					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII24					Naziv dokumenta: **Politika privatnosti za CCTV i fizički nadzor**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentirane i operativne kontrole
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Praćenje i korektivna radnja
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	Svrha, pravna osnova, okidač rizika i zapisi
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Raspodjela odgovornosti izvršitelja obrade i zajedničkog voditelja obrade
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	Obveze prema ispitanicima i zahtjevi
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	Prikupljanje, obrada, minimizacija, zadržavanje i zbrinjavanje
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Zapisi o otkrivanju i zahtjevi
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	Ugovori izvršitelja obrade, upute, podrška i zapisi
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	Prava izvršitelja obrade i podrška pri otkrivanju
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Zaštita zapisa i zapisivanje događaja
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Načela i odgovornost
GDPR	Article 6	Controller	Primary	Pravna osnova

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparentnost i obavijesti
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Zahtjevi za ostvarivanje prava
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Upravljanje, izvršitelji obrade, zapisi, sigurnost, DPIA i savjetovanje
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Svrha, prikupljanje, minimizacija, zadržavanje i otkrivanje
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparentnost, sudjelovanje, odgovornost, sigurnost i usklađenost
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Rizik za privatnost i okidači za DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Kontrole privatnosti za zaštitu PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Kontrole pristupa i fizičkog ulaska
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, fizički nadzor, ograničenje pristupa i zapisivanje događaja

1. Opseg

1.1 Ova se politika primjenjuje na CCTV, videonadzor, nadzor posjetitelja, evidencije kontrole fizičkog pristupa, zapise nadzora koje provodi zaštitarsko osoblje, sustave nadzora prostora i povezane aktivnosti fizičkog nadzora kojima se prikuplja ili na drugi način obrađuje PII.

1.2 Ova se politika primjenjuje na organizacije koje djeluju kao voditelji obrade za vlastite prostore i aktivnosti fizičkog nadzora.

1.3 Ova se politika primjenjuje i na aktivnosti podrške izvršitelja obrade ili podizvršitelja obrade kada organizacija upravlja, hostira, pregledava, pohranjuje, otkriva, briše ili na drugi način obrađuje snimke videonadzora, podatke o posjetiteljima ili evidencije fizičkog pristupa u ime klijenta.

1.4 Ova politika obuhvaća definiranje svrhe nadzora, odobrenje, obavijesti i oznake, ograničenja pristupa, otkrivanje, zadržavanje, brisanje, vanjsko ugovaranje, eskalaciju incidenata, usmjeravanje zahtjeva za ostvarivanje prava, pregled i upravljanje dokazima.

1.5 Ova politika ne pruža savjete iz radnog prava, pravne komentare o radničkom vijeću, postupke tijela kaznenog progona ni namjenski registar CCTV-a.

1.6 Dokazi specifični za nadzor održavaju se u kanonskim objektima dokaza PIMS-a utvrđenima u ovoj politici.

2. Svrha

2.1 Svrha je ove politike uspostaviti kontrole privatnosti za CCTV i fizički nadzor kako bi aktivnosti nadzora bile svrhovite, transparentne, razmjerne, kontrolirane u pogledu pristupa, zadržane tijekom definiranih razdoblja, otkrivane samo putem odobrenih kanala i potkrijepljene revizijski provjerljivim dokazima PIMS-a.

2.2 Ova politika podržava dosljedno postupanje sa snimkama videonadzora, zapisima o posjetiteljima, evidencijama fizičkog pristupa i povezanim PII iz nadzora, bez stvaranja dodatnih registara, odbora, nadzornih ploča ili nekanonskih uloga.

3. Ciljevi

3.1 Ciljevi ove politike su:

3.1.1 definirati svrhe nadzora i opseg obrade prije početka nadzora;

3.1.2 dokumentirati CCTV, fizički pristup, nadzor posjetitelja i aktivnosti fizičkog nadzora u REG02;

3.1.3 identificirati aktivnosti nadzora koje zahtijevaju pregled rizika za privatnost ili provjeru potrebe za DPIA-om u REG04;

3.1.4 održavati dokaze o transparentnoj obavijesti i oznakama u REG07;

3.1.5 ograničiti pristup, pregled, izvoz, otkrivanje i zadržavanje PII iz nadzora;

3.1.6 usmjeravati zahtjeve ispitanika kroz REG06;

3.1.7 upravljati vanjskim pružateljima usluga nadzora i dokazima o dijeljenju podataka kroz REG08;

3.1.8 eskalirati sumnje na incidente u vezi s PII povezane s nadzorom kroz REG10;

3.1.9 evidentirati preglede, iznimke, nesukladnosti, korektivne radnje, nalaze revizije i poboljšanja u REG12.

4. Izjave politike

4.1 Popis aktivnosti nadzora, svrha i odobrenje

4.1.1 [Controller] Process Owner / Business Owner mora evidentirati svaku aktivnost CCTV-a, nadzora posjetitelja, evidencije kontrole fizičkog pristupa ili fizičkog nadzora u REG02 prije početka aktivnosti.

4.1.2 [Controller] Privacy Lead / PIMS Manager mora potvrditi unos u REG02 u pogledu svrhe, pravne osnove, nadzirane lokacije, kategorija PII, kategorija ispitanika, zadržavanja, obavijesti, pristupa i polja za otkrivanje prije aktivacije nove ili značajno izmijenjene aktivnosti nadzora.

4.1.3 [Controller] Process Owner / Business Owner mora evidentirati odobrene nadzirane zone, isključene zone i granice prikupljanja u REG02 prije omogućavanja kamera, senzora, zapisa o posjetiteljima ili zapisivanja kontrole pristupa.

4.1.4 [Conditional] Process Owner / Business Owner mora pribaviti odluku o riziku za privatnost u REG04 prije aktiviranja nadzora koji uključuje sustavni nadzor, audio snimanje, biometrijsku identifikaciju, detekciju omogućenu analitikom, osjetljive lokacije, ranjive pojedince ili neočiti nadzor.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager mora evidentirati raspodjelu odgovornosti za zajednički nadzor u REG08 prije početka zajedničkog nadzora s najmodavcem, partnerom za upravljanje objektima, klijentom ili drugim zajedničkim voditeljem obrade.

4.1.6 [Processor] Privacy Lead / PIMS Manager mora evidentirati upute klijenta za nadzor i dopuštene granice obrade u REG08 prije obrade snimki videonadzora, zapisa o posjetiteljima ili evidencija fizičkog pristupa u ime klijenta.

4.2 Obavijest i transparentnost

4.2.1 [Controller] Process Owner / Business Owner mora osigurati da se dokazi o oznakama videonadzora ili jednakovrijednoj pravodobnoj obavijesti evidentiraju u REG07 prije otvaranja nadziranih područja ispitanicima.

4.2.2 [Controller] Privacy Lead / PIMS Manager mora povezati svaku obavijest o nadzoru u REG07 s odgovarajućom svrhom obrade u REG02 prije objave ili značajne promjene.

4.2.3 [Processor] Privacy Lead / PIMS Manager mora pružiti informacije za podršku obavijesti o nadzoru u REG08 kada organizacija upravlja uslugama nadzora prema uputama klijenta.

4.2.4 [Conditional] Process Owner / Business Owner mora evidentirati alternativne mjere transparentnosti u REG07 i REG04 prije aktiviranja neočitog ili hitnog nadzora.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Iznimke

9.1 [All] Privacy Lead / PIMS Manager mora evidentirati svaku iznimku od ove politike u REG12 prije uporabe iznimke.

9.2 [Conditional] Data Protection Officer / Privacy Advisor mora dokumentirati savjet o privatnosti u REG04 ili REG12 prije odobrenja iznimaka koje uključuju neočiti nadzor, audio snimanje, biometrijsku identifikaciju, nadzor omogućen analitikom ili osjetljive lokacije nadzora.

9.3 [All] Top Management mora odobriti iznimke dulje od 90 dana u REG12 prije produljenja izvan početnog razdoblja iznimke.

9.4 [All] Privacy Lead / PIMS Manager mora pregledavati otvorene iznimke nadzora u REG12 najmanje mjesečno do zatvaranja.

10. Provedba

10.1 [All] Privacy Lead / PIMS Manager mora evidentirati neuspjehe kontrola nadzora kao nesukladnosti u REG12 u roku od pet radnih dana od potvrde.

10.2 [Both] Information Security Lead mora suspendirati neovlašteni pristup sustavu nadzora u roku od jednog radnog dana od potvrde i evidentirati radnju u REG10 ili REG12.

10.3 [All] Top Management mora dodijeliti vlasništvo nad korektivnom radnjom u REG12 u roku od 10 radnih dana za ponovljena ili značajna kršenja politike.

10.4 [Conditional] Incident Response Coordinator mora pokrenuti tijek rada za incident u vezi s PII u REG10 nakon sumnje na neovlašteno otkrivanje, gubitak ili kompromitaciju PII iz nadzora.

11. Pregled i održavanje

11.1 [All] Privacy Lead / PIMS Manager mora pregledati ovu politiku i povezane dokaze nadzora u REG12 najmanje jednom godišnje.

11.2 [Controller] Process Owner / Business Owner mora ponovno potvrditi svaku aktivnu svrhu nadzora, obavijest, opseg lokacije i unos zadržavanja u REG02 i REG07 najmanje jednom godišnje.

11.3 [Both] System Owner / Application Owner mora ponovno potvrditi kontrole pristupa, zapisivanja događaja, brisanja i izvoza za sustav nadzora u REG12 najmanje jednom godišnje i nakon značajne promjene sustava.

11.4 [Conditional] Vendor / Procurement Owner mora ponovno potvrditi dokaze o vanjsko ugovorenom pružatelju usluga nadzora u REG08 najmanje jednom godišnje i prije obnove ugovora.

11.5 [All] Privacy Lead / PIMS Manager mora ažurirati povezane dokaze REG02, REG04, REG07, REG08, REG10 ili REG12 u roku od 30 kalendarskih dana nakon odobrenih promjena politike.

12. Povezane politike

12.1 PII02 - Politika uloga, odgovornosti i odgovornosti za privatnost

12.2 PII03 - Politika popisa obrade PII i pravne osnove

12.3 PII04 - Politika obavijesti o privatnosti i transparentnosti

12.4 PII06 - Politika upravljanja pravima ispitanika

12.5 PII07 - Politika procjene rizika za privatnost i DPIA-e

12.6 PII08 - Politika ugrađene i zadane zaštite privatnosti

12.7 PII09 - Politika prikupljanja, uporabe, otkrivanja i dijeljenja PII

12.8 PII10 - Politika zadržavanja, brisanja i zbrinjavanja PII

12.9 PII12 - Politika upravljanja privatnošću izvršitelja obrade, podizvršitelja obrade i trećih strana

12.10 PII13 - Politika međunarodnog prijenosa PII

12.11 PII14 - Politika sigurnosti i kontrole pristupa PII

12.12 PII15 - Politika upravljanja incidentima i povredama PII

12.13 PII17 - Politika dokumentiranih informacija i upravljanja dokazima PIMS-a

12.14 PII18 - Politika praćenja, revizije i poboljšanja PIMS-a

12.15 PII19 - Politika privatnosti zaposlenika

12.16 PII21 - Politika privatnosti za AI i automatizirano donošenje odluka

12.17 PII23 - Politika za izvršitelje obrade PII u oblaku

13. Referentni standardi i okviri

13.1 Ova je politika mapirana na sljedeće standarde i propise. Mapiranje objašnjava kako politika podržava navedene zahtjeve i identificira interne točke koje ih provode ili podržavaju.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapirano na dokumentirane dokaze nadzora, operativno planiranje, kontrole aktivacije, zapise svrhe, poveznicu na obavijest, konfiguraciju pristupa, konfiguraciju zadržavanja i kontrolu promjena za aktivnosti CCTV-a i fizičkog nadzora. 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** - Mapirano na mjerenje kontrola nadzora, pregled pružatelja usluga, pregled pristupa, nalaze revizije, nesukladnosti, korektivne radnje, eskalaciju dospjelih

neprovedenih radnji i dokaze poboljšanja. 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** - Mapirano na definiranje svrhe nadzora voditelja obrade, dokumentiranje pravne osnove, odluke o okidačima rizika za privatnost i zapise o aktivnostima obrade nadzora u 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** - Mapirano na raspodjelu odgovornosti vanjsko ugovorenog pružatelja usluga nadzora, raspodjelu odgovornosti za zajednički nadzor te dokaze o izvršitelju obrade ili zajedničkom voditelju obrade u 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** - Mapirano na obveze prema ispitanicima povezane s nadzorom, usmjeravanje zahtjeva, očuvanje potrebno za procjenu zahtjeva i dokaze upravljanja za podršku pravima. 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** - Mapirano na ograničavanje prikupljanja nadzorom, granice obrade, minimizaciju, razdoblja zadržavanja, brisanje, prepisivanje, obustave brisanja i kontrolu izdvojenih kopija. 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** - Mapirano na zapise o vanjskom otkrivanju, postupanje sa zahtjevima za otkrivanje, minimizaciju prije otkrivanja i otkrivanja povezana s incidentima koja uključuju PII iz nadzora. 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** - Mapirano na upute klijenta izvršitelju obrade, dopuštene granice obrade, podršku obavijesti, upute za zadržavanje i brisanje, pomoć pri ostvarivanju prava i zapise izvršitelja obrade za vanjsko ugovorene usluge nadzora. 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** - Mapirano na podršku izvršitelja obrade obvezama klijenta, odobrenje otkrivanja, zapise o otkrivanju, obavješćivanje o zahtjevima za otkrivanje i postupanje s pravno obvezujućim otkrivanjem za PII iz nadzora. 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** - Mapirano na zaštitu zapisa nadzora, ograničeni pristup, pregled privilegiranog pristupa, zapisivanje pristupa, ograničavanje neovlaštenog pristupa i dokaze zapisivanja događaja za sustave nadzora. 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)** - Mapirano na zakonitost, poštenost, transparentnost, ograničenje svrhe, minimizaciju podataka, ograničenje pohrane i dokaze o odgovornosti za aktivnosti nadzora. 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 - Mapirano na dokumentiranje pravne osnove za CCTV, nadzor posjetitelja, evidencije fizičkog pristupa i druge aktivnosti fizičkog nadzora. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mapirano na transparentne obavijesti o nadzoru, dokaze o oznakama, poveznicu obavijesti sa svrhama obrade, informacije izvršitelja obrade za podršku obavijesti i alternativne mjere 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** - Mapirano na pristup, ispravak, brisanje, ograničenje, prigovor, usmjeravanje zahtjeva, očuvanje potrebno za procjenu

zahtjeva i pomoć klijentu povezanu s nadzorom. 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** - Mapirano na upravljanje voditelja obrade, raspodjelu odgovornosti zajedničkih voditelja obrade, upravljanje izvršiteljem obrade, evidencije obrade, sigurnost sustava nadzora, pregled rizika za privatnost, okidače za DPIA i savjet o privatnosti. 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** - Mapirano na određivanje svrhe, ograničenje prikupljanja, minimizaciju podataka, ograničenje uporabe, ograničenje zadržavanja i ograničenje otkrivanja za PII iz nadzora. 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** - Mapirano na transparentnost, sudjelovanje pojedinaca, odgovornost, informacijsku sigurnost, pregled usklađenosti, pregled pristupa, usmjeravanje zahtjeva za ostvarivanje prava, eskalaciju incidenata i dokaze korektivnih radnji. 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** - Mapirano na provjeru okidača rizika za privatnost i DPIA za sustavni, neočiti, audio, biometrijski, analitikom omogućeni nadzor, nadzor osjetljivih lokacija, ranjivih pojedinaca ili drugi fizički nadzor povišenog rizika. 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** - Mapirano na kontrole zaštite PII za svrhu, prikupljanje, minimizaciju, zadržavanje, otkrivanje i sudjelovanje ispitanika u kontekstima nadzora. 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** - Mapirano na dodjelu pristupa, ograničenje pristupa informacijama i kontrole fizičkog ulaska relevantne za pristup sustavu nadzora i zapise kontrole fizičkog pristupa. 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 - Mapirano na privatnost i zaštitu PII, fizički ulazak, nadzor fizičke sigurnosti, privilegirani pristup, ograničenje pristupa informacijama i kontrole zapisivanja događaja za CCTV i sustave fizičkog nadzora. 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].