					Sem vložte název registrované právnické osoby						
Číslo dokumentu: PII24					Název dokumentu: **Politika ochrany soukromí pro kamerové systémy (CCTV) a fyzické monitorování**						
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:						
X	Politika		Standard		Postup		Formulář		Registr		Jiné

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / opatření / článek	Použitelnost	Typ pokrytí	Komentář
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentovaná a provozní opatření
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorování a nápravná opatření
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	Účel, právní základ, rizikový spouštěč a záznamy
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Přiřazení zpracovatele a společného správce
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	Povinnosti vůči subjektům PII a žádosti
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	Shromažďování, zpracování, minimalizace, uchovávání a likvidace
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Záznamy o zpřístupnění a žádosti
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	Smlouvy se zpracovateli, pokyny, podpora a záznamy
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	Práva a podpora zpřístupnění u zpracovatele
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ochrana záznamů a protokolování
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Zásady a odpovědnost
GDPR	Article 6	Controller	Primary	Právní základ
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparentnost a oznámení

GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Žádosti o uplatnění práv
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Správa a řízení, zpracovatelé, záznamy, bezpečnost, DPIA a poradenství
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Účel, shromažďování, minimalizace, uchovávání a zpřístupnění
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparentnost, účast, odpovědnost, bezpečnost a soulad
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Riziko pro soukromí a spouštěče DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Opatření ochrany soukromí pro ochranu PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Řízení přístupu a fyzického vstupu
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, fyzické monitorování, omezení přístupu a protokolování

1. Rozsah

1.1 Tato politika se vztahuje na kamerové systémy (CCTV), videomonitoring, monitorování návštěvníků, logy řízení fyzického přístupu, záznamy z monitorování prováděného ostrahou, systémy monitorování prostor a související činnosti fyzického monitorování, které shromažďují nebo jinak zpracovávají PII.

1.2 Tato politika se vztahuje na organizace jednající jako správci PII pro vlastní prostory a činnosti fyzického monitorování. Vztahuje se také na podpůrné činnosti zpracovatele nebo dílčího zpracovatele, kdy organizace provozuje, hostuje, přezkoumává, ukládá, zpřístupňuje, maže nebo jinak zpracovává kamerové záznamy, údaje návštěvníků nebo logy fyzického přístupu jménem zákazníka.

1.3 Tato politika zahrnuje vymezení účelu monitorování, schvalování, oznámení a značení, omezení přístupu, zpřístupnění, uchovávání, výmaz, outsourcing, eskalaci incidentů, směrování žádostí o uplatnění práv, přezkum a správu důkazů.

1.4 Tato politika neposkytuje pracovněprávní poradenství, právní komentář k zaměstnaneckým radám, postupy pro orgány činné v trestním řízení ani samostatný registr kamerových systémů (CCTV). Důkazy specifické pro monitorování jsou vedeny v kanonických důkazních objektech PIMS uvedených v této politice.

2. Účel

2.1 Účelem této politiky je stanovit opatření ochrany soukromí pro kamerové systémy (CCTV) a fyzické monitorování tak, aby činnosti monitorování měly jasný účel, byly transparentní, přiměřené, řízené z hlediska přístupu, uchovávané po vymezenou dobu, zpřístupňované pouze schválenými kanály a podložené auditovatelnými důkazy PIMS.

2.2 Tato politika podporuje konzistentní nakládání s kamerovými záznamy, záznamy návštěvníků, logy fyzického přístupu a souvisejícími PII z monitorování bez vytváření dalších registrů, výborů, řídicích panelů nebo nekanonických rolí.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 vymezit účely monitorování a rozsah zpracování před zahájením monitorování;

3.1.2 dokumentovat kamerové systémy (CCTV), fyzický přístup, monitorování návštěvníků a činnosti fyzického monitorování v REG02;

3.1.3 identifikovat činnosti monitorování, které vyžadují přezkum rizik pro soukromí nebo předběžné posouzení nutnosti DPIA v REG04;

3.1.4 uchovávat důkazy o transparentním oznámení a značení v REG07;

3.1.5 omezit přístup, prohlížení, export, zpřístupnění a uchovávání PII z monitorování;

3.1.6 směrovat žádosti subjektů PII prostřednictvím REG06;

3.1.7 spravovat outsourcované poskytovatele monitorování a důkazy o sdílení údajů prostřednictvím REG08;

3.1.8 eskalovat podezření na incidenty týkající se PII související s monitorováním prostřednictvím REG10;

3.1.9 zaznamenávat přezkumy, výjimky, neshody, nápravná opatření, zjištění auditu a zlepšení v REG12.

4. Prohlášení politiky

4.1 Evidence monitorování, účel a schválení

4.1.1 [Controller] Process Owner / Business Owner musí zaznamenat každou činnost kamerových systémů (CCTV), monitorování návštěvníků, logování řízení fyzického přístupu nebo fyzického monitorování v REG02 před zahájením této činnosti.

4.1.2 [Controller] Privacy Lead / PIMS Manager musí před aktivací nové nebo významně změněné činnosti monitorování ověřit záznam v REG02 z hlediska účelu, právního základu, monitorovaného místa, kategorií PII, kategorií subjektů PII, uchovávání, oznámení, přístupu a polí zpřístupnění.

4.1.3 [Controller] Process Owner / Business Owner musí v REG02 zaznamenat schválené monitorované zóny, vyloučené zóny a hranice shromažďování před zapnutím kamer, senzorů, návštěvních knih nebo logování řízení přístupu.

4.1.4 [Conditional] Process Owner / Business Owner musí před aktivací monitorování, které zahrnuje systematické monitorování, zvukový záznam, biometrickou identifikaci, detekci s analytickými funkcemi, citlivá místa, zranitelné osoby nebo nezjevné monitorování, získat rozhodnutí o riziku pro soukromí v REG04.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager musí v REG08 zaznamenat přiřazení odpovědností za společné monitorování před zahájením sdíleného monitorování s pronajímatelem, partnerem pro správu budov, zákazníkem nebo jiným společným správcem.

4.1.6 [Processor] Privacy Lead / PIMS Manager musí v REG08 zaznamenat pokyny zákazníka k monitorování a povolené hranice zpracování před zpracováním kamerových záznamů, záznamů návštěvníků nebo logů fyzického přístupu jménem zákazníka.

4.2 Oznámení a transparentnost

4.2.1 [Controller] Process Owner / Business Owner musí zajistit, aby důkazy o značení monitorování nebo rovnocenném just-in-time oznámení byly zaznamenány v REG07 před zpřístupněním monitorovaných prostor subjektům PII.

4.2.2 [Controller] Privacy Lead / PIMS Manager musí před zveřejněním nebo významnou změnou propojit každé oznámení o monitorování v REG07 s odpovídajícím účelem zpracování v REG02.

4.2.3 [Processor] Privacy Lead / PIMS Manager musí poskytnout podpůrné informace k oznámení o monitorování v REG08, pokud organizace provozuje monitorovací služby podle pokynů zákazníka.

4.2.4 [Conditional] Process Owner / Business Owner musí zaznamenat alternativní opatření transparentnosti v REG07 a REG04 před aktivací nezjevného nebo nouzového monitorování.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Výjimky

9.1 [All] Privacy Lead / PIMS Manager musí zaznamenat každou výjimku z této politiky v REG12 před jejím použitím.

9.2 [Conditional] Data Protection Officer / Privacy Advisor musí před schválením výjimek zahrnujících nezjevné monitorování, zvukový záznam, biometrickou identifikaci, monitorování s analytickými funkcemi nebo citlivá místa monitorování zdokumentovat poradenství k ochraně soukromí v REG04 nebo REG12.

9.3 [All] Top Management musí před prodloužením nad počáteční období výjimky schválit v REG12 výjimky přesahující 90 dnů.

9.4 [All] Privacy Lead / PIMS Manager musí alespoň měsíčně přezkoumávat otevřené výjimky z monitorování v REG12 až do jejich uzavření.

10. Uplatňování politiky

10.1 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů od potvrzení zaznamenat selhání opatření monitorování jako neshody v REG12.

10.2 [Both] Information Security Lead musí do jednoho pracovního dne od potvrzení pozastavit neoprávněný přístup k monitorovacímu systému a zaznamenat toto opatření v REG10 nebo REG12.

10.3 [All] Top Management musí do 10 pracovních dnů přiřadit vlastnictví nápravného opatření v REG12 u opakovaných nebo významných porušení politiky.

10.4 [Conditional] Incident Response Coordinator musí při podezření na neoprávněné zpřístupnění, ztrátu nebo kompromitaci PII z monitorování zahájit pracovní postup pro incident týkající se PII v REG10.

11. Přezkum a údržba

11.1 [All] Privacy Lead / PIMS Manager musí tuto politiku a související důkazy monitorování přezkoumat v REG12 alespoň jednou ročně.

11.2 [Controller] Process Owner / Business Owner musí alespoň jednou ročně znovu validovat každý aktivní účel monitorování, oznámení, rozsah umístění a záznam o uchovávání v REG02 a REG07.

11.3 [Both] System Owner / Application Owner musí alespoň jednou ročně a po významné systémové změně znovu validovat přístup k monitorovacímu systému, protokolování, výmaz a opatření pro export v REG12.

11.4 [Conditional] Vendor / Procurement Owner musí alespoň jednou ročně a před obnovením smlouvy znovu validovat důkazy o outsourcovaném poskytovateli monitorování v REG08.

11.5 [All] Privacy Lead / PIMS Manager musí do 30 kalendářních dnů po schválených změnách politiky aktualizovat související důkazy v REG02, REG04, REG07, REG08, REG10 nebo REG12.

12. Související politiky

12.1 PII02 - Politika rolí, odpovědností a odpovědnosti v oblasti soukromí

12.2 PII03 - Politika evidence zpracování PII a právního základu

12.3 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti

12.4 PII06 - Politika správy práv subjektů PII

12.5 PII07 - Politika posouzení rizik pro soukromí a DPIA

12.6 PII08 - Politika ochrany soukromí již od návrhu a ve výchozím nastavení

12.7 PII09 - Politika shromažďování, používání, zpřístupnění a sdílení PII

12.8 PII10 - Politika uchovávání, výmazu a likvidace PII

12.9 PII12 - Politika řízení ochrany soukromí u zpracovatelů, dílčích zpracovatelů a třetích stran

12.10 PII13 - Politika mezinárodního předávání PII

12.11 PII14 - Politika bezpečnosti PII a řízení přístupu

12.12 PII15 - Politika řízení incidentů a porušení zabezpečení PII

12.13 PII17 - Politika dokumentovaných informací a správy důkazů PIMS

12.14 PII18 - Politika monitorování, auditu a zlepšování PIMS

12.15 PII19 - Politika ochrany osobních údajů zaměstnanců

12.16 PII21 - Politika ochrany soukromí pro AI a automatizované rozhodování

12.17 PII23 - Politika zpracovatele PII v cloudu

13. Referenční normy a rámce

13.1 Tato politika je mapována na následující normy a právní předpisy. Mapování vysvětluje, jak politika podporuje citované požadavky, a identifikuje interní články, které je implementují nebo podporují.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapováno na dokumentované důkazy o monitorování, operativní plánování, opatření aktivace, záznamy o účelu, vazbu na oznámení, konfiguraci přístupu, konfiguraci uchovávání a řízení změn pro kamerové systémy (CCTV) a činnosti fyzického monitorování. 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** - Mapováno na měření opatření monitorování, přezkum poskytovatelů, přezkum přístupu, zjištění auditu, neshody, nápravná opatření, eskalaci prodlených opatření a důkazy o zlepšování. 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** - Mapováno na vymezení účelu monitorování správcem, dokumentaci právního základu, rozhodnutí o spouštěčích rizik pro soukromí a záznamy o činnostech zpracování monitorování v REG02 a 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** - Mapováno na přiřazení outsourcovaného poskytovatele monitorování, přiřazení odpovědností za společné monitorování a důkazy o zpracovateli nebo společném správci v 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** - Mapováno na povinnosti vůči subjektům PII související s monitorováním, směrování žádostí, uchování nezbytné k posouzení žádostí a důkazy o správě a řízení pro podporu práv. 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** - Mapováno na omezení shromažďování při monitorování, hranice zpracování, minimalizaci, doby uchovávání, výmaz, přepisování, pozastavení uchovávání a kontrolu extrahovaných kopií. 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** - Mapováno na záznamy o externím zpřístupnění, vyřizování žádostí o zpřístupnění, minimalizaci před zpřístupněním a zpřístupnění spojená s incidenty zahrnujícími PII z monitorování. 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** - Mapováno na pokyny zákazníka pro zpracovatele, povolené hranice zpracování, podporu oznámení, pokyny k uchovávání a výmazu, součinnost při právech a záznamy zpracovatele pro outsourcované monitorovací služby. 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** - Mapováno na podporu zpracovatele pro povinnosti zákazníka, schválení zpřístupnění, záznamy o zpřístupnění, oznámení žádostí o zpřístupnění a nakládání s právně závazným zpřístupněním PII z monitorování. 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** - Mapováno na ochranu záznamů monitorování, omezený přístup, přezkum privilegovaného přístupu, protokolování přístupu, zamezení šíření neoprávněného přístupu a důkazy o protokolování u monitorovacích systémů. 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)** - Mapováno na zákonnost, korektnost, transparentnost, omezení účelu, minimalizaci údajů, omezení uložení a důkazy o odpovědnosti za činnosti monitorování. 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 - Mapováno na dokumentaci právního základu pro kamerové systémy (CCTV), monitorování návštěvníků, logy fyzického přístupu a jiné činnosti fyzického monitorování. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mapováno na transparentní oznámení o monitorování, důkazy o značení, vazbu oznámení na účely zpracování, podpůrné informace ke zpracovatelskému oznámení a alternativní opatření transparentnosti. 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** - Mapováno na přístup, opravu, výmaz, omezení, námitku, směrování žádostí, uchování nezbytné k posouzení žádostí a součinnost zákazníkovi související s monitorováním. 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** - Mapováno na správu a řízení správcem, přiřazení společného správce, řízení zpracovatelů, záznamy o zpracování, bezpečnost monitorovacích systémů, přezkum rizik pro soukromí, spouštěče DPIA a poradenství k ochraně soukromí. 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** - Mapováno na specifikaci účelu, omezení shromažďování, minimalizaci údajů, omezení použití, omezení uchovávání a omezení zpřístupnění PII z monitorování. 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** - Mapováno na transparentnost, účast jednotlivce, odpovědnost, bezpečnost informací, přezkum souladu, přezkum přístupu, směrování práv, eskalaci incidentů a důkazy o nápravných opatřeních. 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** - Mapováno na předběžné posouzení rizik pro soukromí a spouštěčů DPIA pro systematické, nezjevné, zvukové, biometrické, analytikou podporované monitorování, monitorování citlivých míst, zranitelných osob nebo jiné fyzické monitorování s vyšším rizikem. 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** - Mapováno na opatření ochrany PII pro účel, shromažďování, minimalizaci, uchovávání, zpřístupnění a účast subjektů PII v kontextech monitorování. 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** - Mapováno na zřizování přístupu, omezení přístupu k informacím a řízení fyzického vstupu relevantní pro přístup k monitorovacím systémům a záznamy řízení fyzického přístupu. 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 - Mapováno na ochranu soukromí a ochranu PII, fyzický vstup, monitorování fyzické bezpečnosti, privilegovaný přístup, omezení přístupu k informacím a opatření protokolování pro kamerové systémy (CCTV) a systémy fyzického monitorování. 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].