Jelentés

GDPR szakértői feladatok elvégzése
a
NÉMET NEMZETISÉGI GIMNÁZIUM ÉS KOLLÉGIUM
(DNG)
részére

Kiadás dátuma 2019.12.12.
Verzió: V01

Tartalomjegyzék

1 Vezetői összefoglaló

Magyarországi Németek Országos Önkormányzata (a továbbiakban: MNOÖ) megbízta a FORTIX Consulting Kft.-t az MNOÖ és az irányítása alá tartozó szervezetek GDPR szakértői feladatainak elvégzésére, az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: GDPR, Rendelet) szóló jogszabály alapján. A Rendelet 2018. május 25-én lépett hatályba.

Tárgyi Jelentés a **Német Nemzetiségi Gimnázium és Kollégium** (a továbbiakban: DNG) részére készült, az intézményegységek részére külön Jelentés készül.

FELMÉRÉS, BEVEZETÉS

Leszállítandók

Vizsgálatunk az egyes szakterületi egységek vezetőivel való strukturált interjúkkal, továbbá az átadott dokumentumok vizsgálatával történt. Átfogó és intézményegység-specifikus javaslatainkat e felmérés alapján alakítottuk ki és jelen dokumentumban foglaltuk össze.

A jelentés mellékleteként átadjuk a GDPR 30. cikke szerinti Adatkezelési tevékenységek nyilvántartása első verzióját, amelyet szintén a területi interjúk alapján építettünk fel. Ennek további pontosítása és folyamatos karbantartása a GDPR-nak való megfelelés fontos eleme lesz a továbbiakban.

A DNG-ről a felmérés során kialakult átfogó kép alapján megállapítható, hogy bár az adatvédelmi intézkedések felügyelete a Rendelet alapján a kinevezésre került Adatvédelmi Tisztviselő kezében egységesítendő és fejlesztendő, továbbá egyes területeken nem megfelelő gyakorlatot tapasztaltunk a biztonsági szint tekintetében.

A személyes adatok kezelésének intézményi szintű szabályozása a kritikus területeken még nem felel meg a hatályos jogszabályoknak és a GDPR irányelveinek, továbbá az adatkezelés jogszabályi háttere az Iskolaközpont jogi képviselője által ismert és folyamatosan követett, amely megfelelő alapot teremt a szükséges adminisztratív változtatások, illetve a követendő jó gyakorlat bevezetéséhez. Az Iskolaközpont részéről – értékelésünk szerint – a szükséges eszköz és informatikai jellegű fejlesztések, átalakítások igényelnek jelentősebb erőforrás-ráfordítást.

Jelentésünkben a GDPR-ra való felkészülés szempontjából kritikus, jelenleg nem kezelt intézkedéseket emeltük ki. Továbbá a Rendelet egyes cikkeinek való megfelelést, a DNG méretének és komplexitásának, illetve jelenlegi képességeinek tükrében a 2. sz. Mellékletben tételesen is megadjuk.

1.1 Átfogó megállapítások

- A DNG jelenlegi adatkezelési szabályozása nem teljes egészében felel meg a GDPR-nak, és a hatályos további jogszabályoknak. Ezek kiegészítése a szükséges terminológiák és hivatkozások átvezetése javasolt.
- A kezelt iratok fizikai elhelyezése, tárolása, illetve azok megőrzési, selejtezési ideje tekintetében területenként eltérő gyakorlatot tapasztaltunk a DNG-ben, az Iratkezelési Szabályzat nem tér ki valamennyi papír alapon megjelenő adat iratkezelési szempontú szabályozására. Ennek kiegészítése (Irattári terv) szükséges, melyet ezen iratok elektronikus formájának kezelése, tárolása tekintetében is javaslunk követni.
- Fontosnak tartjuk az egyes informatikai rendszerekhez, alkalmazásokhoz történő hozzáférési jogosultságok beállításának (illetve visszavonásának) a célhoz kötöttség és az elszámoltathatóság elvei mentén történő megvalósítását, ennek érdekében szabályozott és dokumentált folyamat bevezetése szükséges a munkaüggyel, és az érintett gimnáziumi vezetőkkel egyeztetve.
- A DNG jelenlegi információbiztonsága jelenleg nem teljesíti a GDPR 32. cikkében leírt adatbiztonsági követelményeket.
- A DNG kötelezettsége a személyes adatok kezelésével érintettek – GDPR 12-22. cikkekben részletezett – jogainak biztosítása (hozzáféréshez, helyesbítéshez, törléshez, az adatkezelés korlátozásához, adathordozhatósághoz). Ennek teljesíthetősége érdekében szükséges tisztában lenni azzal, hogy az egyes személyek mely adatai és mely rendszerekben kerülnek tárolásra/kezelésre, továbbá az adatkezelési tevékenységek nyilvántartása is szükséges.

1.1.1 Fizikai biztonság

Az adatvédelem fontos része – az Iskolaközpont működésébe épített intézkedések mellett – az e folyamatokat támogató fizikai és informatikai infrastruktúra biztonsági szintje. Ennek felmérését az alábbiak szerint végeztük, és eredményét jelen dokumentumban foglaltuk össze:

1. A fizikai biztonsági intézkedéseket a rendszergazdával lefolytatott interjú keretében mértük fel.
2. Az informatikai védelem szintjét átfogóan, az rendszergazdával történt strukturált interjú keretében mértük fel.

A GDPR nem határoz meg konkrét fizikai biztonsági követelményeket, de – az IT-hoz hasonlóan – a kezelt személyes adatok megfelelő és egyenszilárd védelme érdekében szükséges – a helyi adottságok figyelembevételével – a „jó gyakorlat" kialakítása.

Jellemző hiányosság a személyes adatokat tartalmazó okiratok tárolására szolgáló szekrények, illetve helyiségek zárásának megoldatlansága, helyenként a kulcsok (zárak) hiánya vagy működésképtelensége, egyes informatikai eszközök (szerver, hálózati eszköz) nem biztonságos elhelyezése és illetéktelen hozzáférés fenyegetése. **Javasoljuk a jövőben a helyiségek zárására, illetve a kulcsfelvétel/kiadás nyomon követhetőségére vonatkozóan elfogadható, formalizált rendszer kialakítását, valamint a telephelyek esetében a helyszínen futó szerver fizikai védelmének megerősítését.**

1.1.2 Informatikai biztonság

Az informatikai infrastruktúra védelmi szintjének felmérésére több, az informatikai terület képviselőjével folytatott tematikus interjú keretében került sor. Részletes megállapításainkat és javaslatainkat a 3. sz. Melléklet tartalmazza. Abban említésre kerül többek között:

- a személyes adatokhoz történő hozzáférés szabályozásának kiemelt fontossága, a **hozzáférési jogosultságok** meghatározásához, beállításához és naplózásához kötődő feladatok, melyek részben érintik azt és a személyügyi területeket is
- felhívjuk a figyelmet a kívülről érkező **illetéktelen hozzáférés elleni védelem** különböző lehetőségeire
- a **sérülékenységek kezelésének** fontosságára
- a **biztonság tudatossági szintjének** emelésére
- emellett kiemeljük az **Információbiztonsági Szabályzat készítésének** szükségességét
- az informatikai **rendszerek fizikai védelmével** kapcsolatos feladatokat
- javaslunk további, a személyes adatok **bizalmasságának védelmét** célzó intézkedéseket

1.2 Javasolt további lépések

A hatékony felkészülés és a továbbiakban fenntartható megfelelés érdekében szükséges lépések az alábbiak szerint foglalhatók össze:

1. Adatvédelmi tisztviselő bejelentése, képzése
2. A gap assessment felhasználásával a GDPR-nak megfelelő adatvédelmi szabályozás (egységes Adatkezelési Szabályzat, személyes adat kezelésre vonatkozó operatív utasítások), eljárások és felügyeleti, ellenőrzési rendszer kialakítása, adatkezelőkkel történő dokumentált megismertetése. A meglévő dokumentumokban a GDPR-nak (és a hazai új jogszabályoknak) megfelelő jogszabályi hivatkozások és terminológiák átvezetése
3. Adatvédelmi hatásvizsgálat elvégzése az egyes azonosított adatkörökre
4. A jelen dokumentumban összefoglalt átfogó hiányosságok kezelése, különös tekintettel az érintetti jogok gyakorlásának biztosítására
5. A jelen dokumentumban területenként jelzett hiányosságok kezelése
6. Informatikai infrastruktúra és alkalmazások biztonsági szintjének növelése
7. Belső adatvédelmi tudatosító kampány, oktatások
8. Az átadott Adatkezelési Tevékenységek Nyilvántartásának kiegészítése
9. Incidens-nyilvántartás elkészítése, továbbá ennek és az átadott Adatkezelési Tevékenységek Nyilvántartásának folyamatos karbantartása

2 Módszertan

Gyakorlatunk alapján, a vizsgálatunk első lépéseként megismertük az Iskolaközpont működésének alapvető elemeit és személyes adatkezelési gyakorlatát a GDPR szemüvegén keresztül, úgymint az Iskolaközpont:

- felépítését és működését
- támogató területek és kontrollfunkciók működését: jogi, személyzeti, biztonsági és informatikai területeken
- személyes adatok kezelésében érintett informatikai rendszereit, informatikai folyamatait és azok szabályozását
- az átadást az Iskolaközponton belül, illetve más Hivatalok, joghatóságok felé.

Vizsgálatunkkal az előzetes egyeztetések alapján az Iskolaközpont valamennyi egységét lefedtük.

A Rendelet követelményeinek átfogó vizsgálata mellett **a felkészülés első fázisában hangsúlyos kérdésekre** kiemelten fókuszáltunk, az alábbi cikkek mentén. A továbbiakban e kérdéskörök megfelelő kezelése biztosítja az alapot a Rendelet mélyebb követelményeinek való megfelelésre:

5	A személyes adatok kezelésére vonatkozó elvek
6	Az adatkezelés jogszerűsége
7	A hozzájárulás feltételei
9	A személyes adatok különleges kategóriáinak kezelése
10	A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése
15	Az érintett hozzáférési joga
16	A helyesbítéshez való jog
17	A törléshez való jog („az elfeledtetéshez való jog”)
18	Az adatkezelés korlátozásához való jog
25	Beépített és alapértelmezett adatvédelem
32	Az adatkezelés biztonsága

Vizsgálatunk eredményeképpen előállt a Rendelet **minden alkalmazandó cikkére** vonatkozó **eltérési jelentés** (2. Melléklet: GDPR gap assessment), amely a következő fejezetekben megfogalmazott **javaslataink** alapját képezte. A DNG-nél feltárt hiányosságok konkrét kezelésére nincs kialakult gyakorlat. Ezek esetében a potenciális nem-megfelelőség felvetésére volt lehetőségünk. E témák mélyebb kivizsgálását és egy – a gördülékeny működés és a GDPR szempontrendszerét is figyelembe vevő – jó gyakorlat dokumentált bevezetését javasoljuk.

3 Általános javaslatok

Jelen fejezet azokat a megállapításokat és javaslatokat tartalmazza, amelyek az egyes területekkel folytatott feltáró megbeszélések során több esetben felmerültek és amelyeket ezért **általános hiányosságnak** találtunk. Ezek kezelését átfogóan és egységesen célszerű elvégezni.
Az egyes megállapítások GDPR követelmények szerinti megfeleltetése a 2. sz. Mellékletben található.

Ssz.	Megállapítás	Javaslat
1.	A kezelt iratok fizikai elhelyezése, tárolása, illetve azok megőrzési, selejtezési ideje tekintetében területenként eltérő és sok esetben magasabb kockázatot rejtő gyakorlat található a DNG-ben (Pl.: szerződések; egészségügyi adatok).	• iratkezelési szabályzat/irattári terv készítése/ kiegészítése • tárolásra vonatkozó intézkedések • iratmegsemmisítők rendszeresítése • ellenőrzés
2.	Adott szakterület szempontjából fontosnak ítélt információk, adatok kimentése történik fájlszerverre, saját gépre.	A napi munkamenet szempontjából lényeges információk eseti letöltésén felül, tömegesen ne történjen táblák, adatbázisok letöltése a rendszerből, lehetőség szerint kerüljenek tiltásra/korlátozásra az ún. „adatbázis kiöntések”.
3.	Az egyes rendszerekhez, alkalmazásokhoz történő hozzáférési jogosultságok beállítása (ill.	Szükséges szabályozott és dokumentált folyamat a gazdasági vezetővel és érintett intézmény

Ssz.	Megállapítás	Javaslat
	visszavonása) a célhoz kötöttség és az elszámoltathatóság elvei mentén valósuljon meg.	vezetőkkel egyeztetve. A téma részletesen kifejtve a 3. sz. Mellékletben.
4.	Személyes adatok továbbítására vonatkozó tájékoztatás formája, tartalma.	A közalkalmazottakat tájékoztatni kell arról, hogy személyes adataik mely célra, esetleg magánszemély(ek)hez kerülnek továbbításra és milyen célból. Ezt formálisan kinevezésben, munkaszerződésben, megbízási szerződésben célszerű megtenni. Munkatársak és ellátottak esetében is szükséges lehet egy további klauzula az előre nem tervezhető, de kötelező adattovábbítások esetére, például: "Az érintett jelen szerződés aláírásával tudomásul veszi, hogy jogszabály jogalapot teremthet arra nézve, hogy az Adatfeldolgozó az érintett személyes adatait kezelje, azokat a jogszabályban feljogosított szerv(ek) számára – így különösen de nem kizárólagosan Pl.: rendőrség, bíróság, önkormányzat, s más hatóság, közhatalmi szerv stb. számára – továbbítsa."
5.	Bizonyos esetekben harmadik feleknek csak anonimizált vagy összesített adatok, kimutatások továbbítása szükséges.	Ezen esetek kerüljenek meghatározásra, egyúttal kerüljön szabályozásra a folyamat, melynek során biztosítható, hogy az érintett valóban nem lesz azonosítható.
6.	Előállítottuk az Adatvédelmi Incidensek nyilvántartása, folyamata és eljárása dokumentumokat.	• létrehozása szükséges a GDPR 33. cikk alapján, az abban feltüntetett tartalommal • naprakészen tartása a leendő Adatvédelmi Tisztviselő feladata • javasoljuk a belső rendszeren belül történő kialakítást (intranet) • intézkedési terv készítését adatvédelmi incidens esetére • Adatvédelmi Hatásvizsgálat készítése szükséges
7.	„Tájékoztató és nyilatkozat adatkezeléshez” elnevezésű nyomtatványt elkészítettük	Mivel a személyes adatok kezelése jogi kötelezettség teljesítéséhez szükséges (az Iskolaközpont működtetése), – nem kell alkalmazni a 2. oldalon található keretben kijelölt "Adatkezeléshez *hozzájáruló* nyilatkozata" elnevezésű részt. A dokumentumot ugyanakkor javasoljuk aktualizálni az alábbiakkal: • a személyes adatokat az Iskolaközpontnál mely munkatársak köre láthatja, kezelheti • mely konkrét (pl. mely email vagy levelezési) címre írhat a gondozott/ellátott bejelentéseket (ha elektronikus úton teszi ezt, akkor célszerű egy regisztrált e-mail cím, amelyről érkező nyilatkozatok elfogadhatók az Ügyfél részéről

Ssz.	Megállapítás	Javaslat
		• rendelkezés a személyes adatok megőrzésének időtartamára vonatkozóan • az érintett – GDPR 12-22 cikkelyekben foglalt – jogairól lehet bővebb tájékoztatást adni, már a GDPR szövegével is összhangban (erősítve a GDPR kompatibilitást, szöveghasználatot, arra utalást, stb.) • A tájékoztató szövegének rövidítését és egyszerűsítését javasoljuk (tömör, átlátható, közérthető megfogalmazás követelménye).
8.	Az érintetti jogok biztosításának feltételei nincsenek meghatározva, nincs bejelentve a Rendelet szerinti Adatvédelmi Tisztviselő, szükséges az átadott Adatkezelési Tevékenységek Nyilvántartásának véglegesítése és karbantartása.	• Az érintetti jogok gyakorlásának biztosítására folyamat felvázolását és sablonok készítését javasoljuk, mivel ezen jogok teljesülésének biztosításához több terület együttműködése szükséges. • Adatvédelmi Tisztviselő bejelentése szükséges minden területre. Az Adatkezelési Tevékenységek Nyilvántartásában kiegészítendő: • Adatvédelmi Tisztviselő személyére vonatkozó információk feltüntetése • kezelt adatok körének esetleges kiegészítése, pontosítása – minden szakterület önállóan • címzettek (ahová személyes adatot továbbítanak) azonosítása, illetve továbbításra vonatkozó információk és garanciák • Irattári terv rendelkezéseinek megfelelően a törlési határidők feltüntetése • technikai és szervezési intézkedések általános leírása (IT, fizikai biztonság)

4 Intézmény-specifikus javaslatok

Jelen fejezet azokat a megállapításokat és javaslatokat tartalmazza, amelyek **az egyes szakterületeknél specifikus esetekben fordulnak elő**, kezelésük egyedi figyelmet igényel az adott területen. Javasolt e kérdések kezelése területi szinten, illetve szükség szerint az ezekből levonható tanulságoknak az Iskolaközpont átfogó adatvédelmi szabályozásába való beillesztése a továbbiakban.

Az egyes megállapítások GDPR követelmények szerinti megfeleltetése a 2. sz. Mellékletben található.

4.1 Intézményvezető

Ssz.	Megállapítás	Javaslat
1.	E-mailen történő megkeresések (kérelmek és panaszok elbírálása esetében is) esetében nincs dokumentált hozzájárulás/tájékoztatás.	Javasolt az intézményvezető e-mail levelezésébe egy automatikus válaszüzenetet beépíteni (rendszergazda), amely szerint az Érintett személyes adatai kezeléséhez hozzájárul. Válasz hiányában az önkéntes hozzájárulásként kezelendő.
2.	Okiratok, dokumentumok intézményvezető szobájában történő nyílt tárolása.	Javasoljuk az őrzés, tárolás feltételeinek átgondolását. Az intézményvezető irodájában csak arra jogosult személyek tartózkodjanak. Zárt szekrényben történő őrzés minden személyes adatot tartalmazó dokumentum esetében indokolt.
3.	Intézményvezetői iroda, tanári szoba, titkárság őrizetlenül hagyása.	Mindkét helyiségben, ha nem tartózkodik senki, célszerű zárni a nagy mennyiségű személyes adatot tartalmazó dokumentumon felül vagyonvédelmi szempontból is.
3.	Intézményvezető irodája három - ebből egy lezárt – irányból közelíthető meg.	Javasoljuk az intézményvezető irodájának egy irányból történő megközelítését. Adatvédelmi, és vagyonvédelmi kérdéseket is felvet a jelenlegi gyakorlat.

4.2 Intézményvezető-helyettes 1.

Ssz.	Megállapítás	Javaslat
1.	Nevelési ügyek esetében nincs dokumentált hozzájárulás/tájékoztatás.	Javasolt az Érintettek személyes adatai kezeléséhez történő hozzájárulás/tájékoztatás módjának kialakítása.
2.	Személyes adatok kategóriái tartalmaznak felesleges elemeket.	Javasoljuk a nevelési ügyek tekintetében a gyűjtött személyes adatkategóriák felülvizsgálatát az adatvédelmi tisztviselő közreműködésével 2020. évben. A GDPR előírja az adatkezelési célhoz és jogalaphoz rendelt lehető legminimálisabb tartalmat. Lásd: GDPR rendelet 5. cikk) „az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”)”

4.3 Intézményvezető-helyettes 2.

Ssz.	Megállapítás	Javaslat
1.	Ösztöndíjak esetében nincsen dokumentált hozzájárulás/tájékoztatás.	Javasolt az Érintettek személyes adatai kezeléséhez történő hozzájárulás/tájékoztatás módjának kialakítása. Célszerű már az ösztöndíj kiírásban elhelyezni egy, a személyes adatok kezelésére vonatkozó kitételt.

Ssz.	Megállapítás	Javaslat
2.	Közösségi platformok (DNG saját honlapja, és Facebook oldala) nem tartalmaznak adatkezelési tájékoztatót.	Javasoljuk a DNG honlapján egy hasonló Adatkezelési tájékoztató elkészítését az adatvédelmi tisztviselő bevonásával, mint az LDU esetében. Lásd: http://www.ldu.hu/page/560

4.4 Gazdasági vezető

Ssz.	Megállapítás	Javaslat
1.	NAIH gazdasági területre vonatkozó tájékoztatóinak, ajánlásainak figyelemmel követése.	A www.naih.hu weboldalon a gazdasági tárgyú állásfoglalások adatvédelmi vonatkozásainak figyelemmel kísérése. Pl. számviteli szempontból az egyéni vállalkozó adatai nem számítanak személyes adatnak, azonban a Joghatóság NAIH-2018-5233-4-V számú állásfoglalása szerint az egyéni vállalkozó természetes személy. Személyes adatait a GDPR rendelet szerint kell kezelnie az Adatkezelőnek/Adatfeldolgozónak. Célszerű ezt a feladatot becsatornázni a DPO-hoz.
2.	A folyamatok adatvédelmi szempontból megfelelően zajlanak – zárt rendszerben -, a zárt őrzés feltételei nem minden esetben adottak.	Javasoljuk a személyes adatokat tartalmazó dokumentumok őrzését zárt szekrényben, szükség esetén lemez, - vagy páncélszekrényben.
3.	SQL Forrás adatai, dokumentumai duplán kerülnek megőrzésre.	Javasoljuk a program adatainak egy helyen történő őrzésének, tárolásának megoldását. Célszerű rendszergazda, és a DPO bevonása a kialakításba. Továbbá célszerű a folyamathoz őrzési/selejtezési határidőket rendelni, akár ügycsoportonként.

NAIH állásfoglalásai elérhetőek: https://www.naih.hu/az-adatvedelmi-reformmal-kapcsolatos-allasfoglalasok.html honlapon.

4.5 Iskolatitkár

Ssz.	Megállapítás	Javaslat
1.	A Titkárság terület kialakítása adatvédelmileg aggályos.	Javasoljuk a Titkárság, mint helyiség újra gondolt átalakítását. Tekintettel a nagy átmenő forgalomra pl. diákok/pedagógusok. A dokumentumok nagy része nem zárt szekrényben kerül őrzésre. Az iskolatitkár munkaterülete adatvédelmileg nem megfelelő, asztali számítógépébe, asztalán tárolt dokumentumaiba bárki betekinthet. Javaslatunk egy megemelt munkapult, amely alá gátolt a jogosulatlan betekintés és az asztali számítógép monitora nem látható. Célszerű a monitort a bejáratnak háttal elhelyezni. Célszerű a feltételrendszer szempontjait 2020-ban a DPO bevonásával kialakítani.
2.	Az iratkezelési szabályzat túl általános, nincs lebontva a:	Javasoljuk az iratkezelési szabályzat 2020. évi felülvizsgálatát az új folyamatok, feladatok

Ssz.	Megállapítás	Javaslat
	• felvételi, beiratkozás, tanulói adatok, • iktatás, levelezés (kimenő, bejövő) folyamataira.	keletkező dokumentumainak őrzése, és selejtezése tárgyában. Célszerű 2020. évben a DPO-t bevonni a tevékenységbe.
3.	Az iktatás nem programban, elektronikusan történik.	Javasoljuk a jelenlegi MS Excel tábla vezetése helyett iktatóprogram megvásárlását. Az Excel tábla használata komoly problémákat vet fel: jogosulatlan hozzáférés, törlés, megsemmisülés.

4.6 Könyvtár

Ssz.	Megállapítás	Javaslat
1.	A keletkező dokumentumok megsemmisítése manuálisan történik, nincs helyben iratmegsemmisítő gép.	A dokumentumok eseti, ad-hoc megsemmisítése adatvédelmi szempontból nem támogatott. Nincs kialakítva az őrzés, selejtezés folyamata. A megsemmisítések jegyzőkönyvvel történő felvétele nem gyakorlat a Könyvtárban. Javasoljuk iratmegsemmisítő gép beszerzését a manuális megoldás (eltépés) helyett.
2.	A könyvtárhasználat feltételei, rendszere nem egyértelmű.	Javasoljuk a Könyvtár, mint szakterület adatvédelmi felülvizsgálatát 2020. évben a DPO bevonásával elvégezni. A feladatot jelenleg helyettes látja el, célszerű a véglegesen kinevezett közalkalmazottal elkezdeni majd a könyvtárhasználat rendjének kialakítását.

4.7 Fizikai biztonság

A Gimnázium fizikai biztonságának felmérése tekintetében kiemelt cél volt annak feltárása, hogy az adott telephely milyen biztonsági szinten van, azaz mennyire képes garantálni, hogy az által kezelt személyes, illetve különleges személyes adatok illetéktelenek által nem hozzáférhetőek, megismerhetőek, módosíthatóak vagy megsemmisíthetőek. Ezt a célt több eszközzel is el lehet érni, nem szükségszerű egységes gyakorlatok alkalmazása, lévén a biztonság kialakítása során tekintettel kell lenni az egyes helyszínek adottságaira, továbbá arra is, hogy a védelem a kockázattal arányos mértékű legyen.

A Gimnázium telephelyéről általánosan elmondható, hogy a fizikai biztonságuk a kockázatokkal arányos. A belépés kontrollált, portaszolgálat működik, továbbá az épületben riasztó és kamerarendszer van telepítve.

Az irattár ajtaját zárják és a belépésre jogosult személyek köre korlátozott. A Gimnázium ugyan rendelkezik zárható szekrényekkel, de ajánlott megvizsgálni a papíralapú adatok mennyiségét és szükség esetén javasoljuk további zárható szekrények beszerzését. Ezen túlmenően azt ajánljuk, hogy a személyes adatokat tartalmazó dokumentumok esetleges megmaradt nyílt tárolási gyakorlatát rendszeresen ellenőrizzék és a tudatosítások keretében hangsúlyozzák a nyílt tárolási gyakorlat nemmegfelelőségét és kockázatát. Az irattárakról és az irodákról általánosan elmondható, hogy a kulcskezelés a gyakorlatban működik, és az interjúk során elhangzott, hogy dokumentált szabályozás is vonatkozik a területre.

Külön figyelmet kell fordítani az informatikai eszközök biztonságos elhelyezésére. A felmérés során elhangzott, hogy a fájlszerver az úgynevezett „kis tanáriban" van elhelyezve, ahol nincs elzárva és a helyiségbe belépő pedagógusok fizikailag szabadon hozzáférhetnek. A hálózati eszközök közül nem mindegyik van elhelyezve zárt rack szekrényben, ami ismételten lehetőséget ad az illetéktelen hozzáférésre. A hálózati eszközök nem megfelelő elhelyezése magas kockázatot jelent, amelyek korrigálását minél hamarabb javasoljuk.

4.8 IT

Gimnázium által használt informatikai rendszerek működését üzemszerűvé és biztonságossá kell tenni, ezek képezik az alapját a személyes adatkezelés GDPR-szerinti megfelelőségének is. Ennek érdekében az informatikai terület biztonsága lényeges részét képezte felmérésünknek, az itt összefoglalt megállapítások és javaslatok részletes kifejtése a **3. sz. Mellékletben** található.

Ssz.	Megállapítás	Javaslat
a)	Nincs Információbiztonsági Szabályzat.	Szükségesnek tartjuk az Információbiztonsági Szabályzat elkészítését, betartatását és folyamatos fejlesztését.
b)	A szállítói szolgáltatásokban nem szerepelnek és nem érvényesülnek az adatvédelmi érdekek.	Javasoljuk az informatikai szolgáltatások nyújtásában közreműködő szereplőkkel kötött szerződések adatvédelmi rendelkezésekkel és felelősségekkel történő kiegészítését.
c)	A hozzáférési jogosultságok kiosztása és a felhasználók hitelesítése nem megfelelő	Felül kell vizsgálni a) a Gimnázium IT rendszereinek, valamint a webes alkalmazások hozzáférési jogosultságainak koncepcióját, b) formális jelszókövetelmények meghatározását, c) a nem nevesített rendszergazdai fiókok használatát, d) a jelszavak kiosztásának módszerét.
d)	Ingyenes vírusvédelmi szoftvert alkalmaznak.	Javasoljuk egy jogtiszta, központilag menedzselhető vírusvédelmi vagy komplex végpontvédelmi szoftver beszerzését.
e)	A fájlszerveren nem támogatott operációs rendszer fut.	Javasoljuk a fájlszerver operációs rendszerének újabb, gyártói támogatással rendelkező verziójára történő frissítését.
f)	Az adathordozók használatának szabályai nincsenek kialakítva.	Ki kell alakítani a külső adathordozók (pendrive, hordozható merevlemez) használatának szabályait, illetve ajánlott az eszközök titkosítása.
g)	A hálózati kapcsolatokon kívül nem alkalmaznak titkosítást.	Ajánlott az elektronikus levelezés során csatolt fájlok titkosítása. A fájlszerveren tárolt adatok titkosításáról kockázatelemzés alapján kell döntést hozni.

Ssz.	Megállapítás	Javaslat
h)	A mobil eszközök használata, távoli elérés és az otthoni munkavégzés nincs szabályozva.	A javasolt Információbiztonsági Szabályzaton belül ajánlott rendezni: a) mobil eszközök (telefon, laptop) használatának biztonsági szabályait, b) távoli elérés és az otthoni munkavégzés fizikai és informatikai biztonsági szabályait, c) ha van, akkor a saját tulajdonú eszközök használatának tiltását, vagy engedélyezésének feltételeit.
i)	A nem használt számítógépek selejtezése még nem történt meg.	Javasoljuk a leselejtezni kívánt számítógépek beépített adathordozóinak biztonságos törlését vagy fizikai megsemmisítését.
j)	Nem készült biztonsági mentés és a fájlszerver nem redundáns.	Javasoljuk a biztonsági mentések rendjének meghatározását, kockázatelemzés alapján az elkülönített, offline mentések elkészítését és szükség esetén a kulcsfontosságú rendszerek redundanciájának biztosítását.
k)	Az elszámoltathatóság biztosítása nem elégséges.	A naplózott események körének, tartalmának, valamint a naplóállományok kezelésének és elemzésének ki kell kialakítani a – kockázatérzékenységhez igazodó – megfelelő szintjét.
l)	Nincs szabályozva incidenskezelés.	Javasoljuk a szervezetet érintő biztonsági incidens (pl. adatlopás, helytelen adatfelhasználás, rendszerleállás, adatvesztés, jogosulatlan adathozzáférés) esetére vonatkozó eljárásrend kidolgozását.
m)	Nincs változásfelügyelet.	Javasoljuk a felhasználók által kért, vagy az üzemeltetési tevékenységekhez kapcsolódó rendszerváltozások igénylésére, jóváhagyására, végrehajtására és tesztelésére vonatkozó eljárásrend kidolgozását.
n)	Nem történt meg a rendszerek biztonsági tesztelése.	Kockázatelemzés alapján javasoljuk a rendszerek külső és belső biztonsági tesztelését (penetrációs teszt) vagy automatizált sérülékenységvizsgálatok rendszeres végrehajtását.
o)	Nem megfelelő szintű információbiztonsági tudatosság szintje.	Javasoljuk a felhasználók biztonság-tudatosságának fejlesztésére irányuló rendszeres felhasználói tájékoztatások bevezetését.

1. Melléklet: Adatkezelési tevékenységek nyilvántartása

Külön fájlban kerül átadásra. Lásd: **...**

2. Melléklet: GDPR gap assessment

Az alábbi táblázatban a GDPR releváns cikkei szerint mutatjuk be a felmérés eredményét. A sorszámok megfelelnek az egyes - fenti - megállapításoknak, ahol a projekt során nem találtunk hiányosságot, ott ezt jelöltük.

A felmérés során a gyakorlatot mértük fel. Ahol a „nem találtunk eltérést" megállapítás szerepel, ott az interjúk alapján a gyakorlati felkészültség, adott esetben szabályozás híján is, de alapvetően ma is megfelelő vagy alkalmas a GDPR szerinti működés bevezetésére. Javasolt mindazonáltal egy GDPR-nak megfelelő adatvédelmi szabályozást kialakítani, abban a rendelet minden cikkére vonatkozóan szükséges követelményeket megfogalmazni és azokat megfelelően bevezetni. Azon cikkeknél, ahol nem találtunk eltérést, a bevezetés a felmérésünk szerint kevesebb ráfordítással lesz megoldható.

Cikk	Cikk címe	Megállapítás sorszáma
5	A személyes adatok kezelésére vonatkozó elvek	2., 3., 7., 8., 11., 17., 18., 19., 20., 22., 23., 24., 25., 27., 28., 30., 31. 34.
6	Az adatkezelés jogszerűsége	nem találtunk eltérést
7	A hozzájárulás feltételei	8., 14., 21.
8	A gyermek hozzájárulására vonatkozó feltételek az információs társadalommal összefüggő szolgáltatások vonatkozásában	nem találtunk eltérést
9	A személyes adatok különleges kategóriáinak kezelése	nem találtunk eltérést
10	A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése	nem találtunk eltérést
11	Azonosítást nem igénylő adatkezelés	nem találtunk eltérést
12	Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések	4., 8., 12., 13., 14., 16.
13	Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik	8., 12., 13., 14.
14	Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg	nem találtunk eltérést
15	Az érintett hozzáférési joga	9., 29.
16	A helyesbítéshez való jog	9., 29.
17	A törléshez való jog („az elfeledtetéshez való jog")	9., 29.
18	Az adatkezelés korlátozásához való jog	9., 29.
19	A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség	9.
20	Az adathordozhatósághoz való jog	9.
21	A tiltakozáshoz való jog	9.

Cikk	Cikk címe	Megállapítás sorszáma
22	Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást	nem találtunk eltérést
23	Korlátozások	nem találtunk eltérést
24	Az adatkezelő feladatai	1., 5., 15., 17., 19., 22., 23., 24., 29., 32., 33.
25	Beépített és alapértelmezett adatvédelem	1., 3., 17., 18., 19., 27., 30., 31.
26	Közös adatkezelők	10.
27	Az Unióban tevékenységi hellyel nem rendelkező adatkezelők vagy adatfeldolgozók képviselői	nem találtunk eltérést
28	Az adatfeldolgozó	nem találtunk eltérést
29	Az adatkezelő vagy az adatfeldolgozó irányítása alatt végzett adatkezelés	nem találtunk eltérést
30	Az adatkezelési tevékenységek nyilvántartása	9.
31	Együttműködés a felügyeleti hatósággal	nem találtunk eltérést
32	Az adatkezelés biztonsága	1., 5., 15., 17., 18., 19., 24., 26., 27., 31., 32., 35.
33	Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak	6.
34	Az érintett tájékoztatása az adatvédelmi incidensről	6.
35	Adatvédelmi hatásvizsgálat	6.
36	Előzetes konzultáció	nem találtunk eltérést
37	Az adatvédelmi tisztviselő kijelölése	9.
38	Az adatvédelmi tisztviselő jogállása	9.
39	Az adatvédelmi tisztviselő feladatai	9.
40	Magatartási kódexek	nem találtunk eltérést
41	A jóváhagyott magatartási kódexeknek való megfelelés ellenőrzése	nem találtunk eltérést
42	Tanúsítás	nem találtunk eltérést
43	Tanúsító	nem találtunk eltérést
44	Az adattovábbításra vonatkozó általános elv	4., 10., 16.
45	Adattovábbítás megfelelőségi határozat alapján	nem találtunk eltérést
46	Megfelelő garanciák alapján történő adattovábbítások	10.
47	Kötelező erejű vállalati szabályok	10.
48	Az uniós jog által nem engedélyezett továbbítás és közlés	nem találtunk eltérést

3. Melléklet: Informatikai infrastruktúra kontroll-felmérésének eredménye

4.9 Összefoglaló

A GDPR előírásainak való megfelelésre felkészítő vizsgálatunk egyik területe volt, hogy a Rendelet szempontjaival, követelményeivel súlyozva vizsgáljuk az IT infrastruktúra jelenlegi állapotát és javaslatokat tegyünk a szükséges módosításokra.

A Gimnázium IT infrastruktúráját az intézménnyel szerződéses jogviszonyban álló üzemeltető cég rendszergazdája üzemelteti. A felmérés során elsősorban a Gimnázium által üzemeltetett és igénybe vett rendszerekre (fájlszerver, O365 e-mail, Mozanapló) összpontosítottunk, melyekben a legtöbb személyes adatot kezelik. A Gimnázium olyan webes alkalmazásokat is használ (KIRA, KIR, Adafor, Netbank), amelyet harmadik fél üzemeltet. Ezen rendszerek esetében a Gimnázium a biztonságos belépésért, biztonságos végpontokért, rendeltetésszerű használatért és a felhasználói tudatosságért tartozik felelősséggel.

A felmérés során azt tapasztaltuk, hogy az információbiztonság területén lemaradás van a szabályozottság, az irányítás, valamint a felhasználói tudatosság terén. Általánosan javasoljuk, hogy minden rendszer esetében vizsgálják meg és teszteljék, hogy a GDPR érintetti jogainak biztosításának technikai oldalának maradéktalanul eleget tudnak-e tenni, illetve milyen változásokat célszerű ennek érdekében végrehajtani (pl. adatbázisokból, biztonsági mentésekből való törlés, rekordok módosítása).

A tapasztaltak alapján javasoljuk, hogy a Gimnázium tekintse át részletesen az információbiztonsági státuszát, végezzen kockázatelemzést: mely hiányosság mekkora kockázatot jelent nem csak a GDPR megfelelés, hanem a Gimnázium működése számára egyaránt és ez alapján készítse el azt az intézkedési tervet, amely mentén célszerűnek látja működésének fejlesztését.

4.10 Megállapítások

4.10.1 Információbiztonsági szabályozás

A GDPR megfeleléshez kulcsfontosságú az adatbiztonság, információbiztonság megfelelő szintjének kialakítása, fenntartása, irányítása, ami a szervezethez illeszkedő információbiztonsági szabályozást igényel.

Javasoljuk az Információbiztonsági Szabályzat kialakítását olyan irányban, hogy a Gimnázium szintjén meglévő folyamatok, védelmi intézkedések és szükséges felelősségek kerüljenek benne összefoglalásra, kiegészítve a GDPR megfelelés kapcsán meghatározandó feladatokkal. A szabályzat belső felhasználásra készül, csak olyan információkat, folyamat meghatározásokat és szabályokat célszerű tartalmaznia, amelyek minden dolgozót érintenek és számukra hozzáférhető.

A szabályzat tartalmának összeállításakor és a szabályozni szükséges területek kiválasztásakor ajánlott figyelembe venni az ezzel kapcsolatos szabványokat (pl. ISO 27001), jó gyakorlatokat és a felmérés során azonosított hiányosságokat, kockázatokat.

A megalkotott Szabályzat akkor tud a gyakorlatban érvényesülni, ha a megalkotása során figyelembe veszik a Gimnázium szervezeti sajátosságait, az oktatási tevékenység jellegzetességeit és a felhasználók számára egy tudatosító előadás keretében is érdekfeszítően, gyakorlati példákkal illusztrálva ismertetik.

4.10.2 Szállítói szolgáltatások adatvédelmi biztosítása

A Gimnázium személyes adatot kezelő informatikai rendszereinek egy részét külső partner által alkalmazott rendszergazda üzemelteti, illetve a Gimnázium a működése során több külső informatikai szolgáltatást is igénybe vesz (pl. e-mail, Mozanapló). A szolgáltatásokat szerződés alapján nyújtják, de a szerződések adatvédelmi, illetve információbiztonsági rendelkezéseket, követelményeket és felelősségi köröket, valamint adatfeldolgozói megállapodásokat nem tartalmaznak.

A GDPR megfeleléshez szükséges adatbiztonság megteremtésében és fenntartásában, valamint az incidenskezelésben nem csak a Gimnázium, hanem a szolgáltató is felelős lehet, ezért a szolgáltatások kiválasztása és a szerződés megkötése során ajánlott érvényesíteni az adatvédelmi és az információbiztonsági követelményeket.

4.10.3 Személyes adatokhoz történő hozzáférés

A GDPR egyértelműen megköveteli, hogy a Gimnázium el tudjon számolni azzal, hogy kik férhetnek hozzá az általa kezelt személyes adatokhoz. Ennek alapvető feltétele, hogy a hozzáférési jogosultságok kezelése meghatározott folyamat mentén dokumentálva történjen.

Általánosan elmondható, hogy a jogosultság kezelést viszont számos ponton fejleszteni szükséges. Az, hogy ki kapott és milyen hozzáféréseket az informatikai erőforrásokhoz, ki mit igényelt – ki hagyta azt jóvá – és ki állította be azt, dokumentált módon bizonyítandó. Ennek megvalósítása nem csupán a rendszergazda feladata, a hozzáférési jogok meghatározása a vezetők felelőssége is, amelyet a Gimnáziumi folyamatokban meghatározott munkakörökhöz rendelten kezelni szükséges. A jó gyakorlatok szerepkörökhöz rendelik a hozzáférési jogosultságokat és célszerű alkalmazni a legkisebb (szükséges) jogosultság elvét.

A hozzáférések kezelése során az egyes hiányosságok összeadódva halmozottan növelik a kockázatot. A jelszavak komplexitása és általános karakterhossza nincs szabályozva és beállítva, emiatt a rendszerek nem kényszerítik ki a biztonságosnak tekinthető jelszavak használatát, a felhasználókról pedig más felmérések alapján általánosan elmondható, hogy könnyen kitalálható egyszerű jelszavakat használnak. A felhasználói fiók létrehozásakor a rendszergazda által megadott jelszó megváltoztatását szintén nem kényszeríti ki a rendszer, emiatt a felhasználón kívül a rendszergazda is be tud lépni a nevében, emiatt a felhasználó nehezen felelősségre vonható. A jelszavak nem járnak le, ezért, ha azok a felhasználó tudomása nélkül kompromittálódnak, a támadó folyamatosan hozzá tud férni az adott felhasználói fiókhoz. Emiatt javasoljuk a jelszavak 60-90 napos lejáratát és kötelező változtatását, valamint a korábban használt jelszavak tiltását.

Aggályosak tartjuk, hogy a rendszergazda névhez nem kötött fiókból látja el az üzemeltetési feladatait, amelyet a munkába állásakor nem változtatott meg, így más személy is tudja. A rendszergazdai fiók által végzett tevékenységek ugyan valamilyen szinten nyomon követhetőek, de nem lehet teljes bizonyossággal, letagadhatatlanul személyhez rendelni, ebből kifolyólag egy esetleges incidensnél nem lehet megtalálni a felelőst. Az előbbiek alapján javasoljuk a névhez kötött rendszergazdai fiókok létrehozását, amelyhez az általános felhasználói fiókokhoz képest hosszabb, erősebb jelszó tartozik és csak az adott rendszergazda ismeri. A rendszergazdát helyettesítő munkatársnak szintén az előző feltételeknek megfelelő külön fiók létrehozását javasoljuk.

4.10.4 Rosszindulatú szoftverek elleni védelem

A rosszindulatú szoftverek (vírusok, kémprogramok, stb.) minden informatikai rendszerre és szolgáltatásra fenyegetést jelentenek: sok típusuk van, könnyen terjednek és nagy károkat okozhatnak. Az elektronikusan kezelt személyes adatok bizalmasságát és rendelkezésre állását is veszélyeztethetik, emiatt az információbiztonság technikai oldaláról a rosszindulatú szoftverek elleni védelem kiemelt fontosságú.

A Gimnázium ingyenes, otthoni célra szánt vírusvédelmi szoftvert használ, amely a kategóriájában ugyan jó értékeléseket kapott, de a jelenlegi felhasználási célra nem alkalmas. A Gimnáziumban több munkaállomáson és szerveren kell alkalmazni a védelmet, amit központilag menedzselhető

megoldással lehet hatékonyan végezni. A jelenleg alkalmazott vírusvédelmi szoftver nem jogtiszta, mivel a végfelhasználói licencszerződése alapján azt nem engedélyezik „vállalatok, állami szervek, civil szervezetek, illetve egyéb nonprofit szervezetek vagy oktatási intézmények számára”.

A fenti tények figyelembevételével javasoljuk egy jogtiszta, több munkaállomáson és szerveren alkalmazható, jogtiszta, központilag menedzselhető rosszindulatú szoftverek elleni védelmi megoldás (vírusirtó) beszerzését. A védelmi megoldást úgy kell konfigurálni, hogy az folyamatosan üzemeljen, mindig naprakész legyen és a felhasználók ne tudják leállítani.

4.10.5 Elavult operációs rendszer használata a fájlszerveren

A Gimnázium fájlszerverén rendkívül régi, elavult operációs rendszer (Windows Server 2003) fut, amely gyártói támogatása 2015. júliusában megszűnt, így már nem érkeznek javítócsomagok a gyártótól. Az operációs rendszerek frissítése, javítócsomagokkal való ellátása (patchelés) kiemelt üzemeltetési feladatnak és információbiztonsági kontrollnak számít, mivel napról napra új sérülékenységek látnak napvilágot, amelyeket a támadók könnyedén kihasználva be tudnak hatolni a rendszerekbe.

Hozzávetőleg érdemes tudni, hogy az eggyel újabb verzió (Windows Server 2008) gyártói támogatása 2020.-ban jár le, ezért javasoljuk, hogy a fájlszerver operációs rendszerét frissítsék legalább Windows Server 2012-re, vagy annál újabb verzióra. Számolni kell azzal, hogy a frissítés miatt a hardver fejlesztése vagy cseréje is indokolt lehet.

4.10.6 Adathordozók használata

A Gimnázium rendelkezik saját, nyilvántartott pendrive-okkal, amelyeket dokumentált átadás-átvétellel lehet igénybe venni, de a külső adathordozók, különösen a pendrive-ok és hordozható merevlemezek használata nincs szabályozva, illetve titkosítást sem alkalmaznak az eszközökön.

A külső adathordozók nem megfelelő használata magas kockázatot jelent, emiatt javasoljuk, hogy a kialakítandó Információbiztonsági Szabályzatban erre a témára is helyezzenek hangsúlyt. Alapvető szabályként érdemes lefektetni, hogy a dolgozók munkavégzés céljából csak a – már most is meglévő – Gimnázium által beszerzett, nyilvántartásba vett adathordozót használjanak, amit kizárólag a Gimnázium számítógépeihez csatlakoztatnak. A saját tulajdonú adathordozók használatát, illetve a Gimnázium adathordozóinak a saját tulajdonú számítógépekhez történő csatlakoztatását ajánlott megtiltani. A visszavett adathordozókon ajánlott víruskeresést futtatni és – ha már nem szükséges – ha személyes adatot tartalmaznak, akkor azt biztonságos módon ajánlott törölni. A külső adathordozókat ajánlott titkosítással ellátni, hiszen anélkül egy elhagyott vagy eltulajdonított pendrive-on található személyes adatok illetéktelen személy számára is hozzáférhetővé válnak, ami nagy számú személyes adatot tartalmazó fájlok esetén súlyos incidensnek minősülhet. Az adathordozók titkosításához nem szükséges külön biztonsági szoftvert beszerezni és telepíteni, hiszen az operációs rendszerek is képesek erre a funkcióra (pl. Windows esetében Bitlocker).

4.10.7 Titkosítás

Az adatvédelmi nyilvántartás felvétele során gyakoriak voltak az interjúk, ahol az elektronikus levelezést jelölték meg személyes adatot tartalmazó IT rendszerként. Ebből kifolyólag az adathordozók titkosításán kívül javasoljuk az e-mail csatolmányok titkosítását is.

Az e-mail üzenetek nem rendelkeznek védelemmel, ezért illetéktelen személyek – ideértve téves címzés esetén más felhasználókat is – hozzáférhetnek a levelek tartalmához, illetve

csatolmányaihoz. Egy nagy számú személyes adatot tartalmazó e-mail csatolmány téves küldése az elhagyott pendrive-hoz hasonlóan szintén súlyos adatvédelmi incidenst generálhat.

Az e-mail üzenetek és csatolmányaik titkosítására léteznek központilag menedzselhető titkosítási megoldások, amelyek nem igényelnek különösebb felhasználói beavatkozást. Költséghatékonyabb megoldásként javasoljuk, hogy kockázatelemzés alapján, szükség esetén titkosítsák a személyes adatokat tartalmazó csatolmányokat. Erre különböző tömörítőprogramokat lehet használni, amelyek segítségével jelszóvédelemmel lehet ellátni a csatolt állományokat. Kockázatelemzés után javasoljuk, hogy mérlegeljék a fájlszerveren található fájlok és adatbázisok titkosítását is.

4.10.8 Mobil eszközök használata, otthoni munkavégzés

A Gimnázium informatikai infrastruktúrájában több mobil eszköz (mobiltelefonok és laptopok) található és az interjúkon kiderült, hogy eseti jelleggel az otthoni munkavégzés is előfordul.

A Gimnázium csak néhány iskolai mobiltelefonnal rendelkezik, amelyek biztonságos használatára jelenleg nincs szabályozás. Napjainkban a mobiltelefonokra is legalább annyi vírus és más kártékony kód jelent veszélyt, mint a számítógépekre. Ha a telefonokat hivatalos levelezésre is használják, akkor ezt a tevékenységet is ajánlott szabályozni, valamint az eszközöket is ajánlott legalább vírusvédelemmel, jelszavas képernyőzárral ellátni.

A pedagógusok dokumentált átadás-átvételt követően hazavihetik a Gimnázium hordozható munkaállomásait. Ezek a munkaállomások nem rendelkeznek a fájlszerverhez történő távoli eléréssel és az interjún elhangzottak szerint csak lokális munka zajlik, ami nem jelent magas kockázatot. Tekintettel arra, hogy a hordozható munkaállomások mégis tartalmazhatnak több személyes adatot, ezért a felhasználókat ajánlott tudatosítani az eszközök biztonságos szállításával, használatával kapcsolatban, valamint ezeken az eszközökön is vírusvédelemnek kell futnia, a titkosítást is érdemes mérlegelni a kockázatelemzésnél.

4.10.9 Leselejtezett számítógépek törlése

Az interjún elhangzottak szerint a Gimnázium még nem selejtezett számítógépeket, de a jövőben selejtezni kívánt számítógépek, informatikai eszközöket már összegyűjtötték. Általános javaslat, hogy a leselejtezni kívánt eszközöket ne csak formázzák, hiszen a formázással eltávolított adatokat különböző célszoftverekkel könnyedén vissza lehet állítani, aminek következményeként illetéktelen személyek férhetnek a személyes adatokhoz.

Ennek elkerülése végett javasoljuk a leselejtezett számítógépek adathordozóinak biztonságos törlését (többszörös törléssel és felülírással) vagy az adathordozó fizikai megsemmisítését és jegyzőkönyv felvételét az elvégzett műveletekről.

4.10.10 Biztonsági mentés és redundancia

A GDPR előírása szerint nem elegendő csak a személyes adatok bizalmasságára fókuszálni, azok sértetlenségét és rendelkezésre állását is biztosítani kell. Jelenleg a Gimnázium fájlszerveréről nem készül biztonsági mentés, a munkaállomásokról ad-hoc módon készítenek biztonsági mentést külső merevlemezre, ami nem jelent megfelelő megoldást. Ha a Gimnázium által használt fájlszerver meghibásodik, vagy rosszindulatú kód (pl. zsarolóvírus) fertőzi meg a Gimnázium hálózatát, akkor fennáll az adatvesztés kockázata.

Az előbbiek miatt javasoljuk a biztonsági mentések stratégiájának megtervezését és ettől függően a szükséges hardverek (pl. hálózati adattároló – NAS, további külső merevlemez) beszerzését. A

mentési stratégia tervezésénél figyelembe kell venni a kezelt és tárolt személyes adatok mennyiségét, a jelenlegi infrastruktúra adottságait és természetesen a Gimnázium igényeit. Az automatizált inkrementális vagy differenciális mentéseken kívül célszerű offline mentést készíteni. Az elkülönített biztonsági mentés adathordozójának elhelyezése során a kiválasztásánál kiemelt hangsúlyt kell fektetni a biztonságos helyszín kiválasztására, zárt tárolására és lehetőleg az adathordozó titkosítására.

A fájlszerver nem redundáns, így a meghibásodása és leállása esetén nincs olyan rendszerelem, amely átvenné a működését. Megfelelő biztonsági mentéssel ez nem feltétlen okoz adatvesztést, de az elérni kívánt adatok nem fognak megfelelő időn belül rendelkezésre állni. Az előbbiek miatt javasoljuk, hogy mérjék fel a kritikus folyamatokat, végezzenek kockázatelemzést és ennek eredményeként döntsenek jelenlegi infrastruktúra fejlesztéséről. A harmadik fél által biztosított szolgáltatásoknál (e-mail, Mozanapló) a redundancia biztosított.

4.10.11 Az elszámoltathatóság biztosítása

A végzett tevékenységekkel való elszámoltathatóság biztosítása az informatikai rendszerek fejlesztése és üzemeltetése során általában háttérbe szorul. Az informatikai rendszerekben a számítógépes naplózás hivatott ezt a feladatot teljesíteni, a naplózott események körének, tartalmának és a naplóállományok kezelésének, elemzésének kell kialakítani a – kockázatérzékenységhez igazodó – megfelelő szintjét.

Az interjúk során kiderült, hogy egy alapszintű naplózás jelenleg nem üzemel. Javasoljuk, hogy tekintsék át naplózni kívánt események körét, a naplózást végző eszközöket, valamint azt, hogy milyen eseményekről fontos riasztást generálni.

4.10.12 Incidenskezelés

A Gimnázium jelenleg nem rendelkezik a szervezetét érintő biztonsági incidens (pl. adatlopás, helytelen adatfelhasználás, rendszerleállás, adatvesztés, jogosulatlan adathozzáférés) kezelésére vonatkozó eljárásrenddel.

A kidolgozandó biztonsági incidenskezelési eljárásrendben meg kell határozni a rendszereket érintő biztonsági események jelentésének és kezelésének rendjét, az ezekkel összefüggő felelősségeket és szerepköröket a biztonsági incidensek azonnali és hatékony kezelése, ezáltal az incidens által okozott károk minimalizálása érdekében. A kidolgozandó eljárásrendnek illeszkednie kell a Gimnázium adatvédelmi incidenskezelési eljárásához.

A FORTIX Consulting Kft. által elkészített folyamat, nyilvántartás és eljárás rend itt érhető el: …

4.10.13 Változásfelügyelet

A Gimnázium nem rendelkezik dokumentált változáskezelési eljárásrenddel. Ha az informatikai rendszerekben végrehajtani kívánt változást nem hagyják jóvá, nem tesztelik, nem tervezik meg a visszaállítási lehetőségeket, vagy éppen nem hajtják végre megfelelően a műveletet, az rendszerleállással, rosszabb esetben adatvesztéssel is járhat. Az ismertetett tények alapján javasoljuk, hogy alakítsák ki a változáskezelés rendjét, illetve alkalmazzanak ún. ticketing rendszert vagy más módon dokumentálják az üzemeltetési tevékenységeket.

4.10.14 Biztonsági tesztelés, sérülékenységvizsgálat

A Gimnázium informatikai infrastruktúráján még egyszer sem hajtottak végre biztonsági tesztelést. A biztonsági tesztelés és a feltárt sérülékenységek javítása kulcsfontosságú, hiszen az ismert és még nem javított sérülékenységek kihasználásával fel lehet törni az informatikai rendszereket.

Kockázatelemzés után javasoljuk a Gimnázium informatikai rendszereinek biztonsági tesztelését, ún. penetrációs teszt végrehajtását. Tekintettel arra, hogy a penetrációs tesztek végrehajtása magas költséggel jár, a sérülékenységeket automatizált sérülékenységkereső szoftverekkel (vulnerability scanner) is fel lehet tárni. A szerverek és a munkaállomások rendszeres biztonsági frissítésekkel való ellátása (patchelés) kulcsfontosságú és létező folyamat, azonban így sem derül fény számos sérülékenységre. Továbbá ajánlott feliratkozni a Nemzeti Kibervédelmi Intézet sérülékenységekről tájékoztató hírleveleire.

4.10.15 Folyamatos tudatosság növelés

Jelen projekt keretében a Gimnázium igazgatója az alábbi mérőszámokkal rendelkező adatvédelmi tudatosítást végezték el:

Dátum	Időpont	Leoktatott munkavállaló	Helyszín
2019. szeptember 10.	...	Nevelőtestületi ülés	...
Mindösszesen		**... fő**	

5. Melléklet: Vizsgált területek és dokumentumok

Munkánk során az alábbi területeken, és résztvevőkkel végeztünk személyes interjúkat.

Területek	Felelős	Interjú időpontja	Helyszín
Intézményvezető	Tápai Ildikó	2019. november 14. és 2. kör: 2019. november 27.	DNG/MS Teams
Intézményvezető-helyettes 1.	Varsányi Krisztina	2019. november 14.	DNG
Intézményvezető-helyettes 2.	Lipták Tünde	2019. november 14.	DNG
Gazdasági vezető	Tóthné Szabó Ildikó	2019. november 15.	DNG
Iskolatitkár	Gerhard Csilla	2019. november 14. és 2. kör: 2019. november 22.	DNG/MS Teams
Könyvtár	Gáspár Anita	2019. november 14.	DNG

Munkánk során az alábbi Iskolaközpont által rendelkezésre bocsátott szabályzatokat vizsgáltuk:

- Szervezeti Működési Szabályzat (SzMSz)

- Iratkezelési Szabályzat (2011.)
- Szervezeti felépítés
- Ellenőrzési nyomvonalak

Releváns jogszabályok:

- 2011. évi CXC. törvény a nemzeti köznevelésről
- 2011. évi CLXXXIX. törvény Magyarország helyi önkormányzatairól
- 2011. évi CLXXIX. törvény a nemzetiségek jogairól
- 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről
- 2011. évi CXCV. törvény az államháztartásról
- 2012. évi I. törvény a munka törvénykönyvéről
- 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- Az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
- 2019. évi XXXIV. törvény az Európai Unió reformjának végrehajtása érdekében szükséges törvénymódosításokról.