

ADATKEZELÉSI ÉS ADATVÉDELMI SZABÁLYZAT

Dunaújvárosi Egyetem Bánki Donát Technikum

Jóváhagyta: Bartal Orsolya

Hatálybalépés: 2022. augusztus 1.

Dokumentum- és verziókövetés

Megnevezés	Adat
Dokumentum neve	Adatkezelési és adatvédelmi szabályzat
Intézmény	Dunaújvárosi Egyetem Bánki Donát Technikum
Hatálybalépés	2022.augusztus 1.
Felülvizsgálat	Jogszábeli, szervezeti, informatikai vagy adatkezelési változás esetén
Jóváahagyó	Intézményvezető
Adatvédelmi tisztviselő / kapcsolattartó	Bartal Orsolya

Dokumentumkezelési megjegyzés

A szabályzat véglegesítése előtt az intézmény **adatkezelői és adatfeldolgozói szerepeit, az adatvédelmi tisztviselő vagy adatvédelmi kapcsolattartó adatait, az alkalmazott informatikai rendszereket és szolgáltatókat, valamint az egyes adatkezelésekhez kapcsolódó megőrzési időket** össze kell hangolni a Dunaújvárosi Egyetem és a Bánki Donát Technikum hatályos dokumentumaival és gyakorlataival.

A szabályzat módosításait **verziószámmal, dátummal és a módosítás rövid megjelölésével** kell nyomon követni.

Módosítások nyilvántartása

Verzió	Dátum	Módosítás rövid leírása	Jóváahagyó
1.0	2022.08.1.	Első kiadás – tervezet	Intézményvezető

Tartalomjegyzék

1. A Szabályzat célja.....	6
2. A szabályzat hatálya	8
2.1. Személyi hatály.....	8
2.2. Tárgyi hatály.....	8
2.3. Területi hatály.....	9
2.4. Időbeli hatály	10
3. Jogszabályi és intézményi háttér.....	11
3.1. Az adatkezelés jogszabályi háttére.....	11
4. Alapfogalmak.....	12
5. Az adatkezelés alapelvei.....	14
5.1. Jogszerűség, tisztességesség és átláthatóság.....	14
5.2. Célhoz kötöttség	14
5.3. Adattakarékosság.....	14
5.4. Pontosság	14
5.5. Korlátozott tárolhatóság	14
5.6. Integritás és bizalmas jelleg	14
5.7. Elszámoltathatóság.....	15
5.8. Titoktartási kötelezettség	15
6. Az adatkezelő és a felelősségi rendszer.....	16
6.1. Az adatkezelő adatai.....	16
6.2. Az intézményvezető felelőssége.....	16
6.3. Az adatvédelmi tisztviselő vagy adatvédelmi kapcsolattartó	16
6.4. Az adatkezelésben részt vevő munkatársak felelőssége	17
6.5. Adatfeldolgozók és külső szolgáltatók.....	17
7. A kezelt személyes adatok főbb körei.....	18
7.1. Tanulói adatok	18
7.2. Szülők és törvényes képviselők adatai.....	18
7.3. Oktatók és munkatársak adatai	19
7.4. Egyéb érintettek és partnerek adatai	19
7.5. MICS/MIR és minőségirányítási tevékenységhez kapcsolódó adatok	19
8. Tanulói és szülői adatok kezelése	20
8.1. Különleges adatok kezelése	20
8.2. Szülők és törvényes képviselők adatainak kezelése	20
8.3. Tanulói adatok továbbítása.....	20
8.4. Titoktartás	20

9. Oktatók és munkatársak adatainak kezelése	21
9.1. Személyi iratok kezelése	21
9.2. Az adatokhoz való hozzáférés	21
9.3. Szakmai fejlődéssel és teljesítményértékeléssel kapcsolatos adatok	21
9.4. Az adatok továbbítása	21
9.5. Adatváltozás bejelentése	21
10. Az adatkezelés jogalapjai	22
10.1. Jogi kötelezettség teljesítése	22
10.2. Közérdekű feladat végrehajtása	22
10.3. Hozzájárulás	22
11. Elektronikus tanulmányi és intézményi rendszerek	23
11.1. KRÉTA rendszer adatkezelése	23
12. Microsoft 365 és Teams használata	24
13. MICS, MIR, önértékelés, elégedettségmérések és monitoring	25
13.1. Elégedettségmérések és visszajelzések	25
13.2. Oktatói egyéni cselekvési tervek és monitoring	26
13.3. Indikátorok és intézményi fejlesztések	26
13.4. Adatokhoz való hozzáférés és adattovábbítás	26
14. Honlap és elektronikus kommunikáció	27
15. Fotó- és videófelvevételek kezelése	28
15.1. Fényképek és videófelvevételek készítése	28
15.2. Felvevételek közzététele a honlapon és közösségi médiában	28
16. Honlap és közösségi média	29
17. Kamerarendszer	30
18. Papíralapú és elektronikus dokumentumok kezelése	31
18.1. Papíralapú dokumentumok kezelése	31
18.2. Elektronikus dokumentumok kezelése	31
19. Adattovábbítás és adatfeldolgozók	32
19.1. Adatfeldolgozók	32
19.2. Adattovábbítás általános szabályai	33
19.3. Külső megkeresés alapján történő adattovábbítás	33
19.4. Intézményen belüli adattovábbítás és hozzáférés	34
19.5. A tanulók adatainak továbbítása	34
19.6. Az alkalmazottak személyes adatainak továbbítása	34
19.7. Adatbiztonság és felelősségi szabályok	35
19.8. Az érintettek tájékoztatása és jogai	35

19.9. Külföldre, illetve harmadik országba történő adattovábbítás.....	35
19.10. Az adattovábbítás dokumentálása	36
20. Adatbiztonság és hozzáférési jogosultságok.....	37
20.1. Informatikai hozzáférések.....	37
20.2. Papíralapú adatok fizikai védelme.....	38
20.3. Adathordozók és elektronikus dokumentumok védelme	38
20.4. Biztonsági mentés és technikai védelem	38
20.5. A munkatársak adatbiztonsági felelőssége	39
21. Adatvédelmi incidensek kezelése.....	40
21.1. Az adatvédelmi incidens bejelentése	40
21.2. Az adatvédelmi incidens kivizsgálása.....	40
21.3. Az adatvédelmi incidens dokumentálása és nyilvántartása	41
21.4. Hatósági bejelentés	41
21.5. Az érintettek tájékoztatása.....	42
21.6. Intézkedési terv	42
22. Az érintettek jogai.....	43
23. Adatmegőrzés, törlés és selejtezés	44
24. Panaszok és adatvédelmi kérelmek	45
25. Ellenőrzés, oktatás és adatvédelmi tudatosság	46
26. A szabályzat felülvizsgálata	47
26.1. A felülvizsgálat szempontjai	47
26.2. A MICS/MIR szerepe	48
26.3. A szabályzat módosítása.....	48
26.4. A felülvizsgálat dokumentálása	48
27. Záró rendelkezések	50
27.1. A szabályzat hatálya	50
27.2. A szabályzat hatálybalépése	50
27.3. A szabályzat megismerése és hozzáférhetősége.....	50
27.4. A szabályzat karbantartása	50

1. A Szabályzat célja

Jelen Adatkezelési és Adatvédelmi Szabályzat célja, hogy a **Dunaújvárosi Egyetem Bánki Donát Technikumban** kezelt személyes adatok védelmének, az adatkezelések jogszerűségének, átláthatóságának és biztonságának egységes intézményi rendjét meghatározza.

A szabályzat célja továbbá, hogy az intézmény adatkezelési és adatfeldolgozási tevékenysége során érvényesítse a személyes adatok védelmére vonatkozó hatályos jogszabályi rendelkezéseket, különös tekintettel az Európai Parlament és a Tanács (EU) 2016/679 rendeletében meghatározott adatvédelmi alapelvekre.

Az intézmény a személyes adatokat kizárólag meghatározott és jogszerű célból, a cél megvalósításához szükséges mértékben, megfelelő jogalap alapján és csak a szükséges ideig kezeli.

A szabályzat célja, hogy egységesen meghatározza:

- az intézményben folyó adatkezelés és adattovábbítás alapvető szabályait;
- az intézmény által kezelt személyes adatok védelmének rendjét;
- az egyes adatkezelések célját, valamint az adatkezelés során érvényesítendő alapelveket;
- az adatkezelésben és adatfeldolgozásban részt vevő személyek feladatait és felelősségét;
- a személyes adatokhoz hozzáférésre jogosult személyek körének meghatározására vonatkozó alapvető szabályokat;
- az adattovábbítás rendjét és feltételeit;
- az adatok helyesbítésének, törlésének, valamint szükség szerinti korlátozásának rendjét;
- az érintettek személyes adataik kezelésével kapcsolatos jogait és azok érvényesítésének lehetőségeit;
- a személyes adatok megfelelő biztonságának biztosítására szolgáló alapvető szervezési és technikai követelményeket;
- az adatvédelmi incidensek megelőzésének, bejelentésének és kezelésének alapvető rendjét.

A szabályzat célja továbbá annak biztosítása, hogy az intézmény valamennyi adatkezelési tevékenysége során tiszteletben tartsa az érintettek személyes adatok védelméhez és információs önrendelkezéshez való jogát.

Az intézmény ennek érdekében különösen érvényesíti a személyes adatok kezelésére vonatkozó jogszerűség, tisztességes eljárás és átláthatóság, a célhoz kötöttség, az adattakarékosság, a pontosság, a korlátozott tárolhatóság, valamint az integritás és bizalmas jelleg elvét.

A szabályzat célja az is, hogy az intézményben kezelt személyes adatokkal kapcsolatos feladatok és felelősségi körök egyértelműen meghatározottak legyenek. Az adatkezelésben

részt vevő személyek kötelesek a tudomásukra jutott személyes adatokat bizalmasan kezelni, és azokat kizárólag feladatuk ellátásához szükséges mértékben felhasználni.

Jelen szabályzat az intézményben folyó oktatási, nevelési, szakképzési, foglalkoztatási, ügyviteli és szervezési tevékenység során megvalósuló adatkezelések egységes keretét biztosítja. A szabályzat alkalmazásával az intézmény törekszik arra, hogy a személyes adatok kezelése minden esetben ellenőrizhető, biztonságos és az érintettek számára átlátható módon történjen.

2. A szabályzat hatálya

2.1. Személyi hatály

Jelen szabályzat személyi hatálya kiterjed a **Dunaújvárosi Egyetem Bánki Donát Technikumra**, valamint mindazon természetes személyekre, akiknek személyes adatait az intézmény a feladatainak ellátása során kezeli.

A szabályzat rendelkezései különösen az alábbi személyekre terjednek ki:

- az intézmény vezetőire;
- az intézmény valamennyi oktatójára és foglalkoztatottjára;
- a technikai és adminisztratív dolgozókra;
- a munkavégzésre irányuló jogviszony létesítésére jelentkező személyekre;
- az intézmény tanulóira;
- a tanulók szüleire és törvényes képviselőire;
- az intézménnyel szerződéses vagy egyéb együttműködési jogviszonyban álló természetes személyekre;
- az intézménnyel kapcsolatba kerülő, illetve az intézmény által szervezett tevékenységben részt vevő személyekre;
- az intézmény területére belépő és ott személyes adatkezeléssel érintett személyekre;
- minden olyan természetes személyre, akinek személyes adata az intézmény működése során az intézmény kezelésébe kerül.

A szabályzat rendelkezéseinek betartása kötelező minden olyan személy számára, aki az intézmény nevében, az intézmény feladatellátásával összefüggésben vagy az intézmény rendelkezésére álló rendszerekben személyes adatot kezel.

Az intézmény vezetői és munkatársai a munkájuk során tudomásukra jutott személyes adatokat kizárólag feladatellátásukhoz szükséges mértékben használhatják fel, és kötelesek azok bizalmas kezelésére.

A szabályzat rendelkezéseit a munkaviszony, foglalkoztatási jogviszony vagy egyéb jogviszony létesítését megelőző eljárások során is alkalmazni kell, amennyiben azok személyes adatok kezelésével járnak.

A jogviszony megszűnése nem mentesít az érintett személyes adatokkal kapcsolatban fennálló titoktartási és adatvédelmi kötelezettségek alól.

2.2. Tárgyi hatály

A szabályzat tárgyi hatálya kiterjed az intézmény valamennyi személyes adatot érintő adatkezelési és adatfeldolgozási tevékenységére, függetlenül attól, hogy az adatkezelés milyen formában vagy milyen technikai eszközzel történik.

A szabályzat hatálya kiterjed különösen:

- a tanulók személyes adatainak nyilvántartására és kezelésére;
- a szülők és törvényes képviselők személyes adatainak kezelésére;
- az oktatók és egyéb munkatársak személyes adatainak kezelésére;
- a munkára jelentkezők és pályázók személyes adatainak kezelésére;
- a szerződéses partnerekkel és együttműködő szervezetekkel kapcsolatos természetes személyek adatainak kezelésére;
- az intézményi nyilvántartásokban szereplő személyes adatok kezelésére;
- a papíralapú iratokban és nyilvántartásokban szereplő személyes adatok kezelésére;
- az elektronikus nyilvántartásokban és informatikai rendszerekben kezelt személyes adatokra;
- a digitális oktatási, tanulmányi és együttműködési rendszerekben kezelt adatokra;
- az elektronikus levelezés és egyéb elektronikus kommunikáció során kezelt személyes adatokra;
- a kép-, hang- és videófelvevételek kezelésére;
- az intézményi honlapon és közösségi médiafelületeken megjelenő személyes adatokra;
- az intézmény területén működő kamerarendszerrel összefüggő adatkezelésekre;
- a belépéssel, az intézmény területén tartózkodással vagy rendezvényeken való részvétellel összefüggésben kezelt személyes adatokra;
- a személyes adatokat tartalmazó számítástechnikai eszközökre, nyilvántartási rendszerekre és adathordozókra;
- a személyes adatok tárolására, továbbítására, felhasználására, archiválására és törlésére;
- a MICS és MIR működésével összefüggő személyes adatkezelésekre, így különösen az elégedettségmérések, önértékelések, monitoringtevékenységek és fejlesztési folyamatok során kezelt személyes adatokra.

A szabályzat rendelkezéseit az intézmény tulajdonában, használatában vagy kezelésében álló azon informatikai eszközök, rendszerek és alkalmazások használata során is alkalmazni kell, amelyek személyes adatok kezelésére alkalmasak.

A szabályzat hatálya nemcsak az adatok tényleges feldolgozására és felhasználására terjed ki, hanem azok gyűjtésére, rögzítésére, rendszerezésére, tárolására, megismerésére, lekérdezésére, továbbítására, nyilvánosságra hozatalára, korlátozására és törlésére is.

2.3. Területi hatály

A szabályzat területi hatálya elsősorban a **Dunaújvárosi Egyetem Bánki Donát Technikum által használt intézményi területekre és helyiségekre** terjed ki.

A szabályzat rendelkezéseit azonban akkor is alkalmazni kell, ha az adatkezelés nem az intézmény területén történik, hanem például:

- intézményen kívüli rendezvényen;
- tanulmányi kiránduláson;
- versenyen;
- külső helyszínen szervezett oktatási vagy szakmai programon;
- duális képzőhelyhez kapcsolódó együttműködés során;
- online oktatás vagy digitális munkavégzés során;
- az intézmény által használt távoli elérésű elektronikus rendszerben.

Az adatkezelés helyétől függetlenül jelen szabályzat rendelkezéseit kell alkalmazni, amennyiben az adatkezelés az intézmény feladatellátásához kapcsolódik.

2.4. Időbeli hatály

Jelen szabályzat az intézményvezető jóváhagyásával és a szabályzatban meghatározott időpontban lép hatályba, és visszavonásig vagy módosításig hatályos.

A szabályzat rendelkezéseit a hatálybalépését követően megkezdett valamennyi adatkezelési tevékenységre alkalmazni kell.

A szabályzat hatálybalépésekor már folyamatban lévő adatkezeléseket is felül kell vizsgálni abból a szempontból, hogy azok megfelelnek-e a szabályzat rendelkezéseinek és a hatályos adatvédelmi követelményeknek.

Az egyes személyes adatok megőrzésének időtartamát nem önmagában jelen szabályzat, hanem az adott adatkezelés célja, a vonatkozó jogszabályok, az iratkezelési szabályok és egyéb intézményi előírások határozzák meg.

A jogviszony megszűnése önmagában nem jelenti az összes személyes adat azonnali törlését. Az adatokat az intézmény csak addig őrizheti meg, ameddig azt jogszabály, jogi kötelezettség, az intézmény feladatának ellátása vagy az adott adatkezelés célja indokolja.

3. Jogszabályi és intézményi háttér

3.1. Az adatkezelés jogszabályi háttere

A Dunaújvárosi Egyetem Bánki Donát Technikum adatkezelési és adatfeldolgozási tevékenységét a hatályos európai uniós és magyar jogszabályok, valamint az intézményre irányadó belső szabályozások alapján végzi.

Az intézmény adatkezelése során különösen az alábbi jogszabályokat és szabályozó dokumentumokat kell figyelembe venni:

- Magyarország Alaptörvénye;
- az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről, a továbbiakban: **GDPR**;
- a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, a továbbiakban: **Infotv.**;
- a 2019. évi LXXX. törvény a szakképzésről, a továbbiakban: **Szkt.**;
- a szakképzésről szóló törvény végrehajtásáról szóló **12/2020. (II. 7.) Korm. rendelet**;
- a 2011. évi CXCV. törvény a nemzeti köznevelésről, különösen azokban az esetekben, amikor annak rendelkezései az intézmény működésére vagy az érintett személyek jogaira irányadók;
- a nevelési-oktatási intézmények működéséről szóló **20/2012. (VIII. 31.) EMMI rendelet**, az alkalmazandó rendelkezések tekintetében;
- a 2012. évi I. törvény a Munka Törvénykönyvéről;
- a 2013. évi LXXVII. törvény a felnőttképzésről, amennyiben az intézmény tevékenysége során annak rendelkezései alkalmazandók;
- az iratkezelésre, az irattári megőrzésre és a levéltári anyag védelmére vonatkozó hatályos jogszabályok;
- az államháztartási, számviteli, adózási és társadalombiztosítási kötelezettségekkel összefüggő adatkezelések esetében az adott adatkezelésre vonatkozó külön jogszabályok;
- a kép-, hang- és videófelvételek, valamint az elektronikus kommunikáció során kezelt személyes adatok esetében az adott adatkezelésre irányadó egyéb hatályos jogszabályok.

A felsorolás nem teljes körű. Az intézmény minden adatkezelése során az adott adatkezelés céljára és jellegére vonatkozó hatályos jogszabályokat is figyelembe veszi.

4. Alapfogalmak

A jelen kézikönyv alkalmazásában az alábbi fogalmak értelmezése irányadó:

Érintett: azonosított vagy azonosítható természetes személy, akire a személyes adat vonatkozik.

Személyes adat: azonosított vagy azonosítható természetes személyre vonatkozó bármely információ.

Különleges személyes adat: olyan személyes adat, amely többek között az érintett egészségi állapotára, genetikai vagy biometrikus adataira vonatkozik, illetve amelynek kezelése fokozott adatvédelmi követelményekhez kötött.

Adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így különösen az adatok gyűjtése, rögzítése, rendszerezése, tárolása, lekérdezése, felhasználása, továbbítása, korlátozása, törlése vagy megsemmisítése.

Adatkezelés korlátozása: a tárolt személyes adatok megjelölése abból a célból, hogy azok további kezelése korlátozott legyen.

Adatkezelő: az a természetes vagy jogi személy, illetve szervezet, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.

Adatfeldolgozó: az a természetes vagy jogi személy, illetve szervezet, amely az adatkezelő nevében és utasításai alapján személyes adatokat kezel.

Címzett: az a természetes vagy jogi személy, közhatalmi szerv vagy egyéb szervezet, akivel vagy amellyel a személyes adatot közlik.

Harmadik fél: az érintetten, az adatkezelőn, az adatfeldolgozón, valamint az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt eljáró, adatkezelésre felhatalmazott személyeken kívüli természetes vagy jogi személy, illetve szervezet.

Az érintett hozzájárulása: az érintett akaratának önkéntes, konkrét, megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel beleegyezését adja személyes adatainak kezeléséhez.

Adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Profilalkotás: személyes adatok automatizált kezelésének olyan formája, amelynek során az adatokat valamely természetes személy bizonyos jellemzőinek értékelésére, elemzésére vagy előrejelzésére használják.

Álnevesítés: a személyes adatok olyan módon történő kezelése, amelynek eredményeként további, külön tárolt információk felhasználása nélkül nem állapítható meg, hogy az adat mely konkrét természetes személyre vonatkozik.

Anonimizálás: olyan eljárás, amelynek eredményeként az adat véglegesen nem kapcsolható vissza az érintetthez, ezért az már nem minősül személyes adatnak.

Nyilvántartási rendszer: a személyes adatok bármely strukturált állománya, amely meghatározott ismérvek alapján hozzáférhető.

Adattovábbítás: a személyes adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Hozzáférés: a személyes adatok vagy az azokat tartalmazó nyilvántartás megismerésének lehetősége.

Betekintés: a nyilvántartott személyes adatok részleges vagy teljes megismerése jogosultság alapján.

Adatmegsemmisítés: az adatokat tartalmazó adathordozó olyan fizikai vagy technikai megsemmisítése, amelynek eredményeként az adatok helyreállítása nem lehetséges.

Adattörlés: az adatok olyan módon történő eltávolítása, amelynek eredményeként azok helyreállítása nem lehetséges vagy aránytalan nehézséggel jár.

Közérdekű adat: az intézmény közfeladatának ellátásával összefüggésben keletkezett vagy kezelésében lévő, a személyes adat fogalma alá nem tartozó, bármilyen formában rögzített információ.

Közérdekből nyilvános adat: olyan adat, amelynek nyilvánosságát vagy megismerhetőségét jogszabály közérdekből elrendeli.

Adatvédelem: a személyes adatok kezelésére vonatkozó jogszabályi, szervezési és technikai követelmények összessége, amelyek az érintettek jogainak és szabadságainak védelmét szolgálják.

5. Az adatkezelés alapelvei

Az intézmény a személyes adatok kezelése során a vonatkozó jogszabályok, különösen az adatvédelmi jogszabályok és a GDPR rendelkezéseinek megfelelően jár el. Az adatkezelés során az intézmény az alábbi alapelveket alkalmazza:

5.1. Jogszerűség, tisztességeség és átláthatóság

Az intézmény a személyes adatokat kizárólag megfelelő jogalap alapján, jogszerűen, tisztességesen és az érintettek számára átlátható módon kezeli. Az érintettek számára az adatkezelés céljáról, jogalapjáról és lényeges körülményeiről megfelelő tájékoztatást kell biztosítani.

5.2. Célhoz kötöttség

Személyes adat kizárólag meghatározott, egyértelmű és jogszerű célból kezelhető. Az adatkezelésnek annak teljes időtartama alatt meg kell felelnie az adatkezelés eredeti céljának. Az intézmény a személyes adatokat a megjelölt céltól eltérő célra kizárólag jogszabályban **meghatározott esetben vagy megfelelő jogalap megléte esetén használhatja fel.**

5.3. Adattakarékosság

Az intézmény kizárólag olyan személyes adatokat kezel, amelyek az adatkezelés céljának megvalósításához szükségesek és azzal arányban állnak. Nem gyűjthető és nem tárolható olyan személyes adat, amely az adott adatkezelési cél teljesítéséhez nem szükséges.

5.4. Pontosság

Az intézmény törekszik arra, hogy a kezelt személyes adatok pontosak, szükség esetén naprakészek legyenek. A pontatlan vagy hiányos személyes adatokat megfelelő eljárás keretében helyesbíteni, kiegészíteni vagy törölni kell.

5.5. Korlátozott tárolhatóság

A személyes adatok csak addig őrizhetők meg, ameddig az adatkezelés céljának megvalósításához szükséges, illetve ameddig azt jogszabály vagy az intézmény iratkezelési és megőrzési szabályai előírják. A továbbiakban szükségtelen személyes adatokat megfelelő módon törölni vagy megsemmisíteni kell.

5.6. Integritás és bizalmas jelleg

Az intézmény megfelelő technikai és szervezési intézkedésekkel gondoskodik a személyes adatok biztonságáról. Biztosítani kell az adatok védelmét a jogosulatlan vagy jogellenes hozzáféréssel, megváltoztatással, nyilvánosságra hozattal, elvesztéssel, megsemmisítéssel vagy károsodással szemben.

A személyes adatokhoz kizárólag azok a személyek férhetnek hozzá, akiknek az adatok kezelése feladataik ellátásához szükséges, és erre megfelelő jogosultsággal rendelkeznek.

5.7. Elszámoltathatóság

Az intézmény felelős azért, hogy az adatkezelés megfeleljen a vonatkozó adatvédelmi követelményeknek, és szükség esetén képes legyen ennek igazolására. Ennek érdekében az intézmény megfelelő szabályozási, szervezési és technikai intézkedéseket alkalmaz.

Az intézmény az új adatkezelési folyamatok, elektronikus rendszerek vagy digitális megoldások kialakítása során már a tervezés szakaszában figyelembe veszi az adatvédelmi követelményeket, valamint biztosítja, hogy az adatkezelés alapértelmezés szerint csak a szükséges mértékben történjen.

5.8. Titoktartási kötelezettség

Az intézmény munkatársai a feladataik ellátása során tudomásukra jutott személyes adatokat kötelesek bizalmasan kezelni. A személyes adatok harmadik személy számára kizárólag jogszabályi felhatalmazás, az érintett hozzájárulása vagy más megfelelő jogalap alapján továbbíthatók vagy tehetők hozzáférhetővé.

Az adatkezelésben vagy adatfeldolgozásban közreműködő személyek a tudomásukra jutott személyes adatokat kizárólag munkaköri vagy feladatellátási kötelezettségük teljesítéséhez használhatják fel. A személyes adatok saját célra történő felhasználása tilos.

6. Az adatkezelő és a felelősségi rendszer

6.1. Az adatkezelő adatai

Adatkezelő neve: Dunaújvárosi Egyetem Bánki Donát Technikum

Székhely: 2400 Dunaújváros, Tácsics M. u. 1-1.

Telefon: +36 30 299 5437

E-mail: titkarsag@bankisuli.hu

Képviselő: Bartal Orsolya igazgató

Az intézmény a személyes adatok kezelése során adatkezelőként jár el azokban az esetekben, amikor az adatkezelés célját és eszközeit önállóan vagy más szervezettel együtt határozza meg.

Amennyiben valamely adatkezelési folyamatban az intézmény adatfeldolgozóként vagy közös adatkezelőként vesz részt, az adatkezelésben betöltött szerepet a vonatkozó jogszabályok, megállapodások és intézményi szabályozások alapján kell meghatározni.

6.2. Az intézményvezető felelőssége

Az intézményvezető felel az intézmény adatvédelmi működésének megfelelő szervezéséért és az adatkezelés jogszerű feltételeinek biztosításáért.

Feladata különösen:

- az adatvédelmi követelmények intézményi érvényesülésének biztosítása;
- a szükséges szervezési és adatbiztonsági intézkedések megtétele;
- az adatkezelési szabályzat és a kapcsolódó belső szabályozások betartatásának biztosítása;
- az adatkezelésben részt vevő munkatársak megfelelő tájékoztatásának és szükség szerinti felkészítésének biztosítása;
- az adatvédelmi incidensekkel kapcsolatos intézkedések megtétele vagy azok elrendelése;
- az érintettek jogainak érvényesüléséhez szükséges intézményi feltételek biztosítása.

Az intézményvezető az adatvédelmi feladatok ellátására munkatársat vagy más kijelölt személyt bízhat meg, azonban ez nem érinti az intézmény, mint adatkezelő jogszabályban meghatározott felelősségét.

6.3. Az adatvédelmi tisztviselő vagy adatvédelmi kapcsolattartó

Az intézmény adatvédelmi tisztviselője, illetve az intézmény által kijelölt adatvédelmi kapcsolattartó közreműködik az adatvédelmi követelmények érvényesülésének elősegítésében.

Név: Bartal Orsolya

Beosztás: igazgató

E-mail: bartalo@bankisuli.hu

Telefon: +36-30/2995437

Feladata különösen:

- az adatvédelmi megfelelés figyelemmel kísérése;
- az intézményvezetés és a munkatársak tájékoztatása és tanácsadása;
- közreműködés az adatkezelési folyamatok adatvédelmi szempontú ellenőrzésében;
- közreműködés az adatvédelmi incidensek kezelésében;
- az érintetti jogok gyakorlásával kapcsolatos eljárások támogatása;
- kapcsolattartás a felügyeleti hatósággal, szükség esetén a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

6.4. Az adatkezelésben részt vevő munkatársak felelőssége

Az intézmény valamennyi munkatársa köteles a feladatai ellátása során tudomására jutott személyes adatokat bizalmasan kezelni és azokat kizárólag a munkaköri vagy feladatellátási kötelezettségeinek teljesítéséhez szükséges mértékben használni.

A munkatárs különösen köteles:

- a személyes adatokat kizárólag jogszerűen és a meghatározott cél érdekében kezelni;
- az adatkezelés során az intézményi szabályzatokat és utasításokat betartani;
- megakadályozni, hogy illetéktelen személy személyes adatokhoz férjen hozzá;
- a tudomására jutott adatvédelmi incidenst vagy annak gyanúját haladéktalanul jelezni;
- a személyes adatokat saját céljára nem felhasználni;
- a munkavégzés során tudomására jutott személyes adatokat a titoktartási kötelezettségnek megfelelően kezelni.

6.5. Adatfeldolgozók és külső szolgáltatók

Amennyiben az intézmény személyes adatok kezeléséhez külső szolgáltatót vagy adatfeldolgozót vesz igénybe, az adatfeldolgozó csak az intézmény utasításai alapján és a vonatkozó jogszabályoknak megfelelően járhat el.

Az adatfeldolgozó igénybevételének feltételeit megfelelő írásbeli megállapodásban vagy szerződésben kell rögzíteni. Az adatfeldolgozó köteles biztosítani a személyes adatok megfelelő biztonságát, valamint a tudomására jutott személyes adatokat kizárólag az intézmény által meghatározott célból és mértékben kezelheti.

7. A kezelt személyes adatok főbb körei

Az intézmény működése során a feladatellátásához, a jogszabályi kötelezettségek teljesítéséhez és az intézményi folyamatok támogatásához különböző személyes adatok kezelése történik. Az intézmény kizárólag a meghatározott célhoz szükséges, megfelelő és releváns személyes adatokat kezeli.

7.1. Tanulói adatok

A tanulókkal kapcsolatban kezelt adatok különösen:

- név, születési név;
- születési hely és idő;
- anyja neve;
- lakóhely, tartózkodási hely;
- elérhetőségi adatok;
- oktatási azonosító;
- bankszámlaszám (KRÉTA, NSZFH)
- jogszabály alapján szükséges azonosító adatok;
- tanulói jogviszonyra vonatkozó adatok;
- osztályba és képzésbe sorolás adatai;
- tanulmányi és értékelési adatok;
- hiányzásokra vonatkozó adatok;
- vizsgákkal és teljesítménnyel kapcsolatos adatok;
- fegyelmi és kártérítési ügyekhez kapcsolódó adatok;
- a jogszabály alapján kezelhető, különleges kategóriába tartozó adatok (szakszolgálati vélemények, orvosi, szakorvosi és kórházi dokumentumok);
- a tanulói jogviszony teljesítéséhez szükséges egyéb adatok.

7.2. Szülők és törvényes képviselők adatai

A szülőkkel, illetve törvényes képviselőkkel kapcsolatban az intézmény különösen:

- nevet;
- lakcímet;
- telefonszámot;
- e-mail-címet;
- egyéb kapcsolattartási adatokat;
- a képviseleti jogosultságra vonatkozó adatokat, határozatokat, bíróségi végzéseket kezeli.

7.3. Oktatók és munkatársak adatai

A munkatársakkal kapcsolatban kezelt adatok különösen:

- személyazonosító és kapcsolattartási adatok;
- foglalkoztatási és munkajogi adatok;
- végzettségre, szakképesítésre és szakmai tapasztalatra vonatkozó adatok;
- munkakörre és feladatellátásra vonatkozó adatok;
- illetmény-, bér- és juttatási adatok;
- adózással és társadalombiztosítással kapcsolatos adatok;
- bankszámlaszám;
- munkavégzéshez, szabadsághoz és egyéb munkáltatói feladatokhoz kapcsolódó adatok;
- jogszabály alapján vezetett nyilvántartásokhoz szükséges adatok;
- szakmai fejlődéssel, teljesítményértékeléssel és egyéni cselekvési tervekkel kapcsolatos adatok.

7.4. Egyéb érintettek és partnerek adatai

Az intézmény működése során szükség lehet az együttműködő partnerek, gyakorlati képzőhelyek, szolgáltatók, szerződéses partnerek és egyéb kapcsolattartók személyes adatainak kezelésére.

Az ilyen adatok köre elsősorban a kapcsolattartáshoz, a szerződéses vagy együttműködési kötelezettségek teljesítéséhez, valamint az intézményi programok és rendezvények lebonyolításához szükséges adatokra terjed ki.

7.5. MICS/MIR és minőségirányítási tevékenységhez kapcsolódó adatok

Az intézmény minőségirányítási és fejlesztési tevékenysége során személyes adatok kezelése történhet különösen:

- elégedettségmérések;
- kérdőíves visszajelzések;
- monitoringtevékenység;
- önértékelés;
- teljesítményértékelés;
- fejlesztési és intézkedési tervek;
- szakmai fejlődés;
- intézményi fejlesztési folyamatok során.

A minőségirányítási célú adatkezelések során is érvényesül a célhoz kötöttség és az adattakarékosság elve.

8. Tanulói és szülői adatok kezelése

Az intézmény a tanulók személyes adatait a tanulói jogviszony létesítésével és fenntartásával, az oktatási és nevelési feladatok ellátásával, a tanulók értékelésével, vizsgáztatásával, hiányzásainak nyilvántartásával, valamint a jogszabályban előírt nyilvántartások vezetésével összefüggésben kezeli.

A tanulói adatok kezelése során az intézmény kizárólag a meghatározott célhoz szükséges mértékben kezelhet személyes adatokat. Az adatkezelés során különösen figyelembe kell venni a célhoz kötöttség, az adattakarékosság, a pontosság és a bizalmasság követelményeit.

A tanulói adatok kezelése történhet papíralapú és elektronikus formában, az intézmény által használt, jogszerűen alkalmazott nyilvántartásokban és informatikai rendszerekben.

A tanulói adatokhoz csak azok a vezetők, oktatók és munkatársak férhetnek hozzá, akiknek az adott adat megismerése munkaköri feladatuk ellátásához szükséges. A hozzáférés mértékét az ellátott feladat és a jogosultság határozza meg.

8.1. Különleges adatok kezelése

A különleges kategóriába tartozó személyes adatok – így különösen az egészségi állapotra, sajátos nevelési igényre, beilleszkedési, tanulási vagy magatartási nehézségre vonatkozó adatok – kizárólag megfelelő jogalap alapján, az adott feladat ellátásához szükséges mértékben kezelhetők.

Ezen adatokhoz csak az arra jogosult, illetve az adott feladat ellátásában közreműködő személyek férhetnek hozzá.

8.2. Szülők és törvényes képviselők adatainak kezelése

A szülők és törvényes képviselők adatait az intézmény elsősorban a tanulóval kapcsolatos kapcsolattartás, tájékoztatás, valamint a jogszabályban meghatározott szülői és törvényes képviselői jogok gyakorlásának biztosítása érdekében kezeli.

Az adatok kezelésénél figyelembe kell venni a szülő, illetve törvényes képviselő képviseleti jogosultságát. Az intézmény az adatokat és a tanulóval kapcsolatos információkat csak az arra jogosult személy részére adhatja át.

8.3. Tanulói adatok továbbítása

Tanulói személyes adatok harmadik személy vagy szerv részére kizárólag megfelelő jogalap alapján és a szükséges mértékben továbbíthatók. A jogszabály alapján kötelező adattovábbítás esetén az érintett hozzájárulása nem feltétlenül szükséges.

Az adattovábbításra az intézmény vezetője, illetve az általa kijelölt, megfelelő jogosultsággal rendelkező személy jogosult.

8.4. Titoktartás

Az intézmény oktatóit és munkatársait a munkájuk során tudomásukra jutott, tanulókkal és családjukkal kapcsolatos személyes adatok és bizalmas információk tekintetében titoktartási kötelezettség terheli.

A titoktartási kötelezettség az érintett munkatárs foglalkoztatási jogviszonyának megszűnését követően is fennállhat, amennyiben azt jogszabály vagy az adat jellegéből fakadó kötelezettség előírja.

9. Oktatók és munkatársak adatainak kezelése

Az intézmény az oktatók és egyéb munkatársak személyes adatait a foglalkoztatási jogviszony létesítésével, fenntartásával és megszüntetésével, a munkáltatói jogok gyakorlásával, a munkabér és egyéb juttatások megállapításával és kifizetésével, valamint a jogszabályban meghatározott nyilvántartási és adatszolgáltatási kötelezettségek teljesítésével összefüggésben kezeli.

Az intézmény kezeli különösen a munkaviszonyhoz, a munkakörhöz, a végzettséghez és szakképesítéshez, a munkabérhez és juttatásokhoz, valamint az adó- és társadalombiztosítási **kötelezettségek teljesítéséhez szükséges adatokat.**

9.1. Személyi iratok kezelése

A munkatársak személyi iratai a foglalkoztatási jogviszony létesítésével, fennállásával és megszűnésével kapcsolatos, személyes adatokat tartalmazó dokumentumokat foglalják magukban.

A személyi iratokban kizárólag olyan adat és megállapítás szerepelhet, amelynek megfelelő jogszabályi, munkáltatói, hatósági vagy egyéb jogszerű alapja van.

A személyi iratokhoz való hozzáférés csak az intézményben meghatározott jogosultság alapján történhet.

9.2. Az adatokhoz való hozzáférés

A munkatársak személyes adataihoz csak azok a vezetők és munkatársak férhetnek hozzá, akiknek az adatok megismerése munkaköri feladatuk ellátásához szükséges.

A bér-, illetmény-, egészségügyi, adózási, társadalombiztosítási és egyéb bizalmas adatok kezelése során fokozottan biztosítani kell a jogosulatlan hozzáférés megakadályozását.

9.3. Szakmai fejlődéssel és teljesítményértékeléssel kapcsolatos adatok

Az intézmény a munkatársak szakmai fejlődésével, továbbképzéseivel, teljesítményértékelésével, szakmai tevékenységével és egyéni cselekvési terveivel kapcsolatos adatokat a munkáltatói és intézményi fejlesztési feladatok ellátása érdekében kezelheti.

Az ilyen adatokhoz kizárólag a feladatellátáshoz szükséges személyek férhetnek hozzá. Az adatok felhasználása során biztosítani kell, hogy azok csak a meghatározott munkáltatói, értékelési vagy fejlesztési célra kerüljenek felhasználásra.

9.4. Az adatok továbbítása

A munkatársak személyes adatai kizárólag jogszabályi kötelezettség, jogszerű munkáltatói feladat, szerződéses kötelezettség vagy egyéb megfelelő jogalap alapján továbbíthatók.

Az adattovábbítás során az intézménynek biztosítani kell, hogy csak a továbbítás céljához szükséges adatok kerüljenek átadásra.

9.5. Adatváltozás bejelentése

A munkatárs köteles az intézmény részére megadott személyes adataiban bekövetkező, a foglalkoztatási jogviszony szempontjából releváns változásokat a munkáltató részére bejelenteni, és szükség esetén az adatváltozást igazoló dokumentumot rendelkezésre bocsátani.

Az intézmény az adatokat a bejelentett változás alapján, a vonatkozó jogszabályoknak megfelelően aktualizálja.

10. Az adatkezelés jogalapjai

Az intézmény személyes adatokat kizárólag meghatározott, jogszerű célból és megfelelő jogalap alapján kezel.

Az adatkezelés jogalapja az adott adatkezelés céljától és körülményeitől függően különösen az alábbi lehet:

10.1. Jogi kötelezettség teljesítése

Az intézmény jogszabályban meghatározott kötelezettségeinek teljesítése során személyes adatokat kezelhet. Ide tartozhatnak különösen:

- a köznevelési és szakképzési nyilvántartások vezetése,
- a tanulói jogviszonnyal kapcsolatos kötelezettségek teljesítése,
- a munkajogi és foglalkoztatási kötelezettségek teljesítése,
- az adó- és járulékkötelezettségek teljesítése,
- a jogszabályban előírt adatszolgáltatások teljesítése.

10.2. Közérdekű feladat végrehajtása

Az intézmény közfeladatot ellátó szervezatként a jogszabályban meghatározott oktatási, nevelési és egyéb intézményi feladatok végrehajtása során személyes adatokat kezelhet.

Az adatkezelés ebben az esetben az intézmény közfeladatának ellátásához szükséges mértékben történik.

10.3. Hozzájárulás

Hozzájáruláson alapuló adatkezelésre olyan esetekben kerülhet sor, amikor az adatkezelés más jogalapon nem végezhető el, és az érintett hozzájárulása szükséges.

Ilyen lehet különösen:

- fényképek és videófelvevételek közzététele,
- intézményi eseményekről készült felvételek publikálása,
- marketing- vagy tájékoztató jellegű kommunikáció egyes formái.

A hozzájárulásnak önkéntesnek, konkrétan, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie. Az érintett a hozzájárulását a jogszabályi feltételek szerint visszavonhatja.

11. Elektronikus tanulmányi és intézményi rendszerek

Az intézmény feladatainak ellátása során elektronikus tanulmányi és intézményi rendszereket használ. E rendszerek célja az oktatási, tanulmányi, adminisztratív és szervezési feladatok támogatása, valamint az intézményi működéshez szükséges adatok kezelése.

Az elektronikus rendszerekben személyes adatok kezelése kizárólag az adott rendszer céljának megfelelően, a szükséges mértékben és megfelelő adatkezelési jogalap alapján történhet.

A rendszerekhez való hozzáférés személyhez kötött, és a felhasználó munkaköréhez, illetve feladataihoz igazodik. A felhasználók csak azokhoz az adatokhoz férhetnek hozzá, amelyek megismerése feladataik ellátásához szükséges.

A felhasználói fiókok, belépési adatok és jelszavak más személy részére nem adhatók át. A jogosulatlan hozzáférés megakadályítása érdekében a felhasználók kötelesek a hozzáférési adataikat bizalmasan kezelni.

A hozzáférési jogosultságokat a munkakör vagy feladat változása esetén, valamint a foglalkoztatási vagy egyéb jogviszony megszűnésekor felül kell vizsgálni, és szükség esetén módosítani vagy megszüntetni.

11.1. KRÉTA rendszer adatkezelése

Az intézmény a **KRÉTA rendszert** tanulmányi, oktatási és adminisztratív célokra használja.

A KRÉTA rendszerben kezelt személyes adatok tekintetében az intézmény adatkezelőként jár el, míg a KRÉTA szolgáltatója az adatkezeléshez kapcsolódó feladatok tekintetében adatfeldolgozóként működik.

A KRÉTA rendszerben az intézményi feladatellátáshoz kapcsolódóan különösen az alábbi adatok kezelhetők:

- tanulói adatok,
- szülői és törvényes képviselői adatok,
- osztályzatok és egyéb értékelési adatok,
- jelenléti adatok,
- hiányzások és azok igazolására vonatkozó adatok,
- elektronikus üzenetek,
- órarendek,
- pedagógusok és egyéb felhasználók adatai.

A KRÉTA rendszerhez való hozzáférés a felhasználó feladat- és hatásköréhez igazodik. A rendszerben csak a feladatellátáshoz szükséges adatok ismerhetők meg.

Az intézmény törekszik arra, hogy a KRÉTA rendszerben kezelt adatokhoz való hozzáférés és azok felhasználása megfeleljen az adatbiztonsági és adatvédelmi követelményeknek.

12. Microsoft 365 és Teams használata

Az intézmény a Microsoft 365 szolgáltatásait, valamint a Microsoft Teams alkalmazást oktatási, kapcsolattartási, együttműködési és adminisztrációs célokra használhatja.

A Microsoft 365 és a Teams használata során személyes adatok kezelése történhet. A kezelt adatok körét az alkalmazott szolgáltatás és az adott intézményi feladat határozza meg.

Kezelt adatok különösen:

- név,
- intézményi e-mail-cím,
- dokumentumok és egyéb feltöltött állományok,
- OneDrive-ban tárolt állományok,
- Teams-ben folytatott kommunikációhoz kapcsolódó adatok,
- online értekezletekhez és megbeszélésekhez kapcsolódó adatok.

A Microsoft 365 és a Teams használata során az intézményi adatokat csak a feladatellátáshoz szükséges mértékben és az intézmény által engedélyezett módon lehet kezelni és megosztani.

A hozzáférés kizárólag jogosultságkezelés alapján történhet. A felhasználók csak azokhoz az állományokhoz, csoportokhoz és kommunikációs felületekhez férhetnek hozzá, amelyekhez munkakörük vagy feladatuk alapján jogosultsággal rendelkeznek.

A dokumentumok és egyéb személyes adatokat tartalmazó állományok megosztásakor különös figyelmet kell fordítani arra, hogy azokhoz illetéktelen személy ne férhessen hozzá.

A felhasználók kötelesek az intézményi Microsoft 365-fiókjukhoz tartozó belépési adatokat bizalmasan kezelni, és azokat más személy részére nem adhatják át.

13. MICS, MIR, önértékelés, elégedettségmérések és monitoring

Az intézményi minőségirányítási rendszer (MIR) működtetése, az önértékelési és fejlesztési feladatok, valamint a Minőségirányítási Csoport (MICS) tevékenysége során személyes adatokat tartalmazó dokumentumok és nyilvántartások keletkezhetnek.

Az adatkezelés célja az intézmény minőségirányítási feladatainak ellátása, az intézményi működés értékelése, a fejlesztendő területek azonosítása, a fejlesztési intézkedések meghatározása, valamint az intézményi fejlesztések eredményességének nyomon követése.

A minőségirányítási tevékenység során személyes adatot tartalmazhatnak különösen:

- partneri elégedettségmérések és kérdőívek,
- tanulói, szülői és oktatói visszajelzések,
- fókuszbeszélgetések dokumentumai,
- panelbeszélgetések dokumentumai,
- oktatói egyéni cselekvési tervek,
- oktatói teljesítményhez és szakmai fejlődéshez kapcsolódó monitoringadatok,
- intézményi önértékelési dokumentumok,
- fejlesztési és intézkedési tervek,
- MICS-dokumentumok és beszámolók,
- monitoringdokumentumok,
- indikátorok és azok teljesülését igazoló adatok,
- elégedettségmérések összesített eredményei,
- a fejlesztési intézkedések végrehajtásához kapcsolódó dokumentumok.

13.1. Elégedettségmérések és visszajelzések

Az intézmény a tanulók, szülők, oktatók és egyéb partnerek véleményének megismerése érdekében elégedettségméréseket és egyéb visszajelzési formákat alkalmazhat.

A kérdőíves és egyéb mérések megkezdése előtt meg kell határozni az adatkezelés célját, a szükséges adatkört és azt, hogy a méréshez szükséges-e név szerinti adatgyűjtés.

Ahol a mérés célja lehetővé teszi, az adatokat **anonim vagy összesített formában** kell gyűjteni és feldolgozni. Személyhez köthető adat csak akkor kezelhető, ha annak megismerése és felhasználása a meghatározott cél eléréséhez szükséges.

A fókuszbeszélgetések és panelbeszélgetések során elhangzó személyes adatok kezelése esetén is az adattakarékosság és a célhoz kötöttség elvét kell alkalmazni.

13.2. Oktatói egyéni cselekvési tervek és monitoring

Az oktatói egyéni cselekvési tervek, a szakmai fejlődéshez kapcsolódó dokumentumok és a személyhez kötött monitoringadatok az érintett oktató szakmai tevékenységével kapcsolatos személyes adatokat tartalmazhatnak.

Ezen adatok kezelése kizárólag az intézményi minőségirányítási, fejlesztési és értékelési feladatok ellátásához szükséges mértékben történhet.

A személyhez kötött cselekvési tervekhez, monitoringadatokhoz és értékelési dokumentumokhoz csak a feladat ellátására kijelölt és arra jogosult személyek férhetnek hozzá.

A monitoring során törekedni kell arra, hogy az eredmények értékelése és bemutatása lehetőség szerint **összesített formában** történjen.

13.3. Indikátorok és intézményi fejlesztések

Az intézményi minőségirányítás során az intézmény a meghatározott indikátorok alapján követi nyomon a fejlesztési célok és intézkedések megvalósulását.

Az indikátorok gyűjtése és értékelése során csak a cél eléréséhez szükséges személyes adatok kezelhetők. Amennyiben az eredményesség megállapításához elegendő az összesített adat, személyhez kötött adatot nem szükséges kezelni.

Az intézményi önértékelés, a fejlesztési tervek és az intézkedések eredményeinek bemutatása során elsődlegesen az összesített, anonimizált vagy személyhez nem köthető adatok alkalmazására kell törekedni.

13.4. Adatokhoz való hozzáférés és adattovábbítás

A MICS, a MIR és az önértékelés során kezelt személyes adatokhoz csak azok a személyek férhetnek hozzá, akiknek az adatok megismerése a minőségirányítási feladatok ellátásához szükséges.

A dokumentumokat és adatokat úgy kell tárolni és kezelni, hogy azokhoz illetéktelen személy ne férhessen hozzá.

Külső szervezet vagy személy részére személyes adat csak megfelelő jogalap fennállása, az adattovábbítás szükségességének vizsgálata és a vonatkozó adatvédelmi feltételek teljesülése esetén adható át.

A fenntartó, illetve az intézményi működés ellenőrzésére jogosult szervek részére történő adatszolgáltatás során is törekedni kell arra, hogy amennyiben a cél eléréséhez elegendő, **összesített vagy anonimizált adatok** kerüljenek továbbításra.

14. Honlap és elektronikus kommunikáció

Az intézmény honlapját és elektronikus kommunikációs csatornáit az oktatási, tájékoztatási, kapcsolattartási és intézményi működési feladatok ellátása érdekében használja.

A honlapon vagy az elektronikus kommunikáció során kezelt személyes adatok különösen:

- kapcsolatfelvétel során megadott név és elérhetőségi adatok,
- e-mail címek,
- telefonszámok, amennyiben azok megadására sor kerül,
- a megkeresésekben, üzenetekben szereplő személyes adatok,
- az intézményi kommunikációhoz kapcsolódó egyéb, szükséges adatok.

Az intézmény elektronikus kommunikációját kizárólag az oktatási, tájékoztatási, kapcsolattartási és működési céloknak megfelelően használja.

A honlapon közzétett személyes adatok esetében az intézménynek biztosítania kell, hogy csak a közzététel céljához szükséges és megfelelő joggal rendelkező adatok kerüljenek nyilvánosságra.

A honlapra és az elektronikus kommunikációs rendszerekbe érkező megkereséseket csak az ügyintézéshez szükséges mértékben lehet kezelni. Az adatokhoz kizárólag az adott feladat ellátására jogosult munkatársak férhetnek hozzá.

Az elektronikus kommunikáció során különös figyelmet kell fordítani arra, hogy személyes vagy bizalmas adatokat csak az arra alkalmas és megfelelően védett intézményi kommunikációs csatornán továbbítsanak.

15. Fotó- és videófelvevételek kezelése

15.1. Fényképek és videófelvevételek készítése

Az intézmény az oktatási, nevelési, közösségi, tájékoztatási és intézményi rendezvények dokumentálása érdekében fénykép- és videófelvevételeket készíthet.

A felvevételek készítése előtt meg kell határozni az adatkezelés célját és a megfelelő jogalapot.

A felvevételekhez kizárólag azok a személyek férhetnek hozzá, akiknek ez a feladataik ellátásához szükséges.

Hozzájáruláson alapuló adatkezelés esetén az intézmény biztosítja a hozzájárulások megfelelő dokumentálását és nyilvántartását.

15.2. Felvevételek közzététele a honlapon és közösségi médiában

Az intézmény honlapján és közösségi médiafelületein fénykép, videó, név vagy más személyes adat csak megfelelő jogalap alapján tehető közzé.

A közzététel jogalapja különösen:

- az érintett vagy szükség esetén törvényes képviselőjének hozzájárulása;
- jogszabályban meghatározott egyéb esetek.

A nyilvánosságra hozatal nem automatikus következménye annak, hogy a fénykép- vagy videófelvevétel elkészült. A közzététel előtt minden esetben vizsgálni kell az érintett azonosíthatóságát, a közzététel célját és annak jogalapját.

Az intézményi események és eredmények bemutatása során csak a szükséges és arányos mértékű személyes adat használható fel.

Különös figyelmet kell fordítani arra, hogy az érintett az adatok, a felvétel vagy azok együttes tartalma alapján azonosíthatóvá válik-e.

A már közzétett felvevételek kezelését és esetleges eltávolítását is az adatkezelés céljára, jogalapjára és az érintetti jogok érvényesülésére figyelemmel kell végezni.

16. Honlap és közösségi média

Az intézmény honlapján és közösségi médiafelületein személyes adat csak az adatkezelés céljának megfelelően és megfelelő jogalap birtokában tehető közzé.

A közzétett személyes adatok körébe különösen tartozhat:

- név;
- fénykép;
- videófelvétel;
- tanulmányi, verseny- vagy egyéb intézményi eredménnyel kapcsolatos adat;
- az intézményi eseményeken való részvételhez kapcsolódó egyéb személyes adat.

A személyes adatok közzététele előtt minden esetben vizsgálni kell, hogy az érintett az adott adat, fénykép, videófelvétel vagy azok együttes tartalma alapján azonosíthatóvá válik-e.

A közzététel során csak a szükséges és az adatkezelési céllal arányos személyes adatok használhatók fel.

Az intézményi események, programok, eredmények és sikerek bemutatása során külön figyelmet kell fordítani a közzététel jogalapjára, valamint az érintettek adatvédelmi jogainak tiszteletben tartására.

A fényképek és videófelvételek készítésére és kezelésére vonatkozó részletes szabályokat a **15. Fotó- és videófelvételek kezelése** fejezet tartalmazza.

A közösségi médiafelületeken történő közzététel esetében figyelembe kell venni, hogy a közzétett tartalom az intézményen kívüli, szélesebb nyilvánosság számára is hozzáférhetővé válhat.

17. Kamerarendszer

Az intézményben működtetett kamerarendszer kizárólag jogszerű és előzetesen meghatározott célból használható.

A kamerarendszer célja különösen:

- vagyonvédelem;
- személyvédelem;
- jogsértések megelőzése és szükség esetén azok kivizsgálásának elősegítése.

A kamerarendszer működtetése nem irányulhat az érintettek indokolatlan vagy folyamatos megfigyelésére.

A megfigyelt területeket megfelelő és jól látható tájékoztatással kell ellátni.

A kamerafelvételekhez kizárólag kijelölt és erre jogosult személyek férhetnek hozzá.

A felvételek megőrzési idejét az adatkezelés céljának megfelelően, a vonatkozó jogszabályok és intézményi szabályozás alapján kell meghatározni. **A megőrzési idő főszabály szerint legfeljebb 30 nap.**

A kamerafelvételek csak a meghatározott célhoz szükséges mértékben használhatók fel, és jogosulatlan személy számára nem tehetők hozzáférhetővé.

18. Papíralapú és elektronikus dokumentumok kezelése

Az intézményben keletkező, személyes adatot tartalmazó papíralapú és elektronikus dokumentumokat úgy kell kezelni és tárolni, hogy azokhoz illetéktelen személy ne férhessen hozzá.

18.1. Papíralapú dokumentumok kezelése

A személyes adatot tartalmazó papíralapú iratokat illetéktelen hozzáféréstől védett helyen kell tárolni.

Az ilyen dokumentumokat különösen:

- zárható irodában, szekrényben vagy más megfelelően védett helyen kell elhelyezni;
- csak a feladatellátáshoz szükséges személyek számára szabad hozzáférhetővé tenni;
- őrizetlenül hagyni olyan helyen, ahol illetéktelen személy hozzáférhet, nem szabad.

Nyomtatott, személyes adatot tartalmazó dokumentumot közös hulladékba helyezni tilos.

A már nem szükséges dokumentumok selejtezését és megsemmisítését az intézmény iratkezelési és selejtezési szabályai szerint kell elvégezni. A személyes adatot tartalmazó iratok megsemmisítése során biztosítani kell, hogy az adatok helyreállítása vagy jogosulatlan felhasználása ne legyen lehetséges.

18.2. Elektronikus dokumentumok kezelése

Elektronikus dokumentumot és személyes adatot tartalmazó digitális állományt csak az arra jogosult személyek számára hozzáférhető, megfelelően védett intézményi tárhelyen vagy informatikai rendszerben lehet tárolni.

Az elektronikus dokumentumokhoz való hozzáférést felhasználói jogosultságokkal kell szabályozni.

Személyes adatot tartalmazó elektronikus dokumentumot lehetőség szerint nem szabad jogosulatlanul hozzáférhető eszközön, nyilvános tárhelyen vagy ellenőrizetlen személyes adathordozón tárolni.

Az elektronikus dokumentumok továbbítása során is biztosítani kell, hogy azokhoz kizárólag az arra jogosult személyek férhessenek hozzá.

A feleslegessé vált elektronikus dokumentumokat az adatmegőrzési és iratkezelési szabályok figyelembevételével kell törölni vagy archiválni.

19. Adattovábbítás és adatfeldolgozók

19.1. Adatfeldolgozók

Az intézmény a feladatai ellátásához személyes adatok kezelésével járó szolgáltatásokat vehet igénybe. Az adatfeldolgozó az intézmény nevében, annak utasításai alapján végzi az adatkezeléssel kapcsolatos feladatokat.

Az intézmény által igénybe vehető adatfeldolgozók különösen:

- KRÉTA rendszer szolgáltatója,
- Vizsgaközpont rendszer,
- KIFIR,
- kétszintű érettségi nyilvántartó rendszer (www.kettszintu.hu),
- Microsoft által biztosított informatikai szolgáltatások,
- könyvelési szolgáltató,
- bérszámfejtési szolgáltató,
- informatikai szolgáltató,
- tárhelyszolgáltató,
- az intézmény működéséhez kapcsolódó egyéb, személyes adatok kezelését végző szolgáltató.

Az adatfeldolgozókkal az adatfeldolgozásra vonatkozó feltételeket írásban, szerződésben vagy más megfelelő jogi aktusban kell rögzíteni. Az adatfeldolgozó a személyes adatokat kizárólag az intézmény dokumentált utasításai alapján, a meghatározott célból és a szükséges mértékben kezelheti.

Az adatfeldolgozó önállóan nem határozhatja meg a személyes adatok kezelésének célját és eszközeit, és a tudomására jutott adatokat saját céljára nem használhatja fel. Az adatfeldolgozó köteles biztosítani az adatok biztonságát, valamint a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés, megsemmisítés, elvesztés vagy sérülés elleni megfelelő védelmet.

Az adatfeldolgozó kizárólag azoknak a munkatársainak biztosíthat hozzáférést a személyes adatokhoz, akiknek az adatfeldolgozási feladat ellátásához az szükséges. A hozzáféréssel rendelkező személyeket titoktartási kötelezettség terheli.

Az adatfeldolgozó köteles az intézménnyel együttműködni az érintetti jogok gyakorlásával, az adatbiztonsági eseményekkel és az adatvédelmi kötelezettségek teljesítésével kapcsolatban. Adatvédelmi incidens vagy annak gyanúja esetén az intézményt indokolatlan késedelem nélkül értesíteni kell.

19.2. Adattovábbítás általános szabályai

Az intézmény személyes adatot harmadik személy vagy más szerv részére kizárólag megfelelő jogalap fennállása esetén továbbíthat. Az adattovábbítás során biztosítani kell a célhoz kötöttség, az adattakarékosság és az adatbiztonság követelményeinek érvényesülését.

Adat csak olyan címzett részére továbbítható, aki az adat megismerésére és kezelésére jogosult. A továbbítás előtt ellenőrizni kell az adattovábbítás jogalapját, célját, a címzett jogosultságát, valamint azt, hogy a kért adatok köre szükséges-e az adott ügy intézéséhez.

Az intézmény által kezelt személyes adatok továbbíthatók különösen:

- az Oktatási Hivatal részére,
- a fenntartó részére,
- jogszabály alapján eljáró hatóságok részére,
- bíróság részére,
- ügyészség vagy rendőrség részére, jogszabályban meghatározott esetben,
- egészségügyi szervek részére, ha az adattovábbítás jogszabály alapján szükséges,
- gyermekvédelmi és gyermekjóléti szervek részére, jogszabályban meghatározott esetben,
- társadalombiztosítási, illetmény- és bérszámfejtési feladatokat ellátó szervezet részére,
- egyéb, jogszabályban meghatározott szervezet vagy szerv részére.

19.3. Külső megkeresés alapján történő adattovábbítás

Az intézményhez érkező, személyes adatok kiadására irányuló külső megkeresést az adatkezelést végző munkatárs haladéktalanul továbbítja az intézmény igazgatójának vagy az általa kijelölt, erre jogosult személynek.

A megkeresés teljesítése előtt meg kell vizsgálni:

- az adattovábbítás célját,
- az adattovábbítás jogalapját,
- a megkereső szerv vagy személy jogosultságát,
- a kért adatok pontos körét,
- az érintett személy vagy személyek azonosíthatóságát,
- az adattovábbítás szükségességét és arányosságát.

Ha az adattovábbítás jogszerűsége nem állapítható meg egyértelműen, az adat nem továbbítható mindaddig, amíg a jogalap és a jogosultság nem tisztázott.

A továbbított adatok körét minden esetben a szükséges minimumra kell korlátozni. Az adattovábbítás tényét és a kapcsolódó dokumentumokat az intézmény az iratkezelési szabályoknak megfelelően dokumentálja.

19.4. Intézményen belüli adattovábbítás és hozzáférés

Az intézményen belül személyes adat csak annak a munkatársnak továbbítható vagy hozzáférhetővé tehető, akinek az adat a munkaköri feladata ellátásához szükséges.

A tanulók személyes adatainak kezelésére és az azokhoz való hozzáférésre különösen:

- az intézmény igazgatója,
- az igazgató által kijelölt igazgatóhelyettes,
- az iskolatitkár,
- gazdasági munkatársak, könyvelők,
- az adatkezelési feladattal megbízott oktató vagy más munkatárs

jogosult a számára meghatározott feladat- és hozzáférési körben.

Az intézményvezető a munkavégzéséhez szükséges mértékben teljes körű adatkezelési és betekintési jogosultsággal rendelkezik. Az igazgató által kijelölt igazgatóhelyettes jogosult és köteles a tanulói, tanügyi és egyéb nyilvántartásokban szereplő adatok ellenőrzésére.

Az iskolatitkár és az egyéb munkatársak csak a munkakörük ellátásához szükséges mértékben férhetnek hozzá a személyes adatokhoz.

A rendszergazda a számítógépes rendszerekben tárolt személyes adatokhoz kizárólag a munkavégzéséhez szükséges mértékben férhet hozzá. Technikai feladat ellátása során megismert személyes adatot nem használhat fel saját céljára, és azt illetéktelen személy részére nem adhatja át.

19.5. A tanulók adatainak továbbítása

A tanulók személyes adatai csak az intézmény feladatainak ellátásához szükséges mértékben és meghatározott célból kezelhetők.

A tanulókkal kapcsolatos adatok továbbítása jogszabályban meghatározott esetben történhet különösen oktatási, tanügyi, gyermekvédelmi, gyermekjóléti, iskola-egészségügyi, valamint hatósági feladatok ellátása érdekében.

A kiskorú tanuló veszélyeztetettsége esetén az intézmény a jogszabályban meghatározott szervek részére köteles lehet a szükséges adatokat továbbítani. Ilyen esetben az adattovábbításhoz külön hozzájárulás nem szükséges, ha az adattovábbítás jogszabályon alapul.

Az oktatót, valamint a nevelő-oktató munkát közvetlenül segítő munkatársat a munkája során tudomására jutott, a tanulóra és családjára vonatkozó személyes adatok tekintetében titoktartási kötelezettség terheli.

19.6. Az alkalmazottak személyes adatainak továbbítása

Az intézmény alkalmazottainak személyes adatai a foglalkoztatási jogviszonnyal kapcsolatos feladatok ellátásához, a munkabér és egyéb juttatások megállapításához, valamint a jogszabályban meghatározott nyilvántartási és adatszolgáltatási kötelezettségek teljesítéséhez kezelhetők és továbbíthatók.

Az alkalmazotti adatok kezeléséért és célhoz kötött továbbításáért az intézményvezető, az általa kijelölt vezető, az érintett munkatárs felettese, valamint a munkaügyi feladatokat ellátó munkatárs felelős a saját feladat- és hatáskörében.

Az alkalmazott köteles az intézmény részére átadott személyes adatairól gondoskodni arról, hogy azok pontosak, teljesek és aktuálisak legyenek.

Az alkalmazottak személyes adatai illetéktelen személy részére nem adhatók át és nem hozhatók nyilvánosságra. Az adatok továbbítása kizárólag megfelelő jogalap alapján, a szükséges mértékben történhet.

19.7. Adatbiztonság és felelősségi szabályok

Az intézmény minden munkatársa köteles a személyes adatokat védeni a jogosulatlan hozzáféréssel, megváltoztatással, továbbítással, nyilvánosságra hozattal, törléssel vagy megsemmisítéssel szemben.

A személyes adatokhoz való hozzáférési jogosultságokat munkakör és feladat alapján kell meghatározni. A jogosultságokat rendszeresen felül kell vizsgálni, és a munkakör vagy a foglalkoztatási jogviszony megszűnésekor, illetve megváltozásakor a szükséges módosításokat el kell végezni.

A személyes adatok továbbítása során biztosítani kell, hogy az adatokat kizárólag a jogosult címzett ismerhesse meg. Elektronikus továbbítás esetén megfelelő technikai és szervezési intézkedéseket kell alkalmazni.

Az adatkezeléssel megbízott munkatárs felelős azért, hogy az általa kezelt személyes adatot kizárólag a munkaköri feladatának megfelelően használja fel.

19.8. Az érintettek tájékoztatása és jogai

Az érintett jogosult tájékoztatást kérni az intézmény által kezelt személyes adatairól, az adatkezelés céljáról és jogalapjáról, az adatkezelés időtartamáról, valamint az adatok címzettjeiről és az adatfeldolgozóról.

Az érintett jogosult továbbá a jogszabályban meghatározott feltételek szerint személyes adatainak helyesbítését, törlését vagy kezelésének korlátozását kérni, illetve tiltakozhat az adatkezelés ellen, amennyiben annak feltételei fennállnak.

Az intézmény az érintetti kérelmeket a vonatkozó adatvédelmi jogszabályokban meghatározott határidőn belül és az előírt módon kezeli.

19.9. Külföldre, illetve harmadik országba történő adattovábbítás

Az Európai Gazdasági Térségen belüli adattovábbításra az uniós adatvédelmi szabályok alkalmazandók.

Harmadik országba vagy nemzetközi szervezet részére személyes adat csak a GDPR-ban meghatározott feltételek fennállása esetén továbbítható. Ilyen adattovábbítás esetén biztosítani kell a személyes adatok megfelelő védelmét és az érintettek jogainak érvényesíthetőségét.

Az intézmény által használt informatikai szolgáltatások esetében a külföldi vagy harmadik országbeli adatkezelés lehetőségét az adott szolgáltatás feltételei, az adatfeldolgozói megállapodás és az intézményi adatkezelési tájékoztató alapján kell megítélni.

19.10. Az adattovábbítás dokumentálása

Az intézmény a jelentősebb vagy külön jogszabály alapján dokumentálandó adattovábbításokat nyilvántartja, vagy az intézményi iratkezelési rendszerben rögzíti.

A dokumentációnak – amennyiben az adott adattovábbítás esetében releváns – tartalmaznia kell:

- az adattovábbítás időpontját,
- a címzett megnevezését,
- az érintett vagy érintettek körét,
- a továbbított adatok körét,
- az adattovábbítás célját,
- az adattovábbítás jogalapját,
- az adattovábbítást engedélyező személyt,
- az adattovábbítással kapcsolatos dokumentumot.

Az adattovábbításért felelős személy köteles gondoskodni arról, hogy az adatátadás jogszerűsége és szükségessége utólag is ellenőrizhető legyen.

Az intézmény adatfeldolgozóinak aktuális jegyzékét, valamint az adatfeldolgozók feladatait és az adatkezeléshez kapcsolódó főbb feltételeket az intézmény a vonatkozó szerződések és adatvédelmi dokumentumok alapján tartja nyilván.

20. Adatbiztonság és hozzáférési jogosultságok

Az intézmény a kezelt személyes adatokat megfelelő technikai és szervezési intézkedésekkel védi annak érdekében, hogy azokhoz kizárólag az arra jogosult személyek férhessenek hozzá.

A személyes adatokhoz való hozzáférési jogosultságot az ellátott munkakör és az elvégzendő feladat alapján kell meghatározni. Minden munkatárs kizárólag azokhoz az adatokhoz és olyan mértékben férhet hozzá, amelyek feladatai ellátásához szükségesek.

Az intézményben a személyes adatokhoz való hozzáférés különösen az alábbiak szerint történhet:

- az intézmény vezetője a feladatai ellátásához szükséges körben jogosult az intézmény által kezelt adatok megismerésére;
- a vezetők és az egyes munkakörökben dolgozó munkatársak a feladataik ellátásához szükséges adatokhoz férhetnek hozzá;
- az oktatók a tanulók adatait kizárólag az oktatási, nevelési és adminisztrációs feladataik ellátásához szükséges mértékben kezelhetik;
- az iskolatitkár az ügyviteli és adminisztrációs feladataihoz szükséges adatokhoz férhet hozzá;
- az informatikai rendszerek üzemeltetését végző személy a technikai feladatok ellátásához szükséges mértékben férhet hozzá az adatokhoz;
- külső személy vagy szervezet személyes adatokhoz csak megfelelő jogosultság vagy jogalap alapján férhet hozzá.

A hozzáférési jogosultságokat az intézménynek rendszeresen felül kell vizsgálnia. A munkakör, a feladat vagy a jogviszony megváltozása, illetve megszűnése esetén a szükségtelenné vált hozzáférési jogosultságokat haladéktalanul módosítani vagy megszüntetni kell.

20.1. Informatikai hozzáférések

Az elektronikus rendszerek használata során minden munkatárs köteles saját felhasználói azonosítóját és jelszavát bizalmasan kezelni.

A jelszó:

- más személy részére nem adható át;
- más személy jelszavának használata nem megengedett;
- nem rögzíthető olyan helyen, ahol illetéktelen személy hozzáférhet;
- illetéktelen hozzáférés gyanúja esetén haladéktalanul meg kell változtatni.

A munkatársak csak a részükre biztosított felhasználói fiókot használhatják. A közösen használt felhasználói fiókok alkalmazását az intézménynek lehetőség szerint kerülni kell.

A felügyelet nélkül hagyott számítógépet és egyéb informatikai eszközt úgy kell lezárni vagy más módon védeni, hogy az azon kezelt személyes adatokhoz illetéktelen személy ne férhessen hozzá.

Az intézményi informatikai rendszerekben – így különösen a KRÉTA, Teams és egyéb oktatási, ügyviteli vagy kommunikációs rendszerekben – a hozzáférési jogosultságokat az adott munkakörhöz és feladathoz szükséges mértékben kell biztosítani.

20.2. Papíralapú adatok fizikai védelme

A személyes adatokat tartalmazó papíralapú iratokat úgy kell tárolni, hogy azokhoz illetéktelen személy ne férhessen hozzá.

A személyes adatokat tartalmazó iratokat:

- használaton kívül zárt vagy illetéktelen hozzáféréstől védett helyen kell tárolni;
- az intézményen belül csak a munkavégzéshez szükséges mértékben szabad hozzáférhetővé tenni;
- azokat felügyelet nélkül nyitott helyen vagy olyan helyiségben hagyni, ahol illetéktelen személy hozzáférhet, nem megengedett.

A nyomtatott dokumentumok kezelésénél törekedni kell arra, hogy személyes adatok ne maradjanak fénymásolóban, nyomtatóban vagy más, közösen használt eszközben.

A személyes adatot tartalmazó iratok megsemmisítését az intézmény iratkezelési szabályainak megfelelően kell elvégezni.

20.3. Adathordozók és elektronikus dokumentumok védelme

A személyes adatokat tartalmazó elektronikus dokumentumokat és adathordozókat megfelelő védelemmel kell ellátni.

Az adatokat tartalmazó hordozható eszközök – például pendrive, külső meghajtó vagy hordozható számítógép – használata során különös figyelmet kell fordítani az illetéktelen hozzáférés és az elvesztés kockázatának csökkentésére.

Személyes adatot tartalmazó dokumentumot csak az intézmény által engedélyezett vagy a munkavégzéshez megfelelően biztosított elektronikus csatornán szabad továbbítani.

A személyes adatokat tartalmazó dokumentumok továbbításakor a címzettet és a továbbítás módját úgy kell megválasztani, hogy az adat csak az arra jogosult személyhez jusson el.

20.4. Biztonsági mentés és technikai védelem

Az intézmény az elektronikus adatok rendelkezésre állásának biztosítása érdekében a fontos intézményi adatok tekintetében megfelelő biztonsági mentési és helyreállítási eljárásokat alkalmaz.

Az informatikai rendszerek védelme érdekében gondoskodni kell a rendelkezésre álló technikai biztonsági megoldások megfelelő alkalmazásáról, különösen:

- a jogosulatlan hozzáférés elleni védelemről;
- a kártékony programok elleni védelemről;
- az informatikai eszközök fizikai védelméről;
- az adatok biztonsági mentéséről;

- az informatikai rendszerekhez kapcsolódó jogosultságok megfelelő kezeléséről.

Az informatikai rendszerek üzemeltetésével kapcsolatos részletes technikai feladatokat az intézmény informatikai rendje, illetve az arra vonatkozó belső szabályozás határozza meg.

20.5. A munkatársak adatbiztonsági felelőssége

Az intézmény valamennyi munkatársa felelős azért, hogy a munkája során megismert személyes adatokat az adatvédelmi és adatbiztonsági előírásoknak megfelelően kezelje.

A munkatárs köteles:

- a számára biztosított hozzáférési jogosultságot rendeltetésszerűen használni;
- a személyes adatokat illetéktelen személy számára nem hozzáférhetővé tenni;
- a jelszavakat és belépési adatokat bizalmasan kezelni;
- a papíralapú és elektronikus dokumentumokat megfelelően védeni;
- az intézményi informatikai eszközöket rendeltetésszerűen használni;
- az adatbiztonságot veszélyeztető körülményt a megfelelő intézményi személynek jelezni.

A személyes adatokhoz való hozzáférés nem jogosítja fel a munkatársat az adatok saját célú felhasználására, jogosulatlan továbbítására vagy nyilvánosságra hozatalára.

Az adatbiztonság megsértésének vagy személyes adatok jogosulatlan hozzáférésének, elvesztésének, továbbításának vagy nyilvánosságra kerülésének gyanúját a munkatárs köteles haladéktalanul jelezni az intézményben meghatározott felelős személynek. Az ilyen események részletes kezelését a 19. Adatvédelmi incidensek című fejezet tartalmazza.

21. Adatvédelmi incidensek kezelése

Adatvédelmi incidens minden olyan, a személyes adatok biztonságát érintő esemény, amely a személyes adatok véletlen vagy jogellenes megsemmisüléséhez, elvesztéséhez, megváltoztatásához, jogosulatlan közléséhez vagy jogosulatlan hozzáféréséhez vezethet.

Adatvédelmi incidens lehet különösen:

- személyes adatot tartalmazó e-mail téves címzetthez történő elküldése;
- személyes adatot tartalmazó dokumentum elvesztése;
- laptop, mobiltelefon vagy egyéb adathordozó elvesztése vagy eltulajdonítása;
- személyes adatokhoz történő jogosulatlan hozzáférés;
- felhasználói fiók illetéktelen használata;
- informatikai rendszer biztonságának megsértése;
- személyes adatot tartalmazó dokumentum jogosulatlan továbbítása vagy nyilvánosságra kerülése;
- személyes adatokat tartalmazó irat vagy elektronikus adatállomány véletlen törlése vagy sérülése;
- olyan informatikai támadás, amely a személyes adatok biztonságát veszélyezteti.

21.1. Az adatvédelmi incidens bejelentése

Az adatvédelmi incidenst vagy annak gyanúját észlelő munkatárs köteles azt **haladéktalanul jelezni az intézményvezetésnek vagy az intézmény által kijelölt adatvédelmi kapcsolattartónak.**

A bejelentés során – amennyiben rendelkezésre állnak – meg kell adni:

- az esemény időpontját;
- az esemény rövid leírását;
- az érintett rendszert, dokumentumot vagy adathordozót;
- az érintett személyes adatok jellegét;
- az érintettek körét, amennyiben ismert;
- az addig megtett intézkedéseket.

Az incidens bejelentésekor nem szükséges a munkatársnak annak jogi minősítését elvégeznie. A bejelentés célja, hogy az intézmény az eseményt mielőbb megvizsgálhassa és a szükséges intézkedéseket megtehesse.

21.2. Az adatvédelmi incidens kivizsgálása

A bejelentést követően az intézmény megvizsgálja az eseményt, és megállapítja, hogy az adatvédelmi incidensnek minősül-e.

A kivizsgálás során meg kell határozni különösen:

- mi történt;
- mikor és milyen körülmények között történt az esemény;
- milyen személyes adatok érintettek;
- hozzávetőlegesen hány személyt érint az esemény;
- történt-e jogosulatlan hozzáférés, közlés, elvesztés vagy adatvesztés;
- milyen következményekkel járhat az esemény az érintettekre nézve;
- milyen azonnali intézkedések szükségesek a további károk megelőzéséhez vagy csökkentéséhez.

Informatikai rendszert érintő incidens esetén az intézmény az informatikai feladatokat ellátó személy vagy rendszergazda közreműködését is igénybe veheti.

Az incidens kivizsgálása során az intézmény törekszik arra, hogy a veszélyeztetett adatokhoz való további jogosulatlan hozzáférést megszüntesse, illetve az adatbiztonságot helyreállítsa.

21.3. Az adatvédelmi incidens dokumentálása és nyilvántartása

Az adatvédelmi incidenseket az intézmény dokumentálja és nyilvántartja.

A nyilvántartásnak alkalmasnak kell lennie annak megállapítására, hogy:

- mikor és milyen incidens történt;
- milyen személyes adatok voltak érintettek;
- kiket érintett az esemény;
- milyen körülmények között következett be;
- milyen kockázatokat azonosítottak;
- milyen intézkedések történtek az incidens kezelésére;
- szükségessé vált-e hatósági vagy érintetti tájékoztatás.

A dokumentációt úgy kell vezetni, hogy az intézmény az adatvédelmi incidens kezelését és az alkalmazott intézkedéseket utólag igazolni tudja.

21.4. Hatósági bejelentés

Amennyiben az adatvédelmi incidens az érintett természetes személyek jogaira és szabadságaira nézve kockázattal járhat, az intézmény megvizsgálja a felügyeleti hatóság, vagyis a **Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)** felé történő bejelentés szükségességét.

Ha a bejelentés a GDPR alapján szükséges, azt az adatkezelő **indokolatlan késedelem nélkül és lehetőség szerint az incidens tudomására jutásától számított 72 órán belül** teljesíti.

Amennyiben a bejelentéshez szükséges valamennyi információ nem áll rendelkezésre a határidőn belül, a rendelkezésre álló információkat kell megadni, a további adatokat pedig indokolatlan késedelem nélkül kell pótolni.

Ha az incidens valószínűsíthetően nem jelent kockázatot az érintettek jogaira és szabadságaira nézve, hatósági bejelentésre nem feltétlenül kerül sor. Ennek megítélését az intézmény az incidens körülményeinek és kockázatainak vizsgálata alapján végzi el.

21.5. Az érintettek tájékoztatása

Amennyiben az adatvédelmi incidens az érintett természetes személyek jogaira és szabadságaira nézve **magas kockázattal járhat**, az intézmény megvizsgálja az érintettek közvetlen tájékoztatásának szükségességét.

A tájékoztatásnak közérthető formában tartalmaznia kell az incidens lényegét, a várható következményeket, valamint az érintettek kockázatának csökkentése érdekében megtett vagy tervezett intézkedéseket.

Az érintettek tájékoztatása nem szükséges azokban az esetekben, amikor annak feltételei a GDPR alapján nem állnak fenn.

Az érintettek adatkezeléssel kapcsolatos általános jogait és az azok gyakorlására vonatkozó szabályokat a **21. Az érintettek jogai** című fejezet tartalmazza.

21.6. Intézkedési terv

Az adatvédelmi incidens kivizsgálását követően – amennyiben az esemény jellege vagy ismétlődésének kockázata indokolja – az intézmény intézkedési tervet készít.

Az intézkedési tervben meg kell határozni:

- az incidens okának megszüntetéséhez szükséges feladatokat;
- a további hasonló események megelőzésére szolgáló intézkedéseket;
- a szükséges technikai vagy szervezési változtatásokat;
- a feladatok felelőseit;
- a végrehajtás határidejét;
- az intézkedések eredményének ellenőrzését.

Az intézkedési terv végrehajtását az intézményvezetés nyomon követi.

22. Az érintettek jogai

Az érintett jogosult arra, hogy személyes adatainak kezeléséről megfelelő, közérthető tájékoztatást kapjon, valamint megismerhesse a róla kezelt személyes adatokat és azok kezelésének célját.

Az érintett jogosult:

- a személyes adataihoz való hozzáférésre,
- a pontatlan vagy hiányos adatok helyesbítésére,
- a jogszabályban meghatározott esetekben személyes adatainak törlésére,
- az adatkezelés korlátozására,
- az adatkezelés elleni tiltakozásra, amennyiben annak feltételei fennállnak,
- az adathordozhatóságra, ha annak jogszabályi feltételei teljesülnek,
- a hozzájáruláson alapuló adatkezeléshez adott hozzájárulás visszavonására.

Az érintett jogosult továbbá panaszt tenni a felügyeleti hatóságnál, ha megítélése szerint személyes adatainak kezelése nem felel meg az adatvédelmi előírásoknak.

Az intézmény az érintetti kérelmeket a kijelölt adatvédelmi felelős vagy kapcsolattartó közreműködésével kezeli. A kérelem teljesítése előtt szükség esetén ellenőrizni kell a kérelmező személyazonosságát.

Az érintetti kérelmeket az intézmény indokolatlan késedelem nélkül, a jogszabályban meghatározott határidőn belül vizsgálja meg és válaszolja meg. Ha a kérelem teljesítésének jogszabályi akadálya van, az érintettet annak okáról tájékoztatni kell.

Kiskorú tanuló esetében az érintetti jogok gyakorlására a tanuló életkorára, jogi helyzetére és az adott ügy jellegére tekintettel kerül sor, szükség esetén a szülő vagy törvényes képviselő bevonásával.

Az érintetti jogok gyakorlása során az intézmény törekszik arra, hogy az érintett számára az adatkezeléssel kapcsolatos információk és a jogorvoslati lehetőségek egyértelműen és közérthetően rendelkezésre álljanak.

23. Adatmegőrzés, törlés és selejtezés

A személyes adatokat az intézmény csak addig őrzi meg, ameddig az adatkezelés céljának megvalósításához, illetve az adatkezelésre vonatkozó jogszabályi kötelezettség teljesítéséhez szükséges.

Az egyes adatkörök megőrzési idejét elsősorban a vonatkozó jogszabályok, az iratkezelési szabályok, valamint az adatkezelés célja alapján kell meghatározni. Az intézmény nem alkalmazhat egységes megőrzési időt valamennyi személyes adatra.

Adatmegőrzési idők

Adatkör	Megőrzési idő
Tanügyi, tanulói nyilvántartások	A vonatkozó jogszabály és irattári szabályok szerint
Vizsgákkal, értékeléssel kapcsolatos iratok	A vonatkozó jogszabály és irattári szabályok szerint
Munkáltatói és munkaügyi dokumentumok	A vonatkozó jogszabály és iratkezelési szabályok szerint
Bérszámfejtési és társadalombiztosítási adatok	A vonatkozó jogszabályban meghatározott ideig
Hozzájáruló nyilatkozatok	A hozzájáruláson alapuló adatkezelés céljának fennállásáig, illetve a jogszabályban meghatározott ideig
MICS/MIR dokumentumok és monitoring adatok	Az intézményi és jogszabályi előírások szerint, a dokumentációs és fejlesztési célhoz szükséges ideig
Kamerafelvételek	Az intézményi kamerás adatkezelésre vonatkozó szabályokban meghatározott, szükséges és arányos időtartamig
Egyéb személyes adatot tartalmazó dokumentumok	Az adatkezelés céljának fennállásáig, illetve a vonatkozó megőrzési szabály szerint

A megőrzési idő lejártát követően a személyes adatokat – amennyiben további jogszabályi vagy intézményi megőrzési kötelezettség nem áll fenn – törölni, megsemmisíteni vagy szabályos irattári selejtezés keretében kezelni kell.

Az irattári megőrzésre kötelezett dokumentumok esetében az adatkezelés céljának megszűnése önmagában nem jelenti az irat azonnali törlését. Az ilyen dokumentumokat az iratkezelési és selejtezési szabályok szerint kell megőrizni.

A digitális adatok törlése során arra is figyelni kell, hogy a személyes adatok az intézmény által használt elektronikus rendszerekben, tárhelyeken és egyéb nyilvántartásokban se maradjanak indokolatlanul hozzáférhetők.

A MICS/MIR tevékenységhez kapcsolódó hosszabb távú elemzések esetében – ahol az adatkezelés célja ezt lehetővé teszi – az egyéni személyes adatok helyett **összesített vagy anonimizált adatok** alkalmazása javasolt.

A törlés és selejtezés végrehajtását úgy kell dokumentálni, hogy az intézmény igazolni tudja a szabályos adatkezelést és az adatmegőrzési kötelezettségek teljesítését.

24. Panaszok és adatvédelmi kérelmek

Az adatkezeléssel kapcsolatos panaszokat és az érintetti kérelmeket az intézmény a vonatkozó adatvédelmi előírások szerint kezeli. Az érintett kérelmével elsősorban közvetlenül az intézményhez fordulhat.

Az adatvédelmi kérelem benyújtható különösen a személyes adatokhoz való hozzáférés, azok helyesbítése, törlése, az adatkezelés korlátozása vagy az adatkezelés elleni tiltakozás céljából. Az érintetti jogokat és azok tartalmát a **21. Az érintettek jogai** című fejezet tartalmazza.

Az intézmény a kérelmet indokolatlan késedelem nélkül megvizsgálja, és főszabály szerint a kérelem beérkezésétől számított **egy hónapon belül** tájékoztatja az érintettet a megtett intézkedésről. A határidő összetett vagy nagy számú kérelmet érintő esetben további két hónappal meghosszabbítható, amelyről az intézmény az érintettet az első hónapon belül tájékoztatja.

A kérelem kezelése során az intézmény szükség esetén ellenőrzi a kérelmező személyazonosságát, és csak a kérelem elbírálásához szükséges személyes adatokat kezeli.

Ha az intézmény a kérelmet nem teljesíti, az érintettet tájékoztatni kell az elutasítás okáról és a rendelkezésére álló jogorvoslati lehetőségekről.

Panasz a felügyeleti hatóságnál

Az érintett jogosult panaszt tenni a **Nemzeti Adatvédelmi és Információszabadság Hatóságnál (NAIH)**, ha megítélése szerint személyes adatainak kezelése sérti az adatvédelmi előírásokat. A NAIH kifejezetten javasolja, hogy az érintett lehetőség szerint először közvetlenül az adatkezelővel vegye fel a kapcsolatot és éljen érintetti jogaival.

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)

Székhely: 1055 Budapest, Falk Miksa utca 9–11.

Postacím: 1363 Budapest, Pf. 9.

Telefon: +36 (1) 391-1400

E-mail: ugyfelszolgalat@naih.hu

Weboldal: [Nemzeti Adatvédelmi és Információszabadság Hatóság](https://www.naih.hu)

A NAIH-nál az érintett adatvédelmi hatósági eljárás megindítását is kérelmezheti, illetve bizonyos esetekben a Hatóság vizsgálatát kezdeményezheti.

25. Ellenőrzés, oktatás és adatvédelmi tudatosság

Az intézmény törekszik arra, hogy a személyes adatok kezelésében részt vevő munkatársak ismerjék és alkalmazzák az adatvédelmi szabályokat. A GDPR az adatvédelmi tisztviselő feladatai között is nevesíti a munkatársak tudatosságának növelését, képzését és a megfelelés ellenőrzését.

Az adatvédelmi oktatás során különösen az alábbi területekre kell felhívni a figyelmet:

- a személyes adatok biztonságos kezelése,
- az adatok továbbításának és megosztásának szabályai,
- a papíralapú és elektronikus dokumentumok kezelése,
- az intézményi elektronikus rendszerek biztonságos használata,
- az érintetti kérelmek felismerése és továbbítása,
- az adatvédelmi incidensek felismerése és haladéktalan jelzése.

Az új munkatársakat a személyes adatok kezelésével kapcsolatos feladataik megkezdése előtt, illetve a munkakörükhöz igazodóan megfelelő adatvédelmi tájékoztatásban kell részesíteni. A munkatársak számára szükség esetén ismétlő vagy célzott adatvédelmi oktatást kell biztosítani. A képzések megtörténtét az intézmény dokumentálhatja.

Az adatvédelmi szabályok betartását az intézmény időszakosan ellenőrzi. Az ellenőrzés kiterjedhet különösen a személyes adatok kezelésének gyakorlatára, a hozzáférési jogosultságokra, az elektronikus rendszerek használatára és az adatvédelmi előírások betartására. A GDPR az adatbiztonsági intézkedések rendszeres tesztelését és értékelését is előírja.

Új elektronikus rendszer, digitális szolgáltatás vagy jelentősebb új adatkezelés bevezetése előtt az adatvédelmi szempontokat is meg kell vizsgálni. Szükség esetén be kell vonni az adatvédelmi tisztviselőt vagy az adatvédelmi feladatok ellátására kijelölt személyt. A GDPR szerint az adatvédelmi tisztviselőt a személyes adatok védelmével kapcsolatos ügyekbe megfelelően és időben be kell vonni.

Az ellenőrzések, adatvédelmi incidensek, érintetti kérelmek és egyéb tapasztalatok alapján szükség esetén módosítani kell a belső eljárásokat, az oktatási tartalmakat vagy a technikai és szervezési intézkedéseket.

Az intézmény az adatvédelmi tudatosság fenntartása érdekében a munkatársak számára könnyen hozzáférhetővé teszi az aktuális adatvédelmi szabályokat és a kapcsolattartó személy elérhetőségét.

26. A szabályzat felülvizsgálata

A szabályzat célja, hogy az intézményben a személyes adatok kezelése folyamatosan megfeleljen a hatályos jogszabályoknak, az intézményi működésnek és az adatbiztonsági követelményeknek. Az adatkezelőnek a GDPR alapján a megfelelő technikai és szervezési intézkedéseket rendszeresen felül kell vizsgálnia, és szükség esetén naprakésszé kell tennie.

A szabályzatot **legalább évente felül kell vizsgálni**, valamint soron kívüli felülvizsgálat szükséges különösen:

- adatvédelmi vagy adatkezelést érintő jogszabályváltozás esetén;
- az intézmény szervezeti vagy működési rendjének jelentős változásakor;
- új adatkezelési folyamat vagy új digitális rendszer bevezetésekor;
- jelentős informatikai vagy technikai változás esetén;
- adatvédelmi incidens bekövetkezése után, ha annak tapasztalatai módosítást indokolnak;
- adatvédelmi ellenőrzés, audit vagy hatósági vizsgálat megállapítása alapján;
- új adatfeldolgozó vagy jelentős adattovábbítási folyamat alkalmazásakor;
- az adatkezeléssel kapcsolatos kockázatok jelentős változása esetén.

26.1. A felülvizsgálat szempontjai

A felülvizsgálat során az intézmény áttekinti különösen:

- az adatkezelések célját és jogalapját;
- az adatkezelési tevékenységek nyilvántartásának aktualitását;
- az érintettek jogainak biztosítását;
- a személyes adatokhoz való hozzáférési jogosultságokat;
- az adatmegőrzési, törlési és selejtezési gyakorlatot;
- a papíralapú és elektronikus adatok védelmét;
- az informatikai rendszerek és digitális platformok adatvédelmi beállításait;
- az adatfeldolgozókkal kapcsolatos adatvédelmi követelményeket;
- az adatvédelmi incidensek tapasztalatait;
- az érintetti kérelmek és adatvédelmi panaszok tapasztalatait;
- az adatvédelmi oktatások és tudatosságnövelő intézkedések eredményeit.

A felülvizsgálat során külön figyelmet kell fordítani arra, hogy az intézmény gyakorlata ténylegesen megfelel-e a szabályzatban foglaltaknak. Az adatvédelmi megfelelés igazolhatósága érdekében a felülvizsgálat eredményét és a szükséges intézkedéseket dokumentálni kell.

26.2. A MICS/MIR szerepe

A felülvizsgálat során figyelembe kell venni a **MICS/MIR keretében végzett monitoring, ellenőrzés és értékelés tapasztalatait**.

A felülvizsgálat során felhasználhatók különösen:

- a MICS/MIR jelentések megállapításai;
- az intézményi monitoring eredményei;
- az ellenőrzések tapasztalatai;
- az adatvédelmi incidensek értékelése;
- az intézményi panaszok és kérelmek tapasztalatai;
- az oktatói, tanulói és egyéb partneri visszajelzések;
- a feltárt hiányosságokhoz kapcsolódó intézkedési tervek;
- a korábbi fejlesztési intézkedések eredményei.

A feltárt hiányosságok esetén szükség szerint **intézkedést, felelőst, határidőt és ellenőrizhető eredményt** kell meghatározni. Ez illeszkedik az intézményi MIR/MICS fejlesztési és monitoringfolyamataihoz, valamint az adatvédelmi elszámoltathatóság követelményéhez.

26.3. A szabályzat módosítása

Amennyiben a felülvizsgálat alapján a szabályzat módosítása szükséges, a módosításokat az intézmény vezetése hagyja jóvá.

A módosított szabályzat hatálybalépéséről az érintett munkatársakat tájékoztatni kell. Amennyiben a változás az intézmény adatkezelési gyakorlatát is érinti, a kapcsolódó adatkezelési tájékoztatókat, nyilvántartásokat és egyéb dokumentumokat is aktualizálni kell.

A szabályzat felülvizsgálatát és módosításait **dokumentált módon, verziószámmal és dátummal** kell nyomon követni.

26.4. A felülvizsgálat dokumentálása

A felülvizsgálat eredményét dokumentálni kell. A dokumentációnak lehetőség szerint tartalmaznia kell:

- a felülvizsgálat időpontját;
- a felülvizsgálatban részt vevő személyeket;
- a vizsgált adatkezelési területeket;
- a feltárt hiányosságokat és kockázatokat;
- a szükséges módosításokat és fejlesztési feladatokat;
- a kijelölt felelőst;
- a teljesítési határidőt;

- az elvégzett intézkedéseket és azok eredményét.

A szabályzat felülvizsgálata nem egyszeri adminisztratív feladat, hanem az intézményi adatvédelem folyamatos fejlesztésének része. A felülvizsgálat során szerzett tapasztalatokat a MICS/MIR fejlesztési folyamatába is be kell építeni, amennyiben azok intézményi szintű fejlesztést indokolnak.

27. Záró rendelkezések

27.1. A szabályzat hatálya

Jelen szabályzat az intézmény valamennyi olyan munkatársára és közreműködőjére kiterjed, aki az intézmény működése során személyes adatok kezelésében, felhasználásában, továbbításában, tárolásában vagy megsemmisítésében részt vesz.

A szabályzat rendelkezéseit alkalmazni kell az intézmény által kezelt valamennyi papíralapú és elektronikus személyes adatra, nyilvántartásra, dokumentumra és informatikai rendszerre.

A szabályzatban foglaltak megismerése és betartása az adatkezelési tevékenységben részt vevő munkatársak számára kötelező.

27.2. A szabályzat hatálybalépése

Jelen szabályzat az intézményvezető jóváhagyásával, a meghatározott napon lép hatályba.

A szabályzat hatálybalépésével egyidejűleg az ugyanazon tárgykörben korábban kiadott intézményi rendelkezések és szabályzatok az új szabállyal ellentétes részeikben hatályukat veszítik.

A szabályzatot az intézmény egyéb szabályzataival, valamint a fenntartó és az egyetem vonatkozó rendelkezéseivel összhangban kell alkalmazni.

27.3. A szabályzat megismerése és hozzáférhetősége

A szabályzatot az érintett munkatársak számára hozzáférhetővé kell tenni.

Az intézmény gondoskodik arról, hogy az adatkezelésben részt vevő munkatársak a rájuk vonatkozó adatvédelmi előírásokat megismerjék, és szükség esetén megfelelő tájékoztatást vagy oktatást kapjanak.

A szabályzat aktuális, hatályos változatát az intézmény által meghatározott elektronikus vagy papíralapú formában kell hozzáférhetővé tenni.

27.4. A szabályzat karbantartása

A szabályzat folyamatos karbantartásáról és szükség szerinti aktualizálásáról az intézményvezető által kijelölt személy vagy szervezeti egység gondoskodik.

A módosítások során figyelembe kell venni:

- a vonatkozó jogszabályok változásait;
- az intézmény szervezeti és működési változásait;
- az új vagy módosított adatkezelési folyamatokat;
- az informatikai rendszerek változásait;
- az adatvédelmi incidensek tapasztalatait;
- az ellenőrzések és auditok megállapításait;
- a MICS/MIR monitoring és fejlesztési tapasztalatait.

A szabályzat módosításait verziószámmal és dátummal dokumentálni kell.

27.5. A szabályzatban nem rendezett kérdések

A jelen szabályzatban nem szabályozott, illetve vitás kérdésekben a **hatályos európai uniós és magyar adatvédelmi, köznevelési, szakképzési, munkajogi, iratkezelési és egyéb vonatkozó jogszabályok**, valamint az intézmény és az egyetem hatályos belső szabályzatai az irányadók.

Jogszabály és jelen szabályzat rendelkezése közötti eltérés esetén a magasabb szintű jogszabály rendelkezéseit kell alkalmazni, és a szabályzatot szükség szerint felül kell vizsgálni.

27.6. Jóváhagyás

Jelen szabályzatot az intézményvezető jóváhagyta.