					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: PII24					Dokumentum címe: **CCTV- és fizikai megfigyelési adatvédelmi szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Jogi nyilatkozat (szerzői jog és felhasználási korlátozások)

(C) 2025 Clarysec LLC. All rights reserved.

Ez a dokumentum a Clarysec LLC szellemi tulajdona. A dokumentum semmilyen része nem másolható, nem használható fel újra, nem terjeszthető és nem módosítható kereskedelmi vagy bevezetési célból előzetes, kifejezett írásbeli engedély nélkül.

A jogosulatlan felhasználás szigorúan tilos, és jogi eljárást vonhat maga után.

Licenceléssel kapcsolatban keresse: info@clarysec.com

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány / jogszabály	Pont / kontroll / cikk	Alkalmazhatóság	Lefedettség típusa	Megjegyzés
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentált és működési kontrollok
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Nyomon követés és helyesbítő intézkedés
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Cél, jogalap, kockázati kiváltó ok és nyilvántartások
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Adatfeldolgozói és közös adatkezelői feladatmegosztás
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	PII-alanyokkal kapcsolatos kötelezettségek és kérelmek
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Gyűjtés, adatkezelés, adattakarékosság, megőrzés és megsemmisítés
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Adatközlési nyilvántartások és kérelmek
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Adatfeldolgozói megállapodások, utasítások, támogatás és nyilvántartások
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Adatfeldolgozói jogok és adatközlési támogatás
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Nyilvántartások védelme és naplózás
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Alapelvek és elszámoltathatóság
GDPR	Article 6	Controller	Primary	Jogalap

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Átláthatóság és tájékoztatók
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Joggyakorlási kérelmek
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Irányítás, adatfeldolgozók, nyilvántartások, biztonság, DPIA és tanácsadás
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Cél, gyűjtés, adattakarékosság, megőrzés és adatközlés
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Átláthatóság, részvétel, elszámoltathatóság, biztonság és megfelelés
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Adatvédelmi kockázat és DPIA kiváltó okok
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	PII-védelmi adatvédelmi kontrollok
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Hozzáférési és fizikai belépési kontrollok
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, fizikai megfigyelés, hozzáférés-korlátozás és naplózás

1. Hatály

1.1 Ez a szabályzat a CCTV-re, videómegfigyelésre, látogatók megfigyelésére, fizikai hozzáférés-szabályozási naplókra, őrszolgálat által vezetett megfigyelési nyilvántartásokra, telephelyi megfigyelő rendszerekre, valamint azokra a kapcsolódó fizikai megfigyelési tevékenységekre vonatkozik, amelyek PII-t gyűjtenek vagy más módon kezelnek.

1.2 Ez a szabályzat azokra a szervezetekre vonatkozik, amelyek saját telephelyeik és fizikai megfigyelési tevékenységeik tekintetében PII-adatkezelőként járnak el. Vonatkozik továbbá az adatfeldolgozói vagy al-adatfeldolgozói támogatási tevékenységekre is, amikor a szervezet ügyfél nevében megfigyelési felvételeket, látogatói adatokat vagy fizikai hozzáférési naplókat üzemeltet, hosztol, felülvizsgál, tárol, közöl, töröl vagy más módon kezel.

1.3 Ez a szabályzat kiterjed a megfigyelés céljának meghatározására, jóváhagyására, a tájékoztatásra és jelzésekre, a hozzáférés-korlátozásokra, az adatközlésre, a megőrzésre, a törlésre, a kiszervezésre, az incidenseszkalációra, a joggyakorlási kérelmek továbbítására, a felülvizsgálatra és a bizonyítékkezelésre.

1.4 Ez a szabályzat nem ad munkajogi tanácsot, üzemi tanácsi jogi kommentárt, bűnüldözési eljárásrendet, illetve külön CCTV-nyilvántartást. A megfigyeléshez kapcsolódó bizonyítékokat a jelen szabályzatban azonosított kanonikus PIMS bizonyítékobjektumokban kell fenntartani.

2. Cél

2.1 A szabályzat célja, hogy adatvédelmi kontrollokat állapítson meg a CCTV és a fizikai megfigyelés tekintetében annak érdekében, hogy a megfigyelési tevékenységek célhoz kötöttek, átláthatók, arányosak, hozzáférés-szabályozottak, meghatározott ideig megőrzöttek, kizárólag jóváhagyott csatornákon keresztül közöltek, valamint auditálható PIMS-bizonyítékokkal alátámasztottak legyenek.

2.2 Ez a szabályzat támogatja a megfigyelési felvételek, látogatói nyilvántartások, fizikai hozzáférési naplók és kapcsolódó megfigyelési PII egységes kezelését anélkül, hogy további nyilvántartásokat, bizottságokat, irányítópultokat vagy nem kanonikus szerepköröket hozna létre.

3. Célkitűzések

3.1 A szabályzat célkitűzései a következők:

3.1.1 a megfigyelési célok és az adatkezelési kör meghatározása a megfigyelés megkezdése előtt;

3.1.2 a CCTV, a fizikai hozzáférés, a látogatók megfigyelése és a fizikai megfigyelési tevékenységek dokumentálása a REG02-ben;

3.1.3 azon megfigyelési tevékenységek azonosítása, amelyek adatvédelmi kockázati felülvizsgálatot vagy DPIA-előszűrést igényelnek a REG04-ben;

3.1.4 az átlátható tájékoztatási és jelzésekre vonatkozó bizonyítékok fenntartása a REG07-ben;

3.1.5 a megfigyelési PII-hez való hozzáférés, megtekintés, exportálás, adatközlés és megőrzés korlátozása;

3.1.6 a PII-alanyok kérelmeinek továbbítása a REG06-on keresztül;

3.1.7 a kiszervezett megfigyelési szolgáltatók és adatmegosztási bizonyítékok kezelése a REG08-on keresztül;

3.1.8 a megfigyeléssel kapcsolatos feltételezett PII-incidensek eszkalálása a REG10-en keresztül;

3.1.9 a felülvizsgálatok, kivételek, meg nem felelések, helyesbítő intézkedések, auditmegállapítások és fejlesztések rögzítése a REG12-ben.

4. Szabályzati rendelkezések

4.1 Megfigyelési leltár, cél és jóváhagyás

4.1.1 [Controller] The Process Owner / Business Owner köteles minden CCTV-, látogatók megfigyelésére irányuló, fizikai hozzáférés-szabályozási naplózási vagy fizikai megfigyelési tevékenységet a tevékenység megkezdése előtt rögzíteni a REG02-ben.

4.1.2 [Controller] The Privacy Lead / PIMS Manager köteles az új vagy lényegesen módosított megfigyelési tevékenység aktiválása előtt ellenőrizni a REG02-bejegyzést a cél, a jogalap, a megfigyelt helyszín, a PII-kategóriák, a PII-alany kategóriák, a megőrzés, a tájékoztatás, a hozzáférés és az adatközlési mezők tekintetében.

4.1.3 [Controller] The Process Owner / Business Owner köteles a kamerák, érzékelők, látogatói naplók vagy hozzáférés-szabályozási naplózás engedélyezése előtt rögzíteni a jóváhagyott megfigyelt zónákat, a kizárt zónákat és a gyűjtési határokat a REG02-ben.

4.1.4 [Conditional] The Process Owner / Business Owner köteles REG04 szerinti adatvédelmi kockázati döntést beszerezni olyan megfigyelés aktiválása előtt, amely szisztematikus megfigyelést, hangrögzítést, biometrikus azonosítást, analitikával támogatott észlelést, érzékeny helyszíneket, kiszolgáltatott személyeket vagy nem nyilvánvaló megfigyelést foglal magában.

4.1.5 [Joint Controller] The Privacy Lead / PIMS Manager köteles a bérbeadóval, létesítményüzemeltetési partnerrel, ügyféllel vagy más közös adatkezelővel végzett közös megfigyelés megkezdése előtt rögzíteni a közös megfigyelési felelősségek megosztását a REG08-ban.

4.1.6 [Processor] The Privacy Lead / PIMS Manager köteles az ügyfél nevében végzett megfigyelési felvételek, látogatói nyilvántartások vagy fizikai hozzáférési naplók kezelése előtt rögzíteni az ügyfél megfigyelési utasításait és az engedélyezett adatkezelési határokat a REG08-ban.

4.2 Tájékoztatás és átláthatóság

4.2.1 [Controller] The Process Owner / Business Owner köteles biztosítani, hogy a megfigyelési jelzések vagy azzal egyenértékű, megfelelő időben nyújtott tájékoztatás bizonyítékai a megfigyelt területek PII-alanyok előtti megnyitása előtt rögzítésre kerüljenek a REG07-ben.

4.2.2 [Controller] The Privacy Lead / PIMS Manager köteles minden REG07-ben szereplő megfigyelési tájékoztatót a közzététel vagy lényeges módosítás előtt összekapcsolni a megfelelő REG02 szerinti adatkezelési céllal.

4.2.3 [Processor] The Privacy Lead / PIMS Manager köteles megfigyelési tájékoztatást támogató információt biztosítani a REG08-ban, ha a szervezet ügyfélutasítások alapján megfigyelési szolgáltatásokat üzemeltet.

4.2.4 [Conditional] The Process Owner / Business Owner köteles a nem nyilvánvaló vagy vészhelyzeti megfigyelés aktiválása előtt alternatív átláthatósági intézkedéseket rögzíteni a REG07-ben és a REG04-ben.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Kivételek

9.1 [All] The Privacy Lead / PIMS Manager köteles a jelen szabályzat alóli minden kivételt a kivétel alkalmazása előtt rögzíteni a REG12-ben.

9.2 [Conditional] The Data Protection Officer / Privacy Advisor köteles adatvédelmi tanácsot dokumentálni a REG04-ben vagy a REG12-ben a nem nyilvánvaló megfigyelést, hangrögzítést, biometrikus azonosítást, analitikával támogatott megfigyelést vagy érzékeny megfigyelési helyszíneket érintő kivételek jóváhagyása előtt.

9.3 [All] Top Management köteles a 90 napot meghaladó kivételeket a REG12-ben jóváhagyni az eredeti kivételi időszakon túli meghosszabbítás előtt.

9.4 [All] The Privacy Lead / PIMS Manager köteles a nyitott megfigyelési kivételeket lezárásukig legalább havonta felülvizsgálni a REG12-ben.

10. Betartatás

10.1 [All] The Privacy Lead / PIMS Manager köteles a megfigyelési kontrollhibákat a megerősítéstől számított öt munkanapon belül meg nem felelésként rögzíteni a REG12-ben.

10.2 [Both] The Information Security Lead köteles a jogosulatlan megfigyelőrendszer-hozzáférést a megerősítéstől számított egy munkanapon belül felfüggeszteni, és az intézkedést a REG10-ben vagy a REG12-ben rögzíteni.

10.3 [All] Top Management köteles ismétlődő vagy lényeges szabályzatsértések esetén 10 munkanapon belül kijelölni a helyesbítő intézkedés felelősét a REG12-ben.

10.4 [Conditional] The Incident Response Coordinator köteles a megfigyelési PII feltételezett jogosulatlan közlése, elvesztése vagy kompromittálódása esetén megindítani a PII-incidens munkafolyamatot a REG10-ben.

11. Felülvizsgálat és karbantartás

11.1 [All] The Privacy Lead / PIMS Manager köteles legalább évente felülvizsgálni a jelen szabályzatot és a kapcsolódó megfigyelési bizonyítékokat a REG12-ben.

11.2 [Controller] The Process Owner / Business Owner köteles legalább évente újra megerősíteni minden aktív megfigyelési célt, tájékoztatót, helyszíni hatókört és megőrzési bejegyzést a REG02-ben és a REG07-ben.

11.3 [Both] The System Owner / Application Owner köteles legalább évente és lényeges rendszerváltozás után újra megerősíteni a megfigyelő rendszer hozzáférési, naplózási, törlési és exportálási kontrolljait a REG12-ben.

11.4 [Conditional] The Vendor / Procurement Owner köteles legalább évente és a szerződés megújítása előtt újra megerősíteni a kiszervezett megfigyelési szolgáltatói bizonyítékokat a REG08-ban.

11.5 [All] The Privacy Lead / PIMS Manager köteles a jóváhagyott szabályzatmódosításokat követő 30 naptári napon belül frissíteni a kapcsolódó REG02, REG04, REG07, REG08, REG10 vagy REG12 bizonyítékokat.

12. Kapcsolódó szabályzatok

12.1 PII02 - Adatvédelmi szerepkörök, felelősségek és elszámoltathatósági szabályzat

12.2 PII03 - PII adatkezelési nyilvántartási és jogalap-szabályzat

12.3 PII04 - Adatvédelmi tájékoztatási és átláthatósági szabályzat

12.4 PII06 - PII-alanyi jogok kezelésére vonatkozó szabályzat

12.5 PII07 - Adatvédelmi kockázatértékelési és DPIA-szabályzat

12.6 PII08 - Beépített és alapértelmezett adatvédelmi szabályzat

12.7 PII09 - PII gyűjtésére, felhasználására, közlésére és megosztására vonatkozó szabályzat

12.8 PII10 - PII megőrzési, törlési és megsemmisítési szabályzat

12.9 PII12 - Adatfeldolgozói, al-adatfeldolgozói és harmadik fél adatvédelmi menedzsment szabályzat

12.10 PII13 - Nemzetközi PII-továbbítási szabályzat

12.11 PII14 - PII-biztonsági és hozzáférés-szabályozási szabályzat

12.12 PII15 - PII-incidens- és adatsértés-kezelési szabályzat

12.13 PII17 - PIMS dokumentált információs és bizonyítékkezelési szabályzat

12.14 PII18 - PIMS nyomon követési, audit- és fejlesztési szabályzat

12.15 PII19 - Munkavállalói adatvédelmi szabályzat

12.16 PII21 - AI- és automatizált döntéshozatali adatvédelmi szabályzat

12.17 PII23 - Felhőalapú PII-adatfeldolgozói szabályzat

13. Hivatkozott szabványok és keretrendszerek

13.1 Ez a szabályzat az alábbi szabványokhoz és jogszabályokhoz van hozzárendelve. A megfeleltetés bemutatja, hogyan támogatja a szabályzat a hivatkozott követelményeket, és azonosítja az azokat végrehajtó vagy támogató belső pontokat.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Hozzárendelve a dokumentált megfigyelési bizonyítékokhoz, a működéstervezéshez, az aktiválási kontrollokhoz, a cél nyilvántartásaihoz, a tájékoztató összekapcsolásához, a hozzáférési konfigurációhoz, a megőrzési konfigurációhoz, valamint a CCTV- és fizikai megfigyelési tevékenységek változáskezeléséhez. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Hozzárendelve a megfigyelési kontrollok méréséhez, a szolgáltatói felülvizsgálathoz, a hozzáférés-felülvizsgálathoz, az auditmegállapításokhoz, a meg nem felelésekhez, a helyesbítő intézkedésekhez, a lejárt intézkedések eszkalációjához és a fejlesztési bizonyítékokhoz. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Hozzárendelve az adatkezelői megfigyelési cél meghatározásához, a jogalap dokumentálásához, az adatvédelmi kockázati kiváltó okokra vonatkozó döntésekhez és a megfigyelési adatkezelési tevékenységek REG02-ben és REG04-ben vezetett nyilvántartásaihoz. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Hozzárendelve a kiszervezett megfigyelési szolgáltatói feladatmegosztáshoz, a közös megfigyelési felelősségek megosztásához, valamint az adatfeldolgozói vagy közös adatkezelői bizonyítékokhoz a REG08-ban. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Hozzárendelve a megfigyeléssel kapcsolatos PII-alanyi kötelezettségekhez, a kérelmek továbbításához, a kérelmek értékeléséhez szükséges megőrzéshez és a jogok támogatására vonatkozó irányítási bizonyítékokhoz. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Hozzárendelve a megfigyelési adatgyűjtés korlátozásához, az adatkezelési határokhoz, az adattakarékossághoz, a megőrzési időtartamokhoz, a törléshez, a felülíráshoz, a megőrzési zárolásokhoz és a kivont másolatok kontrolljához. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Hozzárendelve a külső adatközlések nyilvántartásaihoz, az adatközlési kérelmek kezeléséhez, az adatközlés előtti adattakarékossághoz, valamint a megfigyelési PII-t érintő incidenshez kapcsolódó adatközlésekhez. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Hozzárendelve az adatfeldolgozói ügyfélutasításokhoz, az engedélyezett adatkezelési határokhoz, a tájékoztatási támogatáshoz, a megőrzési és törlési utasításokhoz, a joggyakorlási támogatáshoz és a kiszervezett megfigyelési szolgáltatások adatfeldolgozói nyilvántartásaihoz. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Hozzárendelve az ügyfél kötelezettségeinek adatfeldolgozói támogatásához, az adatközlési engedélyezéshez, az adatközlési nyilvántartásokhoz, az adatközlési kérelmekről szóló értesítéshez és a megfigyelési PII-re vonatkozó, jogilag kötelező adatközlés kezeléséhez. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Hozzárendelve a megfigyelési nyilvántartások védelméhez, a korlátozott hozzáféréshez, az emelt jogosultságú hozzáférés felülvizsgálatához, a hozzáférési naplózáshoz, a jogosulatlan hozzáférés elszigeteléséhez és a megfigyelő rendszerek naplózási bizonyítékaihoz. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Hozzárendelve a jogszerűséghez, tisztességességhez, átláthatósághoz, célhoz kötöttséghez, adattakarékossághoz, tárolási korlátozáshoz és a megfigyelési tevékenységek elszámoltathatósági bizonyítékaihoz. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Hozzárendelve a CCTV, a látogatók megfigyelése, a fizikai hozzáférési naplók és más fizikai megfigyelési tevékenységek jogalapjának dokumentálásához. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Hozzárendelve az átlátható megfigyelési tájékoztatókhoz, a jelzések bizonyítékaihoz, a tájékoztatók adatkezelési célokhoz kapcsolásához, az adatfeldolgozói tájékoztatási támogatási információkhoz és az alternatív átláthatósági intézkedésekhez. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Hozzárendelve a hozzáféréshez, helyesbítéshez, törléshez, korlátozáshoz, tiltakozáshoz, a kérelmek továbbításához, a kérelmek értékeléséhez szükséges megőrzéshez és a megfigyeléssel kapcsolatos ügyféltámogatáshoz. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Hozzárendelve az adatkezelői irányításhoz, a közös adatkezelői feladatmegosztáshoz, az adatfeldolgozói irányításhoz, az adatkezelési nyilvántartásokhoz, a megfigyelő rendszerek biztonságához, az adatvédelmi kockázati felülvizsgálathoz, a DPIA kiváltó okokhoz és az adatvédelmi tanácsadáshoz. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Hozzárendelve a cél meghatározásához, a gyűjtés korlátozásához, az adattakarékossághoz, a felhasználás korlátozásához, a megőrzési korlátozáshoz és a megfigyelési PII adatközlési korlátozásához. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Hozzárendelve az átláthatósághoz, az egyéni részvételhez, az elszámoltathatósághoz, az információbiztonsághoz, a megfelelőségi felülvizsgálathoz, a hozzáférés-felülvizsgálathoz, a joggyakorlási kérelmek továbbításához, az incidenseszkalációhoz és a helyesbítő intézkedések bizonyítékaihoz. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Hozzárendelve a szisztematikus, nem nyilvánvaló, hang-, biometrikus, analitikával támogatott, érzékeny helyszínhez kapcsolódó, kiszolgáltatott

személyeket érintő vagy más magasabb kockázatú fizikai megfigyelés adatvédelmi kockázati és DPIA kiváltó okainak előszűréséhez. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Hozzárendelve a célra, gyűjtésre, adattakarékosságra, megőrzésre, adatközlésre és a PII-alanyok megfigyelési környezetben való részvételére vonatkozó PII-védelmi kontrollokhoz. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Hozzárendelve a megfigyelő rendszerek hozzáférése és a fizikai hozzáférés-szabályozási nyilvántartások szempontjából releváns hozzáférés-kiosztáshoz, információ-hozzáférési korlátozáshoz és fizikai belépési kontrollokhoz. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Hozzárendelve a PII adatvédelméhez és védelméhez, a fizikai belépéshez, a fizikai biztonsági megfigyeléshez, az emelt jogosultságú hozzáféréshez, az információ-hozzáférési korlátozáshoz, valamint a CCTV- és fizikai megfigyelő rendszerek naplózási kontrolljaihoz. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].