



**Óbudai Szent Péter és Pál
Szalézi Általános Iskola és Óvoda**

KAMERA SZABÁLYZAT

Adatkezelő elérhetősége: 1036 Budapest, Tímár utca 10-16.

Az adatkezelő képviselőjének neve és elérhetősége:

Lux Ambrus Tibor, igazgato@peterpaliskola.hu

Budapest, 2025. augusztus 30.

Lux Ambrus
igazgató

Tartalomjegyzék

Általános rendelkezések	3
Az Adatkezelő	5
A Szabályzat hatálya és vonatkozó jogszabályok	6
Értelmező rendelkezések	8
A kamerarendszer biztonsági felelősei	11
A kamerarendszer működtetésének jogalapja	12
A kamerarendszer elhelyezése	14
A felvételek tárolása.....	15
Biztonsági intézkedések.....	16
Az adatvédelmi incidens.....	17
Az érintettek kamerarendszerrel összefüggő jogai	18
Hatálybalépés, egyéb rendelkezések.....	20
1. sz. Melléklet: Kamera tájékoztató	21

Általános rendelkezések

Jelen szabályzat (a továbbiakban: „**Szabályzat**”) célja az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda, mint adatkezelőnek az elektronikus megfigyelő rendszerekkel (kamerarendszer) összefüggésben, a személyes adatok kezelésére vonatkozó kötelezettségeinek szabályozása. A Szabályzat meghatározza az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda személyes adatok kezelése és védelme körében teendő intézkedéseit, illetve rögzíti belső adatvédelmi eljárásait.

Az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda elkötelezett a természetes személyek személyes adatainak védelmében, ebből fakadóan kiemelten fontosnak tartja az információs önrendelkezési jog tiszteletben tartását. Ennek megfelelően az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda adatkezelési-, és adatfeldolgozási tevékenységei kapcsán tudomására jutott személyes adatokat bizalmasan kezeli, és megtesz minden olyan biztonsági, technikai és szervezési intézkedést, mely az adatok biztonságát garantálja.

Az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda, mint adatkezelő magára nézve kötelezőnek ismeri el a szabályzat tartalmát és kötelezettséget vállal arra, hogy tevékenységével kapcsolatos minden adatkezelés megfelel a jelen szabályzatban-, valamint a hatályos nemzeti és európai uniós jogi aktusokban foglaltaknak.

A szabályzat által megvalósítani kívánt cél, hogy az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda a szervezeti és a szervezetén kívüli jogviszonyokban is biztosítsa az alábbi feltételeket:

- az Adatkezelő székhelyén tartózkodó személyek életének, testi épségének, személyi szabadságának védelme;
- az Adatkezelő székhelyén tartózkodó személyek, illetve az adatkezelő által tulajdonolt vagy használt vagyontárgyainak védelme (vagyonvédelem);
- az Adatkezelő birtokában lévő személyes adatok védelme, az információk bizalmas jellegének, helyességének és integritásának megóvása, épségük védelme;
- az Adatkezelő tevékenysége során keletkezett személyes adatok védelme;
- a nemzeti és európai uniós adatvédelmi és adatbiztonsági előírásoknak történő megfelelés.
- az elektronikus megfigyelőrendszerekben (a továbbiakban: „kamerarendszer”) tárolt adatok biztonsága és megfelelő rendelkezésre állása;
- a kamerák felvételeit, illetve a kamerákkal kapcsolatosan tárolt adatokat őrző helyiségek biztonságának megóvása;
- a kamerarendszerrel összefüggő információk illetéktelen hozzáféréséből és felhasználásából eredő hátrányos hatások elkerülése, megszüntetése, és minimális nagyságúra való csökkentése;
- az Adatkezelő székhelyén elkövetett jogsértések észlelése, feltárása, felderítése, bizonyítékok gyűjtése;
- illetve az Adatkezelő jogszabályban rögzített feladatainak megfelelő, jogszerű és hatékony ellátása.

Az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda kiemelt feladatának tartja és biztosítja, hogy az őt képviselő, valamint nevében eljáró személyek, közalkalmazottak és munkavállalók, szerződéses partnerei, továbbá bármely olyan személy, aki Óbudai Szent Péter

és Pál Szalézi Általános Iskola és Óvoda nevében eljár – így különösen a kamerarendszer üzemeltetését végző személyzet - e szabályzat tartalmát megismerje és magatartását, eljárását a szabályzat tartalmához alakítsa. Az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda mindenkor ellenőrzi és kötelezi a fent említett személyeket, hogy a személyes adatok legalább ugyanolyan szintű védelmét biztosítsák, mint a jelen szabályzatban foglalt biztonsági intézkedések.

A Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda a személyes adatokhoz való hozzájutás, tárolásuk, kezelésük és feldolgozásuk során mindenkor biztosítja az olyan szervezési és technikai intézkedéseket, melyek a GDPR Rendeletben meghatározott alapelvek betartását és az érintettek jogainak védelmét szolgálják. Az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda kijelenti és jelen szabályzatában megerősíti, hogy kizárólag olyan személyes adatokat gyűjt, tárol és kezel, melyek az Adatkezelési Tevékenységek Nyilvántartásában foglalt célok megvalósításának érdekében feltétlenül szükséges.

Az Adatkezelő

Az adatkezelő megnevezése:

Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda (a továbbiakban: „**Adatkezelő**”)

Az Adatkezelő székhelye: 1036 Budapest, Tímár utca 10-16.

Az Adatkezelő vezetője és az adatkezelésért felelős személy: Lux Ambrus Tibor, igazgató

Az Adatkezelő tevékenysége: Az Adatkezelő egyházi fenntartású alapfokú közoktatási intézmény

A Szabályzat hatálya és vonatkozó jogszabályok

1. A Szabályzat személyi hatálya

Jelen Szabályzat személyi hatálya kiterjed az Adatkezelő valamennyi megbízási-, vállalkozási-, továbbá munkaviszonyban foglalkoztatott munkatársára, - így különösen a kamerarendszer üzemeltetésével és felügyeletével megbízott személyzet munkatársaira, - továbbá bármely olyan személyre, akinek képmását (esetlegesen hangfelvételt) a kamerarendszer rögzíti.

2. A Szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya kiterjed

- az Adatkezelő kamerarendszerében tárolt és kezelt adataira;
- az Adatkezelő tulajdonát képező, illetve az Adatkezelő által bérelt kamerarendszer eszközeire;
- az Adatkezelő székhelyén lévő-, valamint az Adatkezelő megbízásából harmadik személy által az Adatkezelőnek, vagy alkalmazottai részére biztosított kamerarendszer eszközeire, ideértve az eszközök és berendezések műszaki dokumentációját is;
- az Adatkezelő kamerarendszerén és a kamerák által közvetített képmást megjelenítő eszközökön futó rendszerprogramokra, programokra.

Jelen szabályzat rendelkezései alkalmazandók minden olyan esetre, mely során az Adatkezelő megbízása vagy meghatalmazása alapján harmadik személy végez adatkezelést vagy adatfeldolgozást az Adatkezelő részére.

3. Az Adatkezelő adatkezeléseire vonatkozó jogszabályok

GDPR	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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
Szmtv.	2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

Az Adatkezelő vállalja, hogy a személyes adatok kezelésével kapcsolatos kötelezettségeit a mindenkor hatályos magyar és európai uniós jogszabályoknak megfelelően – így különösen a fent megjelölt jogszabályi rendelkezéseknek megfelelően teljesíti.

Értelmező rendelkezések

személyes adat: azonosított vagy azonosítható természetes személyre 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.

adat: minden olyan ismeret, mely korábban már rögzítésre került, így az információ hordozója, a tények, fogalmak vagy utasítások formális ábrázolása, amely személyek számára vagy informatikai eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

adatátvitel: adatok informatikai rendszerek, illetve a rendszer elemei között történő továbbítása.

adatbiztonság: a személyes adatok illetéktelen megszerzése, tárolása, kezelése, feldolgozása ellen létesített szervezeti, szervezési, technikai megoldások és eljárásrend, kötelező érvényű rendelkezések együttese, az informatikai és egyéb rendszerek azon biztonságos állapota, mely során az adatok integritásának fenntartása érdekében az egyes kockázati tényezők a lehető legcsekélyebb mértékűre kerülnek csökkentésre.

adatbiztonság megsértése: az a tevés vagy mulasztás, amely sérti vagy veszélyezteti az adatok védelmére tett intézkedések, szabályok és eljárásrend érvényesülését.

adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az Adatkezelő nevében személyes adatokat kezel.

adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.

adatgazda: az a természetes személy, aki az Adatkezelő által részére biztosított engedéllyel és jogosultsággal adatokat birtokol, minősít, osztályoz, valamint az általa birtokolt, minősített és osztályozott adatok feldolgozásához szükséges rendszerek jogosultságaiért kezeléséért felelős.

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.

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.

adathordozó: adatot tartalmazó, illetve adat tárolására alkalmas eszköz vagy anyag, függetlenül előállításának módjától, eszközétől és céljától.

adatvédelem: a személyes adatok gyűjtésének, kezelésének és felhasználásának szabályozása annak érdekében, hogy a GDPR, valamint a vonatkozó jogszabályoknak megfelelő szintű és minőségű adatkezelés biztonságos formában érvényesülni tudjon.

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.

bizalmasság: az informatikai biztonsági rendszer azon tulajdonsága, hogy az ott megtalálható adatot, információt kizárólag az arra jogosultak és csak a jogosultságuk szintjének mértékében ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

biztonság: Az Adatkezelő működésének olyan állapota, melynek fennállása esetén az Adatkezelőnek az adatok sérülésének, elvesztésének, illetéktelen eltulajdonításának a lehető legkisebb bekövetkezési valószínűségével kell számolnia, szolgáltatásait a meghatározott feltételekkel és korlátozások nélkül képes biztosítani, feladatai ellátásával összefüggésben érdemi veszteség nem éri, a lehetséges kockázat az Adatkezelő számára elfogadhatóan alacsony és a belső kockázatkezelési eljárások eredményeként kialakuló maradvány kockázat a szervezet számára az elfogadható tartományban marad..

biztonsági esemény: valamennyi olyan történés, mely a fennálló biztonsági előírásokat és kötelező rendelkezéseket sérti vagy veszélyezteti, illetve amely a fennálló előírások és kötelező rendelkezések sérülésének gyanújával jár, így ide tartozik különösen a rendszerbiztonságban létrejövő olyan kedvezőtlen fordulat, mely hatására a biztonság, valamint az Adatkezelő által tárolt, kezelt és feldolgozott adatok integritása, biztonsága, helyessége, hitelessége, valamint rendelkezésre állása sérül vagy veszélybe kerül.

biztonsági esemény elhárítása: az informatikai biztonsági rendszerben bekövetkezett biztonsági esemény leírása és feljegyzése, következményeinek elhárítása és enyhítése, a bekövetkezés okainak és felelőseinek feltárása, és a hasonló biztonsági események jövőbeni előfordulásának prevenciója érdekében végzett tervszerű folyamat.

biztonsági követelmények: a belső kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági előírások, követelmények összessége.

elszámoltathatóság: az az állapot, illetve követelmény, amely fennállása esetén valamennyi adat, információ, valamint az informatikai rendszerrel kapcsolatos tevékenység egyértelműen azonosítható, átlátható, utólag visszakövethető, továbbá meghatározható az a személy aki az adott tevékenységet elrendelte és az a személy aki ezt a tevékenységet végrehajtotta.

érintett: : bármely információ alapján azonosított vagy azonosítható természetes személy.

biztonsági rendszer: az Adatkezelő székhelyének vagyónvédelmi, személyvédelmi rendszere, illetve az ehhez kapcsolódó beléptető rendszerek és a beléptetés módja.

hálózat: informatikai eszközök közti adatátvitelt lehetővé tevő logikai és fizikai eszközök összessége.

hitelesség: az adat olyan tulajdonsága, amely azt reprezentálja, hogy egy adat bizonyítottan vagy bizonyíthatóan a meghatározott forrásból származik.

hozzáférés: olyan metódus, amely valamely informatikai rendszer felhasználója számára – a jogosultságának kiosztásának függvényében – adott célra, helyben és időben elérhetővé teszi az informatikai rendszer szegmenseit, valamint elérhetővé tesz a rendszerben adatokként tárolt információkat.

információs önrendelkezési jog: az Alaptörvény VI. cikkének (3) bekezdésében megjelölt, mindenkit megillető, „személyes adatai védelméhez” való jognak azon alapvető tartalma, hogy minden természetes személy maga rendelkezik személyes adatairól és azok felhasználásáról.

illetéktelen személy: bármely olyan személy, aki az adatok megismerésére nem jogosult.

kamerarendszer: Az Adatkezelő tulajdonában lévő-, vagy általa bérelt, külön erre feljogosított személyek által működtetett képmás (és hangfelvétel) rögzítésére alkalmas digitális felvevőeszköz, valamint a kamerafelvételek megtekintéséhez és a kamerák üzemeltetéséhez szükséges valamennyi más eszköz.

kockázat: az informatikai rendszer fenyegetettsége, amely valamely fenyegető tényezőtől ered és amely a belső kockázatelemzés során az ilyen tényezők értékelése révén került megismerésre.

kockázatkezelés: olyan megelőző intézkedések kidolgozása, elemzése és meghozatala, melynek következtében a maradványkockázatok elfogadható szintűre mérséklődnek. A kockázatkezelés az elektronikus információs rendszerben megjelenő és erre ható kockázatok csökkentését célzó intézkedésrendszer megállapítása.

különleges adat: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviselési szervezeti tagságra, a szexuális életre vonatkozó személyes adat; az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint az Infotv. 3. § 4. pontja szerinti bűnügyi személyes adat.

mentés: a kamerarendszerben digitálisan tárolt információkról történő biztonsági másolat készítése speciális adathordozóra, arra az esetre, mikor az eredeti forrásadatokat tartalmazó tároló megsérül.

üzleti titok: az Adatkezelő tevékenységéhez kapcsolódó, titkos - egészben, vagy elemeinek összességéként nem közismert vagy az érintett tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennél fogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja.

A kamerarendszer biztonsági felelősei

4. A kamerarendszer biztonságáért felelős személyek

A kamerarendszer biztonságának mindenkor felelőse az Adatkezelő vezetője. A jelen szabályzatban foglaltak szakszerű és hatékony érvényesülését a vezetőnek kell biztosítania.

4.1. A vezető (igazgató) feladatai a kamerarendszer üzemeltetésének körében

- a kamerarendszert felügyelő biztonsági szolgálat kiválasztása;
- a kamerarendszer technikai paramétereinek áttekintése és jóváhagyása;
- jelen szabályzat kiadása, vezetése, naprakészen tartása, módosítások átvezetése;
- a kamerarendszerrel kapcsolatos adatkezelés és adatfeldolgozás ellenőrzése;
- a kamerarendszer védelmét szolgáló eszközökre vonatkozó szabályozás kialakítása;
- az adatvédelmi tevékenységeket biztosító követelményrendszer kialakítása és naprakészen tartása;
- az adatvédelmi feladatok ismertetése;
- az alkalmazottak képzése;
- esetlegesen adatvédelmi tisztviselő kijelölése.

4.2. A biztonsági szolgálat vezetőjének feladatai

- a kamerarendszer működése szempontjából fontos adatok változásainak követése;
- az Adatkezelő kamerás megfigyelőeszközeinek nyilvántartása;
- a kamerarendszer védelmének biztosítása;
- a kamerarendszer hibája esetén a rendszer helyreállítása;
- a kamerarendszer üzembiztonságának ellenőrzése és fenntartása;
- a kamerarendszer védelmét szolgáló eszközök működtetése és felügyelete.

A kamerarendszer működtetésének jogalapja

5. A megfelelő munkavégzés biztosítása

A 2012. évi I. törvény a munka törvénykönyve (Mt.) rendelkezései szerint, a munkavállaló köteles a munkáltató irányítása alapján munkát végezni. A munkavállaló köteles munkaideje alatt a munkáltató rendelkezésére állni és munkáját az általában elvárható szakértelemmel és gondossággal, a munkájára vonatkozó szabályok, előírások, utasítások és szokások szerint végezni.

Az Mt. 11. § (1) bekezdése lehetőséget biztosít a munkáltató számára, hogy a munkavállalót a munkaviszonnyal összefüggő magatartása körében ellenőrizze. Ez a jogosultság szükségszerűen együtt jár személyes adatok kezelésével. Ezen adatkezelés jogszerűségéhez nem szükséges a munkavállalók hozzájárulása.

A GDPR előtt hatályban lévő Adatvédelmi Irányelv alapján létrehozott Adatvédelmi Munkacsoport több állásfoglalásában is kifejtette, hogy a munkavállaló-munkáltató viszonyában megkérdőjelezhető az önkéntes hozzájárulás lehetősége. A Munkacsoport álláspontja szerint, „a foglalkoztatás kontextusában nehézségek merülhetnek fel az érintett beleegyezésének önkéntes voltával kapcsolatban, hiszen a munkáltató és az alkalmazott között alá-fölérendeltségi viszony van.

Az érvényes beleegyezés ebben az értelemben azt jelenti, hogy az alkalmazottnak valós lehetőséget kell biztosítani beleegyezése megtagadására vagy utólagos visszavonására – amennyiben meggondolja magát – anélkül, hogy hátrány érne emiatt. A hierarchikus függés e helyzeteiben az alkalmazott továbbítással kapcsolatos elutasítása vagy fenntartása anyagi vagy nem anyagi természetű hátrányt okozhat neki, ami teljes mértékben ellentétes a személyes adatok védelmére vonatkozó európai jogalkotás szövegével és szellemével.”

A Munkacsoport nézete szerint ezért a munkajog világában az Adatvédelmi Irányelvben szereplő más jogalapok alkalmazása indokolt. Az Adatvédelmi Munkacsoport a hozzájárulás fogalom meghatározásáról szóló 15/2011. számú véleményében azt is kifejtette, hogy a jogszerű adatkezelésnek nem csak a hozzájárulás lehet az egyetlen jogalapja, hanem az Adatvédelmi Irányelv 7. cikkében szereplő többi jogalap is alkalmazható az adatkezelők számára.

Ezt a GDPR is megerősíti, vagyis a munkavállalók esetleges kamerarendszeren keresztül történő ellenőrzésének jogalapja nem az érintett hozzájárulása, hanem az Adatkezelő jogos érdeke.

- Az Adatkezelői ellenőrzés akkor tekinthető jogszerűnek, amennyiben az a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges;
- A munkáltatói ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével; illetőleg a munkavállaló magánélete nem ellenőrizhető;
- A munkavállalót előzetesen tájékoztatni kell az adatkezelés lényeges követelményeiről;
- Az adatkezelés akkor jogszerű, ha a munkáltató az adatkezeléssel kapcsolatban betartja a GDPR alapvető rendelkezéseit.

6. Vagyonvédelem

Elektronikus kamerarendszert elsődlegesen az emberi élet, testi épség, személyi szabadság védelme, a veszélyes anyagok őrzése, az üzleti, fizetési, bank- és értékpapírtitok védelme, vagyonvédelem céljából lehet alkalmazni. Így például a kamerás megfigyelés esetkörébe tartozhat a veszélyforrást hordozó létesítmények, munkahelyiségek (nagy teljesítményű gépeket tartalmazó szerelőcsarnokok, egyes gyártási folyamatok). Indokolt esetben, így a munkahelyen tárolt, jelentős értéket képviselő eszközök, nyersanyagok, illetőleg egyéb értéktárgyak védelme céljából, a védelem szempontjából szükséges helyiségek (elsősorban raktárak és az azokhoz vezető folyosók) is megfigyelhetők.

Az Adatkezelő a kamerarendszer üzemeltetését Adatkezelői személy-, és vagyonvédelem szempontjából veszi igénybe, azonban a kamerás megfigyelés abszolút korlátja az emberi méltóság tiszteletben tartása, melyet az Adatkezelő mindenkor tiszteletben is tart.

Tekintettel arra, hogy az Adatkezelő székhelyén minősített iratokat őriz, így a kamerarendszer üzemeltetése mindenképpen indokolt.

A kamerarendszer működtetésével kapcsolatosan az adatkezelés jogalapja tehát a GDPR 6. cikk (1) f) pontjának megfelelően az Adatkezelő jogos érdeke.

A kamerarendszer elhelyezése

7. A kezelt személyes adatok

Az Adatkezelő által alkalmazott kamerarendszerben személyes adatok közül az érintettek képmása (és esetlegesen hangfelvétele) kerül rögzítésre, mint személyes adat. A kamerarendszer által készített felvételeken beazonosítható személyek tűnhetnek fel, így a kamerarendszer ezen személyek mozgásának, illetve bizonyos magatartásának meghatározására is alkalmas.

8. A kamerás megfigyelés abszolút korlátja az emberi méltóság tiszteletben tartása. Az Adatkezelő ebből kifolyólag az alábbi alapelveket rögzíti kamerarendszerének üzemeltetése körében:

Nem lehet olyan kamerát elhelyezni, amely kizárólag egy munkavállalót és az általa végzett tevékenységét figyeli meg.

Jogellenesnek tekinthető az olyan elektronikus megfigyelőrendszer alkalmazása, amelynek célja a munkavállalók munkahelyi viselkedésének a befolyásolása.

Az elektronikus megfigyelőrendszerek alkalmazhatóságának további alapelve az is, hogy semmiképp sem lehet kamerát elhelyezni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti, így különösen az öltözőkben, zuhanyzóknak, az illemhelyiségekben vagy például orvosi szobákban, illetve az ahhoz tartozó váróban.

Emellett nem lehet elektronikus megfigyelőrendszert alkalmazni az olyan helyiségben sem, amely a munkavállalók munkaközi szünetének eltöltése céljából lett kijelölve.

Ha a munkahely területén jogszerűen senki sem tartózkodhat (így különösen munkaidőn kívül vagy a munkaszüneti napokon), akkor a munkahely teljes területe megfigyelhető.

Az Adatkezelő elektronikus kamerarendszert kizárólag a saját tulajdonában/használatában álló épületrészek, helyiségek és területek, illetőleg az ott történt események megfigyelésére alkalmaz, közterületet semmilyen körülmények között nem figyel meg.

Az kamerarendszerhez tartozó kamerák darabszáma: 4

A kamerák elhelyezkedése:

Kamerák helye	Megfigyelési tartománya
Udvar – műfüves pálya	Udvar
Udvar – salakos pálya	Udvar
Udvar – aszfaltos pálya	Udvar
Főbejárat	Bejárat
Földszinti aula	Aula

A felvételek tárolása

9. A felvételek rögzítése és tárolása

Az Adatkezelő által alkalmazott kamerarendszer kép-, és esetlegesen hangfelvételeket folyamatosan rögzít. A felvételek rögzítésének helye az Adatkezelő irodája.

A felvételeket a kamerarendszer automatikusan szerverre rögzíti, mely szerver jelszóvédelemmel van ellátva. A szerverhez kizárólag az Adatkezelő erre a feladatra kijelölt munkatársa, illetve a vezető férhetnek hozzá.

Azok a felvételek, melyek 3 munkanapnál régebbi kép-, és esetlegesen hangfelvételeket tartalmaznak a 3 munkanap elteltét követően automatikusan törlésre kerülnek.

Kivétel a fenti eset alól az az eset, amikor a kamerarendszerben rögzített felvételeket bármely jogszerű célból felhasználni szükséges. Ebben az Adatkezelő gondoskodik a kamerafelvételek megfelelő és biztonságos tárolásáról és a jogszerű cél megvalósulását követő 3 napon belül törlik manuálisan a kamerarendszerről.

A felvételekről bármiféle másolat kizárólag jogszabályokban, vagy hatósági határozatban meghatározott esetekben készülhet. Amennyiben ilyen módon másolat készül, úgy az Adatkezelő lehetőség szerint gondoskodik arról, hogy a másolat kizárólag olyan személynek kerüljön átadásra, aki erre vonatkozóan titoktartási megállapodást írt alá az Adatkezelővel.

A kamerarendszer által digitális formában rögzített felvételekhez az Adatkezelőtől független, külső hálózaton keresztül nem lehet hozzáférni.

Az Adatkezelő a jelen szabályzat személyi hatálya alá tartozó személyeknek mindenkor megadja a szükséges tájékoztatást a kamerarendszer alkalmazásáról.

- Alkalmazottak esetében a munkavégzésre irányuló szerződéshez kapcsolódó tájékoztató tartalmazza az erre vonatkozó tájékoztatást;
- Egyéb érintettek tekintetében kihelyezett tájékoztató biztosítja a kamerarendszer üzemeltetésére való figyelemfelhívást.

Biztonsági intézkedések

10. A személyes adatok védelme érdekében eszközölt biztonsági intézkedések

Tilos a kamerarendszer által készített és sugárzott felvételekről bármilyen eszközzel – a kamerarendszer központi felvevő egységét leszámítva – felvételt készíteni, felvételt tárolni, illetve felvételt bármilyen módon továbbítani.

A kamerarendszer által készített felvételekhez kizárólag az Adatkezelő erre kijelölt munkatársai, illetve az Adatkezelő által igénybe vett biztonságtechnikai cég munkatársai férhetnek hozzá és azokat kizárólag az Adatkezelő erre kijelölt munkatársai ismerhetik meg. Amennyiben tőlük eltérő személy számára szükséges a kamerarendszer által készített felvételek megtekintése, úgy erre minden esetben kizárólag az Adatkezelő vezetőjének jelenlétében kerülhet sor.

Amennyiben a már mentett kamerafelvétel visszajátszása indokolt, úgy a visszajátszást és a kamerarendszerről készített bármiféle másolat készítését dokumentálnia kell az Adatkezelő munkatársának.

Az Adatkezelő minden esetben biztosítja, és a tőle elvárható magatartást mindenkor megteszi annak érdekében, hogy a kamerafelvételek integritásának megváltozása, sérülése, megváltozása, a felvételekhez történő illetéktelen hozzáférést elkerülje.

Az Adatkezelő által használt informatikai rendszer frissített tűzfallal van védve, és vírusvédelemmel van ellátva.

Az Adatkezelő által a kamerarendszer üzemeltetésével összefüggésben használt informatikai eszközök minden esetben megfelelő logikai és fizikai védelemmel vannak ellátva.

Az adatvédelmi incidens

11. Adatvédelmi incidens/biztonsági incidens cselekvési terv

Abban az esetben, ha a kamerarendszer használatával összefüggésben az Adatkezelőnél adatvédelmi incidens bekövetkezése fenyeget, vagy adatvédelmi incidens következik be az Adatkezelő vezetője az Adatkezelési és Adatvédelmi Szabályzat-, valamint a GDPR és az Infotv. vonatkozó rendelkezései alapján jár el.

Az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Az adatvédelmi incidenst minden esetben fontos kiemelten kezelni, hiszen a szükséges intézkedés hiányában jelentős károkat okozhat a személyes adatok kezelése körében. Az adatvédelmi incidens alkalmas arra, hogy a személyes adatok integritását, jogszerű kezelését veszélyeztesse, illetve sértse, ezzel az érintettek számára jelentős károkat okozhat.

Az adatvédelmi incidens során követendő eljárás:

Amennyiben az Adatkezelő munkatársának adatvédelmi incidens jut a tudomására, ezt haladéktalanul, de legkésőbb 24 órával az észlelést követően köteles jelenteni a vezetőnek. A vezető legkésőbb 72 órán belül jelzi és jelenti az adatvédelmi incidenst a felügyeleti hatóságnak.

Az Adatkezelő mellőzi a bejelentést, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a hatósághoz történő bejelentés nem történik meg 72 órán belül, az Adatkezelő köteles mellékelni a bejelentéshez a késedelem igazolására szolgáló indokokat is.

Az Adatkezelő az alkalmazottak és a felhasználók részére tartott informatikai biztonsági képzésen biztosítja az adatvédelmi incidens esetén követendő eljárás megismerését, és felkészíti alkalmazottait, és a felhasználókat, hogy egy esetleges adatvédelmi incidens bekövetkezése esetén milyen teendőket kell ellátniuk.

Az Adatkezelő informatikai rendszerét érintő adatvédelmi incidensre utalhat különösen, amennyiben:

- a kamerarendszer működése a vonatkozó jogszabályokkal és a jelen szabályzatban foglaltakkal nyilvánvalóan ellentétes;
- a kamerarendszer olyan módosulásokat produkál, melyekről az Adatkezelő munkatársai nem kaptak előzetesen értesítést;
- a kamerarendszerben kezelt adatok elvesznek, vagy hozzáférhetetlenné válnak;
- a kamerarendszer egyébként rendellenesen reagál vagy működik;
- az Adatkezelő munkatársának tudomására jut, hogy a kamerarendszerhez jogosulatlan hozzáférés történt;
- az Adatkezelő munkatársa a kamerarendszerrel összefüggésben akár szoftveres, akár hardveres hibát észlel.

Az érintettek kamerarendszerrel összefüggő jogai

12. Az érintetti jogok

Azok a személyek, akiknek jogát vagy jogos érdekét a kép-, hang-, vagy a kép- és hangfelvétel, illetve más személyes adatának törlése érinti, a kép-, hang-, valamint kép- és hangfelvétel, illetve más személyes adat rögzítése kapcsán kérheti az Adatkezelőtől, hogy az adatot az Adatkezelő ne semmisítse meg, illetve ne törölje.

Bíróság vagy más hatóság megkeresésére a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre - attól számított harminc napon belül, hogy a megsemmisítés mellőzését kérték - nem kerül sor, a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell.

Az érintett bármikor jogosult tájékoztatást kérni postai, elektronikus, vagy telefonos úton az Adatkezelő elérhetőségein keresztül az Adatkezelő által kezelt személyes adatairól.

Az Adatkezelő a hozzá beérkező kérdés vonatkozásában tájékoztatja az érintettet:

- a kezelt adatokról;
- az adatkezelés céljáról;
- jogalapjáról;
- időtartamáról;
- arról, hogy kik és milyen célból kapják vagy kapták meg adatait.

A tájékoztatást az Adatkezelő a kérelem benyújtásától számított 25 napon belül írásban, a tájékoztatáskérés formájától függően papír, vagy elektronikus úton adja meg.

A tájékoztatás ingyenes, ha a kérelmező ugyanabban az évben ugyanarra a tevékenységre, adatkörre vonatkozó tájékoztatási kérelmet az Adatkezelőhöz még nem nyújtott be.

Ettől eltérő esetekben az Adatkezelő költségtérítést állapít meg, és a tájékoztatást a költségtérítés megfizetését követően biztosítja.

Az érintett bármikor tiltakozhat személyes adatai kezelése ellen. A tiltakozást annak benyújtásától számított legrövidebb időn belül, de legfeljebb 25 nap alatt az Adatkezelő megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és a döntésről az érintettet tájékoztatja.

Az érintett bármikor jogosult az Adatkezelő által kezelt személyes adatok törlését, vagy a helytelenül rögzített személyes adatok helyesbítését kérni.

Az érintett kérelmére, valamint az Infotv. által meghatározott esetekben az érintett személyes adatai kezelését az Adatkezelő korlátozza.

Az Adatkezelő zárolja az érintett személyes adatát, ha az érintett ezt kéri, vagy ha az Adatkezelő rendelkezésére álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így zárolt személyes adatot az Adatkezelő addig kezeli, ameddig fennáll az adatkezelési cél vagy jogos érdek, amely a személyes adat törlését kizárta.

A törlési, helyesbítési és zárolási kérelemnek a lehetőségekhez képest leghamarabb, de legfeljebb 25 napon belül tesz eleget az Adatkezelő és erről az érintettet értesíti. Ha az Adatkezelő az érintett kérelmének nem tud helyt adni, ez esetben is 25 napon belül értesítik erről.

Ha az adatot az érintett hozzájárulásával az Adatkezelő más személy számára továbbította, az adattovábbítás címzettjét is értesíti a szükséges lépésekről.

Az érintett jogosult panaszával a Nemzeti Adatvédelmi és Információszabadság Hatósághoz

1125 Budapest, Szilágyi Erzsébet fasor 22/c.

www.naih.hu,

Telefon: +36 (1) 391-1400,

Telefax: +36 (1) 391-1410,

E-mail: ugyfelszolgalat@naih.hu)

fordulni vagy a Polgári perrendtartásról szóló 2016. évi CXXX. törvény szerint hatáskörrel és illetékességgel rendelkező Bíróság előtt érvényesíteni személyes adatok kezelésével kapcsolatos jogait.

A személyes adatokra vonatkozó tájékoztatásra, helyesbítésre, törlésre, zárolásra és tiltakozásra vonatkozó jogosultságait az érintett bármikor gyakorolhatja, amennyiben e-mailben vagy egyéb módon írásban kapcsolatba lép az Adatkezelővel.

Az Adatkezelő az érintett megkeresésével összefüggésben kérheti, hogy a megkereső személy azonosítsa magát vagy olyan egyéb adatokat adjon meg, melyek a személyére vonatkoznak, melyek a jogosultság igazolására szolgálnak. A megkeresést az Adatkezelő mindenkor a GDPR és az irányadó egyéb adatvédelmi jogszabályoknak megfelelően kezeli.

Hatálybalépés, egyéb rendelkezések

17. Jelen Szabályzatot az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda vezetője hagyta jóvá és léptette hatályba.

Az Adatkezelő vezetője gondoskodik arról, hogy a Szabályzatot az Adatkezelő minden alkalmazottja megismerhesse.

Jelen szabályzat felülvizsgálatát el kell végezni abban az esetben, ha a jelen szabályzat szabályozási tárgyában lényeges változás áll be; amennyiben a jelen szabályzat szabályozási tárgyára vonatkozó jogszabályi változások következnek be és ezért a szabályzat módosítása szükséges; illetve az előző két ponttól függetlenül a jelen szabályzat hatályba lépését követő minden ötödik évben.

Budapest, 2025. augusztus 31.

Lux Ambrus
igazgató

1. sz. Melléklet: Kamera tájékoztató

KÉPRÖGZÍTÉSRE ALKALMAS KAMERÁVAL

MEGFIGYELT TERÜLET!

1./ Az adatgyűjtés ténye: Az EU Parlament és Tanács Általános Adatvédelmi Rendelete (2016/679. sz. – „GDPR”) és a 2005. évi CXXXIII. törvény (ún. „személy és vagyonvédelmi törvény”) alapján a kamera látószögével érzékelt magánterületen elektronikus megfigyelő rendszer működik.

2./ Az érintett magánszemélyek és a kezelt személyes adatok köre: a kamera hatáskörzetében képfelvétel rögzítésére alkalmas elektronikus megfigyelőrendszer által megfigyelt területre belépő és ott tartózkodó személyekről készülő kép- és hangfelvétel, mozgásból, viselkedésből származó következtetés.

3./ Az adatkezelés célja: az élet- és vagyonbiztonság, valamint a jogsértések, szabálysértések, bűncselekmények észlelése, az elkövető tettenérése, a jogsértő cselekmények megelőzése, azok bizonyítása, valamint az Adatkezelő mint közfeladatot ellátó szerv feladatállítása körülményeinek biztosítása.

4./ Az adatkezelés jogalapja: közhatalmi feladat végrehajtása (GDPR 6. cikk (1) e) pont).

5./ Az adatkezelés időtartama: a törvényi felhatalmazás alapján a kép- és hangfelvétel a rögzítéstől számított 3 munkanapig tárolható felhasználás hiányában, ezt követően haladéktalanul megsemmisítésre, törlésre kerül, amennyiben nem szükséges a felhasználása.

6./ Az adatkezelő meghatározása: Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda

7./ Adattárolás helye és biztonsága: Az Adatkezelő kamerarendszerének szerverén, melynek biztonságáról az Adatkezelő a mindenkori Kamera-szabályzatban rendelkezik.

8./ Felvételek megtekintésére jogosult személyi kör: Az Adatkezelő erre hatáskörrel rendelkező munkatársai.

9./ Jogorvoslat: az érintettek az adatkezelés teljes időtartama alatt élhetnek a GDPR-ban biztosított jogaikkal a következő elérhetőségeken: Tel.: +36-1-388-8301, E-mail: titkarsag@peterpaliskola.hu , további igényérvényesítés esetén az illetékes adatvédelmi hatósághoz (www.naih.hu, tel: +361-391-1400), illetve bírósághoz is fordulhatnak.

Legitimációs záradék

Az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda Diákönkormányzata képviselőjében aláírással tanúsítom, hogy a Diákönkormányzat az iskolai Szervezeti és Működési Szabályzat kiegészítésének elfogadásához előírt véleményezési jogát gyakorolta.

Budapest, 2025. augusztus 27.


DÖK elnök

Az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda Szülői Tanács képviselőjében aláírással tanúsítom, hogy a Szülői Tanács az iskolai Szervezeti és Működési Szabályzat kiegészítésének elfogadásához előírt véleményezési jogát gyakorolta.

Budapest, 2025. augusztus 27.


Szülői Tanács megbízottja

Az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda Nevelőtestülete képviselőjében aláírással tanúsítom, hogy az iskolai Szervezeti és Működési Szabályzat kiegészítésének elfogadásához előírt véleményezési jogát gyakorolta. A Nevelőtestület a módosított SZMSZ-t - a munkaközösségek javaslatai alapján – megtárgyalta és a diákönkormányzati és a szülői véleményezés után elfogadta.

Budapest, 2025. augusztus 28.


igazgató


Nevelőtestület képviselője

A Fenntartó képviselőjében az Óbudai Szent Péter és Pál Szalézi Általános Iskola és Óvoda iskolai Szervezeti és Működési Szabályzat kiegészítését a Nkt. 32. § (1) pontja alapján jóváhagyom.

Budapest, 2025. augusztus 29.


SZIF pedagógiai igazgató