					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII24					Naslov dokumenta: **Politika zasebnosti za videonadzor in fizično spremljanje**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/kontrola/člen	Uporabljivost	Vrsta pokritosti	Komentar
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentirane in operativne kontrole
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Spremljanje in korektivni ukrepi
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	Namen, pravna podlaga, sprožilec tveganja in evidence
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Dodelitev odgovornosti obdelovalca in skupnega upravljavca
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	Obveznosti in zahteve posameznikov, na katere se nanašajo osebno določljivi podatki
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	Zbiranje, obdelava, minimizacija, hramba in odstranitev
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Evidence in zahteve glede razkritij
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	Pogodbe z obdelovalci, navodila, podpora in evidence
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	Pravice obdelovalca in podpora pri razkritjih
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Zaščita evidenc in beleženje
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Načela in odgovornost
GDPR	Article 6	Controller	Primary	Pravna podlaga

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Preglednost in obvestila
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Zahteve za uveljavljanje pravic
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Upravljanje, obdelovalci, evidence, varnost, DPIA in svetovanje
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Namen, zbiranje, minimizacija, hramba in razkritje
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Preglednost, sodelovanje, odgovornost, varnost in skladnost
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Tveganje za zasebnost in sprožilci DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Kontrole zasebnosti za varstvo osebno določljivih podatkov
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Kontrole dostopa in fizičnega vstopa
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	Osebno določljivi podatki, fizično spremljanje, omejitev dostopa in beleženje

1. Področje uporabe

1.1 Ta politika se uporablja za videonadzor, video spremljanje, spremljanje obiskovalcev, dnevnike nadzora fizičnega dostopa, evidence spremljanja, ki ga izvajajo varnostniki, sisteme spremljanja prostorov in povezane dejavnosti fizičnega spremljanja, pri katerih se zbirajo ali drugače obdelujejo osebno določljivi podatki.

1.2 Ta politika se uporablja za organizacije, ki nastopajo kot upravljavci osebno določljivih podatkov za svoje prostore in dejavnosti fizičnega spremljanja.

1.3 Ta politika se uporablja tudi za podporne dejavnosti obdelovalca ali podobdelovalca, kadar organizacija v imenu naročnika upravlja, gosti, pregleduje, hrani, razkriva, briše ali drugače obdeluje posnetke videonadzora, podatke o obiskovalcih ali dnevnike fizičnega dostopa.

1.4 Ta politika zajema določitev namena spremljanja, odobritev, obvestila in označbe, omejitve dostopa, razkritje, hrambo, izbris, zunanje izvajanje, eskalacijo incidentov, usmerjanje zahtev za uveljavljanje pravic, pregled in upravljanje dokazil.

1.5 Ta politika ne zagotavlja svetovanja s področja delovnega prava, pravnih komentarjev glede svetov delavcev, postopkov organov pregona ali namenskega registra videonadzora.

1.6 Dokazila, specifična za spremljanje, se vzdržujejo v kanoničnih dokaznih objektih PIMS, opredeljenih v tej politiki.

2. Namen

2.1 Namen te politike je vzpostaviti kontrole zasebnosti za videonadzor in fizično spremljanje, tako da so dejavnosti spremljanja namensko določene, pregledne, sorazmerne, nadzorovane glede dostopa, hranjene za določena obdobja, razkrite samo po odobrenih kanalih in podprte s preverljivimi dokazili PIMS.

2.2 Ta politika podpira dosledno ravnanje s posnetki videonadzora, evidencami obiskovalcev, dnevniki fizičnega dostopa in povezanimi osebno določljivimi podatki spremljanja, ne da bi ustvarjala dodatne registre, odbore, nadzorne plošče ali nekanonične vloge.

3. Cilji

3.1 Cilji te politike so:

3.1.1 opredeliti namene spremljanja in obseg obdelave pred začetkom spremljanja;

3.1.2 dokumentirati dejavnosti videonadzora, fizičnega dostopa, spremljanja obiskovalcev in fizičnega spremljanja v REG02;

3.1.3 opredeliti dejavnosti spremljanja, ki zahtevajo pregled tveganj za zasebnost ali preverjanje potrebe po DPIA v REG04;

3.1.4 vzdrževati dokazila o preglednih obvestilih in označbah v REG07;

3.1.5 omejiti dostop, ogled, izvoz, razkritje in hrambo osebno določljivih podatkov spremljanja;

3.1.6 usmerjati zahteve posameznikov, na katere se nanašajo osebno določljivi podatki, prek REG06;

3.1.7 upravljati zunanje izvajalce spremljanja in dokazila o deljenju podatkov prek REG08;

3.1.8 eskalirati domnevne incidente v zvezi z osebno določljivimi podatki, povezane s spremljanjem, prek REG10;

3.1.9 evidentirati preglede, izjeme, neskladnosti, korektivne ukrepe, ugotovitve presoje in izboljšave v REG12.

4. Izjave politike

4.1 Popis spremljanja, namen in odobritev

4.1.1 [Controller] Process Owner / Business Owner mora vsako dejavnost videonadzora, spremljanja obiskovalcev, vodenja dnevnikov nadzora fizičnega dostopa ali fizičnega spremljanja evidentirati v REG02 pred začetkom dejavnosti.

4.1.2 [Controller] Privacy Lead / PIMS Manager mora pred aktivacijo nove ali bistveno spremenjene dejavnosti spremljanja potrditi vnos v REG02 glede namena, pravne podlage, spremljane lokacije, kategorij osebno določljivih podatkov, kategorij posameznikov, na katere se nanašajo osebno določljivi podatki, hrambe, obvestila, dostopa in polj za razkritje.

4.1.3 [Controller] Process Owner / Business Owner mora pred omogočitvijo kamer, senzorjev, dnevnikov obiskovalcev ali beleženja nadzora dostopa v REG02 evidentirati odobrena spremljana območja, izključena območja in meje zbiranja.

4.1.4 [Conditional] Process Owner / Business Owner mora pred aktivacijo spremljanja, ki vključuje sistematično spremljanje, zvočno snemanje, biometrično identifikacijo, zaznavanje z analitiko, občutljive lokacije, ranljive posameznike ali neočitno spremljanje, pridobiti odločitev o tveganju za zasebnost v REG04.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager mora pred začetkom skupnega spremljanja z najemodajalcem, partnerjem za upravljanje objektov, naročnikom ali drugim skupnim upravljavcem v REG08 evidentirati razporeditev odgovornosti za skupno spremljanje.

4.1.6 [Processor] Privacy Lead / PIMS Manager mora pred obdelavo posnetkov videonadzora, evidenc obiskovalcev ali dnevnikov fizičnega dostopa v imenu naročnika v REG08 evidentirati navodila naročnika glede spremljanja in dovoljene meje obdelave.

4.2 Obvestilo in preglednost

4.2.1 [Controller] Process Owner / Business Owner mora zagotoviti, da so dokazila o obvestilu o izvajanju videonadzora ali enakovrednem sprotnem obvestilu evidentirana v REG07, preden so spremljana območja odprta za posameznike, na katere se nanašajo osebno določljivi podatki.

4.2.2 [Controller] Privacy Lead / PIMS Manager mora pred objavo ali bistveno spremembo vsako obvestilo o spremljanju v REG07 povezati z ustreznim namenom obdelave v REG02.

4.2.3 [Processor] Privacy Lead / PIMS Manager mora v REG08 zagotoviti podporne informacije za obvestilo o spremljanju, kadar organizacija izvaja storitve spremljanja po navodilih naročnika.

4.2.4 [Conditional] Process Owner / Business Owner mora pred aktivacijo neočitnega ali nujnega spremljanja v REG07 in REG04 evidentirati alternativne ukrepe preglednosti.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Izjeme

9.1 [All] Privacy Lead / PIMS Manager mora vsako izjemo od te politike evidentirati v REG12, preden se izjema uporabi.

9.2 [Conditional] Data Protection Officer / Privacy Advisor mora pred odobritvijo izjem, ki vključujejo neočitno spremljanje, zvočno snemanje, biometrično identifikacijo, spremljanje z analitiko ali občutljive lokacije spremljanja, dokumentirati nasvet glede zasebnosti v REG04 ali REG12.

9.3 [All] Top Management mora pred podaljšanjem po začetnem obdobju izjeme v REG12 odobriti izjeme, ki presegajo 90 dni.

9.4 [All] Privacy Lead / PIMS Manager mora najmanj mesečno do zaprtja pregledovati odprte izjeme glede spremljanja v REG12.

10. Uveljavljanje

10.1 [All] Privacy Lead / PIMS Manager mora odpovedi kontrol spremljanja evidentirati kot neskladnosti v REG12 v petih delovnih dneh po potrditvi.

10.2 [Both] Information Security Lead mora nepooblaščen dostop do sistema spremljanja začasno ukiniti v enem delovnem dnevu po potrditvi in ukrep evidentirati v REG10 ali REG12.

10.3 [All] Top Management mora za ponavljajoče se ali bistvene kršitve politike v 10 delovnih dneh v REG12 dodeliti nosilca korektivnega ukrepa.

10.4 [Conditional] Incident Response Coordinator mora ob domnevnem nepooblaščenem razkritju, izgubi ali kompromitaciji osebno določljivih podatkov spremljanja sprožiti delovni tok za incident v zvezi z osebno določljivimi podatki v REG10.

11. Pregled in vzdrževanje

11.1 [All] Privacy Lead / PIMS Manager mora najmanj letno pregledati to politiko in povezana dokazila o spremljanju v REG12.

11.2 [Controller] Process Owner / Business Owner mora najmanj letno ponovno potrditi vsak aktiven namen spremljanja, obvestilo, obseg lokacije in vnos hrambe v REG02 in REG07.

11.3 [Both] System Owner / Application Owner mora najmanj letno in po bistveni spremembi sistema ponovno potrditi kontrole dostopa, beleženja, izbrisa in izvoza v sistemu spremljanja v REG12.

11.4 [Conditional] Vendor / Procurement Owner mora najmanj letno in pred podaljšanjem pogodbe ponovno potrditi dokazila o zunanjih ponudnikih spremljanja v REG08.

11.5 [All] Privacy Lead / PIMS Manager mora v 30 koledarskih dneh po odobrenih spremembah politike posodobiti povezana dokazila REG02, REG04, REG07, REG08, REG10 ali REG12.

12. Povezane politike

12.1 PII02 - Politika vlog, odgovornosti in odgovornosti za zasebnost

12.2 PII03 - Politika popisa dejavnosti obdelave osebno določljivih podatkov in pravne podlage

12.3 PII04 - Politika obvestil o zasebnosti in preglednosti

12.4 PII06 - Politika upravljanja pravic posameznikov, na katere se nanašajo osebno določljivi podatki

12.5 PII07 - Politika presoje tveganj za zasebnost in DPIA

12.6 PII08 - Politika varstva zasebnosti že pri načrtovanju in privzetega varstva zasebnosti

12.7 PII09 - Politika zbiranja, uporabe, razkritja in deljenja osebno določljivih podatkov

12.8 PII10 - Politika hrambe, izbrisa in odstranjevanja osebno določljivih podatkov

12.9 PII12 - Politika upravljanja zasebnosti obdelovalcev, podobdelovalcev in tretjih oseb

12.10 PII13 - Politika mednarodnih prenosov osebno določljivih podatkov

12.11 PII14 - Politika varnosti in nadzora dostopa za osebno določljive podatke

12.12 PII15 - Politika upravljanja incidentov in kršitev v zvezi z osebno določljivimi podatki

12.13 PII17 - Politika dokumentiranih informacij in upravljanja dokazil PIMS

12.14 PII18 - Politika spremljanja, presoje in izboljševanja PIMS

12.15 PII19 - Politika zasebnosti zaposlenih

12.16 PII21 - Politika zasebnosti za AI in avtomatizirano sprejemanje odločitev

12.17 PII23 - Politika obdelovalca osebno določljivih podatkov v oblaku

13. Referenčni standardi in okviri

13.1 Ta politika je preslikana na naslednje standarde in predpise. Preslikava pojasnjuje, kako politika podpira navedene zahteve, in opredeljuje notranje klavzule, ki jih izvajajo ali podpirajo.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Preslikano na dokumentirana dokazila o spremljanju, operativno načrtovanje, kontrole aktivacije, evidence namenov, povezave z obvestili, konfiguracijo dostopa, konfiguracijo hrambe in nadzor sprememb za dejavnosti videonadzora in fizičnega spremljanja. 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** - Preslikano na merjenje kontrol spremljanja, pregled ponudnikov, pregled dostopa, ugotovitve presoje, neskladnosti, korektivne ukrepe, eskalacijo zapadlih ukrepov in dokazila o izboljšavah. 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** - Preslikano na opredelitev namena spremljanja pri upravljavcu, dokumentiranje pravne podlage, odločitve o sprožilcih tveganj za zasebnost in evidence dejavnosti obdelave spremljanja v REG02 in 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** - Preslikano na razporeditev odgovornosti zunanjih ponudnikov spremljanja, razporeditev odgovornosti za skupno spremljanje ter dokazila o obdelovalcu ali skupnem upravljavcu 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** - Preslikano na obveznosti do posameznikov, na katere se nanašajo osebno določljivi podatki, povezane s spremljanjem, usmerjanje zahtev, ohranitev, potrebno za presojo zahtev, in dokazila o upravljanju za podporo pravicam. 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** - Preslikano na omejevanje zbiranja pri spremljanju, meje obdelave, minimizacijo, obdobja hrambe, izbris, prepisovanje, zadržanja hrambe in nadzor izvlečenih kopij. 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** - Preslikano na evidence zunanjih razkritij, obravnavo zahtev za razkritje, minimizacijo pred razkritjem in razkritja, povezana z incidenti, ki vključujejo osebno določljive podatke spremljanja. 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** - Preslikano na navodila naročnika obdelovalcu, dovoljene meje obdelave, podporo pri obvestilih, navodila glede hrambe in izbrisa, pomoč pri pravicah in evidence obdelovalca za zunanje izvajane storitve spremljanja. 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** - Preslikano na podporo obdelovalca obveznostim naročnika, pooblastilo za razkritje, evidence razkritij, obveščanje o zahtevah za razkritje in obravnavo pravno zavezujočih razkritij za osebno določljive podatke spremljanja. 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** - Preslikano na zaščito evidenc spremljanja, omejen dostop, pregled privilegiranega dostopa, beleženje dostopa, zajezitev nepooblaščenega dostopa in dokazila o beleženju za sisteme spremljanja. 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)** - Preslikano na zakonitost, poštenost, preglednost, omejitev namena, minimizacijo podatkov, omejitev hrambe in dokazila o odgovornosti za dejavnosti spremljanja. 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 - Preslikano na dokumentiranje pravne podlage za videonadzor, spremljanje obiskovalcev, dnevnike fizičnega dostopa in druge dejavnosti fizičnega spremljanja. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Preslikano na pregledna obvestila o spremljanju, dokazila o označbah, povezavo obvestila z nameni obdelave, podporne informacije obdelovalca za obvestila in alternativne ukrepe preglednosti. 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** - Preslikano na dostop, popravek, izbris, omejitev, ugovor, usmerjanje zahtev, ohranitev, potrebno za presojo zahtev, in pomoč naročniku, povezano s spremljanjem. 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** - Preslikano na upravljanje upravljavca, razporeditev odgovornosti skupnega upravljavca, upravljanje obdelovalcev, evidence obdelave, varnost sistemov spremljanja, pregled tveganj za zasebnost, sprožilce DPIA in nasvete glede zasebnosti. 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** - Preslikano na določitev namena, omejitev zbiranja, minimizacijo podatkov, omejitev uporabe, omejitev hrambe in omejitev razkritja za osebno določljive podatke spremljanja. 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** - Preslikano na preglednost, sodelovanje posameznika, odgovornost, informacijsko varnost, pregled skladnosti, pregled dostopa, usmerjanje zahtev za uveljavljanje pravic, eskalacijo incidentov in dokazila o korektivnih ukrepih. 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** - Preslikano na tveganje za zasebnost in preverjanje sprožilcev DPIA za sistematično, neočitno, zvočno, biometrično, z analitiko podprto spremljanje, spremljanje občutljivih lokacij, ranljivih posameznikov ali drugo fizično spremljanje z višjim tveganjem. 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** - Preslikano na kontrole varstva osebno določljivih podatkov za namen, zbiranje, minimizacijo, hrambo, razkritje in sodelovanje posameznikov, na katere se nanašajo osebno določljivi podatki, v kontekstih spremljanja. 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** - Preslikano na dodeljevanje dostopa, omejitev dostopa do informacij in kontrole fizičnega vstopa, relevantne za dostop do sistemov spremljanja in evidence nadzora fizičnega dostopa. 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 - Preslikano na zasebnost in varstvo osebno določljivih podatkov, fizični vstop, spremljanje fizične varnosti, privilegirani dostop, omejitev dostopa do informacij in kontrole beleženja za videonadzor in sisteme fizičnega spremljanja. 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].