

Adatvédelmi szabályzat

Neumann János Gimnázium, Szakgimnázium és Kollégium

2018

Tartalom

Adatvédelmi szabályzat	5
1 A szabályozás célja és hatálya	5
2 Általános rendelkezések	6
2.1 Fogalmak meghatározása	6
2.2 Az adatkezelés alapelvei	7
.2.2.1 Átláthatóság.....	7
.2.2.2 Célhoz kötöttség.....	7
.2.2.3 Pontosság	7
.2.2.4 Korlátozott tárolhatóság.....	8
.2.2.5 Integritás és bizalmas jelleg.....	8
.2.2.6 Elszámoltathatóság.....	8
3 Az intézményi adatkezelés szabályai	8
3.1 Adatvédelmi felelős	8
3.2 Az adatkezelés nyilvántartása	9
3.3 Új nyilvántartás bevezetése.....	9
.3.3.1 Célok meghatározása.....	10
.3.3.2 Jogalap meghatározása	10
.3.3.3 A személyes adatok meghatározása.....	11
.3.3.4 Integritás és bizalmas jelleg.....	11
.3.3.5 Az adatkezelés különös szabályai	11
.3.3.6 A nyilvántartás bevezetése.....	11
3.4 Adattovábbítás az intézményen belül	11
3.5 Adattovábbítás harmadik félnek	12
3.6 Papír alapú nyilvántartások különleges szabályai	12
4 Az adatkezelő személyek tevékenysége.....	12
5 A szabályzat megismertetésének rendje.....	14
6 A szabályzat felülvizsgálata.....	14
Érintett panaszkezelési szabályzata.....	15
7 Az érintettek jogai	15
7.1 Tájékoztatáshoz való jog.....	15
7.2 Hozzáférési jog.....	15
7.3 Helyesbítéshez való jog	15
7.4 Törléshez való jog	15

7.5	Az adatkezelés korlátozásához való jog	16
7.6	A helyesbítéshez, törléshez, korlátozáshoz kapcsolódó értesítési kötelezettség.....	16
8	Az érintett panasztevésének módja	16
9	Teendők az érintett panasza esetén	16
10	Intézkedések az érintett panasza esetén	17
11	Jogorvoslati igény.....	18
Incidens kezelési szabályzat		19
12	Fogalom meghatározás	19
13	Teendők adatvédelmi incidens előfordulása esetén.....	19
14	Az adatvédelmi felelős feladatai adatvédelmi incidens esetén	20
15	Az érintett tájékoztatása az adatvédelmi incidensről	20
16	További teendők az incidens kezelésében	21
Mellékletek.....		22

Adatvédelmi szabályzat

1 A szabályozás célja és hatálya

E szabályzat célja, hogy meghatározza a Neumann János Gimnázium, Szakgimnázium és Kollégiumban (továbbiakban Intézmény, illetve Adatkezelő) vezetett nyilvántartások törvényes rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok jogosulatlan megváltoztatását és nyilvánosságra hozatalát, az adatok véletlen elveszését vagy megsemmisülését.

E szabályzat célja továbbá az Intézményben keletkezett közérdekű adatok megismerésére vonatkozó eljárási rend, valamint az általános és különös közzétételi lista alapján kötelezően közzéteendő közérdekű adatok körének megállapítása a jogszabályi keretek között.

E szabályzat személyi hatálya kiterjed az Intézmény valamennyi dolgozójára, tanulója, az iskolai infrastruktúrát használó vendégekre, az Intézménnyel szerződéses vagy megbízási jogviszonyban álló természetes személyekre.

A jelen szabályzat tárgyi hatálya kiterjed az Intézmény által kezelt, jogszabály alapján személyes, közérdekű vagy közérdekből nyilvános adatra.

A szabályzat kiterjed minden az iskola területén, valamint a NIVÁK és a kollégiumok területén található olyan számítógépekre és felhasználóra, amelyek az iskolai infrastruktúrát (hálózatot) közvetlenül vagy közvetve használják, függetlenül a gépek tulajdonjogától.

Jelen szabályzat 2018. május 2.-től visszavonásig érvényes.

Dr. Sipos Mihály

igazgató

2 Általános rendelkezések

2.1 Fogalmak meghatározása

- „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

Iskolai környezetben különösen a név, osztály, OM azonosító, dolgozat, jegy, dolgozat kérdésére adott válasz, bizonyítvány, stb.
- „különleges adat”: 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
- „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;
- „az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
- „profilalkotás”: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;
- „álnevesítés”: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;
- „nyilvántartási rendszer”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális, vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
- „adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
- „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
- „címezett”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal

összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

- „harmadik fél”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
- „az érintett hozzájárulása”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy a megerősített félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok 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;
- „genetikai adat”: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;
- „biometrikus adat”: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;
- „egészségügyi adat”: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
- „felügyeleti hatóság”: Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hivatal (továbbiakban NAIH);

2.2 Az adatkezelés alapelvei

.2.2.1 Átláthatóság

Az Adatkezelő az adatkezelést jogszerűen és tisztességesen, az érintett számára átlátható módon végzi. Az adatkezelésről az érintettnek az adatgyűjtés előtt vagy azzal egyidőben tájékoztatást nyújt az adatkezelésről.

.2.2.2 Célhoz kötöttség

Az Adatkezelő az adatokat meghatározott, egyértelmű és jogszerű célból gyűjti. Azokat nem kezeli a célokkal össze nem egyeztethető módon, kivéve a közérdekű archiválás és tudományos, történelmi kutatás célját vagy a statisztikai célt.

.2.2.3 Pontosság

Az Adatkezelő mindent elkövet azért, hogy a tárolt adatok pontosak, akár napra készek legyenek. Ehhez elvárja az érintettek együttműködését az adatváltozások bejelentésében.

.2.2.4 Korlátozott tárolhatóság

Az Adatkezelő az adatokat olyan formában tárolja, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. A személyes adatok tárolása ennél hosszabb ideig csak közérdekű archiválás, tudományos kutatás vagy statisztikai célból történhet.

.2.2.5 Integritás és bizalmas jelleg

Az Adatkezelő a technikai színvonalnak megfelelő technikai és szervezési intézkedésekkel biztosítja az adatok kezelésénél a személyes adatok megfelelő biztonságát, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is beleértve.

.2.2.6 Elszámoltathatóság

Az Adatkezelő felelősséget érez az előző 1-5. pontokban foglaltak betartására. Jelen szabállyal, valamint az Informatikai Biztonsági Szabállyal (továbbiakban IBSZ), valamint azok betartásával és betartatásával bizonyítja, hogy a jogszabályi kötelezettségeinek eleget tesz.

3 Az intézményi adatkezelés szabályai

A Neumann János Gimnázium, Szakgimnázium és Kollégium a személyes adatok kezelésében elkötelezett a vonatkozó jogszabályok betartása, így különösen:

- a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló 2016/679 (EU) Rendelet (továbbiakban: "GDPR"),
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: "Infó törvény"),
- a polgári törvénykönyvről szóló 2013. évi V. törvény (továbbiakban: "Ptk.")

mellett.

A Neumann János Gimnázium, Szakgimnázium és Kollégium működési körében számos személyes adatot gyűjt, elsősorban tanulóiról és dolgozóiról. A nyilvántartások egy része elektronikus, egy részük pedig papír alapú.

Jelen szabályzat minden adatkezelésre vonatkozik, amely személyes adatot kezel, függetlenül az adathordozótól. A kezelt nyilvántartások listája az ASZ 1-es mellékletében az Adatvagyron leltárban található.

Az Adatkezelő az adatokat harmadik félnek, a jogszabályi kötelezettségeket kivéve, nem adja át és nem használja fel marketing célokra.

3.1 Adatvédelmi felelős

Az Intézmény igazgatója a nagyszámú nyilvántartás és a sok érintettre tekintettel Adatvédelmi felelőst bíz meg. Belső adatvédelmi felelős bárki lehet, aki jogi, közigazgatási, informatikai vagy ezeknek megfelelő felsőfokú végzettséggel rendelkezik. Az adatvédelmi felelős lehet külső adatvédelmi szakértő is.

Az adatvédelmi felelős, nevével ellentétben, nem felelős az adatkezelések jogszerűségéért, az adatkezeléseket érintő döntéseket nem az adatvédelmi felelős hozza meg. Ebben a szerepkörben közvetlenül az igazgatónak van alárendelve.

Az adatvédelmi felelős feladatai:

- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- ellenőrzi az adatvédelmi törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;
- kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
- elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;
- az érintett nyilvántartások vezetőivel együttműködve elkészíti a nyilvántartáshoz kapcsolódó tájékoztató dokumentumokat és nyilatkozatokat;
- vezeti a belső incidenskezelési nyilvántartást;
- vezeti az érintett panaszkezelési nyilvántartást;
- ha szükséges, akkor együttműködik a felügyeleti hatósággal;
- gondoskodik az adatvédelmi ismeretek oktatásáról.

3.2 Az adatkezelés nyilvántartása

Az Adatkezelő a személyes adatokat tartalmazó adatkezelésekről nyilvántartást vezet. A nyilvántartás az ASZ 1. mellékletében található. A nyilvántartásnak tartalmazni kell a következő adatokat:

- az adatkezelő neve és elérhetősége, valamint az adatkezelő képviselőjének és az adatvédelmi felelős neve és elérhetősége;
- az adatkezelés céljai;
- az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását;
- ha lehetséges, a különböző adatkategóriák törlésére előírányzott határidők;
- ha lehetséges, a nyilvántartással kapcsolatos technikai és szervezési intézkedések általános leírása.

A nyilvántartás naprakész állapotáért az adatvédelmi felelős felel. Új nyilvántartás csak az adatvédelmi felelőssel előzetes konzultáció után hozható létre.

3.3 Új nyilvántartás bevezetése

Az Adatkezelő a személyes adatokat kizárólag az előzetesen megfogalmazott célok érdekében kezeli. Ha a korábban felvett adatokat az eredeti céltól eltérő célokra kívánja felhasználni, akkor a következőket kell mérlegelni.

Ha az adatgyűjtés céljától eltérő célból történő adatkezelés nem az érintett hozzájárulásán vagy valamely uniós vagy tagállami jogon alapul, annak megállapításához, hogy az eltérő célú adatkezelés összeegyeztethető-e azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték, az adatkezelő többek között figyelembe veszi:

- a személyes adatok gyűjtésének céljait és a tervezett további adatkezelés céljai közötti esetleges kapcsolatokat;

- a személyes adatok gyűjtésének körülményeit, különös tekintettel az érintettek és az adatkezelő közötti kapcsolatokra;
- a személyes adatok jellegét;
- azt, hogy az érintettek nézve milyen esetleges következményekkel járna az adatok tervezett további kezelése;
- megfelelő garanciák meglétét, ami jelenthet titkosítást vagy álnevesítést is.

Ha a mérlegelés során nem állapítható meg szoros kapcsolat az eredeti és új célok között, akkor új nyilvántartás alakul ki, amelyre az ebben a pontban foglaltakat kell alkalmazni.

Új nyilvántartás alakul ki akkor is, ha az eddigi tevékenységi körben nem szereplő célokból kezd új adatkezelésbe.

Új adatkezelés tervezésekor az adatvédelmi felelőst értesíteni kell, aki segítséget nyújt a jogszabályi megfelelés teljesítésében, az Adatvagyon leltár adatlapjának kitöltésében, valamint elkészíti a szükséges tájékoztatót az érintettek számára.

.3.3.1 Célok meghatározása

Az adatkezelés megkezdése előtt meg kell határozni az adatkezelés pontos célját. A célok megfogalmazása közérthető módon történjen. Az adatkezelés célját a jogalapra hivatkozással kell meghatározni.

.3.3.2 Jogonalap meghatározása

A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- 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;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- 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.

Ha az adatkezelés hozzájáruláson alapul, az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult. A hozzájárulást 16 éven aluliak személyes adatainak kezeléséhez a gondviselőtől kell beszerezni. A 16. életévüket betöltő érintettek maguk nyilatkozhatnak személyes adataik kezeléséről.

Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az

érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti e rendeletet, kötelező erővel nem bír.

.3.3.3 A személyes adatok meghatározása

Az Adatkezelőnek meg kell határoznia, hogy a kitűzött célok eléréséhez milyen adatokra van szükség. A célok eléréséhez szükséges adatok körét a lehető legszűkebben kell meghatározni. (Célhoz kötöttség elve). A célokkal közvetlenül nem indokolható adatok felvétele tilos.

.3.3.4 Integritás és bizalmas jelleg

Az Adatkezelő meghatározza az új nyilvántartás adathordozóját (papír alapú, elektronikus). Meg kell határoznia, hogy a nyilvántartást ki kezeli (adatkezelő). Az adatkezelő vagy kezelők meghatározása történhet szervezeti egység, munkakör vagy konkrét személyek kijelölésével.

Meg kell határozni, hogy az adattartalom helyességéért ki a felelős.

Az adatfelvétel előtt meg kell határozni a tárolás helyét, és hogy ki férhet a tárolt adatokhoz. A korlátozott tárolhatóság elveivel összhangban meg kell határozni a tárolt adatok tárolási határidejét, és a törlés, selejtezés és megsemmisítés módját.

.3.3.5 Az adatkezelés különös szabályai

Az adatkezelés általános szabályait jelen szabályzat (ASZ) tartalmazza, elektronikus adatkezelés esetén a biztonságos kezelés általános szabályait az Informatikai Biztonsági Szabályzat (IBSZ) részletezi.

Ha az érintettek nagy száma, a kezelt adatok érzékenysége vagy az adatkezelés magas kockázata indokolja, akkor az Adatkezelő az érintett nyilvántartásra egyedi szabályzatot alkot. (Például Elektronikus napló) Az így alkotott egyedi szabályzat azonban nem lehet megengedőbb, mint az általános szabályzat, az ASZ vagy az IBSZ.

.3.3.6 A nyilvántartás bevezetése

Legkésőbb az 1.-5. pontok végrehajtása után az illetékes nyilvántartásért felelős értesíti az adatvédelmi felelőst az új nyilvántartás tervezett bevezetéséről. Közösén kitöltik az Adatvagyon leltár adatlapját és a nyilvántartást az adatvédelmi felelős bevezeti az Adatvagyon leltárba. Az adatvédelmi felelős az adatfelvétel vagy adatátvétel előtt elkészíti az érintettek tájékoztatóját, és ha szükséges, akkor a hozzájárulási nyilatkozatot.

Az adatkezelés megkezdése előtt az érintettek részére tájékoztatást kell adni az adatkezelésről a 6.1 pontban megfogalmazott tartalommal. Ha az adatkezelés hozzájáruláson alapul, akkor legkésőbb az adatfelvétel idején be kell szerezni az érintett hozzájárulását, 16 év alatti érintett esetén a gondviselő hozzájárulását.

Elektronikus nyilvántartás esetén az informatikai vezetőt tájékoztatni kell a nyilvántartás bevezetéséről. A hozzáférhetőség technikai megvalósításáért (hálózati jogok) a 3.3.4 pontban meghatározott személyek számára az informatikai vezető felel.

3.4 Adattovábbítás az intézményen belül

Az Intézményben jogszerűen vezetett (ASZ 1. mellékletben szereplő) nyilvántartások között az adattovábbítás megengedett, sőt kívánatos. Adatváltozás esetén a változások az intézményen belül átvezetendők az összes nyilvántartáson. A törlési kérelem azonban csak arra a nyilvántartásra

érvényes, amelyre az érintett fél kéri, illetve hozzájáruláson alapuló adatkezelés esetén, amelyben a hozzájárulást az érintett visszavonja.

A kapcsolódó nyilvántartások adatkezelőinek együttműködése elengedhetetlen a pontosság elvének érvényesüléséhez.

3.5 Adattovábbítás harmadik félnek

Az Intézmény a dolgozók és a tanulók személyes adatait a 2011. évi CXC tv. a nemzeti köznevelésről alapján továbbítja a Köznevelési Információs Rendszerbe (KIR), illetve annak alrendszereibe. Az egyes alrendszerek jogszabályi előírásai a KIR honlapján (https://www.oktatas.hu/hivatali_ugyek) tekinthetők meg. Az adatokért felelős személyt vagy személyeket az igazgató bízza meg.

Olyan megkeresés, amely az Intézmény által kezelt személyes adat továbbítására irányul csak törvényi előírás alapján teljesíthető.

Az olyan esetben, amikor a megkeresés nem törvényi kötelezettségen alapul, csak akkor teljesíthető, ha az érintett ehhez írásban félreérthetetlen hozzájárulását adja. Ha a megkeresés külföldről érkezik, akkor az Adatkezelő köteles meggyőződni arról, hogy az adattovábbítás az Info tv.-ben, illetve a GDPR-ban meghatározott valamely jogalapnak megfelelően történik. Meg kell győződni arról is, hogy az adatok megfelelő védelme biztosított-e a kérelmezőnél. A védelem szintjét nem kell ellenőrizni akkor, ha a célországban is hatályos a GDPR.

3.6 Papír alapú nyilvántartások különleges szabályai

A manuális kezelésű személyes adatok biztonsága érdekében az alábbi intézkedéseket kell fogyanatosítani:

- az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá, a személyzeti, a bér- és munkaügyi, valamint a tanulói jogviszonnyal kapcsolatos iratokat biztonságosan elzárva kell tartani,
- a jelen szabályzatban meghatározott adatkezelések iratainak archiválását évente egyszer el kell végezni, az archivált iratokat az Intézmény iratkezelési és selejtezési szabályzatának, valamint az irattári terveknek megfelelően kell szétválogatni és irattári kezelésbe venni.

A papír alapú dokumentumokat tartalmazó helyiségek, illetve szekrények kulcsához való hozzáférés rendjét az adatkezelő szervezeti egység vezetője állapítja meg.

4 Az adatkezelő személyek tevékenysége

Az adatkezelés megbízhatósága, az integritás és biztonság legfontosabb összetevője az adatkezelő személye. Ez kiemelt feladattá teszi az adatkezelők tevékenységének szabályozását. Az elektronikus nyilvántartások kapcsán felmerülő számítógép használat biztonságáról az IBSZ rendelkezik.

Az Intézménnyel jogviszonyban álló mindazon személy, aki személyes adat birtokába jut vagy munkaköréből fakadóan ilyen adatokat kezel, köteles védeni és őrizni a személyes adatokat, és minden erőfeszítést megtenni annak érdekében, hogy azok megfelelő védelmét biztosítsák.

Az Intézmény munkatársai kötelesek bizalmasan kezelni minden olyan adatot, információt vagy dokumentumot stb., függetlenül attól, hogy ahhoz milyen formában és milyen módon jutottak

hozzá, amely előttük a munkaköri feladataik teljesítése során vagy azzal összefüggésben vált ismertté.

Az Intézménnyel jogviszonyban álló személyek felelősséggel tartoznak minden olyan kárért, amely e szabályzatban és az Informatikai Biztonsági Szabályzatban leírt adatkezelési, adatvédelmi kötelezettségük megszegéséből származik.

Amennyiben az Intézmény harmadik személlyel olyan jogviszonyt létesít, amelyben a harmadik fél személyes adatokba nyert betekintést, akkor titoktartási nyilatkozatot kell aláírni vele, amelyben vállalja az Info törvény és az ASZ rendelkezéseinek betartását.

Az adatkezelő személyek felelősséggel tartoznak azért, hogy az adatokat csak az előre meghatározott (az ASZ 1. mellékletében leírt) célokra használják fel. Ha eltérő célú vagy bővített célú adatkezelést kívánnak végezni, akkor a 3.3 pont szerint kell eljárniuk.

Az adatfelvétel előtt az érintettek számára tájékoztatást kell nyújtani. Az adatkezelő személy a tájékoztatást az Adatvédelmi felelőstől szerezheti be. Köteles meggyőződni arról, hogy a tájékoztatás megtörtént. Ha az adatkezelés az érintett hozzájárulásán alapul, akkor az érintett nyilvántartásért felelős köteles a hozzájárulási nyilatkozatokat áttekinthető és visszakereshető módon tárolni. Ha több nyilatkozat is van egyetlen dokumentumon, akkor a tárolás annak az adatkezelőnek a feladata, aki a leghosszabb lejáratú adatot kezeli. A tárolás ideje megegyezik az érintett nyilvántartás tárolási idejével. Az érintett nyilatkozatokat az adatokkal együtt kell selejtezni.

Az adatkezelő felel az adatok helyes rögzítéséért. A megadott adatokat köteles összevetni a rögzített adatokkal (Pontosság alapelve). Ha az érintett helyesbítési kérelemmel élt, akkor az adatot köteles helyesbíteni. Helyesbítés esetén a csatolt nyilvántartás adatkezelőjét köteles értesíteni a változásról (pl. bér- és munkaügyi nyilvántartás – KIR, enapló – KIR).

A személyes adatokat tartalmazó dokumentumok sokszorosítása, nyomtatása, másolása az adatkezelés valamely rész célja érdekében vagy a nyilvántartások közti adattovábbítás céljára megengedett. Az ilyen dokumentumok kezelésében is köteles az adatkezelő mindent megtenni a személyes adatok védelmében. Az ilyen másolatokat, nyomtatásokat, jegyzeteket a rész cél elérése vagy a másik nyilvántartás módosítása után meg kell semmisíteni.

Az adatkezelő a személyes adatokat tartalmazó dokumentumokat köteles elzárva tartani. A személyes adatok nem hagyhatók bárki által hozzáférhető helyen. Az adatkezelő köteles betartani a személyes adatok tárolási helyére és idejére vonatkozó szabályokat, amelyek az Adatvagyon leltárban vannak megfogalmazva. A kezelés során az IBSZ szabályait betartva kell eljárni.

Az adatkezelő az adott nyilvántartás felelősét köteles tájékoztatni a lejárt tárolási idejű adatokról. A nyilvántartás felelőse intézkedik a tárolási idő lejártakor az adatok törlésére. Az adatkezelő vagy a rendszergazda gondoskodik az adatok törléséről, megsemmisítéséről.

5 Az üzleti titkot képező adatok körének meghatározása

A polgári törvénykönyvről szóló törvény alapján az Intézmény üzleti titoknak minősítheti azokat a tényeket, információkat, adatokat, amelyek titokban tartásához az intézménynek méltányolható érdeke fűződik.

Az üzleti titok körébe vont adatokat az intézmény vezetője határozza meg. A határozatot, az érintett adatok körével és az azokba betekintést nyerhetők listájával az érintettek tudomására hozza. Ha az ebbe a körbe bevont adatok, információk tárolása, feldolgozása, továbbítása számítástechnikai eszközökkel (is) történik, akkor az értesítettek körébe be kell vonni az adatok fizikai kezelését,

mentését végző személyt (személyeket) is. (Informatikai vezető, illetve rendszergazdák) A számítógépes hozzáférés korlátozásáért az informatikai vezető felel.

Az ebbe a körbe tartozó információkat, adatokat, írott vagy nyomtatott formában, a „Titkos” megjelöléssel kell ellátni.

6 A kötelezően közzéteendő adatok nyilvánosságra hozatala

A kötelezően közzéteendő adatok nem minősíthetők üzleti titokká. A kötelezően közzéteendő adatok körét jogszabályok határozzák meg. Különösen a 2011. évi CXCV. tv., a 2000. évi C. törvény, 2011. évi CLXXV. törvény, 2007. évi CLXXXI. törvény, 1996. évi CXXVI. törvény, 2011. évi CXII. tv, 350/2011.(XII.30.) korm.rendelet, 224/2000.(XII.19) korm.rendelet, 229/2012. Korm. rendelet és a 20/2012 EMMI rendelet.

A kötelezően közzéteendő adatok körének meghatározása intézményi szinten a gazdasági igazgatóhelyettes (a pénzügyi, gazdasági adatok körében), illetve az igazgatóhelyettesek (neveléssel, oktatással kapcsolatos ügyekben, valamint a tanügyi dokumentumok, közzétételi lista körében) feladata. A pályázatok körében felmerülő kötelező közzététel az adott pályázat projektvezetőjének a feladata.

Az elektronikus közzététel helye az intézményi portál, amely a www.nejanet.hu címen érhető el az Interneten.

A közzéteendő dokumentumok előállítását az adott vezető feladata, amelyet megbízottja is teljesíthet. A dokumentum közzététele és a honlap üzemeltetése a rendszergazdák feladata.

7 A szabályzat megismertetésének rendje

Jelen szabályzatot minden dolgozó a munkaviszony kezdetekor köteles megismerni. A szabályzat ismeretét, a benne foglaltak tudomásul vételét és betartását aláírásával igazolni. Az adatvédelmi felelős minden tanévben egyszer szemléletformáló tájékoztatást tart a dolgozóknak, amin a megjelenés kötelező és erről jegyzőkönyv készül.

A tanulóknak az osztályfőnök tart tanévenként egy osztályfőnöki órán szemléletformáló órát a személyes adatok védelméről és a magánszféra fontosságáról, amihez más segítségét is kérheti. A tanulók előszeretettel használják a közösségi oldalakat és osztanak meg személyes információkat, amelyek az iskolára is hátrányos következményekkel járhatnak.

8 A szabályzat felülvizsgálata

Az adatvédelmi felelős a szabályzatot évente egyszer felülvizsgálja, és ha szükséges, annak tartalmát aktualizálni kell. Az adatvédelmi felelős javaslatot tesz az igazgatónak a módosításokra.

Bármely dolgozó írásban javaslatot tehet a változtatásra az adatvedelem@nejanet.hu email címen. A változtatásokra azonban évente csak egyszer kerül sor.

Soron kívül változtatni kell a szabályzat 1. mellékletén (Adatvagyron leltár), ha új adatkezelést kezdeményez az Adatkezelő. Soron kívül kell változtatni a szabályzaton akkor is, ha a változtatás alapja a jogszabályok változása. Ilyenkor legkésőbb a megváltozott jogszabályok hatálybalépésekor kell változtatni a szabályzaton.

Érintett panaszkezelési szabályzata

Az Érintett panaszkezelési szabályzata a Neumann János Gimnázium, Szakgimnázium és Kollégium Adatvédelmi szabályzatának elválaszthatatlan része. Célja az érintettek észrevételeinek jogszerű kezelése.

9 Az érintettek jogai

Az érintettek jogainak áttekintése ahhoz szükséges, hogy milyen észrevételekkel élhetnek a személyes adatkezeléssel érintett felek.

9.1 Tájékoztatáshoz való jog

Az Adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó információkat tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

A tájékoztatónak tartalmaznia kell a következőket:

- Az adatkezelő és képviselője kiléte és elérhetősége
- Az adatvédelmi felelős elérhetősége
- Az adatkezelés célja, valamint az adatkezelés jogalapja
- Ha az adatokat másnak is továbbítják, akkor az adatok címzettjei illetve a címzettek kategóriái
- Az adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, akkor ezen időtartam meghatározásának módjáról.
- Az érintett jogairól.
- Az adatkezelés megtagadásának esetleges következményeiről.
- A felügyeleti hatósághoz benyújtott panasz jogáról.

9.2 Hozzáférési jog

Az érintett jogosult arra, hogy az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a tájékoztató kötelező információihoz hozzáférést kapjon.

9.3 Helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok kiegészítését.

9.4 Törléshez való jog

Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az Adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje. A törlést azonban nem kell végrehajtani, ha az adatkezelő valamilyen jogszabály által előírt kötelezettsége érdekében kezeli az adatokat.

9.5 Az adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést. 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.

9.6 A helyesbítéshez, törléshez, korlátozáshoz kapcsolódó értesítési kötelezettség

Az adatkezelő minden olyan címzettet tájékoztat a helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

10 Az érintett panasztevésének módja

Az érintett fél a tájékoztatáshoz való jogával személyesen vagy elektronikus úton élhet. Elektronikus úton email formájában ezzel a jogával csak akkor élhet, ha email címét előzetesen megadta az elektronikus napló számára. A kérelmet az adatvédelem@nejanet.hu email címre kell küldeni.

A helyesbítéshez való jogával személyesen, a személyazonosságát hitelesen igazolva élhet. A szülő, gondviselő adatai változásának átvezetését a gyermekén keresztül is kérheti. Az átvezetési kérelmet az osztályfőnököknek kell eljuttatni, a megváltozott adatokkal együtt. A dolgozók az adatváltozást a munkaügyi előadónak kötelesek bejelenteni 3 napon belül. A tanulók az elektronikus naplóban való érdemjegy, hiányzás helyesbítését az illetékes szaktanárnál kezdeményezhetik.

A helyesbítéshez, törléshez kapcsolódó értesítési kötelezettség jogával éléshez nincs semmilyen kötelezettsége az érintettnek. Az Adatkezelő felel az általa kezelt összes érintett nyilvántartásban az adatok átvezetéséért.

A törlési, korlátozási és hozzáférési jogával az érintett kizárólag személyesen élhet a személyazonosságának hitelt érdemlő igazolása után. Az igényét adatigénylő lapon adhatja be, amit az osztályfőnöktől, iskolatitkártól vagy az adatvédelmi felelőstől kérhet.

Az egyéb úton igényelt jogok (telefon, nem regisztrált email, üzenet, stb) nem teljesíthetők. Erről lehetőség szerint az Adatkezelő tájékoztatást ad a benyújtónak. Ha az érintett fél nem azonosítható, akkor az igényt az intézmény elutasítja.

Ha azok a célok, amelyekből az Adatkezelő a személyes adatokat kezeli, nem vagy már nem teszik szükségessé az érintettnek az adatkezelő általi azonosítását, az adatkezelő nem köteles kiegészítő információkat megőrizni, beszerezni vagy kezelni annak érdekében, hogy pusztán azért azonosítsa az érintettet, hogy megfeleljen az adatvédelmi rendeletnek.

11 Teendők az érintett panasza esetén

Személyes tájékoztatás kérése esetén az érintettet az adatvédelmi felelőshöz kell irányítani, akinél az összes nyilvántartáshoz található tájékoztató elérhető. Az adatvédelmi felelős az érintett észrevételét az Érintett igény bejelentési nyilvántartásba felvezeti.

A tanulói naplóbejegyzések (érdemjegy, hiányzás) helyesbítését az igény megalapozottsága esetén a szaktanár elvégzi. További teendő nincs, ezeket a változtatásokat az intézmény nem tartja külön

nyilván. A tanulói, szülői, gondviselői adatok változását az osztályfőnök vezeti át az elektronikus naplóban. A változásokról az iskolatitkár, és az étkezésért felelős gazdasági dolgozót emailben értesíti, a változásokat a KIR rendszerben az iskolatitkár, az étkezési nyilvántartásban a felelős dolgozó vezeti át. A dolgozói adatváltozásokat az iskolai nyilvántartásban a munkaügyi előadó vezeti át és emailben értesíti a minőségbiztosítási igazgatóhelyettest, aki a változást a KIR rendszerben átvezeti.

Az érintett törlési, korlátozási, hozzáférési jog igényét az adatvédelmi felelős az Érintett igény bejelentési nyilvántartásba felveszi.

12 Intézkedések az érintett panasza esetén

Általános szabályként az Adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az Adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet.

Ha az Adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

A változások átvezetésének a megalapozottság ellenőrzése után lehetőség szerint azonnal, de 3 napon belül mindenképpen meg kell történnie. A csatlakozó nyilvántartásokban az átvezetés határideje további 3 nappal meghosszabbítható. Az átvezetés az érintett nyilvántartást kezelők feladata.

A helyesbítéstől eltérő jogok esetén az adatvédelmi felelős köteles az igényt bejegyezni az Érintett igény bejelentési nyilvántartásba. A bejegyzésnek a 2. melléklet szerinti adatokat kell tartalmaznia.

Az adatvédelmi felelős megvizsgálja az igény jogalapját és az igénylő megfelelő azonosíthatóságát. Amennyiben az érintett hitelt érdemlően azonosítható és a kérelem jogos, akkor intézkedik a végrehajtásról.

A törlési és korlátozási kérelem csak akkor fogadható el, ha az érintett nyilvántartás vezetésére NEM jogszabály kötelezi az Adatkezelőt. Ezekből a nyilvántartásokból az érintett nem törölhető és adatai nem zárolhatók. A jogos törlést az érintett nyilvántartás kezelője végzi el. Az intézkedés időpontját az adatvédelmi felelős az Érintett igény bejelentési nyilvántartásba bejegyzi.

A hozzáférési jog bejelentését az adatvédelmi felelős az Érintett igény bejelentési nyilvántartásba bejegyzi. A bejelentő személyazonosságának hitelt érdemlő igazolása után gondoskodik az elérhető adatok általánosan elterjedt elektronikus formában történő átadásáról. Ennek érdekében igénybe veszi az adott nyilvántartás kezelőjének, indokolt esetben a rendszergazda segítségét.

A nem előírt úton érkező kérelmeket az adatvédelmi felelős bejegyzi a nyilvántartásba. Ha lehetséges, akkor értesíti a kérelem benyújtóját és felhívja a figyelmét a megfelelő benyújtásra vagy kiegészítő információkat kér a megfelelő személyazonosításra. Ha a kérelem benyújtója nem azonosítható hitelt érdemlően, akkor a kérelmet elutasítja, amiről értesítést küld (ha ez lehetséges) a kérelem benyújtójának. Az elutasítás tényét és időpontját bejegyzi az Érintett igény bejelentési nyilvántartásba.

13 Jogorvoslati igény

Bármely érintett a személyes adatainak kezelésével kapcsolatos vélt jogsérelem esetén az illetékes törvényszékhez fordulhat vagy vizsgálatot kezdeményezhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál

Elnök: dr. Péterfalvi Attila,

Cím: 1024 Budapest, Szilágyi Erzsébet fasor 22/C.,

Elehetőség: ugyfelszolgalat@naih.hu, +36-1-3911400, www.naih.hu,

Ha az érintett fél él a jogorvoslat lehetőségével a NAIH vagy az illetékes bíróság felé, akkor az Adatkezelő megfelelő szakjogász bevonásával gondoskodik a panasz további kezeléséről.

Incidens kezelési szabályzat

Az Incidens kezelési szabályzat a Neumann János Gimnázium, Szakgimnázium és Kollégium Adatvédelmi szabályzatának elválaszthatatlan része. Az Adatvédelmi szabályzat egyik célja az adatvédelmi incidensek megelőzése. Nem zárható ki azonban az adatvédelmi incidens előfordulása.

14 Fogalom meghatározás

1. „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;
2. „felügyeleti hatóság”: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv; Magyarországon: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), 1125 Budapest, Szilágyi Erzsébet fasor 22/c
3. „érintett felügyeleti hatóság”: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:
 - a. az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
 - b. az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
 - c. panaszt nyújtottak be az említett felügyeleti hatósághoz;

15 Teendők adatvédelmi incidens előfordulása esetén

Adatvédelmi incidensnek tekintünk minden olyan eseményt, amely során, papíron vagy elektronikusan tárolt személyes adat elveszik, megsemmisül, szándékosan vagy véletlenül törlik. Nem számít azonban incidensnek a tervszerű selejtezés, törlés, illetve az érintett tiltakozására, vagy a hozzájárulás megvonására történő törlés.

Incidensnek számít a jogellenes adatváltoztatás. Különösen annak számít a jogellenes hozzáférés vagy az adatok véletlen vagy szándékos nyilvánosságra hozatala, közzététele.

Ha az intézménnyel jogviszonyban állók közül bárki adatvédelmi incidensről tudomást szerez, akkor azt haladéktalanul, írásban köteles közölni az adatvedelem@nejanet.hu email címen az adatvédelmi felelőssel.

A bejelentésnek tartalmaznia kell:

- melyik nyilvántartásban történt az incidens
- mikor történt az incidens
- az incidens jellegét (mi történt, törlés, változtatás, közzététel, stb.)
- az érintett személyek számát
- milyen adatokat érint az incidens

Ha nem áll rendelkezésre valamennyi adat, akkor azok részletekben is közölhetők. Az első két pont azonban kulcsfontosságú a további teendőkre nézve.

16 Az adatvédelmi felelős feladatai adatvédelmi incidens esetén

Az adatvédelmi felelős az incidenst haladéktalanul bevezeti az Adatvédelmi incidens nyilvántartásba (3. melléklet).

Köteles felmérni az incidens jellegét, az érintettek kategóriáit és számát. Meg kell határozni az érintett adatok körét. Ennek során felmérni, hogy konkrétan milyen adatokat érint az adott incidens.

Köteles kockázatelemzést végezni, amelyben eldönti, hogy az érintettek számára mekkora kockázattal jár az incidens. A kockázatelemzésnek meg kell állapítania, hogy nincs kockázat, alacsony, közepes, magas vagy nagyon magas az érintettekre nézve. A kockázatelemzés eredményét rögzíti az Adatvédelmi incidens nyilvántartásba.

Az érintett nyilvántartás illetékesével együttműködve intézkedési tervet kell készítenie, amely tartalmazza a tett vagy tervezett intézkedéseket, amellyel a károk enyhíthetők és a további incidensek megakadályozhatók. Az intézkedéseket rögzíti az Adatvédelmi incidens nyilvántartásba.

Az adatvédelmi incidenst az adatvédelmi felelős indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak (NAIH), kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

A bejelentést a NAIH erre a célra létrehozott felületén köteles megtenni. A bejelentésnek tartalmaznia kell legalább:

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni kell az adatvédelmi felelős vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

17 Az érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi felelős gondoskodik az érintettek indokolatlan késedelem nélküli tájékoztatásáról.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább:

- közölni kell az adatvédelmi felelős vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

- az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
- az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását. Az intézményi gyakorlatban az értesítés ilyen esetben az iskola honlapján és az elektronikus napló hirdetés funkciójában való közzététellel valósul meg.

Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a tájékoztatást kizáró valamelyik okot.

18 További teendők az incidens kezelésében

Az adatvédelmi felelős és az incidenssel érintett nyilvántartás felelőse az intézkedési tervben foglaltakat végrehajtja vagy végrehajtatja a megfelelő személlyel. Közösén áttekintik, hogy a további hasonló incidensek hogyan akadályozhatók meg.

Ha szükséges, akkor a technikai feltételek változtatásával vagy a szabályozás átdolgozásával alakítják át az adatkezelést a további incidensek megelőzésére.

Ha az illetékes adatvédelmi hatóság az incidens kapcsán szankciókat alkalmaz az intézménnyel szemben, akkor jogorvoslatra van lehetőség. Meg kell vizsgálni szakjogász bevonásával a jogorvoslati lehetőségeket. Azok hiányában a szankcióban foglaltakat végre kell hajtani.

Minden olyan személy, aki az adatvédelmi rendelet megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult.

Amennyiben az érintett fél kártérítési igénnyel lép fel az intézménnyel szemben, akkor szakjogász bevonásával meg kell vizsgálni a kártérítési igény megalapozottságát. Az esetleges bírósági eljárást le kell folytatni megfelelő szakjogász igénybevitelével.

Mellékletek