| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Wprowadź tutaj nazwę zarejestrowanej osoby prawnej | | | | | | | |
| Numer dokumentu:<br>PII24 | | | | | Tytuł dokumentu:<br>**Polityka prywatności dotycząca CCTV i monitoringu fizycznego** | | | | | | | |
| Wersja:<br>1.0 | | Data wejścia w życie:<br>01.01.2025 | | | Właściciel dokumentu: | | | | | | | |
| X | Polityka | | Standard | | Procedura | | Formularz | | Rejestr | | Inne | |

| **Historia zmian** | | | | |
|---|---|---|---|---|
| **Numer zmiany** | **Data zmiany** | **Zmiany** | **Przegląd wykonał** | **Właściciel procesu** |
| | | | | |
| | | | | |

| **Zatwierdzenia** | | | |
|---|---|---|---|
| **Imię i nazwisko** | **Stanowisko** | **Data** | **Podpis** |
| | | | |
| | | | |

## Dostosowanie do norm i regulacji

| Norma / regulacja | Klauzula / środek kontrolny / artykuł | Stosowalność | Typ pokrycia | Komentarz |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Clause 7.5; Clause 8.1 | Both | Primary | Udokumentowane i operacyjne środki kontrolne |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Monitorowanie i działania korygujące |
| 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 | Cel, podstawa prawna, wyzwalacz ryzyka i zapisy |
| ISO/IEC 27701:2025 | Annex A.1.2.7; Annex A.1.2.8 | Controller | Supporting | Podział odpowiedzialności z podmiotem przetwarzającym i współadministratorem |
| 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 | Obowiązki wobec osób, których dane dotyczą, oraz wnioski |
| 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 | Gromadzenie, przetwarzanie, minimalizacja, okres przechowywania i utylizacja |
| ISO/IEC 27701:2025 | Annex A.1.5.4; Annex A.1.5.5 | Controller | Primary | Zapisy ujawnień i wnioski |
| 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 | Umowy z podmiotem przetwarzającym, polecenia, wsparcie i zapisy |
| 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 | Prawa i wsparcie ujawnień po stronie podmiotu przetwarzającego |
| ISO/IEC 27701:2025 | Annex A.3.14; Annex A.3.25 | Both | Supporting | Ochrona zapisów i rejestrowanie |
| GDPR | Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2) | Controller | Primary | Zasady i rozliczalność |
| GDPR | Article 6 | Controller | Primary | Podstawa prawna |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 12; Article 13; Article 14 | Controller | Primary | Przejrzystość i klauzule informacyjne |
| GDPR | Article 15; Article 16; Article 17; Article 18; Article 21 | Controller | Supporting | Wnioski o realizację praw |
| GDPR | Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39 | Both | Supporting | Zarządzanie, podmioty przetwarzające, zapisy, bezpieczeństwo, DPIA i doradztwo |
| ISO/IEC 29100:2020 | Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6 | Controller | Supporting | Cel, gromadzenie, minimalizacja, okres przechowywania i ujawnianie |
| ISO/IEC 29100:2020 | Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12 | Both | Supporting | Przejrzystość, uczestnictwo, rozliczalność, bezpieczeństwo i zgodność |
| ISO/IEC 29134:2020 | Clause 5.1; Clause 6.2 | Controller | Supporting | Ryzyko dla prywatności i wyzwalacze DPIA |
| ISO/IEC 29151:2022 | Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10 | Both | Supporting | Środki kontroli prywatności służące ochronie PII |
| ISO/IEC 29151:2022 | Clause 9.2.3; Clause 9.4.2; Clause 11.1.3 | Both | Supporting | Kontrole dostępu i wejścia fizycznego |
| ISO/IEC 27002:2022 | Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 | Both | Supporting | PII, monitoring fizyczny, ograniczenie dostępu i rejestrowanie |

## 1. Zakres

1.1 Niniejsza polityka ma zastosowanie do CCTV, monitoringu wizyjnego, monitoringu odwiedzających, dzienników kontroli dostępu fizycznego, zapisów monitoringu prowadzonego przez ochronę, systemów monitorowania obiektów oraz powiązanych działań monitoringu fizycznego, które gromadzą lub w inny sposób przetwarzają PII.

1.2 Niniejsza polityka ma zastosowanie do organizacji działających jako administratorzy PII w odniesieniu do własnych obiektów i działań monitoringu fizycznego.

1.3 Niniejsza polityka ma również zastosowanie do działań wsparcia realizowanych przez podmiot przetwarzający lub podwykonawcę przetwarzania, gdy organizacja obsługuje, hostuje, przegląda, przechowuje, ujawnia, usuwa lub w inny sposób przetwarza nagrania z monitoringu, dane odwiedzających lub dzienniki dostępu fizycznego w imieniu klienta.

1.4 Niniejsza polityka obejmuje definiowanie celu monitoringu, zatwierdzanie, klauzule informacyjne i oznakowanie, ograniczenia dostępu, ujawnianie, okres przechowywania, usuwanie, outsourcing, eskalację incydentów, kierowanie wniosków o realizację praw, przegląd oraz zarządzanie dowodami.

1.5 Niniejsza polityka nie stanowi porady z zakresu prawa pracy, komentarza prawnego dotyczącego rady pracowników, procedury organów ścigania ani dedykowanego rejestru CCTV.

1.6 Dowody specyficzne dla monitoringu są utrzymywane w kanonicznych obiektach dowodowych PIMS wskazanych w niniejszej polityce.

## 2. Cel

2.1 Celem niniejszej polityki jest ustanowienie środków kontroli prywatności dla CCTV i monitoringu fizycznego, tak aby działania monitoringu miały określony cel, były przejrzyste, proporcjonalne, objęte kontrolą dostępu, przechowywane przez zdefiniowane okresy, ujawniane wyłącznie zatwierdzonymi kanałami oraz wspierane audytowalnymi dowodami PIMS.

2.2 Niniejsza polityka wspiera spójne postępowanie z nagraniami z monitoringu, zapisami odwiedzających, dziennikami dostępu fizycznego oraz powiązanymi PII z monitoringu bez tworzenia dodatkowych rejestrów, komitetów, pulpitów ani niekanonicznych ról.

## 3. Cele

### 3.1 Celami niniejszej polityki są:

3.1.1 zdefiniowanie celów monitoringu i zakresu przetwarzania przed rozpoczęciem monitoringu;

3.1.2 dokumentowanie działań CCTV, dostępu fizycznego, monitoringu odwiedzających i monitoringu fizycznego w REG02;

3.1.3 identyfikowanie działań monitoringu wymagających przeglądu ryzyka dla prywatności lub oceny potrzeby przeprowadzenia DPIA w REG04;

3.1.4 utrzymywanie dowodów przejrzystych klauzul informacyjnych i oznakowania w REG07;

3.1.5 ograniczenie dostępu, przeglądania, eksportu, ujawniania i okresu przechowywania PII z monitoringu;

3.1.6 kierowanie wniosków osób, których dane dotyczą, przez REG06;

3.1.7 zarządzanie zewnętrznymi dostawcami monitoringu i dowodami udostępniania danych przez REG08;

3.1.8 eskalowanie podejrzewanych incydentów PII związanych z monitoringiem przez REG10;

3.1.9 rejestrowanie przeglądów, wyjątków, niezgodności, działań korygujących, ustaleń z audytu i usprawnień w REG12.

## 4. Postanowienia polityki

### 4.1 Inwentarz monitoringu, cel i zatwierdzenie

4.1.1 [Controller] The Process Owner / Business Owner musi zarejestrować każde działanie CCTV, monitoringu odwiedzających, dziennik kontroli dostępu fizycznego lub działanie monitoringu fizycznego w REG02 przed jego rozpoczęciem.

4.1.2 [Controller] The Privacy Lead / PIMS Manager musi zwalidować wpis w REG02 pod kątem celu, podstawy prawnej, monitorowanej lokalizacji, kategorii PII, kategorii osób, których dane dotyczą, okresu przechowywania, klauzuli informacyjnej, dostępu i pól ujawniania przed aktywacją nowego lub istotnie zmienionego działania monitoringu.

4.1.3 [Controller] The Process Owner / Business Owner musi zarejestrować zatwierdzone strefy monitorowane, strefy wyłączone oraz granice gromadzenia danych w REG02 przed uruchomieniem kamer, czujników, rejestrów odwiedzających lub rejestrowania kontroli dostępu.

4.1.4 [Conditional] The Process Owner / Business Owner musi uzyskać decyzję dotyczącą ryzyka dla prywatności w REG04 przed aktywacją monitoringu obejmującego systematyczne monitorowanie, rejestrację dźwięku, identyfikację biometryczną, wykrywanie z użyciem analityki, lokalizacje wrażliwe, osoby podatne na zagrożenia lub monitoring nieoczywisty.

4.1.5 [Joint Controller] The Privacy Lead / PIMS Manager musi zarejestrować podział odpowiedzialności za wspólny monitoring w REG08 przed rozpoczęciem monitoringu współdzielonego z wynajmującym, partnerem ds. obsługi obiektów, klientem lub innym współadministratorem.

4.1.6 [Processor] The Privacy Lead / PIMS Manager musi zarejestrować polecenia klienta dotyczące monitoringu oraz dozwolone granice przetwarzania w REG08 przed przetwarzaniem nagrań z monitoringu, zapisów odwiedzających lub dzienników dostępu fizycznego w imieniu klienta.

### 4.2 Klauzule informacyjne i przejrzystość

4.2.1 [Controller] The Process Owner / Business Owner musi zapewnić, aby dowody oznakowania monitoringu lub równoważnej klauzuli informacyjnej just-in-time zostały zarejestrowane w REG07 przed udostępnieniem monitorowanych obszarów osobom, których dane dotyczą.

4.2.2 [Controller] The Privacy Lead / PIMS Manager musi powiązać każdą klauzulę informacyjną dotyczącą monitoringu w REG07 z odpowiadającym jej celem przetwarzania w REG02 przed publikacją lub istotną zmianą.

4.2.3 [Processor] The Privacy Lead / PIMS Manager musi przekazać informacje wspierające klauzulę informacyjną dotyczącą monitoringu w REG08, gdy organizacja świadczy usługi monitoringu zgodnie z poleceniami klienta.

4.2.4 [Conditional] The Process Owner / Business Owner musi zarejestrować alternatywne środki przejrzystości w REG07 i REG04 przed aktywacją monitoringu nieoczywistego lub awaryjnego.

[ ... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ... ]

## 9. Wyjątki

9.1 [All] The Privacy Lead / PIMS Manager musi zarejestrować każdy wyjątek od niniejszej polityki w REG12 przed jego zastosowaniem.

9.2 [Conditional] The Data Protection Officer / Privacy Advisor musi udokumentować doradztwo dotyczące prywatności w REG04 lub REG12 przed zatwierdzeniem wyjątków obejmujących

monitoring nieoczywisty, rejestrację dźwięku, identyfikację biometryczną, monitoring z użyciem analityki lub wrażliwe lokalizacje monitoringu.

9.3 [All] Top Management musi zatwierdzić wyjątki przekraczające 90 dni w REG12 przed przedłużeniem poza początkowy okres wyjątku.

9.4 [All] The Privacy Lead / PIMS Manager musi przeglądać otwarte wyjątki dotyczące monitoringu w REG12 co najmniej raz w miesiącu do czasu zamknięcia.

## 10. Egzekwowanie

10.1 [All] The Privacy Lead / PIMS Manager musi rejestrować nieskuteczności środków kontrolnych monitoringu jako niezgodności w REG12 w ciągu pięciu dni roboczych od potwierdzenia.

10.2 [Both] The Information Security Lead musi zawiesić nieuprawniony dostęp do systemu monitoringu w ciągu jednego dnia roboczego od potwierdzenia oraz zarejestrować działanie w REG10 lub REG12.

10.3 [All] Top Management musi przypisać właściciela działania korygującego w REG12 w ciągu 10 dni roboczych w przypadku powtarzających się lub istotnych naruszeń polityki.

10.4 [Conditional] The Incident Response Coordinator musi zainicjować proces obsługi incydentu PII w REG10 po podejrzeniu nieuprawnionego ujawnienia, utraty lub naruszenia PII z monitoringu.

## 11. Przegląd i utrzymanie

11.1 [All] The Privacy Lead / PIMS Manager musi dokonywać przeglądu niniejszej polityki i powiązanych dowodów monitoringu w REG12 co najmniej raz w roku.

11.2 [Controller] The Process Owner / Business Owner musi ponownie zwalidować każdy aktywny cel monitoringu, klauzulę informacyjną, zakres lokalizacji i wpis okresu przechowywania w REG02 i REG07 co najmniej raz w roku.

11.3 [Both] The System Owner / Application Owner musi ponownie zwalidować dostęp do systemu monitoringu, rejestrowanie, usuwanie i środki kontroli eksportu w REG12 co najmniej raz w roku oraz po istotnej zmianie systemu.

11.4 [Conditional] The Vendor / Procurement Owner musi ponownie zwalidować dowody dotyczące zewnętrznego dostawcy monitoringu w REG08 co najmniej raz w roku oraz przed odnowieniem umowy.

11.5 [All] The Privacy Lead / PIMS Manager musi zaktualizować powiązane dowody REG02, REG04, REG07, REG08, REG10 lub REG12 w ciągu 30 dni kalendarzowych od zatwierdzonych zmian polityki.

## 12. Powiązane polityki

12.1 PII02 - Polityka ról, odpowiedzialności i rozliczalności w zakresie prywatności

12.2 PII03 - Polityka inwentarza przetwarzania PII i podstaw prawnych

12.3 PII04 - Polityka klauzul informacyjnych i przejrzystości

12.4 PII06 - Polityka zarządzania prawami osób, których dane dotyczą

12.5 PII07 - Polityka oceny ryzyka dla prywatności i DPIA

12.6 PII08 - Polityka privacy by design i privacy by default

12.7 PII09 - Polityka gromadzenia, wykorzystywania, ujawniania i udostępniania PII

12.8 PII10 - Polityka przechowywania, usuwania i utylizacji PII

12.9 PII12 - Polityka zarządzania prywatnością podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich

12.10 PII13 - Polityka międzynarodowego transferu PII

12.11 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.12 PII15 - Polityka zarządzania incydentami i naruszeniami PII

12.13 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS

12.14 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

12.15 PII19 - Polityka prywatności pracowników

12.16 PII21 - Polityka prywatności dotycząca AI i zautomatyzowanego podejmowania decyzji

12.17 PII23 - Polityka podmiotu przetwarzającego PII w chmurze obliczeniowej

## 13. Normy i ramy odniesienia

13.1 Niniejsza polityka jest zmapowana do następujących norm i regulacji. Mapowanie wyjaśnia, w jaki sposób polityka wspiera wskazane wymagania, oraz identyfikuje wewnętrzne klauzule, które je wdrażają lub wspierają.

### 13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Zmapowano do udokumentowanych dowodów monitoringu, planowania operacyjnego, środków kontroli aktywacji, zapisów celu, powiązania z klauzulą informacyjną, konfiguracji dostępu, konfiguracji okresu przechowywania oraz kontroli zmian dla działań CCTV i monitoringu fizycznego. 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** - Zmapowano do pomiaru środków kontrolnych monitoringu, przeglądu dostawców, przeglądu dostępu, ustaleń z audytu, niezgodności, działań korygujących, eskalacji zaległych działań oraz dowodów doskonalenia. 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** - Zmapowano do definiowania celu monitoringu przez administratora, dokumentowania podstawy prawnej, decyzji dotyczących wyzwalaczy ryzyka dla prywatności oraz zapisów działań przetwarzania związanych z monitoringiem w REG02 i REG04. 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** - Zmapowano do podziału odpowiedzialności dostawcy monitoringu realizowanego w outsourcingu, podziału odpowiedzialności za wspólny monitoring oraz dowodów dotyczących podmiotu przetwarzającego lub współadministratora w REG08. 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** - Zmapowano do obowiązków wobec osób, których dane dotyczą, związanych z monitoringiem, kierowania wniosków, zachowania zapisów potrzebnych do oceny wniosków oraz dowodów zarządzania wspierających realizację praw. 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** - Zmapowano do ograniczania gromadzenia w ramach monitoringu, granic przetwarzania, minimalizacji, okresów przechowywania, usuwania, nadpisywania, wstrzymań okresu przechowywania oraz kontroli wyodrębnionych kopii. 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** - Zmapowano do zapisów ujawnień zewnętrznych, obsługi wniosków o ujawnienie, minimalizacji przed ujawnieniem oraz ujawnień powiązanych z incydentami obejmującymi PII z monitoringu. 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** - Zmapowano do poleceń klienta dla podmiotu przetwarzającego, dozwolonych granic przetwarzania, wsparcia klauzul informacyjnych, poleceń dotyczących okresu przechowywania i usuwania, pomocy przy

realizacji praw oraz zapisów podmiotu przetwarzającego dla usług monitoringu realizowanych w outsourcingu. 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** - Zmapowano do wsparcia podmiotu przetwarzającego dla obowiązków klienta, autoryzacji ujawnienia, zapisów ujawnienia, powiadamiania o wnioskach o ujawnienie oraz obsługi prawnie wiążących ujawnień dotyczących PII z monitoringu. 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** - Zmapowano do ochrony zapisów monitoringu, ograniczonego dostępu, przeglądu dostępu uprzywilejowanego, rejestrowania dostępu, powstrzymywania nieuprawnionego dostępu oraz dowodów rejestrowania dla systemów monitoringu. 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)** - Zmapowano do zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, ograniczenia przechowywania oraz dowodów rozliczalności dla działań monitoringu. 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 - Zmapowano do dokumentowania podstawy prawnej dla CCTV, monitoringu odwiedzających, dzienników dostępu fizycznego i innych działań monitoringu fizycznego. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Zmapowano do przejrzystych klauzul informacyjnych dotyczących monitoringu, dowodów oznakowania, powiązania klauzul informacyjnych z celami przetwarzania, informacji wspierających klauzule informacyjne po stronie podmiotu przetwarzającego oraz alternatywnych środków przejrzystości. 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** - Zmapowano do dostępu, sprostowania, usunięcia, ograniczenia, sprzeciwu, kierowania wniosków, zachowania zapisów potrzebnych do oceny wniosków oraz pomocy klientowi związanej z monitoringiem. 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** - Zmapowano do zarządzania po stronie administratora, podziału odpowiedzialności współadministratorów, zarządzania podmiotami przetwarzającymi, rejestrów przetwarzania, bezpieczeństwa systemów monitoringu, przeglądu ryzyka dla prywatności, wyzwalaczy DPIA oraz doradztwa dotyczącego prywatności. 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** - Zmapowano do określenia celu, ograniczenia gromadzenia, minimalizacji danych, ograniczenia wykorzystania, ograniczenia przechowywania oraz ograniczenia ujawniania dla PII z monitoringu. 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** - Zmapowano do przejrzystości, udziału osób fizycznych, rozliczalności, bezpieczeństwa informacji, przeglądu zgodności, przeglądu dostępu, kierowania wniosków o realizację praw, eskalacji incydentów oraz dowodów działań korygujących. 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** - Zmapowano do ryzyka dla prywatności i oceny wyzwalaczy DPIA dla systematycznego, nieoczywistego, dźwiękowego, biometrycznego, realizowanego z użyciem analityki, prowadzonego w wrażliwych lokalizacjach, obejmującego osoby podatne na

zagrożenia lub innego monitoringu fizycznego wyższego ryzyka. 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** - Zmapowano do środków kontroli ochrony PII dotyczących celu, gromadzenia, minimalizacji, okresu przechowywania, ujawniania oraz uczestnictwa osób, których dane dotyczą, w kontekstach monitoringu. 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** - Zmapowano do nadawania dostępu, ograniczenia dostępu do informacji oraz kontroli wejścia fizycznego istotnych dla dostępu do systemów monitoringu i zapisów kontroli dostępu fizycznego. 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 - Zmapowano do prywatności i ochrony PII, wejścia fizycznego, monitoringu bezpieczeństwa fizycznego, dostępu uprzywilejowanego, ograniczenia dostępu do informacji oraz środków kontroli rejestrowania dla systemów CCTV i monitoringu fizycznego. 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].