MAGYARORSZÁGI REFORMÁTUS EGYHÁZ
OKTATÁSI SZOLGÁLAT

1146 Budapest, Abonyi utca 27.
telefon: +36-30-268-0229
1440 Budapest, Pf.: 23.

oktatasi.szolgalat@reformatus.hu
www.reformatus.hu

Iktatószám: 800531/2026.

ADATVÉDELMI SZABÁLYZAT

Budapest, 2026. augusztus 27.

Bruckner László Zoltán
szolgálatvezető főigazgató
MRE Oktatási Szolgálat

1146 Budapest, Abonyi utca 27.
telefon: +36-30-268-0229
1440 Budapest, Pf.: 23.

oktatasi.szolgalat@reformatus.hu
www.reformatus.hu

I. Általános rendelkezések

1. A szabályzat célja és hatálya

A szabályzat célja, hogy meghatározza az MRE Oktatási Szolgálat (a továbbiakban: az OSZ vagy Adatkezelő) adatkezelési tevékenységének rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, és az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A szabályzat tárgyi hatálya az OSZ által folytatott személyes adatokat érintő adatkezelésre és adatfeldolgozásra, személyi hatálya az OSZ-szel munkavégzésre irányuló jogviszonyban álló valamennyi természetes személyre kiterjed.

2. Alapfogalmak

Személyes adat: bármely meghatározott, azonosított vagy azonosítható természetes személlyel (érintettel) kapcsolatba hozható adat és az adatból levonható, az érintettre vonatkozó következtetés.

Érintett: bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A természetes személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet. A fentiek alapján tehát nem csak az tekintendő érintettnek, akinek adatkezelő kifejezetten a természetes személyazonosító adatait kezeli, az érintetti minőség fennállásához pedig elegendő az is, ha az egyenként személyes adatnak nem minősülő információk kombinációja teszi azonosíthatóvá a természetes személyt.

Különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adat, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok. A különleges adatok kezeléséhez önmagában nem elegendő valamely jogalap fennállása, ahhoz szükséges egy további, a GDPR 9. cikk (2) bekezdésében megjelölt feltétel is.

Adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége. Az adatfeldolgozó az adatkezelőtől elkülönült személy vagy szervezet.

Címzett: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e.

Harmadik ország: minden, az Európai Gazdasági Térségen kívüli ország.

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.

3. Adatkezelő adatvédelmi szervezete

Adatkezelő szervezeti sajátosságaiból fakadóan köteles:

a) e szabályzat megalkotására és jóváhagyására, valamint

b) adatvédelmi tisztviselő kijelölésére.

Adatkezelő adatvédelmi szervezete – a fentiekre is tekintettel – a következők szerint kerül meghatározásra:

Adatkezelő vezetője a főigazgató. A főigazgató meghatározza az adatvédelem szervezetét, továbbá megállapítja az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket.

3.1. A főigazgató

a) felelős az érintetteknek GDPR-ben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért,

b) felelős az Adatkezelő által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért,

c) felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért,

d) felügyeli az adatvédelmi tisztviselő tevékenységét,

e) vizsgálatot rendelhet el, továbbá

f) kiadja az Adatkezelő adatvédelemmel kapcsolatos belső szabályozóit.

A szabályzatban előírtak betartatásáért alapvetően a szervezet vezetője a felelős.

3.2. Az osztályvezetők

Az egyes osztályvezetők a főigazgatóutasításai szerint közreműködnek a 3.1. pontban meghatározott feladatok ellátásában, valamint véleményezik a szakterületükhöz kapcsolódó adatvédelmi dokumentumokat.

3.3. Az adatkezelő egyéb munkatársai

Az Adatkezelő munkatársai munkájuk során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

3.4. Az adatvédelmi tisztviselő

3.4.1. Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai:

a) tájékoztat és szakmai tanácsot ad az Adatkezelő, továbbá az adatkezelést végző munkatársak részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

b) ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését;

d) együttműködik a felügyeleti hatósággal;

e) az adatkezeléssel összefüggő ügyekben – ideértve a GDPR 36. cikkében említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

3.4.2. Az adatvédelmi tisztviselő jogállása:

Az adatvédelmi tisztviselőt szakmai rátermettség, az adatvédelmi jog és gyakorlat szakértői szintű ismerete alapján kell kijelölni.

Adatkezelő az adatvédelmi tisztviselő elérhetőségét közzéteszi honlapján, továbbá gondoskodik az adatvédelmi tisztviselő bejelentéséről a Nemzeti Adatvédelmi és Információszabadság Hatóság részére.

Adatkezelő biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint biztosítja számára, hogy a feladatai ellátása során utasításokat senkitől ne fogadjon el, ezen feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható. Az adatvédelmi tisztviselő szervezetileg közvetlenül az Adatkezelő szervezet vezetőjének tartozik felelősséggel.

II. Az adatkezelés szabályai

1. Adatkezelés és adatfeldolgozás

Azon adatkezelések tekintetében, amelyek vonatkozásában a személyes adatok kezelésének céljait és eszközeit Adatkezelő határozza meg, az OSZ-t kell adatkezelőnek tekinteni. Az OSZ-t kell adatkezelőnek tekinteni akkor is, ha az adatkezelés céljait és eszközeit uniós vagy tagállami jog határozza meg és uniós vagy tagállami norma az OSZ-t határozza meg adatkezelőként.

Az OSZ az adatkezelés során adatfeldolgozót vehet igénybe, aki az adatkezelő nevében, annak megbízásából és adott esetben konkrét utasításai szerint az OSZ számára adatfeldolgozást végez. Kizárólag olyan adatfeldolgozó vehető igénybe, aki megfelelő garanciákat nyújt az adatvédelmi szabályoknak való megfelelést és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

Az OSZ maga is eljárhat adatfeldolgozóként.

Amennyiben az OSZ adatkezelőként jár el és adatfeldolgozót vesz igénybe, vagy amennyiben az OSZ maga is adatfeldolgozóként jár el, úgy **az adatfeldolgozás feltételeit írásbeli megállapodásba** (szerződésbe) **kell foglalni**. A megállapodásban az adatfeldolgozó részére legalább az alábbi feltételeket és kötelezettségeket kell előírni:

a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli - beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is -, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;

b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

c) meghozza a GDPR 32. cikkében előírt intézkedéseket;

d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan a GDPR 28. cikk (2) és (4) bekezdéseiben említett feltételeket;

e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett III. fejezetben foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

f) segíti az adatkezelőt a GDPR 32-36. cikk szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;

g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;

h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely az e cikkben meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

2. Az adatkezelés célja

Az OSZ a Magyarországi Református Egyház köznevelési, szakképzési, hittanoktatási ügyeinek és a református roma szakkollégiumokügyeinek adminisztratív, koordináló és ügyintéző szerve. Az OSZ tevékenysége körében megvalósuló adatkezelések sokrétűek, és a mindenkori feladatellátáshoz, jogszabályi kötelezettségekhez és egyházi döntésekhez igazodva változhatnak. A konkrét adatkezelések pontos célját az adatkezelési tevékenységek nyilvántartása tartalmazza.

Az OSZ tevékenységeivel összefüggésben tipikusan előforduló adatkezelési célkategóriák különösen az alábbiak:

a) hittanoktatással összefüggő adatkezelés;

b) a munkavállalók, megbízottak és az Adatkezelővel egyéb, munkavégzésre irányuló jogviszonyban állók jogviszonyának létesítéséhez, fenntartásához és megszűnéséhez vagy megszüntetéséhez kapcsolódó adatkezelések;

c) az intézményhálózattal való kapcsolattartás körében felmerült adatkezelések;

d) szerződésekkel összefüggő adatkezelések;

e) számviteli kötelezettségek teljesítéséhez kapcsolódó adatkezelések;

f) vagyonvédelem, információbiztonság, ellenőrzés, panaszkezelés, követeléskezelés;

g) támogatáskezeléssel összefüggő adatkezelések.

3. Az adatkezelés jogalapjai

A GDPR 6. cikke értelmében **a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:**

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

b) az adatkezelés olyan **szerződés teljesítéséhez szükséges**, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az adatkezelőre vonatkozó **jogi kötelezettség teljesítéséhez szükséges**;

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

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott **közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges**;

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

A GDPR 9. cikk (1) bekezdése szerint a különleges adatok kezelése főszabály szerint tilos. Különleges adat kezelésére kizárólag akkor kerülhet sor, ha – érvényes jogalap mellett – valamely, a GDPR 9. cikk (2) bekezdésében foglalt feltétel is fennáll.

4. Az adatkezelési tevékenységek nyilvántartása

Adatkezelő a GDPR 30. cikk (1) bekezdése értelmében köteles az általa végzett adatkezelési tevékenységekről nyilvántartást vezetni.

A nyilvántartás az alábbiakat tartalmazza:

a) **az Adatkezelő megnevezését és elérhetőségét**, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az **adatvédelmi tisztviselőnek a nevét és elérhetőségét**;

b) **az adatkezelés céljait**;

c) az **érintettek kategóriáinak**, valamint **a kezelt személyes adatok kategóriáinak ismertetését**;

d) az olyan címzettek kategóriáit, **akikkel a személyes adatokat közlik** vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;

e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információkat, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírását;

f) ha lehetséges, a különböző **adatkategóriák törlésére előirányzott határidőket**;

g) ha lehetséges, a GDPR 32. cikk (1) bekezdésében említett **technikai és szervezési intézkedések általános leírását**.

A nyilvántartás vezetéséért az adatvédelmi tisztviselő felelős. Új adatkezelési tevékenység megkezdését megelőzően a tervezett tevékenységről tájékoztatni kell az adatvédelmi tisztviselőt.

5. Adatkezelési tájékoztatók

A személyes adatok kezelésének körülményeiről az érintetteket előzetesen (de legkésőbb az adatkezelési tevékenység megkezdésekor) **tájékoztatni kell.**

A tájékoztatás megvalósulhat

a) papír alapú tájékoztató átadásával vagy

b) a tájékoztató online közzétételével és legalább a tájékoztatóra mutató hivatkozás érintettnek történő megküldésével.

Bizonyos esetekben – indokolási kötelezettség mellett és az adatvédelmi tisztviselővel történő egyeztetést követően – az adatkezelésért felelős szakterület osztályvezetője a tájékoztatás más módját is választhatja, ám a GDPR és az Infotv. szabályai ekkor sem sérülhetnek.

A tájékoztató tartalmára a GDPR hatálya alá tartozó adatkezelési tevékenység esetében a rendelet 13-14. cikkei, az Infotv. hatálya alá tartozó adatkezelési tevékenység esetében az Infotv. 16.§-a a megfelelően irányadó.

A tájékoztatót az adatvédelmi tisztviselő a szakterületi osztályvezetővel együttműködve készíti elő. A tájékoztatót a szakterületi osztályvezető egyezteti az Igazgatási osztály osztályvezetőjével, majd jóváhagyását követően a főigazgató vagy az általa kijelölt személy kiadmányozza.

6. Adatfeldolgozói szerződések

Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – **szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben.** A szerződés vagy más jogi aktus különösen előírja, hogy az adatfeldolgozó:

a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az

adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;

b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

c) meghozza a GDPR 32. cikkében („az adatkezelés biztonsága") előírt intézkedéseket;

d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan a GDPR 28. cikk (2) és (4) bekezdésben említett feltételeket (további adatfeldolgozó csak előzetes hozzájárulással vehető igénybe, a további adatfeldolgozóra is ugyanazokat az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az Adatkezelő és az adatfeldolgozó közötti szerződésben létrejöttek);

e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett GDPR. III. fejezetben foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

f) segíti az adatkezelőt a GDPR 32–36. cikk szerinti kötelezettségek (adatkezelés biztonsága, adatvédelmi incidensek bejelentése és az érintettek tájékoztatása, adatvédelmi hatásvizsgálat lefolytatása, előzetes konzultáció) teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;

g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;

h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely a GDPR 28. cikkben meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

7. Adatfeldolgozóként végzett tevékenységek nyilvántartása

Amennyiben Adatkezelő adatfeldolgozóként jár el, úgy nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról; a nyilvántartás a következő információkat tartalmazza:

a) az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;

b) az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;

c) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása;

d) ha lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

Adatfeldolgozói tevékenységet Adatkezelő csak adatfeldolgozói megállapodás alapján végezhet.

8. Adattovábbítás és az adattovábbítások nyilvántartása

Az Adatkezelő **személyes adatot az érintett önkéntes**, az adatkezelés körülményeit illetően tájékozott **hozzájárulása hiányában csak jogszabály felhatalmazása alapján, a jogszabályban meghatározott szerv vagy személy részére**, és csak jogszabályban meghatározott adatkörben, a célhoz kötöttség elvének érvényesítése mellett **továbbíthat.**

Az **adattovábbítás tényéről az érintettet** – előzetesen, az adatkezelési tájékoztató megismertetésével, erre irányuló kérése esetén egyedileg is **tájékoztatni kell.** Mindezek érdekében az adatkezelő **adattovábbítási nyilvántartást vezet** vagy az adatkezelési tevékenység vonatkozásában olyan elektronikus naplózást alkalmaz, amelyből a nyilvántartáshoz szükséges adatok utólag is kinyerhetők.

Az adattovábbítási nyilvántartás az alábbiakat tartalmazza:

a) a személyes adatok továbbításának időpontját;

b) a továbbított adatköröket;

c) az adattovábbítás jogalapját;

d) az adattovábbítás címzettjét; valamint

e) az adattovábbításért felelős személy nevét és elérhetőségét.

Amennyiben az **adattovábbítás szervezeten belül** történik, abban az esetben is gondoskodni kell arról, hogy a személyes adat csak olyan személy részére kerüljön továbbításra, aki megfelelő hozzáférési jogosultsággal rendelkezik (összhangban a célhoz kötöttség alapelvével).

Az adatátadás kizárólag **abban az esetben nem minősül adattovábbításnak, ha a személyes adat átadása adatfeldolgozónak történik.** Az adatfeldolgozó kilétéről, a részére továbbított személyes adatok köréről az érintetettet előzetesen tájékoztatni kell.

III. Az adatvédelmi incidens

1. Az incidens bejelentése

Az 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.

Adatkezelő azon **munkavállalój**a, vagy az Adatkezelővel munkavégzésre irányuló jogviszonyban álló azon személy, aki az Adatkezelő által kezelt vagy feldolgozott személyes adatokkal kapcsolatban **adatvédelmi incidenst** (különösen: jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést, megsemmisítést, vagy véletlen megsemmisülést és sérülést) észlel, **köteles azt a főigazgatónak és az adatvédelmi tisztviselőnek haladéktalanul bejelenteni.**

A bejelentésnek minimálisan tartalmaznia kell:

a) a bejelentő nevét és elérhetőségét;

b) az incidens tárgyát; valamint

c) azt a tényt, hogy az incidens informatikai rendszert érint-e.

Ha a főigazgató vagy az adatvédelmi tisztviselő megállapítja, hogy az incidens informatikai rendszert is érint, akkor tájékoztatást kell küldeni a rendszergazdának.

Amennyiben az **adatvédelmi tisztviselő** a fentiek szerint tudomást szerez az incidensről, úgy **a bejelentést megvizsgálja, a bejelentőtől szükség szerint további információt kér, amelyet a bejelentő haladéktalanul köteles megadni.**

Az adatszolgáltatásnak tartalmaznia kell:

a) az incidens bekövetkezésének időpontját és helyét;

b) az incidens leírását, körülményeit, hatásait;

c) az incidens során kompromittálódott adatok körét, számosságát;

d) a kompromittálódott adatokkal érintett személyek körét;

e) az incidens elhárítása érdekében tett intézkedések leírását;

f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

Amennyiben az adatszolgáltatás alapján az adatvédelmi incidens további vizsgálatot igényel, annak végrehajtására az adatvédelmi tisztviselő felkéri a szerv vezetőjét (informatikai rendszerben bekövetkezett adatvédelmi incidens esetében a rendszergazdát is bevonva), majd szaktanácsadóként működik közre a vizsgálat lefolytatásában.

A vizsgálat megállapításai alapján az adatvédelmi tisztviselő (informatikai rendszerben bekövetkezett adatvédelmi incidens esetében a rendszergazda véleményével együtt) – **javaslatot tesz az adatvédelmi incidens elhárításához szükséges intézkedésekről a főigazgató részére.**

A javaslat alapján a megvalósítandó további intézkedésekről a főigazgató dönt.

Az adatvédelmi incidens elhárítása érdekében elrendelt egyes intézkedésekről és azok végrehajtásáról a főigazgató haladéktalanul tájékoztatja az adatvédelmi tisztviselőt.

Az incidens felügyeleti hatóság részére történő bejelentését az adatvédelmi tisztviselő végzi el. A bejelentésre nyitva álló határidő elmulasztása a szervezet felelőssége abban az esetben, ha nem vagy nem haladéktalanul tette meg a fenti bejelentést vagy intézkedéseket.

2. Az incidensek nyilvántartása

Az adatvédelmi incidensekről Adatkezelő nyilvántartást vezet.

A nyilvántartásba rögzíteni kell:

a) az érintett személyes adatok körét;

b) az adatvédelmi incidenssel érintettek körét és számát;

c) az adatvédelmi incidens időpontját;

d) az adatvédelmi incidens körülményeit, hatásait, az adatvédelmi incidens elhárítására megtett intézkedéseket;

e) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat személyes adatokat érintő incidens esetében 5 évig, különleges adatokat érintő incidens esetében 20 évig köteles az Adatkezelő megőrizni.

3. Hatósági bejelentés és az érintettek tájékoztatása az incidensekről

Az adatvédelmi tisztviselő az adatvédelmi incidenst a bekövetkezését követően haladéktalanul, de legkésőbb a bekövetkezéséről való tudomásszerzéstől számított 72 órán belül bejelenti a NAIH részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az adatvédelmi tisztviselő köteles ennek okát igazolni a NAIH részére.

A hatósági bejelentés tartalmazza

a) az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát;

b) az adatvédelmi incidens jellegét, körülményeit;

c) az adatvédelemért felelős személy nevét és elérhetőségét;

d) az adatvédelmi incidens valószínűsíthető következményeit; valamint

e) az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira, szabadságaira nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő a szervezet főigazgatójának közreműködésével haladéktalanul értesíti az érintetteket.

Nem kell az érintetteket értesíteni:

a) ha az Adatkezelő olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét;

b) ha az adatvédelmi incidens bekövetkezését követően az Adatkezelő olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg;

c) ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

IV. Hatásvizsgálat

A GDPR 24. cikk (1) bekezdése alapján Adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és

súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik. Ezeket az intézkedéseket az Adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi. Ennek keretében **a természetes személyek jogaira és szabadságaira nézve magas kockázattal járó esetekben Adatkezelőnek fel kell mérnie a kockázat valószínűségét és súlyosságát.**

A valószínűség és súlyosság felmérésének alapvető módszere az adatvédelmi hatásvizsgálat, amely magában foglalja az említett kockázat mérséklését, a személyes adatok védelmét, valamint a GDPR-nak való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat.

Az eredményes kockázatkezeléshez az alábbiak feltárása szükséges:

a) az adatkezelés jellegének meghatározása;

b) az adatkezelési műveletek szükségességének és arányosságának vizsgálata;

c) annak feltárása, hogy milyen kockázatokkal lehet számolni és azok kezelésére milyen intézkedések szolgálhatnak.

Adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

a) amikor a személyes adatkezelés célja a természetes személyekkel kapcsolatos döntés meghozatala, méghozzá a természetes személyek személyes jellemzőinek szisztematikus, kiterjedt és automatizált értékelése alapján (pl.: profilalkotás);

b) a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok, mint a személyes adatok különleges kategóriáinak kezelése;

c) a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy

d) nyilvános helyek nagymértékű, módszeres megfigyelése, különösen abban az esetben, ha azt elektronikus optikai eszközök alkalmazásával hajtják végre;

e) ha az illetékes felügyeleti hatóság úgy ítéli meg, hogy az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, különösen mivel megakadályozza, hogy az érintettek a jogaikat gyakorolják, vagy szolgáltatásokat vegyenek igénybe, illetve szerződést érvényesítsenek, esetleg mindössze azért, mert az említett műveletekre szisztematikusan és nagy számban kerül sor.

V. Az érintetti jogérvényesítésre vonatkozó rendelkezések

1. Előzetes tájékoztatási kötelezettség

Az érintettek részére a személyes adatok megszerzésének időpontjában tájékoztatást kell adni a személyes adatok kezelésének tényéről, céljáról, jogalapjáról, a kezelt adatok köréről, az adatkezelés módjáról, időtartamáról vagy az időtartam meghatározásának szempontjairól, az adattovábbítás szabályairól, a felügyeleti hatósághoz címzett panasz benyújtásának jogáról.

A fentiek szerinti tájékoztatás mellett az érintett figyelmét kifejezetten fel kell hívni a tiltakozáshoz való jog érvényesítésének lehetőségére, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

A tájékoztatásokat az Adatkezelő honlapján, tömör, átlátható, és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell elhelyezni.

A munkavállalókra, a megbízottakra és az egyéb, munkavégzésre irányuló jogviszonyban álló természetes személyek jogviszonyára vonatkozó tájékoztatást a jogviszony létesítésekor elektronikus formában kell megadni, amelynek megtörténtét az érintett papír alapú nyilatkozatával írásban igazolni köteles.

A tájékoztatási kötelezettségre egyebekben a szabályzat II.5. pontjában foglalt szabályokat kell alkalmazni.

2. A helyesbítéshez való jog gyakorlása

Az érintett kérelmére az adatkezelést végző munkatárs vagy az adatvédelmi tisztviselő indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozó pontatlan személyes adatokat.

3. A törléshez való jog

Az érintett kérelmére az adatkezelést végző munkatárs vagy az adatvédelmi tisztviselő indokolatlan késedelem nélkül törli az érintett személyes adatait vagy azoknak az érintett által meghatározott körét, feltéve, hogy az alábbi esetek valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;

d) a személyes adatokat jogellenesen kezelték;

e) a személyes adatokat az Adatkezelő által alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell.

Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és az első bekezdés értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – a szóban forgó személyes adatokra mutató hivatkozások vagy e személyes adatok másolatának, illetve másodpéldányának törlése érdekében.

Az Adatkezelő a személyes adatok törlését a jogszerű kérelem ellenére sem végezheti el, amennyiben az adatkezelés szükséges:

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

b) a személyes adatok kezelését előíró, az adatkezelő által alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése céljából;

c) közérdekből végzett feladat végrehajtása céljából;

d) közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az adattörlés valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést;

e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

4. Az adatkezelés korlátozásához való jog

Az érintett kérelmére az adatkezelést végző munkatárs korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő ellenőrizze a személyes adatok pontosságát;

b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c) az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy az érintett tiltakozási jogával élt az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

Az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

Az adatkezelés korlátozásához való jog jogi kötelezettségen alapuló adatkezelés (a GDPR 6. cikke (1) bekezdésének c) pontja) vagy közérdekű feladat ellátása esetén (a GDPR 6. cikke (1) bekezdésének e) pontja) a korlátozás nem érintheti az adatkezelőt terhelő jogszabályi adatkezelési vagy adatmegőrzési kötelezettségeket.

5. A címzettek tájékoztatásának kötelezettsége

Az Adatkezelő minden olyan címzettet tájékoztat a személyes adatot érintő valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

6. Az adathordozhatósághoz való jog

Az érintett kérelmére az adatkezelést végző munkatárs biztosítja a személyes adatok hordozhatóságát az alábbi feltételek teljesülése esetén:

a) a személyes adatokat az érintett bocsátotta az Adatkezelő rendelkezésére;

b) az adatkezelés jogalapja hozzájárulás vagy az érintett és az Adatkezelő között kötött szerződés;

c) adatkezelés automatizált módon történik;

d) a személyes adatok hordozása nem érinti hátrányosan mások jogait vagy szabadságait.

Az adathordozhatósághoz való jog gyakorlása során az Adatkezelő köteles a személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban az érintett rendelkezésére bocsátani.

Az érintett kérheti, hogy az Adatkezelő a személyes adatokat közvetlenül egy másik adatkezelő részére továbbítsa. E lehetőséggel az érintett abban az esetben élhet csak, ha az technikailag megvalósítható.

Az Adatkezelő emellett – a hozzáféréshez való jog érvényesülésének elősegítése érdekében – papír alapon is köteles rendelkezésre bocsátani a személyes adatokat.

Az adathordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

7. A tiltakozáshoz való jog

Amennyiben az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, az érintett tiltakozhat a személyes adatok kezelése ellen.

Tiltakozás esetén az Adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen.

Amennyiben az érintett tiltakozik a személyes adatok közvetlen üzletszerzés céljából történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

8. A jogorvoslathoz való jog

Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett – az adatkezelést végző munkatárs útján vagy közvetlenül – az adatvédelmi tisztviselőhöz fordulhat, aki a panaszt megvizsgálja, és ha alapos, intézkedést kezdeményez, ellenkező esetben a panaszt elutasítja.

Az elutasításról az Adatkezelő a panaszost a kérelem kézhezvételét követő 30 napon belül írásban tájékoztatja, a kérelem elutasításának ténybeli és jogi indokait is közölve. A kérelem elutasítása esetén a panaszost tájékoztatni kell a bírósági jogorvoslat, továbbá a felügyeleti szervhez fordulás lehetőségéről is.

Ha az érintett továbbra is sérelmezi azt, ahogy az Adatkezelő kezeli az adatait, vagy közvetlenül hatósághoz szeretne fordulni, akkor bejelentéssel élhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (postacím: 1530 Budapest, Pf.: 5. E-mail: ugyfelszolgalat@naih.hu, honlap: www.naih.hu).

Az érintettnek lehetősége van továbbá személyes adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el. Ebben az esetben az érintett szabadon választhat, hogy a lakóhelye vagy a tartózkodási helye szerinti törvényszéknél (http://birosag.hu/torvenyszekek) nyújtja-e be keresetét.

Az érintett a lakóhelye vagy tartózkodási helye szerinti törvényszéket megtalálhatja a http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso oldalon.

VI. Információbiztonsági előírások

1. Adatbiztonság

Adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatókörei, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve – többek között – adott esetben:

a) a személyes adatok álnevesítését és titkosítását,

b) a személyes adatok kezelésére használt rendszerek folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét,

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen álltani,

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedéseknek hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

2. Fizikai kontroll

A fizikai kontroll az iratokhoz és a számítógépes környezethez való hozzáférés korlátozását, valamint a rendszeres adatmentés biztosítását foglalja magában.

Szervezetünknél az alábbi fizikai kontrollok kerültek bevezetésre:

a) Székhelyünkön riasztórendszer került kiépítésre.

b) A székhelyünkön folyamatosan helyezünk el zárható szekrényeket a személyes adatokat tartalmazó iratok tárolása céljából,

c) Kötelező a jelszó alkalmazása minden munkaállomás (PC, laptop stb.) esetén, ideértve a hibernálás/képernyőkímélő kötelező alkalmazását, amelyet csak jelszóval lehet kikapcsolni,

d) A jelszavakat jelszó-házirend alapján kell képezni, gondoskodni kell arról, hogy azok rendszeres időközönként, de legfeljebb kétévenként megváltoztatásra kerüljenek.

e) Be kell tartani a „tiszta asztal" elvét, azaz gondoskodni kell arról, hogy amennyiben a munkatárs munkavégzésének helyét a nap végén vagy nap közben akár csak ideiglenes jelleggel elhagyja, úgy minden, személyes adatot akár csak potenciálisan tartalmazható dokumentuma zárható szekrénybe vagy zárható fiókba kerüljön.

f) A takarító személyzet köteles titoktartási nyilatkozatot tenni.

Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult és az irat megőrzésére irányadó határidő eltelt, úgy az Adatkezelő intézkedik az irat megsemmisítéséről.

A megsemmisítés során Adatkezelő iratkezelési szabályzata alapján kell eljárni.

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében Adatkezelő az alábbi intézkedéseket és garanciális elemeket alkalmazza:

a) az adatkezelés során használt számítógépek az Adatkezelő tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír az Adatkezelő;

b) amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;

c) a személyes adatokat kezelő hálózaton (munkaállomáson) a vírusvédelemről folyamatosan gondoskodik.

3. Logikai kontroll

Szervezetünknél az alábbi logikai kontrollok kerültek bevezetésre:

a) Jelszó-házirend

b) Jogosultságkezelés rendje

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészsége nagymértékben hozzásegíti Adatkezelőt a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.

Az informatikai rendszerekben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell.

A személyes adatok biztonsága érdekében Adatkezelő az alábbi jogosultságkezelési előírásokat alkalmazza:

a) Új jogosultság beállítását, illetve jogosultság megváltoztatását a jogosultság birtokosának felhatalmazása alapján a rendszergazda végzi.

b) A jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani.

c) El kell kerülni, hogy teljes hozzáférést, illetve adminisztrátori jogosultságokat kapjanak más munkát végző, illetve a jogosultság birtoklására nem igényt tartó személyek.

d) Külső – karbantartó vagy fejlesztő – cég alkalmazottja folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet.

Amennyiben a jogosultsággal rendelkező munkatárs jogviszonya megszűnik, vagy az általa ellátandó feladatkör módosul, akkor az ezáltal meglévő, ám a feladatkör ellátásához a továbbiakban már nem szükséges jogosultságokat haladéktalanul törölni kell. Ennek érdekében a munkáltató haladéktalanul kezdeményezi a rendszergazdánál a jogosultság törlését. A törlésről a rendszergazda köteles visszajelzést küldeni. A névre szóló fiókok egyes esetekben a szervezeti sajátosságok miatt nem törölhetők, mert azok kapcsolódhatnak a kilépő munkatárs más, a Magyarországi Református Egyháznál betöltött tisztségéhez is. Ilyen esetekben a kilépéssel egyidejűleg a kilépő munkatárs köteles a munkavégzéshez kapcsolódóan kezelt, személyes adatokat tartalmazó állományokat az átadás-átvételi eljárást követően haladéktalanul törölni és a törlésről nyilatkozni. A kilépő munkatárs abban az esetben, ha a fiókjában más, az adatkezelő tevékenységéhez nem kapcsolódó adatkezelést is folytatott, úgy köteles e tényt jelezni és amennyiben a fiókjában található adatokat más rendelkezésére kell bocsátania, úgy azok törléséről gondoskodnia kell. A kilépő munkatárs a törlés megtörténtéről a kiléptetési eljárás keretében szintén köteles nyilatkozni.

Az informatikai rendszerben a kilépő felhasználók profiljait fel kell függeszteni, használaton kívül kell helyezni. A felhasználói fiókok törlése a rendszerek ellenőrzését követően történhet meg, ha a törlés nem okoz adatvesztést.

Amennyiben a munkatárs a nevéhez rendelt munkahelyi e-mail-cím megszüntetését kéri, a postafiók megszüntetését megelőzően – amennyiben azt az OSZ működési, iratmegőrzési vagy jogi érdeke indokolja – a postafiók tartalmáról archivált mentés készíthető. Az archiválás technikai műveletként történik, és önmagában nem jogosítja fel az archiválást végző személyt a levelezés tartalmának általános vagy cél nélküli megismerésére. Az archivált állományhoz kizárólag a jelen Szabályzat mellékletében meghatározott személyek, illetve munkakörök jogosultak hozzáférni. Az archivált állományban keresés kizárólag konkrét, előre meghatározott szervezeti célból, a szükséges mértékre korlátozva és dokumentált módon végezhető. A keresést lehetőség szerint technikai szűkítéssel – így különösen időszak, feladó, címzett, tárgy vagy meghatározott keresőkifejezés alapján – kell elvégezni. Amennyiben a keresés során nyilvánvalóan magánjellegű vagy a munkavégzéssel össze nem függő levelezés kerül elő, annak tartalma tovább nem vizsgálható. A postafiók az archiválást követően megszüntetésre kerül. Az archivált állomány megőrzési idejét, valamint a hozzáférések és keresések dokumentálásának rendjét az OSZ a jelen Szabályzatban, illetve annak mellékletében határozza meg.

4. Adminisztratív kontroll

Az adminisztratív kontrollokat a szervezet belső szabályozói, rendelkezései, eljárásrendjei tartalmazzák. Az Adatkezelőnek e körben rendelkeznie szükséges minimálisan egy üzletmenet-folytonossági tervvel, valamint egy katasztrófaelhárítási tervvel.

Az adminisztratív kontrollokat a fentieken túl az alábbi dokumentumok tartalmazzák:

a) Szervezeti és működési szabályzat;

b) Iratkezelési szabályzat;

c) Számviteli politika és annak mellékletei (különösen: pénzkezelési szabályzat).

Az adminisztratív védelem biztosítása érdekében az OSZ rendszeresen, de legalább évi egy alkalommal adatbiztonsági tudatossággal összefüggő képzést tart, amelyen valamennyi, a szervezet által alkalmazott munkatárs köteles részt venni.

A szervezet által a dolgozó részére biztosított valamennyi eszközön (ideértve a használatra átadott mobil eszközöket is) csak az informatikus rendelkezik adminisztrátori jogosultságokkal, így az alkalmazások telepítése ellenőrzött, a felhasználó által nem lehetséges. Ezen eszközökön tilos a magáncélú fájlok tárolása.

VII. Záró rendelkezések

Jelen szabályzat 2026. szeptember 1. napján lép hatályba.

Melléklet

Megszüntetett munkahelyi e-mail-fiókok archiválása és hozzáférése

A megszüntetett munkahelyi e-mail-fiókról – indokolt esetben – archivált mentés készíthető. Az archivált állomány alapértelmezett megőrzési ideje **3 év**.

Az archívumhoz kizárólag az alábbi jogosultak férhetnek hozzá:

Jogosult	**Jogosultság**
Informatikai feladatokat ellátó személy	Archiválás, technikai keresés
Főigazgató vagy kijelölt vezető	Keresés engedélyezése
Adatvédelmi tisztviselő	Adatvédelmi kontroll, véleményezés

Az archivált állományban keresés kizárólag **konkrét, előre meghatározott szervezeti célból** végezhető. Általános jellegű átvizsgálás nem megengedett.

A keresést lehetőség szerint dátum, feladó, címzett, tárgy vagy keresőkifejezés alapján kell szűkíteni. Magánjellegű vagy a munkavégzéssel össze nem függő levelezés tartalma nem vizsgálható tovább.

A keresés tényét, célját, időpontját és a hozzáférő személy nevét dokumentálni kell.

A 3 éves megőrzési idő lejártával az archívumot törölni kell, kivéve, ha további megőrzését konkrét jogi, hatósági vagy egyéb dokumentált szervezeti érdek indokolja.