.
7. Munkáltató az ellenőrzés során betartja a fokozatosság elvét és lépcsőzetes ellenőrzési rendszert dolgozott ki.
8. Az internet használat ellenőrzésének az első lépése: a munkavállaló által az ellenőrzés időpontjában aktuálisan megnyitott honlap megtekintése. Amennyiben ennyiből megállapítható, hogy a munkavállaló nem tiltott oldalt tekint meg, úgy az ellenőrzés le is zárult. Amennyiben nem valószínűsíthető a személyes adathoz való hozzáférés, úgy munkáltató folytathatja az ellenőrzést.
9. Munkáltató az internet használat ellenőrzése során minden esetben biztosítja a munkavállaló jelenlétét, illetve az ellenőrzés a munkavállaló jelenléte nélkül eleve kizárt.
10. A munkáltató tájékoztatja a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról:
 - az ellenőrzés célja: (pl. annak ellenőrzése, hogy nincs-e tiltott oldal megtekintés)
 - az ellenőrzést a munkáltató részéről végző jogosult személy: Intézményvezető, belső ellenőr, és az Intézményvezető által írásban ezzel megbízott személy.
 - eljárási szabályok, lépések: munkavállaló tájékoztatása ellenőrzésről, monitor megtekintése, egyeztetés munkavállalóval, hogy szükséges-e a munkájához a megtekintés alatt álló weboldal, ellenőrzési jegyzőkönyv megírása, aláírása)
 - munkavállaló tájékoztatása a jogorvoslati jogokról.
11. Adatkezelés időtartama, címzettek, adatok tárolásának helye és módja: a munkáltatói tiltás szerint nem kerül sor személyes adatok kezelésére.

9. Munkáltatói számítógép, laptop, tablet használatával kapcsolatos adatkezelés

1. Munkáltató a munkavégzés ellenőrzése céljából ellenőrzi a munkavállalók munkáltató által biztosított lapon, számítógépen, tableten folytatott munkavállalói tevékenységeket, az eszköz memóriáját, az eszközre és a hozzá csatlakoztatott eszközre vonatkozó biztonsági előírások betartását.

2. A munkáltató adatkezelés jogalapja: munkáltató jogos érdeke, s ez alapján munkáltató elvégezte az érdekmérlegelési tesztet, mely a munkavállalóval megismertetésre kerül.
3. Munkáltató tiltja az általa biztosított eszközökön a magánélethez kapcsolódó tevékenységek végzését, személyes adatok kezelését, tárolását. Az eszközöket a munkavállaló csak munkavégzésére használhatja fel.
4. Munkáltató külön felhívja a munkavállaló figyelmét, hogy amennyiben a tiltás ellenére is magáncélra is használja a munkavállaló a biztosított technikai eszközöket, úgy esetlegesen védett személyes adataihoz, vagy az abból származó következtetésekhez való hozzáférés kockázatának teszi ki magát. Az ellenőrzés során talált, nem a munkavégzéshez kapcsolódó személyes adatok, magán tartalmak törlésére a munkáltató felhívja a munkavállalót, aki az adott tartalmak törlését haladéktalanul köteles elvégezni.
5. Munkáltató az ellenőrzés során betartja a fokozatosság elvét és lépcsőzetes ellenőrzési rendszert dolgozott ki. Az eszközökön tárolt adatokról, információkról biztonsági másolat nem készül.
6. A számítástechnikai eszköz ellenőrzésének az első lépése: az adott fájl, információ ellenőrzése. Amennyiben ennyiből megállapítható, hogy ez a munkáltatói tevékenység személyes adathoz való hozzáférést eredményezhet, úgy munkáltató nem tekinti meg, illetve nem nyitja meg az adott fájlt, leírást, információ egységet. Amennyiben nem valószínűsíthető a személyes adathoz való hozzáférés, úgy munkáltató jogosult az adott információ egység, adat megtekintésére, áttanulmányozására.
7. Munkáltató a technikai eszköz ellenőrzése során minden esetben biztosítja a munkavállaló jelenlét, amennyiben ez mégsem lehetséges (pl. betegség, baleset, szabadság), úgy munkáltató képviselője csak tanú jelenlétében végzi el az ellenőrzést.
8. A munkáltató tájékoztatja a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról:
 - az ellenőrzés célja: (pl. annak ellenőrzése, hogy sérül-e az adatbiztonság)
 - az ellenőrzést a munkáltató részéről végző jogosult személy: Intézményvezető, belső ellenőr, és az Intézményvezető által írásban ezzel megbízott személy.
 - eljárási szabályok, lépések: munkavállaló tájékoztatása ellenőrzésről, a technikai eszközbe való belépés, ellenőrző személy szemrevételezi a fájlokat, információ egységeket, egyeztetés munkavállalóval, hogy melyek a személyes adatokkal érintett fájlok, információs egységek, ellenőrzési jegyzőkönyv megírása, aláírása)
 - munkavállaló tájékoztatása a jogorvoslati jogokról.
9. Adatkezelés időtartama, címzettek, adatok tárolásának helye és módja: a munkáltatói tiltás szerint nem kerül sor személyes adatok kezelésére.

10. Munkáltató által biztosított mobiltelefon használatának ellenőrzésével kapcsolatos adatkezelés

1. Munkáltató a munkavégzés ellenőrzése céljából ellenőrzi a munkavállalók munkáltató által biztosított telefonon folytatott munkavállalói tevékenységeket, az eszköz memóriáját, az eszközre és a hozzá csatlakoztatott eszközre vonatkozó biztonsági előírások betartását.
2. A munkáltató adatkezelés jogalapja: munkáltató jogos érdeke, s ez alapján munkáltató elvégezte az érdekmérlegelési tesztet, mely a munkavállalóval megismertetésre kerül.
3. Munkáltató tiltja az általa biztosított telefon eszközökön a magánélethez kapcsolódó tevékenységek végzését, személyes adatok tárolását. Az eszközöket a munkavállaló csak munkavégzésére használhatja fel.
4. Munkáltató külön felhívja a munkavállaló figyelmét, hogy amennyiben a tiltás ellenére is magáncélra is használja a munkavállaló a biztosított telefon eszközt, úgy esetlegesen védett személyes adataihoz, vagy az abból származó következtetésekhez való hozzáférés kockázatának teszi ki magát. Az ellenőrzés során talált, nem a munkavégzéshez kapcsolódó személyes adatok, magán tartalmak törlésére a munkáltató felhívja a munkavállalót, aki az adatott tartalmak törlését haladéktalanul köteles elvégezni.
5. Munkáltató az ellenőrzés során betartja a fokozatosság elvét és lépcsőzetes ellenőrzési rendszert dolgozott ki. Az eszközökön tárolt adatokról, információkról biztonsági másolat nem készül.
6. A telefon eszköz ellenőrzésének az első lépése: az adott fájl, információ ellenőrzése. Amennyiben ennyiből megállapítható, hogy ez a munkáltatói tevékenység személyes adathoz való hozzáférést eredményezhet, úgy munkáltató nem tekinti meg, illetve nem nyitja meg az adott fájlt, leírást, információ egységet. Amennyiben nem valószínűsíthető a személyes adathoz való hozzáférés, úgy munkáltató jogosult az adott információ egység, adat megtekintésére, áttanulmányozására.
7. Munkáltató a telefon eszköz ellenőrzése során minden esetben biztosítja a munkavállaló jelenlét, amennyiben ez mégsem lehetséges (pl. betegség, baleset, szabadság), úgy munkáltató képviselője csak tanú jelenlétében végzi el az ellenőrzést.
8. A munkáltató tájékoztatja a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról:
 - az ellenőrzés célja: (pl. annak ellenőrzése, hogy sérül-e az adatbiztonság)
 - az ellenőrzést a munkáltató részéről végző jogosult személy: Intézményvezető, belső ellenőr, és az Intézményvezető által írásban ezzel megbízott személy.
 - eljárási szabályok, lépések: munkavállaló tájékoztatása ellenőrzésről, a telefon eszközbe való belépés, ellenőrző személy szemrevételezi a fájlokat, információ egységeket, egyeztetés munkavállalóval, hogy melyek a

személyes adatokkal érintett fájlok, információs egységek, ellenőrzési jegyzőkönyv megírása, aláírása)

- munkavállaló tájékoztatása a jogorvoslati jogokról.

9. Adatkezelés időtartama, címzettek, adatok tárolásának helye és módja: a munkáltatói tiltás szerint nem kerül sor személyes adatok kezelésére.

11. Munkáltató által biztosított telefon, autó és egyéb eszköz gps adatainak (földrajzi helyzetének) kezelése

1. Munkáltató az általa biztosított eszköz biztonsága, fellelhetősége, vagyonvédelme, illetve a munkavégzés ellenőrzése, munkahatékonyság növelése céljából ellenőrizheti a munkavállalók munkáltató által biztosított eszköz által sugárzott cellainformáció, jel, GPS koordináta földrajzi adatát.

Munkáltató a jelen szabályzat hatályba lépésének napjáig ilyen ellenőrzési tevékenységet nem alakított ki.

2. A munkáltatói adatkezelés jogalapja: munkáltató jogos érdeke, és ez alapján munkáltató elvégezte az érdekmérlegelési tesztet, mely a munkavállalóval megismertetésre kerül.

3. Munkáltató csak a munkaidőben végez ellenőrzést, a magánszféra, emberi méltóság fokozott figyelembe vételével. A munkavállaló részére fizikai lehetőség van az azonosítás kikapcsolására munkaidőn kívüli időtartamra.

4. Munkáltató az ellenőrzés során betartja a fokozatosság elvét és lépcsőzetes ellenőrzési rendszert dolgozott ki. Az eszközökön tárolt adatokról, információkról biztonsági másolat nem készül.

5. Az ellenőrzés első lépése: az adott fájl, információ ellenőrzése. Amennyiben ennyiből megállapítható, hogy ez a munkáltatói tevékenység személyes adathoz való hozzáférést eredményezhet, úgy munkáltató nem tekinti meg, illetve nem nyitja meg az adott fájlt, leírást, információ egységet. Amennyiben nem valószínűsíthető a személyes adathoz való hozzáférés, úgy munkáltató jogosult az adott információ egység, adat megtekintésére, áttanulmányozására.

6. Munkáltató a technikai eszköz ellenőrzése során minden esetben biztosítja a munkavállaló jelenlétét, amennyiben ez mégsem lehetséges (pl. betegség, baleset, szabadság), úgy munkáltató képviselője csak tanú jelenlétében végzi el az ellenőrzést.

7. A munkáltató tájékoztatja a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról:

- az ellenőrzés célja: (pl. annak ellenőrzése, hogy munkaidőben munkavégzés történik-e)
- az ellenőrzést a munkáltató részéről végző jogosult személy: Intézményvezető, belső ellenőr, és az Intézményvezető által írásban ezzel megbízott személy.

- eljárási szabályok, lépések: munkavállaló tájékoztatása ellenőrzésről, az ellenőrzött információhoz való hozzáférés, ellenőrző személy szemrevételezi a fájlokat, információ egységeket, egyeztetés munkavállalóval, hogy melyek a személyes adatokkal érintett fájlok, információs egységek, ellenőrzési jegyzőkönyv megírása, aláírása)
 - munkavállaló tájékoztatása a jogorvoslati jogokról.
8. Adatkezelés időtartama, címzettek, adatok tárolásának helye és módja: a munkáltató jelen szabályzat hatályba lépésekor ilyen adatkezelést nem végez.

12. Alkalmassági vizsgálatokhoz kapcsolódó adatkezelés

1. Munkáltató munkavállalóval szemben alkalmazhat munkaviszonyra vonatkozó szabály, így különösen a Munka Törvénykönyve által előírt alkalmassági vizsgálatokat, illetve lehetőség van olyan alkalmassági és egyéb vizsgálatok elvégzésére, amelyet nem munkaviszonyra vonatkozó szabály ír elő, de munkaviszonyban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.
2. Munkáltató mindkét esetben részletesen tájékoztatja a munkavállalót arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel és módszerrel történik, illetve arról, hogy azt jogszabály írja-e elő, s melyik jogszabály.
3. A munkaalkalmasságra, a munkaköri feladat ellátásának való megfelelésre, felkészültség ellenőrzésére irányuló vizsgálatokat, kérdősorokat, teszteket a munkáltató mind a munkaviszony létesítése előtt, mind pedig a munkaviszony fennállása alatt alkalmazhat.
4. A kizárólag munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében csak akkor alkalmazható a munkavállaló pszichológiai állapotának vagy személyiségjegyének elemzésére alkalmas tesztlap, ha az nem egyedileg egy munkavállalóra vonatkozik, hanem a munkavállalók egy csoportjára, s ha az elemzés során megállapításra került adatok nem köthetők az egyes konkrét munkavállalóhoz, tehát hiányzik a személyes adat fogalmának alapvető eleme: a beazonosíthatóság.
5. A kezelhető személyes adatok köre: a munkaköri alkalmasság ténye vagy hiánya és az ehhez szükséges feltételek. A vizsgálat eredményét a vizsgálatot végző szakember és az érintett munkavállaló ismerheti meg. A munkáltató számára csak az ismerhető meg, hogy a vizsgált személy az adott munkára alkalmas-e vagy nem.
6. Munkáltató a munkaviszony létesítése előtt és fennállása alatt kérheti a munkavállalótól /álláspályázótól/ feddhetetlen előéletének az igazolását, mely célra az ún. Erkölcsi Bizonyítvány bemutatása szolgál. Fentieken túl munkáltató semmilyen körülmények nem kéri, hogy az érintettek hatósági erkölcsi bizonyítvány helyett bünyügyi nyilvántartó szervtől szerezzenek be nemleges igazolást.

7. Adatkezelés időtartama, címzettek, adatok tárolásának helye és módja: a munkáltató jelen szabályzat hatálybalépésének napján nem alkalmaz alkalmassági vizsgálatokat.

VII. MUNKAVÁLLALÓI ADATBIZTONSÁGI SZABÁLYOK

1. Biztonságra törekvő viselkedés a munkahelyen

- 1) Személyes adatokat tartalmazó dokumentumok, iratok nem hagyhatók felügyelet nélkül az asztalon.
- 2) Munkavégzés során (lehetőleg) csak azok az iratok, illetve dokumentumok lehetnek elől az asztalon, amelyek az adott munka végzéséhez akkor szükségesek.
- 3) Munkavégzés után minden személyes adatot tartalmazó dokumentumot, iratot és elektronikus adathordozót el kell tenni az asztalokról, és zárt, biztonságos helyen kell tárolni.
- 4) A zárható íróasztalokat és szekrényeket is (amennyiben kulcsra zárhatóak) kulcsra zárva kell tartani, és a kulcsokat biztonságos helyen kell őrizni.
- 5) Megbeszélések után a tanácskozóteremből (tárgyalóból) minden bizalmas tartalmú dokumentumot, különösen a személyes adatokat tartalmazó iratokat, papírokat, jegyzeteket el kell távolítani. (Ide beleértendők a használt flip-chart papírok eltávolítása, táblák letörlése, stb.)
- 6) Személyes adatokat tartalmazó dokumentumok, iratok másolásakor sem eredeti példány, sem másolat nem maradhat a másolóban.
- 7) Személyes adatokat tartalmazó dokumentumok, iratok csak olyan személyeknek adhatók át, akik munkaköri feladatuknál fogva vagy jogszabályi előírásnak megfelelően jogosultak azoknak az információnak a megismerésére vagy használatára, és az átadó személy erről meggyőződött.
- 8) Elektronikus átviteli út (pl. telefon, fax, e-mail) esetén a bizalmas információkat ajánlott, az üzleti titoknak minősített információkat kötelező titkosítva átvinni.
- 9) Amennyiben a személyes adatokat tartalmazó dokumentumok, iratok őrzésére, tárolása már nincs szükség, azokat papírdarálással kell megsemmisíteni, vagy biztonságos gyűjtés, tárolás után eljuttatni a szabályozásnak megfelelő, felügyelt megsemmisítésre.
- 10) A személyes adatokat tartalmazó kézi feljegyzéseket, munkapéldányokat, másolati példányokat, stb. ugyanolyan biztonsággal kell kezelni, mint az azokat az információkat tartalmazó eredeti, hivatalos iratokat.

2. Számítógépes munkahely biztonságos használata

- 1) Minden felhasználó köteles az általa használt számítógépet rendeltetésének megfelelően, kizárólag munkájának végzésére, illetve támogatására használni.
- 2) Minden felhasználó köteles az esetleges meghibásodásokat azonnal jelezni az üzemeltetést végző GMK rendszergazdájának.
- 3) TILOS a számítógép (vagy egyéb informatikai eszköz) burkolatát megbontani, az eszköz belső részéhez hozzáférni, azon változtatásokat végezni. A garancia címke nem sérülhet meg!

- 4) TILOS a telepített (nem hordozható) számítógépet (vagy egyéb informatikai eszközt) a rendszergazda értesítése nélkül más munkahelyre áttelepíteni.
- 5) A felhasználó nem változtathatja meg a használatába kapott számítógép (vagy egyéb informatikai eszközök) konfigurációját. A perifériák cseréjét, a szoftverek telepítését csak a rendszergazda végezheti.
- 6) TILOS külső bootolást (számítógép külső egységről vagy perifériáról történő indítását) alkalmazni.
- 7) A felhasználó számítógépét csak saját azonosítójával és jelszavával belépve használhatja. A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett TILOS más azonosítójának használata.
- 8) A felhasználó a számítógépeken csak azokat a szoftvereket használhatja, amelyeket a rendszergazda a munkája elvégzéséhez telepített.
- 9) A felhasználó a számítógépére semmilyen szoftvert nem telepíthet, nem törölhet, és nem módosíthat. E rendelkezés megszegéséért a felhasználó ellen felelősségre vonás kezdeményezhető.
- 10) A felhasználó semmilyen olyan szoftvert, amit nem a rendszergazda telepített, nem futtathat a számítógépén. (Ebbe beleértendő a telepítést nem igénylő, külső eszközről – pl. CD/DVD-ROM, USB Flash drive, stb. – indítható programok, valamint a freeware, shareware szoftverek, illetve bármilyen nem az Intézmény tulajdonát képező szoftverek is.)
- 11) A számítógépes asztalon minél kevesebb alkalmazás, dokumentum legyen egyidejűleg megnyitva, lehetőleg csak azok, amelyek az adott munka végzéséhez akkor szükségesek.
- 12) Rövidebb idejű távollét esetén a számítógépet legalább zárolni kell.
- 13) Hosszabb idejű távollét esetén ki kell jelentkezni az alkalmazásokból, és a számítógépet ki kell kapcsolni.

3. Hordozható számítógépek biztonságos használata

- 1) A hordozható számítógépek biztonságos használatára érvényesek a számítógépek biztonságos használatára, az előző fejezetben előírt minden szabály.
- 2) A hordozható számítógépet extrém hőmérséklet, mágneses tér, magas páratartalom vagy erős füstképződés hatásának kitenni TILOS.
- 3) A számítógépeket működő állapotban szállítani nem szabad. (Ez nem vonatkozik az utazás közbeni használatra.)
- 4) Esetleges repülőutak alkalmával hordozható számítógép kézipoggyászként szállítandó. Lehetőség szerint el kell kerülni a röntgenkészülékkel történő vizsgálatot.

3.1. Adatbiztonsági szabályok

- 1) Személyes adatok csak titkosítva tárolhatók a hordozható számítógépeken.
- 2) A hordozható számítógépen lokálisan tárolt adatok rendszeres mentéséről a felhasználó maga köteles gondoskodni. A mentéseknek az adathordozón titkosítva kell tárolni, és az adathordozókat biztonságosan kell tárolni.

- 3) A külső munkahelyen történő feladat elvégzése után a hordozható számítógépeken keletkezett vagy tárolt adatokat a megfelelő (ha van) hálózati fájlszerverekre kell menteni, és ezt követően a hordozható számítógépről le kell őket törölni.

3.2. Jogosulatlanok általi, információhoz való hozzáférések megakadályozása

- 1) Esetleges bel- és külföldi kiküldetésre vitt (munkahelyi és otthoni használaton kívül) utazó kollégák notebookjainak titkosítását el kell végezni, ennek alkalmazásáért a felhasználó felelős.
- 2) A hordozható számítógépet csak a rendszergazda által beállított felhasználója, a saját bejelentkezésével és jelszavával, a munkavégzés céljára használhatja.
- 3) TILOS a hordozható számítógépet más célra használni, illetve másoknak (pl. családtagoknak, barátoknak, stb.) használatra átengedni.
- 4) Különösen ott kell a használatot követően a tárolt adatok törlésére odafigyelni, ahol a hordozható számítógépet megosztva használják.
- 5) Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát.
- 6) A hordozható számítógép rövid idejű elhagyásakor is azonnal zárolni kell a számítógépet, ezzel megakadályozva azt, hogy kívülállók betekinthesse a rendszerbe.
- 7) A rendszergazda által beállított jelszavas képernyővédő törlése vagy várakozási idejének megváltoztatása TILOS.

3.3. Hordozható számítógépek fokozott vírusveszélye kockázatainak csökkentése

- 1) A rendszergazda által telepített központi vírusvédelmi rendszer használata kötelező, az automatikus beállítást megváltoztatni TILOS.
- 2) Az idegen külső adathordozók (pl. optikai adathordozók, külső merevlemezek, flash drive-ok) vírusmentességét felhasználásuk előtt kötelező megvizsgálni.
- 3) A hordozható számítógép külső hálózatra kapcsolódását (pl. szállodákban, vásárokon, beszállítóknál, otthon) követő használata előtt soron kívüli, teljes gépre vonatkozó vírusellenőrzést kötelező végrehajtani.

3.4. Intézkedések, ha a hordozható számítógépet már ellopták, vagy elveszítették

- 1) Az ellopás, elvesztés tényét a lehető leggyorsabban jelenteni kell a GMK rendszergazdának (informatika@gmkxv.hu).
- 2) Tájékoztatni kell a közvetlen felettes vezetőt arról (előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve), hogy a berendezés tartalmaz-e bármilyen személyes adatot vagy az Intézmény rendszereihez távoli hozzáférési lehetőséget.

- 3) Ha a számítógépet külső helyszínről lopták el értesíteni kell a külső helyszínen vezetőjét.
- 4) Lopás esetén rendőrségi jegyzőkönyvet kell felvetetni.
- 5) Hordozható számítógép ellopása esetén, hogyha az személyes adatot is tartalmazott, azt személyes adatvédelmi incidensnek kell minősíteni, és az annak megfelelő eljárást a mindenkor hatályos Adatvédelmi incidenskezelési szabályzatban foglalt eljárásnak megfelelően, azonnal el kell indítani (adatvedelem@ujpalotaiiovi.hu).

4. Mobil informatikai adathordozók biztonságos használata

- 1) Munkavégzés céljaira csak a rendszergazda által kapott, céges adathordozó használható.
- 2) Az adathordozókat azok feldolgozása és tárolása alatt úgy kell kezelni, hogy biztosítva legyenek elvesztés, megsemmisülés, megsérülés és elcserélés, valamint jogosulatlan hozzáférés ellen.
- 3) Gondosan és elzárva kell a használaton kívüli adathordozókat is tárolni.
- 4) Azokat a mobil adathordozókat, amelyeket privát számítógéppel történő adatcserére használtak, újrafelhasználás előtt újra kell formázni.
- 5) A személyes adatokról készült másolatok érzékenysége – és adatvédelmi igénye – megegyezik az eredeti személyes adat érzékenységével, ezért ugyanúgy kell védeni a másolatokat is.
- 6) Személyes adatot tartalmazó elektronikus adathordozókat egyidejűleg más célra felhasználni TILOS.
- 7) Személyes adatok titkosított tárolása hordozható elektronikus adattárolón ajánlott, amennyiben a hordozható adathordozón a személyes adatok az intézmény telephelyein kívüli szállítása vagy átadása szükséges, akkor viszont minden esetben kötelező.
- 8) A hordozható adathordozókon lévő adatok illetéktelenek általi hozzáféréseért a felhasználó a felelős.
- 9) Személyes adatot tartalmazó, meghibásodott háttértár egységet (merevlemezt) akár garanciális javítás keretében lecserélni, vagy bármely formában kiadni TILOS. (Ez vonatkozik a hálózati merevlemezes nyomtatók és multifunkcionális berendezések merevlemezeire is.)
- 10) Selejtezésre kijelölt, személyes adatokat tartalmazó elektronikus adathordozókat kidobni TILOS. Azt minden esetben dokumentált megsemmisítési eljárással, bizottság előtt kell selejtezni.

5. Az intézmény informatikai hálózatának (ha van) biztonságos használata

- 1) A hálózaton csak a rendszergazda által biztosított és üzemeltetett informatikai eszközök lehetnek.
- 2) Számítógép-hálózati kábel szomszédos helyiségekbe történő áthúzása TILOS!
- 3) A hálózatba a felhasználók csak a saját belépési azonosítójukat használva jelentkeznek be.

- 4) TILOS a saját azonosító és jelszó átadása másnak.
- 5) A rendszergazda által biztosított eszközöket az intézményi hálózatra csatlakoztatás során egy másik, lokális (vezetékes vagy vezeték nélküli) hálózatra kötve megosztani SZIGORÚAN TILOS!
- 6) Az informatikai rendszer használata otthonról csak korlátozottan, felső vezetői engedéllyel, biztonságos VPN csatornán keresztül bejelentkezéssel engedélyezhető.
- 7) Az informatika rendszerek távoli eléréssel történő használata során a rendszergazda által beállított biztonsági eljárások, eszközök és beállítások (pl. titkosított csatorna, VPN, stb.) használata kötelező.

6. Jelszó használati szabályok

6.1. A jelszó képzése

- 1) A jelszónak olyannak kell lennie, hogy tulajdonosa könnyen megjegyezhesse, de a kívülállók nehezen találhassák ki.
- 2) Egy jelszónak, ha az technikailag lehetséges, minimum 8 karakterből kell állnia, nagy és kisbetűket, számokat kell tartalmaznia.
- 3) A korábban már alkalmazott jelszavakat nem szabad többször felhasználni.
- 4) Különböző rendszerekhez történő belépésekre különböző jelszavakat kell használni.

6.2. A jelszavak cseréje

A jelszót a következő esetekben mindig azonnal meg kell változtatni:

- 1) A jelszó tudatos továbbadása esetén, amennyiben az ok már nem áll fenn (pl. karbantartási munkák).
- 2) Minden olyan esetben, amikor fennáll a gyanúja annak, hogy ismertté vált.
- 3) A rendszerrel együtt kiszállított, előre beállított jelszavakat az üzembeállítás követően azonnal.
- 4) Minden egyéb esetben a javasolt jelszavakat rendszeresen cserélni szükséges.

6.3. A jelszó titokban tartása

A felhasználónak titokban kell tartani jelszavait.

- 1) A jelszavakat még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik egymással.
- 2) A feltétlenül szükséges jelszó-feljegyzések csak úgy tárolhatók, hogy ahhoz csak és kizárólag maga a felhasználó férhet hozzá személyesen.
- 3) A jelszó-feljegyzések tárolására nem használhatók az ún. szabadon rendelkezésre álló „emlékezet-segítők”, mint pl. felragasztva monitorra, billentyűzet alá, stb.

- 4) Jelszavak nem tárolhatóak olvasható formátumú fájlokban (pl. txt, doc, xls, stb. fájl).
- 5) A jelszavakat és azonosítókat tartalmazó üzeneteket nem szabad üzenetrögzítőn megadni, FAX készülékkel, vagy nem titkosított csatornán elküldeni.
- 6) A jelszavak bevitelénél ügyelni kell arra, hogy azt begépelés közben mások ne olvashassák el, ne leshessék ki.

6.4. Különleges szabályok helyettesítések/vészhelyzetek esetére

- 1) Kivételes esetekben (pl. a jelszó elvesztése, elfelejtése esetén) a rendszergazdától, a megfelelő személyi azonosítás után egy új jelszó igényelhető. Az új jelszót a belépést követően azonnal le kell cserélni, erre a rendszer automatikusan felszólít.
- 2) Helyettesítés és távollét esetén az érintett helyettesítő személy rendszerbeli meghatalmazása, és ezen keresztül számára – a helyettesítés időtartamára – a szükséges jogosultságok központi (rendszergazda általi) beállítása a helyes, hivatalos eljárás.

7. Munkahelyi elektronikus levelezés biztonságos használata

- 1) Az Intézmény az elektronikus levelezési szolgáltatást (e-mailt) csak és kizárólag munkavégzés céljából, a munkaköri feladatok hatékonyabb ellátásának érdekében biztosítja. A szolgáltatást magán célra és egyéb, a munkavégzéssel nem összefüggő célokra használni TILOS.
- 2) Az elektronikus levelezés használati engedélye személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe.
- 3) A felhasználó saját azonosítójának és jelszavának átadása más felhasználók részére TILOS.
- 4) Helyettesítés és távollét esetén a levelezés továbbításának szabálya beállítható, a válaszlevelek küldése esetében az érintett helyettesítő személy rendszerbeli meghatalmazása a helyes, hivatalos eljárás.
- 5) TILOS a munkahelyi e-mail címmel magánjellegű regisztrációt tenni (pl. közösségi oldalak).
- 6) Az ingyenes levelezőrendszerek (pl. freemail.hu) munkahelyi célú használata TILOS.
- 7) Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

7.1. E-mailek küldésére vonatkozó irányelvek

- 1) A feladó, mint tulajdonos felelős az e-mail tartalmáért.
- 2) TILOS más nevében e-mailt küldeni, kivéve meghatalmazottak (pl. titkárnő) esetében.
- 3) A leveleket mindig célzottan kell kiküldeni, sosem szükségtelenül nagy elosztási kör számára.
- 4) Nagy adatmennyiségeket lehetőleg csak tömörített formátumú csatolmányként szabad küldeni.

- 5) Személyes adatokat tartalmazó dokumentumok e-mail-en keresztül csak titkosított formában küldhetők.
- 6) Zavaró, félreinformáló levelek küldése, jogtalan megrendelések elindítása TILOS és eljárást vonhat maga után.

7.2. Az e-mailek fogadására vonatkozó irányelvek

- 1) A címzett felelős az e-mail tovább-feldolgozásáért és továbbításáért.
- 2) Bizalmas információk (pl. különlegesen személyes adatok) továbbítását kérő elektronikus levelek esetében mindig meg kell győződni az információkérés hitelességéről.
- 3) Ismeretlen helyről származó e-mail-t (pl. a feladó ismeretlen, vagy a feladó e-mail gyanús) megnyitás nélkül, olvasatlanul törölni kell.
- 4) Külső vagy belső e-mail címről érkező, félrevezető tartalmú e-mail-ek esetén azonnal értesíteni kell a rendszergazdát.
- 5) A kapott e-mail mellékleteket először számítógépes víruskeresővel kell átvizsgálni, amennyiben azok pl. futtatható programokat tartalmaznak.

8. Munkahelyi internet biztonságos használata

- 1) Az Intézmény az Internet használatot munkavégzés céljából, a munkaköri feladatok hatékonyabb ellátásának érdekében biztosítja.
- 2) Az Internet használati engedély személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe.
- 3) Az Internetes oldalak elérése monitorozásra és naplózásra kerülhetnek, a munkával összefüggésbe nem hozható oldalak elérhetőségét a rendszergazda biztonsági okból jogosult korlátozni.
- 4) Egyértelműen munkához nem köthető témájú Internetes oldalak látogatása TILOS, különösen ha látogatásuk jogi következményekkel járó – akár BTK-ba ütköző – tevékenységet jelenthet. (Pl. szexuális és pornográf tartalmú oldalak, torrent oldalak, rasszizmust, gyűlöletet, erőszakot népszerűsítő oldalak, stb.)

9. Vírusvédelmi szabályok

9.1. A központi vírusvédelmi szoftver alkalmazására vonatkozó szabályok

- 1) A rendszergazda által telepített vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.
- 2) A felhasználó nem akadályozhatja a vírusvédelmi program és részeinek folyamatos futását.
- 3) A felhasználónak kötelessége jelenteni a rendszergazdának, ha észleli, hogy a gépén a vírusvédelmi szoftver nem működik folyamatosan.
- 4) A hordozható számítógépek esetében a vírusminta frissítésről való gondoskodás a felhasználó kötelessége.
- 5) A számítógépen idegen adathordozót csak vírusvizsgálat után lehet használatba venni.

- 6) Aki az adatait és adathordozóit rendszeres vírus ellenőrzés vagy vírusvédelmi intézkedés (vírusirtás) alól kivonja, felelősségre vonható, illetve az abból eredő károkért felel.
- 7) Office dokumentumok esetében kerülni kell a makrók és aktív tartalmak megnyitását, külső forrásból érkező dokumentum esetében pedig nem szabad engedélyezni a makrókat.

9.2. Teendők vírusfertőzés gyanúja vagy biztos felismerése esetén

- 1) Ha a felhasználó gépén vírus jelenlétére utaló működési zavarok jelentkeznek,– ezt a vírusvédelmi program akár jelzi, akár nem,– a következő lépéseket kell tenni:
 - Ne használja tovább a vírusos vagy vírusgyanús rendszert.
 - Ne változtassa meg a rendszer-állapotot.
 - Azonnal jelentse az esetet a rendszergazdának, és tartsa be annak utasításait.
- 2) A rendszergazda jogosult a vírusveszély elhárításáig a vírusos számítógépet a hálózatról leválasztani, azon a munkavégzést megtiltani.

VIII. IT ÜZEMELTETÉS ADATVÉDELMI SZABÁLYOK

1. Az IT szabályok használata

Jelen adatbiztonsági szabályok azokat az általános informatikai biztonsági jellegű alapelveket foglalják össze, amelyek figyelembe vétele és betartása minimálisan szükségesek az Intézmény informatikai infrastruktúra üzemeltetése során, hogy a személyes adatok kellő adatbiztonsága biztosítható legyen.

Jelen adatbiztonsági szabályok az informatikai biztonság egyes területein csak a betartandó alapelveket mondják ki. Azok konkrét megvalósítása mindig a pillanatnyi konkrét IT infrastruktúra és üzemeltetési mód függvénye, ami többféleképp is megvalósítható. Az itt (ebben a szabályzatban) leírt alapelvek konkrét megvalósítást a rendszergazdának (Külső IT üzemeltető) a saját belső, végrehajtási előírásai kell, hogy tartalmazzák, és azok alapján kell azokat betartaniuk.

Jelen adatbiztonsági szabályok betartása csupán az általános, informatikai biztonsági gyakorlatnak megfelelő alapszintű biztonságot garantálja, egyes rendszerek nagyobb kockázata esetén azon rendszerekhez kockázati kitettség alapon egyedi, szigorúbb biztonsági intézkedések vezethetők / vezetendők be.

2. A fizikai elhelyezés és az üzemeltetés fizikai biztonsága

1. Az informatikai rendszer központi kiszolgáló elemeit (hálózati eszközök, szerver számítógépek, telekommunikációs eszközök) elkülönített, ellenőrizhető, zárt, a fizikai hozzáférést szabályozott szerverszobában kell elhelyezni. A külső szolgáltatónál működő szerverszoba esetén, a külső IT szolgáltató saját belső biztonsági előírásai az irányadók.
2. Az informatikai hálózat szerverszobán kívül elhelyezkedő hálózati elemeit (pl. switchek, routerek, hubok, AP-ok) úgy kell elhelyezni, hogy lehetőleg elzártak és nehezen hozzáférhetőek legyenek, védeni kell minden illetéktelen hozzáféréstől.
3. Személyes adatokat is tartalmazó informatikai eszközök, rendszerek karbantartását csak a rendszergazda, vagy szükség esetén a rendszergazda felügyelete mellett megfelelő szakszerviz munkatársai végezhetik, akikre a karbantartási szerződés érvényes és a Titoktartási nyilatkozatot aláírták.
4. Régi vagy meghibásodott elektronikus adathordozókat, – amelyek személyes adatokat is tartalmaz(hat)nak – kidobni, cserére átadni nem szabad, azokat fizikailag kell használhatatlanná tenni.

3. Jogosultságok menedzselése

1. Az Intézmény erőforrásait kizárólag a feljogosított felhasználók érhetik el.
2. A feljogosítás megfelelő felhasználónevet, jelszavat illetve a felhasználóra meghatározott jogosultságot jelent.
3. A feljogosításokat csak a szervezeti vezető engedélyezheti, a beállításokat csak a rendszergazda végezheti el.
4. A felhasználói jogosultságokat csoportszinten kell meghatározni. (Egyedi, azaz csoporton kívüli felhasználói jogosultságok kizárólag felső vezetői engedéllyel, korlátozott időre adhatók.)
5. A felhasználói csoportokhoz történő rendelés egyértelműen biztosítsa a munkakörhöz szükséges és elégséges erőforrások elérését.
6. A felhasználók a kiszolgálórendszereket számítógépeken keresztül az integrált címtárszolgáltatáson keresztül érhetik csak el, amely a számítógépek részére hitelesítési és jogosultság-kezelési szolgáltatásokkal biztosítja a hálózaton elérhető erőforrások (fájlok, megosztások, perifériák, adatbázisok, felhasználók, csoportok stb.) központosított felügyeletét.
7. Az erőforrásokhoz (szervereken megosztott mappák, nyomtatók, levelezés, informatikai alkalmazások stb.) a felhasználónkénti egyedi hozzáférés minimum felhasználónév/jelszó páros megadásával, az érzékeny, különleges személyes adatokat is tartalmazó rendszerek esetén pedig további második azonosítási mód egyidejű alkalmazásával (ún. két-faktoros autentikáció) legyen biztosított.

4. Hálózatbiztonsági szabályok

4.1. Belső hálózati szabályok

1. Az Intézmény informatikai hálózatáról, annak alkotóelemeiről és működési beállításairól a rendszergazdának dokumentált nyilvántartást kell vezetnie.
2. Az Intézmény belső hálózatára csak az Intézmény saját tulajdonú leltárba vett hálózati eszközei csatlakoztathatók.
3. A hálózati eszközöknek minden esetben IP kapcsolaton keresztül menedzselhető eszközöknek kell lenniük, az eszközöknek egyedi rendszergazdai jelszóval kell rendelkezniük, melyet a rendszergazda a titkosított jelszó tároló rendszerben rögzít.
4. A hálózati eszközök működését a központi monitoring rendszeren keresztül a rendszergazdának folyamatosan ellenőriznie kell.

5. Az Intézmény internet irányába történő kommunikációját tűzfalon keresztül kell kialakítani.
6. A tűzfalon a rendszergazdának szigorú, dokumentált szabályrendszert kell beállítania és fenntartania a külső támadások elhárítása, illetve a kifelé indított kommunikáció felügyelete érdekében.

4.2. Intézmény Wi-Fi használati szabályai

1. Az Intézmény belső hálózatához kapcsolódó Wi-Fi hálózata:
 - hozzáférési engedély csak munkatársaknak, és csak vezetői engedéllyel adható;
 - hozzáférés csak az Intézmény tulajdonát képező, a rendszergazda által felügyelt eszközzel lehetséges;
 - kizárólag csak munkavégzés céljára használható.
2. Az Intézmény belső hálózatához is kapcsolódó Wi-Fi hálózatának szigorú biztonsági beállításait a rendszergazda menedzseli, és szükség szerint aktualizálja.
3. Vendégek számára internet elérés, illetve munkatársak számára saját mobil eszközön keresztüli internetezés céljára csak külön ún. vendég- Wi-Fi hálózat engedélyezhető, amelyről az Intézmény belső hálózata elérése tiltott, nem lehetséges.
4. A Vendég Wi-Fi hálózatot is jelszóval, és minimum WPA2 titkosítással kell védeni.

4.3. Távmunka és otthoni munkavégzés

1. Távmunka illetve az otthoni munkavégzés csak az intézményvezető dokumentált engedélyével lehetséges.
2. Az Intézmény belső hálózatára való távoli csatlakozás:
 - csak a felhasználó egyéni jogosultságával (accountjával) engedélyezett, amit a rendszergazda állít be számára, és amit a felhasználó senki másnak nem adhat át;
 - csak biztonságos VPN kapcsolaton keresztül lehetséges, amelyet a rendszergazda állított be és felügyel;
 - csak olyan munkaállomásról engedélyezett, amelyhez a felhasználó a megfelelő védelmet (biztonsági csomagok telepítve vannak, elégséges vírusvédelem, hardveres tűzfal/router kapcsolódási pont) folyamatosan biztosítja.
3. Személyes adatokat is tartalmazó rendszerekhez, eszközökhöz való távoli hozzáférés esetén kötelező a minimum kétfaktoros azonosítás alkalmazása.

5. Informatikai eszközök üzemeltetésének logikai biztonsága

5.1. Szerverek

1. Az Intézmény informatikai eszközeiről (szerverek, kliensek, perifériák), annak alkotóelemiről és működési beállításairól, a menedzselte felhasználói csoportokról és jogosultsági beállításokról a rendszergazdának dokumentált nyilvántartást kell vezetnie.
2. A szerverek konzoljáról a bejelentkezés csak rendszergazdai jelszó által lehetséges.
3. A szervereken tárolt adatok, a merevlemez fizikai meghibásodása esetén bekövetkező adatvesztés elleni védelmét az alkalmazott RAID technológia biztosítja.
4. A Windows alapú szervereken központi antivírus programrendszer használata kötelező.
5. A szerverek és a központi informatikai alkalmazások működését a központi monitoring rendszeren keresztül a rendszergazdának folyamatosan ellenőriznie kell.

5.2. Személyes adatokat tartalmazó fájl-megosztások és alkalmazások biztonsága

1. A személyes adatokat is tartalmazó fájl-megosztásokhoz, adatbázisokhoz való hozzáférés:
 - csak azoknak a felhasználói csoportoknak adhatók, akik munkakörükben fogva azokat használják;
 - csak szigorúbb, külön hozzáférési azonosítási eljárás alapján valósítható meg;
 - különleges személyes adatokat is tartalmazó fájlok illetve adatbázisok esetén minden hozzáférésnek a rendszergazda által monitorozhatónak (loggolhatóknak) kell lennie.
2. A személyes adatokat is tartalmazó fájl-megosztások, adatbázisok mentésének titkosítva kell történnie.

5.3. Munkaállomások és perifériák

1. A munkaállomások konfigurálását, a felhasználóinak beállítását a rendszergazdának kell végeznie.
2. Bármely munkaállomásra az alapkonzfigurációnak tekinthető programokon túl csak a feladatok elvégzéséhez szükséges további programok telepíthetők.
3. A felhasználói munkaeszközök karbantartása a rendszergazda feladata.

- 4.A munkaállomásokon az operációs rendszer és a telepített alkalmazások biztonsági frissítéseinek használata kötelező.
- 5.A munkaállomásokon keresztül a hálózatba való bejelentkezés a rendszergazda által a szerveren beállított felhasználók számára biztosított.
- 6.A munkaállomásokon a jelszavas képernyővédő beállítása és használata kötelező.
- 7.A Windows alapú munkaállomásokon egységes antivírus programrendszer központi beállítása és használata kötelező. A vírusminták rendszeres frissítésének beállítása, annak kikapcsolási tiltásának beállítása kötelező.
- 8.A munkaállomásokra csatlakoztatott külső adathordozók (pl. pendrive, mobil HDD, ...) csatlakoztatás utáni azonnali automatikus vírusellenőrzésének beállítása kötelező.
- 9.A hordozható informatikai eszközön személyes adatokat tartalmazó fájlokat, adatbázisokat titkosított partíción kell tárolni. Ennek feltételeinek biztosítása a felhasználó számára a rendszergazda feladata.
- 10.A felhasználásból kivont, elavult eszközök biztonságos megsemmisítése a rendszergazda feladata. Az eszközök adathordozójának fizikai megsemmisítése (működésének, adatvisszanyerés lehetőségének megszüntetése) a szintén rendszergazda feladata. A megsemmisítés tényállását a számviteli rendszeren keresztül, selejtezési jegyzőkönyvben kell rögzíteni.
- 11.Rendszergazda felelőssége, hogy jelentse az intézmény vezetőnek amennyiben bármilyen visszaélést, szabálysértést észlel.

6. Mentési szabályok

- 1.Az informatikai rendszerekre megfelelő, dokumentáltan szabályozott adatmentési és visszaállítási eljárásokat kell működtetni.
- 2.A mentések készítésére vonatkozó szabályzásban (nyilvántartásban) – különösen a személyes adatokat tartalmazó adatbázisok, fájl-szerverek mentése esetén – tételesen meg kell adni a következőket:
 - a mentendő berendezéseket,
 - a mentésre kerülő adatok, adatbázisok azonosítását,
 - a mentések módját (pl. teljes, részleges, inkrementális, stb.) és ciklusidejét,
 - a mentések elvégzésének időpontját ill. időtartamát,
 - a mentések automatizált vagy kézzel indított voltát,
 - a mentésért felelős személyt,
 - a mentések titkosítását és annak módját (amennyiben szükséges);
 - a mentések tárolásának módját és helyét,

- a mentések tárolási idejét (meddig visszaállítható egy adat),
- a mentések elvégzése naplózásának módját,
- a mentések nyilvántartásának módját és felelőset,
- a mentések visszaállítási próbáinak szabályozott időciklusát, és elvégzésének módját, és a visszaállítási próbák dokumentálását.

3. Az üzemeltetés, karbantartás napi hibajavítási feladatainak ellátásához szükséges mentéseket úgy kell elhelyezni, hogy a folytonos üzemvitel megszakadása esetén a helyreállítás a lehető leghamarabb megtörténhessen. A tárolás helyét úgy kell meghatározni, hogy a mentések elérhetősége bármely időszakban (normál munkaidőben vagy azon kívül) biztosított legyen.

4. A tartalék mentések tárolását más, azonos káresemény általi sérüléstől védett helyen kell biztosítani.

5. A mentések – különösen a személyes adatokat tartalmazó adatbázisok, fájl-szerverek mentése esetén – tárolásának szabályait úgy kell kialakítani, hogy a mentésekhez csak az arra jogosult rendszergazdák férhessenek hozzá.

7. Titkosítási szabályok

1. Hordozható informatikai eszközökön (pl. notebook, laptop, ipad, iphone, okos-telefon, stb.) és passzív adathordozókon (pl. pendrive, flashdrive, mobil HDD, stb.) tárolt személyes adatokat is tartalmazó fájlok, adatbázisok csak titkosítottan tárolhatók. Ezen eszközök és adathordozók esetében a titkosítási alkalmazás beállítása a rendszergazda feladata és felelőssége.
2. Külső személynek küldött levélben érzékeny személyes adatokat tartalmazó fájlok, adatbázisok sima mellékletben nem küldhetők, csak megfelelő erősségű titkosítás alkalmazásával. A levelezés titkosításának, vagy a küldendő állományok titkosításának megfelelő beállítása és a felhasználók számára annak betanítása a rendszergazda feladata és felelőssége.
3. Érzékeny (esetleg különleges) személyes adatok feldolgozó, kezelő adatbázisok használata esetén:
 - a szoftvergyártó által küldött új verziók az Intézmény általi kipróbálására a tesztrendszer és az éles működő rendszert egymástól élesen el kell választani;
 - a tesztrendszeren, és kiemelten a fejlesztők által hiba-meghatározásra használt tesztrendszeren az éles, valós adatbázis, vagy annak akármelyik (régebbi) mentési állapotának feltöltése tilos;
 - tesztelés, valós rendszeren előforduló hibás működés hibájának beazonosítása célú futtatás számára az éles adatbázis egyik mentése használható oly módon, hogy a tesztelésre való feltöltés előtt az adatbázis **anonimizálás**ra kerül, vagy a tesztelés utáni visszatöltési igény esetén álnevesítésre kerül.

8. Új informatikai rendszerek tervezésére vonatkozó biztonság (privacy by design)

Az Intézmény új, személyes adatot kezelő informatikai rendszere bevezetésekor az adatvédelmi felelős bevonásával az intézményvezető feladatai:

1. Az informatikai rendszer általi adatkezelés céljának, jogalapjának és adatkezelési alapelvek megfelelőségének, valamint a kezelt személyes adatok adatbiztonsági hiánya (pl. illetéktelen adathozzáférés, adatvesztés, adatmódosítás vagy adatszivárgás) általi lehetséges károk és kockázatok mértékének vizsgálata.
2. Az informatikai rendszer számára – a vizsgálat alapján feltárt kockázatok mértékének megfelelően – a következők, mint követelmények meghatározása:
 - az informatikai rendszer által támogatott, a jogalapoknak, alapelveknek megfelelő adatkezelési tevékenységek támogatása, mint működési modell;
 - a meghatározott adatbiztonsági kockázatokat kezelni tudó adatbiztonsági szintnek megfelelő adatbiztonsági funkciók, működés támogatása;
 - a vizsgálatok és a meghatározott követelmények dokumentálása.
3. Csak olyan új informatikai rendszer pályáztatható, tervezethető, vásárolható meg és vezethető be, amely a meghatározott adatbiztonsági követelményeket funkcionalitásában, és működtetése során biztosítani tudja.

9. IT üzletmenet-folytonosság és katasztrófa-elhárítás

1. Adatvédelmi szempontból IT üzletmenet-folytonossági tervet illetve IT katasztrófa-elhárítási (pontosabban katasztrófa-állapot utáni visszaállítási) tervet – azaz IT BCP-DRP tervet – akkor kell készíteni, hogyha a személyes adatokat kezelő egy vagy több informatikai rendszer olyan hosszú időre leáll vagy működésképtelenné válik, hogy az Intézmény számára egyik vagy több személyes adatokat kezelő tevékenységének emiatt bekövetkező leállása már az Intézmény vagy az adatkezelésben érintett személyek számára nagyon komoly károkat jelent.
2. Az IT BCP-DRP terv célja az adott személyes adatokat kezelő informatikai rendszerek működésének visszaállítása
 - (az Intézményvezető által) meghatározott rövid időn belül akár a saját eredeti IT erőforráson, akár másik ideiglenes erőforrással, és az adott személyes adatot kezelő tevékenység működésének (teljes vagy részleges) biztosítása;
 - (az Intézményvezető által) meghatározott időn belül a teljes működésnek visszaállítása, beleértve a teljes informatikai rendszer

normális működését és az az által támogatott személyes adatkezelési folyamatok teljes működését.

3. A személyes adatokat kezelő informatikai rendszerekre (informatikai rendszerenként külön-külön) el kell készíteni dokumentáltan a következőket:
 - Az informatikai rendszer által támogatott személyes adatkezelési tevékenységek listája, és az azok által megengedett azon maximális leállási idő (RTO), amin belül az az által támogatott személyes adatkezelési tevékenységek közül a legelsőknek mindenképp újra kell tudnia indulni.
 - Az informatikai rendszer által támogatott személyes adatkezelési tevékenységek végzése során a nem tervezett leállás miatti megengedetett legnagyobb adatkiesési időtartama (RPO), amennyi működési idő alatt felvitt adatot a rendszer elveszthet, azaz még utólag jelentősebb veszteség nélkül pótolható.
 - Az informatikai rendszer mentési rendjének szabályozásakor mentési ciklusát úgy kell szabályozni, hogy az a meghatározott RPO értékű vagy annál kisebb lehet. A mentések tárolási helyét úgy kell szabályozni, hogy legalább egy mentés elérhető, a szerver közvetlen működésétől független és kellően biztonságos, védett fizikai környezetben legyen.
 - Meg kell határozni az informatikai rendszer működtetéséhez minimálisan szükséges informatikai infrastruktúrát, beleértve a hardver és szoftver környezetet, illetve a felhasználók számára a hálózati elérési feltételeket is.
 - Meg kell határozni azt a tevékenységi forgatókönyvet, amivel – az eredeti működtetési informatikai infrastruktúra működésképtelensége esetén – a helyettesítő minimális informatikai infrastruktúra létrehozható, konfigurálható, azon az adott informatikai rendszer a legutolsó (RPO-nak megfelelő) mentésű adatokkal visszatölthető, és a felhasználók számára újra működőképesen elérhetővé tehető. (A virtuális környezetek kialakítása és használata ebben sokszor segít.) Ezt úgy kell megtervezni, hogy ez az RTO időn belül végrehajtható legyen.
4. Ezt a kialakított forgatókönyvet (ez maga az IT BCP-DRP) működésre legalább induláskor, majd meghatározott ciklikussággal (ajánlott évente minimum egyszer) dokumentáltan letesztelni, kipróbálni kell.

IX. ÉRINTETTI KÉRELMEK TELJESÍTÉSÉNEK RENDJE

1. Az adatkezeléssel érintett magánszemélyek alapvető jogai

Az érintett hozzájárulása a személyes adatainak kezeléséhez az **2. sz. függelék** szerint, mint alapsablon kitöltése szükséges.

Az alább felsorolt alapvető jogok tájékoztatásként és a kérelemhez való hozzáférés érdekében az Intézmény honlapjára is feltöltésre kerül (**3. sz. függelék**).

Előzetes tájékoztatáshoz való jog

Az érintett magánszemély bármikor jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról érthető, tömör tájékoztatást kapjon, ez a joga az adatkezelés megkezdését megelőzően is fennáll.

Hozzáférési jog

Az érintett magánszemély jogosult arra, hogy az adatkezelőtől tömör, közérthető választ kapjon arra nézve, hogy személyes adatainak kezelését végzik-e éppen, és ha igen, akkor jogosult arra, hogy a személyes adatokhoz és az uniós rendeletben meghatározott kapcsolódó információkhoz hozzáférést kapjon.

Helyesbítéshez való jog

Az érintett magánszemély jogosult arra, hogy kérésére az adatkezelő – indokolatlan késedelem nélkül – helyesbítse a rá vonatkozó pontatlan személyes adatokat. Az érintett jogosult arra, hogy kérje a téves, hiányos személyes adatok módosítását, kiegészítését.

A törléshez/ "elfeledtetéshez" való jog

Az érintett magánszemély jogosult arra, hogy kérésére az adatkezelő - indokolatlan késedelem nélkül - törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha annak nincs jogi akadálya.

Az érintettnek ez a joga különösen a hozzájárulása alapján kezelt személyes adataihoz kapcsolódóan áll fent, más jogalapok fennállta, így többek között a jogi kötelezettség teljesítése alapján kezelt adatok esetén pedig kifejezetten korlátozott ez a joga, illetve nem áll fent.

Az adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha bizonyos meghatározott feltételek teljesülnek. Ez az esetkör leginkább egy bizonyos adatkezelési állapot rögzítésére szolgál, amely akár egy jogvita helyzetéhez vezető állapot áll fent vagy már maga a konkrét vitás helyzet is létrejött.

A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség

Az adatkezelő minden olyan címzettet tájékoztat minden helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akikkel a személyes adatot közölték. Van kivétel,

ez: nem várható el ezen kötelezettség teljesítése, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne.

Az adathordozhatósághoz való jog

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik Adatkezelőnek továbbítsa.

A tiltakozáshoz való jog

Az érintett magánszemély jogosult arra, hogy bármikor tiltakozzon személyes adatainak kezelése ellen, ha az

- adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, illetve, ha:
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást

Az érintett magánszemély jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – profilalkotás is! – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené. Az érintett magánszemély ilyenkor kérheti a kézi, emberi beavatkozást és döntés alkotást.

Az érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, abban az esetben az adatkezelő – indokolatlan késedelem nélkül – tájékoztatja az érintettet az adatvédelmi incidensről (lásd még a mindenkor hatályos *Adatvédelmi Incidens kezelési szabályzatot*).

Felügyeleti hatóságnál történő panasztételhez való jog

Az érintett magánszemély jogosult arra, hogy panaszt tegyen a magyar felügyeleti hatóságnál, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti az Unió Adatvédelmi Rendeletét.

Elérhetőségek:

NAIH – Nemzeti Adatvédelmi és Információszabadság Hatóság,
tel: 06 1 391-1400
postacím: 1530 Budapest, Pf. 5., cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c,
e-mail: ugyfelszolgalat@naih.hu

A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog

Minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben

Ez a jog akkor is fennáll, ha a felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

Az adatkezelővel/adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog

Minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak az uniós rendeletnek nem megfelelő kezelése következtében megsértették a jogait. Az bírósági illetékességi szabályok szerinti Törvényszék jogosult az eljárásra.

2. Az érintett magánszemély kérelmének benyújtása

Az érintett magánszemélynek személy azonosítása mellett lehetősége van bármely általa választott módon kérelmet nyújtani be az adatkezelőhöz/adatfeldolgozóhoz, így:

- személyesen
- postai úton
- elektronikus levél útján
- meghatalmazott útján
- egyéb módon.

Az érintett magánszemélynek lehetősége van a jelen szabályzat **3. sz. függelékében** mintaként felkínált kérelmet benyújtani, illetve saját alakszerűtlenül megfogalmazott kérelme sem lehet akadálya a kérelme elbírálásnak.

3. Az érintetti kérelmek elbírálása

Amennyiben az adatkezelő/adatfeldolgozó az érintett kérelme teljesítésének akadályát nem látja, úgy azt 30 naptári napon belül teljesíti és erről értesíti az érintettet (**4. sz. függelék** minta szerint) . A kérelem teljesítésének módja lehetőség szerint (**3. sz. függelékben** felsorolt) az érintett által igényelt mód:

- tájékoztatási kérelem esetén: e-mail-ben, postai úton, személyesen,
- adatpontosítási és korlátozási kérelem esetén a tárolt adatra vonatkozó belső végrehajtással,
- adattörlésre vonatkozóan az adat törlésével,
- adattovábbítás, adathordozás esetén az átadással (CD, DVD átadása, e-mail útján, személyesen)
- tiltakozásnak helyt adó kérelem esetén a kívánt állapot létrehozásával.

Amennyiben az adatkezelő/adatfeldolgozó úgy ítéli meg, hogy az érintett magánszemély kérelmének teljesítésére nincs lehetőség, úgy a kérelem elutasításáról és a jogorvoslati jogokról tájékoztatja a kérelmezőt.

Adatkezelő/adatfeldolgozó jogosult és köteles ellenőrizni a kérelmező személyazonosságát az adatok bizalmasága és jogi kötelezettségek teljesítése érdekében. Az azonosítás lehetőség szerint az adatmegadás, adatszerzés módjához kapcsolódik.

Adatkezelő/adatfeldolgozó az érintetti kérelmek elbírálása során tevékenységéért költséget, díjazást nem számol fel, de ismételt, megalapozatlan, célszerűtlen kérelmek esetén az ügyintézésre jogosult a felmerülő költség felszámítására.

Az érintetti kérelmekről a DPO-nak nyilvántartást **(5. sz. függelék** szerint) kell vezetnie.

4. Adatvédelmi előírások

Érintetti kérelem alapján történő eljárás esetén az adatigénylő személyazonosító adatai **(2. sz. függelék** szerint) csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez - beleértve az esetleges költségek megfizetését is - elengedhetetlenül szükséges. A kérelem teljesítését, illetőleg a költségek megfizetését követően az igénylő személyes adatait haladéktalanul törölni kell, amennyiben erről más jogszabály, különösen a Számvitelről szóló 2000. évi C. törvény másként nem rendelkezik.

X. ADATVÉDELMI INCIDENSKEZELÉSI SZABÁLYOK

Adatvédelmi incidens fogalma

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

Adatvédelmi incidensnek minősülnek például:

- Személyes adatok dokumentumon, hordozható eszközön, adathordozón vagy informatikai rendszeren (pl. levelezéssel) történő illegális továbbítása.
- Illetéktelen hozzáférések személyes adatokat kezelő informatikai rendszerhez vagy alkalmazáshoz (pl. jelenlegi vagy volt alkalmazott vétlen vagy tudatos közreműködése által, vagy biztonsági lyuk kihasználásával).
- Személyes adatokat tartalmazó adatbázis részének vagy egészének sérülése vagy elvesztése.
- Az informatikai rendszer részének vagy egészének használhatatlanná válása vírus vagy egyéb rosszindulatú szoftver által.
- Stb.

Adatvédelmi incidens eljárásrendje (PROTOKOLL)

Az adatvédelmi incidens eljárásrendjének folyamatát az **1. sz. melléklet** szemlélteti.

1. Adatvédelmi incidens észlelése

Az a dolgozó, aki észlel adatvédelemmel kapcsolatos biztonsági sérülést, azonnal köteles a **közvetlen vezetőjét tájékoztatni**, szükség szerint rendőrséget értesíteni **és a DPO-t értesíteni** az adatvedelem@ujpalotaiiovi.hu e-mail címen.

2. Adatvédelmi incidens bizonyítékainak a tárolása

A bejelentéssel egy időben a rendelkezésre álló bizonyítékokat meg kell őrizni. (pl.: kamerafelvételek, rendőrségi jegyzőkönyv, stb.) A kamerafelvételek (törvényi előírás szerinti határidőn belüli) és/vagy informatikai rendszeradatok mentése az informatikai üzemeltetést ellátó GMK kötelessége.

3. Adatvédelmi incidens vizsgálata

Az adatvédelemmel kapcsolatban összehívott szakértői team legalább 3 főből áll. A team tagjait az Újpalotai Összevont Óvoda igazgatója jelöli ki. A vizsgálatról jegyzőkönyv készül, amelyben fel kell tüntetni, hogy személyes adatok biztonsága sérült-e, kik az érintettek, akiket tájékoztatni kell és milyen technikai és/vagy szervezési feladatokat, intézkedéseket kell hozni a veszély elhárítására. A jegyzőkönyv elkészítésével egy időben kell kiállítani az incidens bejelentő lapot **(2.sz. melléklet)**, amelyet az intézményvezető aláírásával hitelesít, és amely

alapján történik (személyes adatok biztonságának sérülése esetén) a bejelentés (lásd: adatvédelmi incidens bejelentés fejezet).

4. Adatvédelmi incidens bejelentése

Ha a jegyzőkönyv alapján sérült a személyes adatok biztonsága, akkor a Hatóság felé bejelentési kötelezettség áll fenn. A Hatóság felé az észleléstől számított 72 órán belül a bejelentést az arra kialakított NAIH felületen (<http://www.naih.hu/adatvedelmi-incidensbejelent-rendszer.html>) **(2. sz. melléklet)** vagy papír alapon postán kell bejelenteni. A bejelentést az igazgató, illetve az általa megbízott dolgozó végzi el.

Ha a személyes adatok sérülését az Újpalotai Összevont Óvoda, mint adattfeldolgozó észleli, akkor az adatkezelő felé az észlelést követően azonnal jelezni kell, amelyet az Intézményvezető nevében az Intézményvezető által kijelölt dolgozó végez el.

5. Adatvédelmi incidens érintettjeinek értesítése

Az adatvédelmi incidens vizsgálata során kell meghatározni, hogy kik azok az érintettek, akiket tájékoztatni kell az incidensről. Az érintettek tájékoztatását a vizsgálat lezárása után 2 munkanapon belül értesíteni kell. Az adatbiztonság sérülése során érintett(ek) tájékoztatását az Intézményvezető által kijelölt személy végzi az adatvédelmi incidens vizsgálat lezárását követő 2 munkanapon belül.

6. Adatvédelmi incidens nyilvántartása

Az adatvédelmi incidens bejelentése után az incidensről a bejelentést nyilvántartásba kell venni, amely a DPO feladata. A bejelentéshez szükséges a kitöltött és Intézményvezető által aláírt incidens bejelentő lap, amelyet a DPO számára másolatban kell eljuttatni.

Az adatvedelem@ujpalotaiiovi.hu e-mail címhez az alábbi személyeket kell hozzárendelni, amelynek beállítását az informatikai feladatokat ellátó GMK végzi: Intézményvezető, DPO, GMK alkalmazásában álló rendszergazda.

XI. ZÁRÓ RENDELKEZÉSEK

Jelen szabályzat 2024.12.02. napján lép érvénybe. Az érvénybelépéssel egy időben

a **254/2020** iktatószámú Munkáltatói adatkezelési szabályzat,
a **398./2020** iktatószámú Munkavállalói adatbiztonsági szabályzat,
a **238/2020** iktatószámú IT Üzemeltetés adatbiztonsági szabályzat,
a **269 /2020** iktatószámú Adatvédelmi incidenskezelési szabályzat,
a **560/2020** iktatószámú Érintetti kérelmek teljesítésének rendje című szabályzatok érvényüket veszítik.

Jelen szabályzatba foglaltak a munkavállalók és egyéb közreműködők részére történő megismertetése az adatkezelő Igazgató feladata és felelőssége. Jelen szabályzat felülvizsgálatáért és aktualizálásáért az intézmény igazgatója felel.

Budapest, 2024. október 31.



.....
Sebestyén Irén
Igazgató

XII. FÜGGELÉKEK

1. függelék (Adatkezelési tájékoztató - munkaerő kiválasztásához és felvételéhez)

Budapest Főváros XV. kerületi Önkormányzat
Újpalotai Összevont Óvoda

ADATKEZELÉSI TÁJÉKOZTATÓ
(Állaspályázatlás és munkaerő kiválasztásához)

Az Európa Parlament és Tanács 2016/679 Általános Adatvédelmi Rendelete – „GDPR”
- A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről
és az ilyen adatok szabad áramlásáról - alapján

Érvényes: 2024. november 04. napjától

1. AZ ADATKEZELŐ

Jelen adatkezelési tájékoztatónak az a célja, hogy az érintett magán személyeket tájékoztasson és főként tájékoztassa a személyes adataik kezeléséről, az Európai Unió Általános Adatvédelmi Rendeletének (2016/679. számú Rendelet – „GDPR”) és a magyar Infotörvénynek (2011. évi CXII. törvény) megfelelően.

A Budapest Főváros XV. kerületi Önkormányzata Újpalotai Összevont Óvoda (a továbbiakban: adatkezelő) magára nézve kötelezőnek ismeri el jelen tájékoztatóban foglalt szabályokat, amennyiben a hatályos jogi szabályozás alapján adatközlő ki. A www.ujpalota.hu web oldal adatai megtekinthető adatkezelési tevékenységekhez kapcsolódó adatvédelmi tájékoztatók elérhetők <http://www.ujpalota.hu/adatvedelem> címen.

Az adatkezelő adatai:

Név:	Újpalotai Összevont Óvoda (Budapesti Főváros XV. kerületi Önkormányzat)
Cím:	HU-1157 Budapest, Páskov park 37.
Telefon:	+36-1/418-2425
E-mail:	kezes@ujpalota.hu
Képviselő:	Sabsthyán Péter igazgató
Adatszám:	15637948-2-42
Adatvédelmi felelős elérhetősége:	adatvedelem@ujpalota.hu

Adatkezelő az a személy, szervezet, aki az adatkezelés célját és eszközeit - önállóan vagy másokkal együtt - meghatározza, aki részben és döntően szabályozza az adatkezelést.

Az adatkezelő a tevékenységét, belső szervezeti felépítését több adatkezelési szabályzattal is korlátozza, s való egyben az érintettek személyes adatai, garanciális jogait.

Az adatkezelő vállalja, hogy az adatkezelése megfelel a mindenkor hatályos uniós és magyar szabályoknak.

Az adatkezelő fenntartja magának a mindenkor jogait a tájékoztató megváltoztatására, de kifejezetten jogát annak nyilvánosságra hozatalára és kizárására.

2. AZ ADATFELDOLGOZÓ

Sikeres pályázat esetén az adatkezelő továbbítja a pályázó személyes adatait a Budapest Főváros XV. kerületi Önkormányzat, mint fenntartó által felhatalmazott adatfeldolgozóval végző Budapest Főváros XV. kerületi Önkormányzati Gazdasági Működéstámogatási Központnak, amely szervezet a Magyar Államkincstár (továbbiakban: MÁK) KIRA (a kikapcsolódott államháztartáshoz tartozó) információs rendszerében (a munkaadófelvételi) kapcsán adatokat rögzít és a felvételi adminisztrációs folyamatot végzi.

A MÁK adatvédelmi tájékoztatóját <http://www.allamkincstar.gov.hu/hu/info/adatvedelem/> oldalon érheti el. A MÁK a 2011. évi CXCV. törvény az államháztartásról (továbbiakban: Áht.) 44.§ (1), (2) és (3) bekezdésében foglaltak szerinti jogszabály előírás alapján végzi adatainak kezelését.

Az adatfeldolgozó adatai:

Név:	Újpalotai Összevont Óvoda (Budapesti Főváros XV. kerületi Önkormányzat)
Cím:	HU-1158 Budapest, Ady Endre utca 31-33.
Telefon:	+36 1 815-1700
E-mail:	kezes@ujpalota.hu
Képviselő:	Bartók Katalin főigazgató
Adatszám:	15792307-2-42
Adatvédelmi felelős elérhetősége:	adatvedelem@ujpalota.hu

Az adatfeldolgozó az, aki az adatkezelés nevében kezeli az adatokat. A MÁK adatkezelési tájékoztatóját a <http://www.allamkincstar.gov.hu/hu/info/adatvedelem/> oldalon érheti el.

3. Munkaadó felvétel (felvételhez)

Az Újpalotai Összevont Óvoda a hozzá munkavégzésre jelentkező sikeres pályázók adatait a munkaerő felvétel során az ebben a pontban összefoglalottak szerint kezeli.

Az Újpalotai Összevont Óvoda lehetőséget biztosít arra is, hogy elektronikus úton is személyes adatokat (adatfeldolgozó) nyújthasson be az érintett.

Az Újpalotai Összevont Óvoda, mint munkáltató a munkaerő felvételkor előzetes tájékoztató keretén belül biztosítja saját adatkezelő voltának és elérhetőségének a megismerését.

Az Újpalotai Összevont Óvoda csak olyan személyes adatot megismerhetőségére tart igényt, amelyek lényegesek az adott munkakörrel kapcsolatban, illetve a MÁK, mint pénzügyi vállalkozás (adatkezelő) a KIRA információs rendszerében rögzített.

Az Újpalotai Összevont Óvoda az adatvédelmi hatóság 2016. évi határozatát alapján megismerheti az adott munkavégzés körében elvégzett munkát, a munkavégzés szempontjából lényeges személyes adatait, de erről a körülményről előzetes tájékoztatót nyújt a munkavállaló számára.

Az Újpalotai Összevont Óvoda a munkavállaló közösségi oldalával kapcsolatban személyes adatot nem ment, nem tárol, nem továbbít.

ADATKEZELÉSI TÁJÉKOZTATÓ

2 / 5

Állaspályázatlás és munkaerő kiválasztásához

4. Jogorvoslat

Adatkezelési eljárásunkkal kapcsolatos panasszal az Újpalotai Összevont Óvoda adatvédelmi felelőséhez fordulhat az alábbi elérhetőségen: adatvedelem@ujpalotaiovi.hu

Amennyiben nem intézkedünk a kérelmére, vagy intézkedésünket nem fogadja el, úgy jogorvoslattal élhet az alábbi Hatóságnál:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Székhely: 1125, Budapest, Szilágyi Erzsébet fasor 22/c
Levelezési cím: 1530 Budapest, Pf: 5
Telefon: +36 1 391 1400
e-mail: ugyfelszolgalat@naih.hu
Honlap: <http://www.naih.hu>

vagy jogszértés esetén a lakóhelye vagy tartózkodási helye szerinti törvényszékhez fordulhat.

2. sz. függelék (Érintetti hozzájárulás magánszemély adatainak a kezeléséhez)



Budapest Főváros XV. kerületi Önkormányzat

Újpalotai Összevont Óvoda

Magánszemély neve:

Értesítési címe:

ÉRINTETT MAGÁNSZEMÉLY HOZZÁJÁRULÁSA

Alulírott (név) lakcím

..... (plusz egy azonosító adat)

az Európai Unió Parlament és Tanács 2016/679. számú Rendelete (ún. „GDPR”) alapján önként, befolyásmentesen és kellő tájékoztatáson alapuló döntésem alapján hozzájárulok ahhoz, hogy személyes adataim kezelésre kerüljenek.

Az érintett adatok (*):

Név:

lakcím:

telefonszám:

e-mail cím:

(*) amelyekhez a hozzájárulást megadja az érintett.

A hozzájárulás időtartama (**): visszavonásig /év.....hó.....napig határozott időtartamra

(**) Megfelelő rész alhúzandó és/vagy kitöltendő!

Adatkezelési cél: Óvodai kapcsolattartás (elérhetőség a gyermek érdekében).

2./ AZ ÉRINTETT MAGÁNSZEMÉLY JOGAI AZ ADATKEZELÉS SORÁN

- Tájékozódhat a kezelt adatokról, célról, jogalapról, időtartamról
- Kérheti az adataihoz való hozzáférést
- Kérheti egy adata pontosítását, helyesbítését
- Kérheti több adata pontosítását, helyesbítését
- Kérheti egy adata korlátozását
- Kérheti több adata korlátozását
- Kérheti egy adata törlését
- Kérheti több adata törlését
- Kérheti adatai átadását vagy továbbítását
- Kérheti, hogy ne terjedjen rá ki az automatizált döntés hatálya
- Tiltakozhat egy adata kezelése ellen
- Tiltakozhat több adata kezelése ellen
- Egyéb:

Budapest, 20.....év.....hó.....nap.

.....
Érintett magánszemély aláírása

3. sz. függelék (Érintettek számára tájékoztatás és kérelem űrlap)

 Budapest Főváros XV. kerületi Önkormányzat Újpalotai Összevont Óvoda	 Budapest Fővárosi XV. kerületi Önkormányzat Újpalotai Összevont Óvoda
Érintetti kérelem és tájékoztatás az érintett magániszemély jogairól (Verzió: 2.0.)	Érintetti kérelem és tájékoztatás az érintett magániszemély jogairól (Verzió: 2.0.)
TÁJÉKOZTATÁS Az adatkezeléssel érintett magániszemélyek alapvető jogairól	
1.1. Előzetes tájékoztatásban való jog Az érintett magániszemély jogosult arra, hogy az adatkezeléssel összefüggő személyi és információk iránti, illetve tájékoztatás kapjon, és a jogát az adatkezelés megkezdése előtt megismerhesse. 1.2. Hozzájárulási jog Az érintett magániszemély jogosult arra, hogy az adatkezeléstől elvonja, kizárja vagy korlátozza az adatkezelést, hogy személyes adatainak kezelését megakadályozza, és ha igen, akkor jogosult arra, hogy a személyes adatait töröltesse, és az adatait rendszeresen megújított információkhoz hozzáférést kapjon. 1.3. Helyesbítéshez való jog Az érintett magániszemély jogosult arra, hogy kijelentsen az adatkezelést – indokolatlan késedelem nélkül – helyesbítés a rá vonatkozó pontos adatok személyes adatait, az érintett jogosult arra, hogy kérje a téves, hiányos személyes adatak módosítását, kiegészítését. 1.4. A törléshez "elfelejtettséghez" való jog Az érintett magániszemély jogosult arra, hogy kérésére az adatkezelő – indokolatlan késedelem nélkül – törölje a rá vonatkozó személyes adatait, az adatkezelő pedig köteles arra, hogy az érintett személyes adatait indokolatlan késedelem nélkül törölje, ha annak nincs jogi alapja. Az érintettnek ez a joga különösen a hozzájárulással alapuló személyes adatokhoz kapcsolódóan áll fenn, más jogalapok hiányában. Egy kivétel kivétel a jogi kötelezettség teljesítése alapján került adatainak esetleg jogszabályban közzétételre ez a joga, illetve nem áll fenn. 1.5. Az adatkezelés korlátozásához való jog Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha bizonyos meghatározott körülmények teljesülnek. Ez az esetek leggyakoribb egy bizonyos adatkezelési alapelv megnevezése, amely akkor egy jogszabályban meghatározott állapot áll fenn vagy más jogszabályban meghatározott állapot áll fenn. 1.6. A személyes adatak helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség Az adatkezelő minden olyan érintettet tájékoztat minden helyesbítésről, törlésről vagy adatkezelés-korlátozásról, ahállyal a személyes adatait érinti. Vm kivétel, az nem várható el ezen kötelezettség teljesítését, ha az lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne. 1.7. Az adatkezelési hatáskörhöz való jog Az érintett jogosult arra, hogy a rá vonatkozó, általa egy Adatkezelő rendelkezésére bocsátott személyes adatait töltsön, az adatok körében használja, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy cserét az adatait egy másik Adatkezelőnek továbbítsa. 1.8. A tiltáshoz való jog Az érintett magániszemély jogosult arra, hogy kérésére a tiltáshoz személyes adatainak kezelését elvonja, ha az – adatkezelés közérdekű vagy az adatkezelésről részletes tájékoztatási jogszabályi gyakorlati szabályok keretében végzett feladat végrehajtásához szükséges, illetve, ha	– az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges. 1.9. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást Az érintett magániszemély jogosult arra, hogy ne legyen kitéve olyan, kizárólag automatizált adatkezelésnek – profilalkotás is – alapú döntés hatálya, amely rá nézve joghatással jellemezhető vagy azonos módon járhat más személyekkel szemben. Az érintett magániszemély jogosult kérésre a kitéve, amelyet beavatkozási és döntési állomást. 1.10. Az érintett tájékoztatása az adatvédelmi incidensekről Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogainak és szabadságainak sérelmére, akkor az esetben az adatkezelő – indokolatlan késedelem nélkül – tájékoztatja az érintettet az adatvédelmi incidensekről. 1.11. Felügyeleti hatósággal történő panaszterjesztéshez való jog Az érintett magániszemély jogosult arra, hogy panaszt tegyen a magyar felügyeleti hatóságnál, ha az érintett megkérdőjelezi az adatainak kezelését, megnevezte az Unió Adatvédelmi Rendeletét. Ellátási feladat: NAH – Nemzeti Adatvédelmi és Információszabadság Hatóság, tel: 391-1400 postacím: 1130 Budapest, Pf. 5., e-mail: info@naih.hu web: naih.hu 1.12. A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslatra való jog Minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság hiányában, jogilag kötelező erejű döntéssel szemben. Ez a jog akkor is fennáll, ha a felügyeleti hatóság nem foglalkozik a panasszal, vagy hiányos bizonyítékai nem támasztják az érintett a bizonyított panaszai kapcsolatát a felügyeleti hatósággal vagy annak elutasításával. 1.13. Az adatkezelővel adófelügyeleti hatóság szembeni hatékony bírósági jogorvoslatra való jog Minden érintett hatékony bírósági jogorvoslatra jogosult, ha meggyőződés az, hogy a személyes adatainak az adatai rendelkezés nem megfelelő körülmények között kerültek kezelésre, vagy a bírósági illetékességi szabályok szerinti törvények jogszabályai alapján.
2 / 3	

4. sz. függelék (Válaszlevél sablon az érintetti kérelemhez)

	<i>Budapest Főváros XV. kerületi Önkormányzat</i> <i>Újpalotai Összevont Óvoda</i>	Érintetti tájékoztató levél (Verzió: 2.0.)
---	--	--

Iktatászsám:/20.....
 Tárgy: Tájékoztatás személyes adatok kezeléséről
 Ügyintéző:.....
 Melléklet: db

Tisztelt Kérelmező, tisztelt !

..... napján érkezett kérelme alapján tájékoztatjuk Önt - az Európai Parlament és Tanács 2016/679. sz. Rendelete („GDPR” – Általános Adatvédelmi Rendelet) 13. cikk (1.) bekezdése alapján - az általunk kezelt személyes adatairól, illetve jogairól:

Adatkezelő (képviselője) neve, elérhetősége: Sebestyén Irén kozpont@ujpalotaiovi.hu
 Adatvédelmi tisztviselő elérhetősége: adatvedelem@ujpalotaiovi.hu

Adatkezelés célja:.....
 Adatkezelési jogalapja:
 Adatkezelő jogos érdekei (ha van ilyen):
 Személyes adatok címzettjei, címzettek kategóriái (ha van ilyen):
 Jogorvoslati jogok: hozzáférési jog, helyesbítési jog, kezelés korlátozásának joga, tiltakozási jog:

Ön kérheti adataihoz való hozzáférést, az adatok helyesbítését, az adatok kezelésének korlátozását, tiltakozhat az adatkezelés ellen.

Jogorvoslat a Hatóságnál:

Ön jogosult panaszt benyújtani a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (1530 Bp. Pf. 5., mail: ugyfelszolgalat@naih.hu, tel: 06 1 391-1400, fax: 06 1 391-1410 cím: 1125 Bp. Szilágyi Erzsébet fasor 22/c.

Bírószághoz fordulás joga:

A magánszemély lakhelye szerinti Törvényszék.

Automatizált döntéshozatal egyedi ügyekben:

Ön jogosult arra, hogy **ne terjedjen ki** Önre az automatizált adatkezelésen - ideértve a profilalkotást is - alapuló **döntés hatálya**, amely Önre nézve joghatással járna vagy Önt hasonlóképpen jelentős mértékben érintené.

Egyéb jogok:

Bármilyen tájékoztatás **közérthető nyelven** történő megfogalmazáshoz való joga, **adathordozáshoz** való jog, korábbi **hozzájárulás** bármikor történő **visszavonásának joga**.

Intézményünk tájékoztatja egyben Önt a kapcsolattartás, ügyintézés lehetséges további módjairól és eszközéről:

- Személyes bejelentések, kérelmek, helyszín: 1157. Budapest, Páskom park 37.
- Elektronikus vagy postai levelezés útján történő kapcsolattartás, kapcsolattartó e-mail cím: kozpont@ujpalotaiovi.hu
- Közvetlen megkeresés telefonon: Telefon: +36 1/418-2425
- Vegyes/kevert eljárási elemek: e-mail, telefon, személyes, meghatalmazott útján (*):

(*) megfelelő rész aláhúzendó!

Budapest, 20.....év.....hó.....nap.

.....
 Sebestyén Irén
 Igazgató

5. sz. függelék (Érintetti kérelmek nyilvántartása)



Budapest Fővárosi XV. Kerületi Önkormányzat
Újpalotai Összevont Óvoda

Érintetti kérelmek
nyilvántartása
Verzió: 2.0
Készlet: 2024.01.04.

ÉRINTETTI KÉRELMEK
NYILVÁNTARTÁSA

Beadó felhívó:
Jóváhagyta:

Vincze-Szankó Katalin
Schostyán Irén

DPO
Igazgató



Budapest Fővárosi XV. Kerületi Önkormányzat
Újpalotai Összevont Óvoda

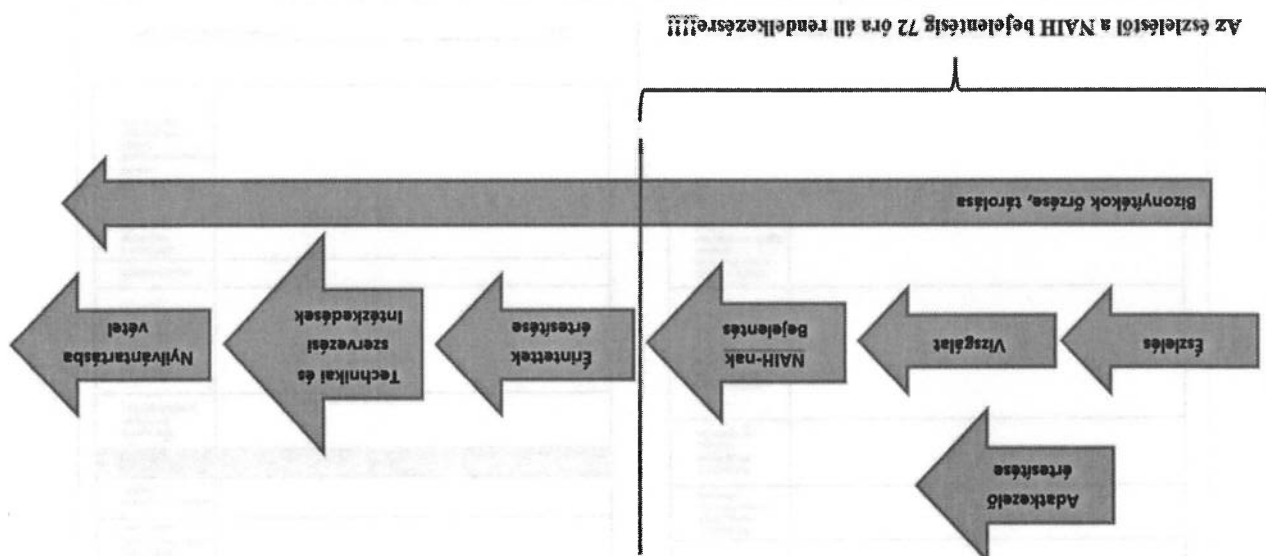
Érintetti kérelmek
nyilvántartása
Verzió: 2.0
Készlet: 2024.01.04.

Beküldés dátuma	Érintett kérelmező	Kéréslem tárgya	Intézkedés leírása	Feladás / határidő	Teljesítés dátuma

2 / 2

XIII. MELLÉKLETEK

1. sz. melléklet (incidenskezelési eljárásrend folyamata – protokoll)



[illegible]

2. sz. melléklet (Incidents bejelentő lap – NAIH honlapjáról letölthető nyomtatvány)

NAHJ Incidents 2006-2015 Jan (V2.2)

2008

NAAT Inc. 3000a Belknap St. #600 PV 23

4/15

NAIHT Incidents belagert de l'op. (v2.2)

5/29

NAnt includes bejeweled logo (V1.2)

6/13

A hatóság kódja	A károsító jelölése
Tájékoztató időpontja („a” válasz esetén)	
Tájékoztató terjedése („b” válasz esetén)	
A tájékoztató terjedése időpontja még nincs előírva („b” válasz esetén)	Ez van előírva/Nincs előírva
Tájékoztató tárgyának indokai („c” válasz esetén)	I. Az adatkezelő magatartás technikai és szervezeti védelmi intézkedéseket hajtott végre, de ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen olyan intézkedéseket, amelyek a személyes adatokhoz való hozzáférést fel nem ismertített személyek számára elérhetőséget nyújtottak az adatokhoz. II. Az adatkezelő az adatvédelmi incidens elhárítását olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaiba és szabadságába jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg. III. Az érintettek egyenkénti tájékoztatása aránytalan erőfeszítást igényelne, különösen az adatkezelő számára.
Indoklások listája, amelyek alapján az érintettek tájékoztatására nem került sor („c” válasz esetén)	

NADH Incidens bejelentő lap (V1.2)

11 / 15

A hatóság kódja	A károsító jelölése
Tájékoztató időpontja („a” válasz esetén)	
Az érintett tájékoztatásának formája („a” válasz esetén)	
Az érintettek közli tájékoztató tartalmát („a” válasz esetén)	
Hyfelyesen közölt információk, vagy technikai intézkedések („c” válasz „d” válasz esetén)	
B.2 Az adatkezelő intézkedése az incidens elhárítására	
Az adatkezelő által az adatvédelmi incidens orvoslására tett intézkedések	
B.3 Jogi bejelentések	
A vezető hatóságok bejelentett határozatai (közölt adatvédelmi incidens)	Igen/Nem
Az EU felügyeleti hatóságok listája, amelyekhez az adatvédelmi incidens bejelentése (jóllehet válasz is elfogadható)	☐ Ausztria ☐ Belgium ☐ Bulgária ☐ Ciprus ☐ Dánia ☐ Egyesült Királyság ☐ Franciaország ☐ Finnország ☐ Franciaország ☐ Görögország ☐ Hollandia ☐ Horvátország ☐ Írország ☐ Island ☐ Lengyelország

NADH Incidens bejelentő lap (V1.2)

12 / 15

A hatóság kódja	A károsító jelölése
	☐ Lettország ☐ Liechtenstein ☐ Litvánia ☐ Luxemburg ☐ Magyarország ☐ Málta ☐ Németország ☐ Norvégia ☐ Olaszország ☐ Portugália ☐ Románia ☐ Spanyolország ☐ Svájc ☐ Svédország ☐ Szlovákia ☐ Szlovénia
Az adatkezelő bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidens elhárítását más tagállami felügyeleti hatóságoknak?	
Az EU felügyeleti hatóságok listája, amelyekhez az adatkezelő bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidens (jóllehet válasz is elfogadható)	☐ Ausztria ☐ Belgium ☐ Bulgária ☐ Ciprus ☐ Dánia ☐ Egyesült Királyság ☐ Franciaország ☐ Finnország ☐ Franciaország ☐ Görögország ☐ Hollandia ☐ Horvátország ☐ Írország ☐ Island ☐ Lengyelország ☐ Lettország ☐ Liechtenstein

NADH Incidens bejelentő lap (V1.2)

13 / 15

A hatóság kódja	A károsító jelölése
	☐ Litvánia ☐ Luxemburg ☐ Magyarország ☐ Málta ☐ Németország ☐ Norvégia ☐ Olaszország ☐ Portugália ☐ Románia ☐ Spanyolország ☐ Svájc ☐ Svédország ☐ Szlovákia ☐ Szlovénia
Bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidens más EGT-tagállam olyan adatkezelőjének, amely részben az incidens elhárítását szolgálja, vagy amely adatkezelő az incidens elhárítását szolgálja?	Igen/Nem
Adott más EGT-tagállami adatkezelő magatartását az adatkezelő, amelyről az incidens bejelentése vagy be fogja jelenteni.	
Bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidens EU-n kívüli adatkezelőjének hatóságok?	Igen/Nem
Az EU-n kívüli felügyeleti hatóságok listája, amelyekhez az adatkezelő bejelentette, vagy be fogja jelenteni az adatkezelő	

NADH Incidens bejelentő lap (V1.2)

14 / 15

A Hatóság kérdése	A közhatal válasz
Bejelentette, vagy be fogja-e jelenteni az adatkezelés az adatvédelmi incidenst egyéb EU-s hatóságok egyikének jogszabály alapján fennálló közzétételére alapján? (NIS irányelv, eIDAS rendelet)?	Igen/Nem
Egyéb EU hatóságok letárgya, amelyeknek az adatkezelés incidenst bejelentette vagy be fogja jelenteni az adatkezelés.	