					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII24					Заглавие на документа: **Политика за поверителност при видеонаблюдение (CCTV) и физическо наблюдение**							
Версия: 1.0		Дата на влизане в сила: 01.01.2025			Собственик на документа:							
X	Политика		Стандарт		Процедура		Формуляр		Регистър		Друго	

История на редакциите				
Номер на редакцията	**Дата на редакцията**	**Промени**	**Прегледано от**	**Собственик на процеса**

Одобрения			
Име	**Длъжност**	**Дата**	**Подпис**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/контрол/член	Приложимост	Тип покритие	Коментар
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Документирани и оперативни контроли
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Мониторинг и коригиращо действие
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	Цел, правно основание, рисков критерий за задействане и записи
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Разпределяне на отговорности за обработващ лични данни и съвместен администратор
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	Задължения и искания на субекта на данни
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	Събиране, обработване, минимизиране, съхранение и унищожаване
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Записи и искания за разкриване
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	Споразумения с обработващи лични данни, нареждания, съдействие и записи
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	Права на обработващия лични данни и съдействие при разкриване
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Защита на записи и журнализиране
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Принципи и отчетност

GDPR	Article 6	Controller	Primary	Правно основание
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Прозрачност и уведомления
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Искания за упражняване на права
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Управление, обработващи лични данни, записи, сигурност, DPIA и консултиране
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Цел, събиране, минимизиране, съхранение и разкриване
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Прозрачност, участие, отчетност, сигурност и съответствие
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Риск за поверителността и критерии за задействане на DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Контроли за защита на PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Контроли за достъп и физическо влизане
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, физическо наблюдение, ограничаване на достъпа и журнализиране

1. Обхват

1.1 Тази политика се прилага за видеонаблюдение (CCTV), видеомониторинг, наблюдение на посетители, журнали за контрол на физическия достъп, записи от наблюдение, извършвано от охрана, системи за наблюдение на помещения и свързани дейности по физическо наблюдение, които събират или по друг начин обработват PII.

1.2 Тази политика се прилага за организации, действащи като администратори на PII за собствените си помещения и дейности по физическо наблюдение. Тя се прилага също за дейности за поддръжка като обработващ лични данни или подизпълнител по обработване, когато организацията управлява, хоства, преглежда, съхранява, разкрива, изтрива или по друг начин обработва записи от видеонаблюдение, данни за посетители или журнали за физически достъп от името на клиент.

1.3 Тази политика обхваща определянето на целите на наблюдението, одобряването, уведомленията и информационните табели, ограниченията за достъп, разкриването, съхранението, изтриването, външното възлагане, ескалацията на инциденти, маршрутизирането на искания за упражняване на права, прегледа и управлението на доказателства.

1.4 Тази политика не предоставя правни съвети по трудово право, правни коментари относно работнически съвети, процедури на правоохранителни органи или отделен регистър за видеонаблюдение (CCTV). Доказателствата, специфични за наблюдението, се поддържат в каноничните доказателствени обекти на PIMS, посочени в тази политика.

2. Цел

2.1 Целта на тази политика е да установи контроли за поверителност при видеонаблюдение (CCTV) и физическо наблюдение, така че дейностите по наблюдение да имат определена цел, да са прозрачни, пропорционални, с контролиран достъп, да се съхраняват за определени срокове, да се разкриват само чрез одобрени канали и да се подкрепят с одитируеми доказателства в PIMS.

2.2 Тази политика подпомага последователното обработване на записи от видеонаблюдение, записи за посетители, журнали за физически достъп и свързаната PII от наблюдение, без да създава допълнителни регистри, комитети, информационни табла или неканонични роли.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 определя целите на наблюдението и обхвата на обработването преди започване на наблюдението;

3.1.2 документира дейностите по видеонаблюдение (CCTV), физически достъп, наблюдение на посетители и физическо наблюдение в REG02;

3.1.3 идентифицира дейности по наблюдение, които изискват преглед на риска за поверителността или проверка за необходимост от DPIA в REG04;

3.1.4 поддържа доказателства за прозрачни уведомления и информационни табели в REG07;

3.1.5 ограничава достъпа, преглеждането, експортирането, разкриването и съхранението на PII от наблюдение;

3.1.6 маршрутизира исканията на субекти на данни чрез REG06;

3.1.7 управлява външно възложени доставчици на наблюдение и доказателства за споделяне на данни чрез REG08;

3.1.8 ескалира предполагаеми инциденти с PII, свързани с наблюдение, чрез REG10;

3.1.9 записва прегледи, изключения, несъответствия, коригиращи действия, одитни констатации и подобрения в REG12.

4. Декларации на политиката

4.1 Инвентар на наблюдението, цел и одобрение

4.1.1 [Controller] Process Owner / Business Owner MUST запише всяка дейност по видеонаблюдение (CCTV), наблюдение на посетители, журнал за контрол на физическия достъп или физическо наблюдение в REG02, преди дейността да започне.

4.1.2 [Controller] Privacy Lead / PIMS Manager MUST валидира записа в REG02 по отношение на цел, правно основание, наблюдавано местоположение, категории PII, категории субекти на данни, съхранение, уведомление, достъп и полета за разкриване преди активиране на нова или съществено променена дейност по наблюдение.

4.1.3 [Controller] Process Owner / Business Owner MUST запише одобрените наблюдавани зони, изключените зони и границите на събиране в REG02, преди камерите, сензорите, журналите за посетители или журнализирането на контрола на достъп да бъдат активирани.

4.1.4 [Conditional] Process Owner / Business Owner MUST получи решение за риска за поверителността в REG04 преди активиране на наблюдение, което включва систематично наблюдение, аудиозапис, биометрична идентификация, откриване чрез аналитични функции, чувствителни местоположения, уязвими лица или неочевидно наблюдение.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager MUST запише разпределението на отговорностите за съвместно наблюдение в REG08, преди да започне споделено наблюдение с наемодател, партньор по управление на сгради, клиент или друг съвместен администратор.

4.1.6 [Processor] Privacy Lead / PIMS Manager MUST запише нарежданията на клиента за наблюдение и разрешените граници на обработване в REG08, преди да обработва записи от видеонаблюдение, записи за посетители или журнали за физически достъп от името на клиент.

4.2 Уведомление и прозрачност

4.2.1 [Controller] Process Owner / Business Owner MUST гарантира, че доказателства за информационни табели за наблюдение или еквивалентно уведомление „точно навреме“ са записани в REG07, преди наблюдаваните зони да бъдат отворени за субекти на данни.

4.2.2 [Controller] Privacy Lead / PIMS Manager MUST свърже всяко уведомление за наблюдение в REG07 със съответната цел на обработването в REG02 преди публикуване или съществена промяна.

4.2.3 [Processor] Privacy Lead / PIMS Manager MUST предостави поддържаща информация за уведомлението относно наблюдението в REG08, когато организацията извършва услуги по наблюдение по нареждания на клиента.

4.2.4 [Conditional] Process Owner / Business Owner MUST запише алтернативни мерки за прозрачност в REG07 и REG04, преди да бъде активирано неочевидно или аварийно наблюдение.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Изключения

9.1 [All] Privacy Lead / PIMS Manager MUST записва всяко изключение от тази политика в REG12 преди използването на изключението.

9.2 [Conditional] Data Protection Officer / Privacy Advisor MUST документира съвети относно поверителността в REG04 или REG12 преди одобряване на изключения, включващи неочевидно наблюдение, аудиозапис, биометрична идентификация, наблюдение чрез аналитични функции или чувствителни местоположения за наблюдение.

9.3 [All] Top Management MUST одобрява изключения, надвишаващи 90 дни, в REG12 преди удължаване извън първоначалния период на изключението.

9.4 [All] Privacy Lead / PIMS Manager MUST преглежда отворените изключения, свързани с наблюдение, в REG12 най-малко ежемесечно до приключване.

10. Прилагане на политиката

10.1 [All] Privacy Lead / PIMS Manager MUST записва откази на контроли за наблюдение като несъответствия в REG12 в рамките на пет работни дни след потвърждение.

10.2 [Both] Information Security Lead MUST спре неоторизиран достъп до система за наблюдение в рамките на един работен ден след потвърждение и да запише действието в REG10 или REG12.

10.3 [All] Top Management MUST възлага собственост върху коригиращо действие в REG12 в рамките на 10 работни дни при повторни или съществени нарушения на политиката.

10.4 [Conditional] Incident Response Coordinator MUST инициира работния поток за инцидент с PII в REG10 при предполагаемо неоторизирано разкриване, загуба или компрометиране на PII от наблюдение.

11. Преглед и поддръжка

11.1 [All] Privacy Lead / PIMS Manager MUST преглежда тази политика и свързаните доказателства за наблюдение в REG12 най-малко ежегодно.

11.2 [Controller] Process Owner / Business Owner MUST повторно валидира всяка активна цел на наблюдение, уведомление, обхват по местоположение и запис за съхранение в REG02 и REG07 най-малко ежегодно.

11.3 [Both] System Owner / Application Owner MUST повторно валидира достъпа до системата за наблюдение, журнализирането, изтриването и контролите за експортиране в REG12 най-малко ежегодно и след съществена промяна в системата.

11.4 [Conditional] Vendor / Procurement Owner MUST повторно валидира доказателствата за външно възложен доставчик на наблюдение в REG08 най-малко ежегодно и преди подновяване на договора.

11.5 [All] Privacy Lead / PIMS Manager MUST актуализира свързаните доказателства в REG02, REG04, REG07, REG08, REG10 или REG12 в рамките на 30 календарни дни след одобрени промени в политиката.

12. Свързани политики

12.1 PII02 - Политика за роли, отговорности и отчетност във връзка с поверителността

12.2 PII03 - Политика за инвентар на обработването на PII и правно основание

12.3 PII04 - Политика за уведомление за поверителност и прозрачност

12.4 PII06 - Политика за управление на правата на субекти на данни

12.5 PII07 - Политика за оценка на риска за поверителността и DPIA

12.6 PII08 - Политика за поверителност още при проектиране и по подразбиране

12.7 PII09 - Политика за събиране, използване, разкриване и споделяне на PII

12.8 PII10 - Политика за съхранение, изтриване и унищожаване на PII

12.9 PII12 - Политика за управление на поверителността при обработващи лични данни, подизпълнители по обработване и трети страни

12.10 PII13 - Политика за международно предаване на PII

12.11 PII14 - Политика за сигурност и контрол на достъпа до PII

12.12 PII15 - Политика за управление на инциденти и нарушения на сигурността на PII

12.13 PII17 - Политика за документирана информация и управление на доказателства в PIMS

12.14 PII18 - Политика за мониторинг, одит и подобрение на PIMS

12.15 PII19 - Политика за поверителност на служителите

12.16 PII21 - Политика за поверителност при AI и автоматизирано вземане на решения

12.17 PII23 - Политика за обработващ лични данни в облачна среда

13. Референтни стандарти и рамки

13.1 Тази политика е съпоставена със следните стандарти и регулации. Съпоставянето обяснява как политиката подпомага цитираните изисквания и идентифицира вътрешните клаузи, които ги прилагат или поддържат.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Съпоставено с документирани доказателства за наблюдение, оперативно планиране, контроли за активиране, записи за целите, връзка с уведомления, конфигурация на достъпа, конфигурация на съхранението и контрол на промените за дейности по видеонаблюдение (CCTV) и физическо наблюдение. 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** - Съпоставено с измерване на контролите за наблюдение, преглед на доставчици, преглед на достъпа, одитни констатации, несъответствия, коригиращи действия, ескалация на просрочени действия и доказателства за подобрение. 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** - Съпоставено с определяне на целите на наблюдението от администратора, документиране на правното основание, решения по рискови критерии за поверителността и записи за дейности по обработване при наблюдение в REG02 и 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** - Съпоставено с разпределение на външно възложени доставчици на наблюдение, разпределение на отговорности за съвместно наблюдение и доказателства за обработващ лични данни или съвместен администратор в 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** - Съпоставено със задължения на субекти на данни, свързани с наблюдение, маршрутизиране на искания, запазване, необходимо за оценяване на искания, и управленски доказателства за подпомагане на правата. 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** - Съпоставено с ограничаване на събирането при наблюдение, граници на обработване, минимизиране, срокове за съхранение, изтриване, презаписване, задържания за съхранение и контрол на извлечени копия. 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** - Съпоставено със записи за външно разкриване, обработване на искания за разкриване, минимизиране преди разкриване и свързани с инциденти разкривания, включващи PII от наблюдение. 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** - Съпоставено с нареждания на клиента към обработващия лични данни, разрешени граници на обработване, поддръжка на уведомления, нареждания за съхранение и изтриване, съдействие при права и записи на обработващия лични данни за външно възложени услуги по наблюдение. 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** - Съпоставено с подкрепа от обработващия лични данни за задълженията на клиента, разрешение за разкриване, записи за разкриване, уведомяване за искания за разкриване и обработване на правно обвързващи разкривания за PII от наблюдение. 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** - Съпоставено със защита на записи от наблюдение, ограничен достъп, преглед на привилегирован достъп, журнализиране на достъпа, ограничаване на неоторизиран достъп и доказателства за журнализиране за системи за наблюдение. 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)** - Съпоставено със законосъобразност, добросъвестност, прозрачност, ограничаване на целите, свеждане на данните до минимум, ограничение на съхранението и доказателства за отчетност за дейностите по наблюдение. 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 - Съпоставено с документиране на правното основание за видеонаблюдение (CCTV), наблюдение на посетители, журнали за физически достъп и други дейности по физическо наблюдение. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Съпоставено с прозрачни уведомления за наблюдение, доказателства за информационни табели, връзка на уведомленията с целите на обработване, поддържаща информация за уведомления от обработващия лични данни и алтернативни мерки за прозрачност. 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** - Съпоставено с достъп, коригиране, изтриване, ограничаване, възражение, маршрутизиране на искания, запазване, необходимо за оценяване на искания, и съдействие за клиента, свързано с наблюдение. 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** - Съпоставено с управление от администратора, разпределение при съвместен администратор, управление на обработващи лични данни, записи за дейности по обработване, сигурност на системи за наблюдение, преглед на риска за поверителността, критерии за задействане на DPIA и съвети относно поверителността. 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** - Съпоставено с определяне на целта, ограничаване на събирането, минимизиране на данните, ограничаване на използването, ограничаване на съхранението и ограничаване на разкриването за PII от наблюдение. 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** - Съпоставено с прозрачност, участие на лицата, отчетност, информационна сигурност, преглед на съответствието, преглед на достъпа, маршрутизиране на права, ескалация на инциденти

и доказателства за коригиращи действия. 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** - Съпоставено с проверка за рискове за поверителността и критерии за задействане на DPIA при систематично, неочевидно, аудио, биометрично, аналитично, свързано с чувствителни местоположения, уязвими лица или друго по-високорисково физическо наблюдение. 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** - Съпоставено с контроли за защита на PII относно цел, събиране, минимизиране, съхранение, разкриване и участие на субекти на данни в контексти на наблюдение. 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** - Съпоставено с предоставяне на достъп, ограничаване на достъпа до информация и контроли за физическо влизане, относими към достъпа до системи за наблюдение и записите за контрол на физически достъп. 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 - Съпоставено с поверителност и защита на PII, физическо влизане, мониторинг на физическата сигурност, привилегирован достъп, ограничаване на достъпа до информация и контроли за журнализиране за видеонаблюдение (CCTV) и системи за физическо наблюдение. 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].