					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII17					Naziv dokumenta: **Politika upravljanja dokumentiranim informacijama i dokazima PIMS-a**							
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/propis	Točka/kontrola/članak	Primjenjivost	Vrsta pokrivenosti	Napomena
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	SoA dokumentirane informacije
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentirane informacije PIMS-a
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Kontrola operativnih dokaza
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Dokazi praćenja
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Revizijski dokazi
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Dokazi preispitivanja od strane uprave
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Dokazi o nesukladnosti i korektivnoj radnji
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Zapisi voditelja obrade o obradi
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Dokazi o ugovoru i uputama izvršitelja obrade
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Zaštita zapisa
GDPR	Article 5(2)	Controller	Supporting	Dokazi o odgovornosti
GDPR	Article 24	Controller	Supporting	Mjere i dokazi voditelja obrade
GDPR	Article 28	Both	Supporting	Dokumentacija izvršitelja obrade
GDPR	Article 30	Both	Supporting	Zapisi o obradi
GDPR	Article 32	Both	Supporting	Zaštita dokaza
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Dokazi usklađenosti privatnosti
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Zaštita zapisa

ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Kontrola dokumentiranih informacija
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Zaštita zapisa
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Zaštita privatnosti i PII

1. Opseg

1.1 Ova politika definira obvezne zahtjeve za izradu, odobravanje, verzioniranje, zaštitu, zadržavanje, dohvat, prevođenje, povlačenje i dokazivanje dokumentiranih informacija PIMS-a.

1.2 Ova politika primjenjuje se na politike PIMS-a, registre, dokumentirana odobrenja, zapise o dokazima, revizijske dokaze, zapise preispitivanja od strane uprave, dokaze o korektivnim radnjama i kontrolirane prijevode koji se koriste za dokazivanje usklađenosti PIMS-a.

1.3 Ova politika primjenjuje se u kontekstima voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade.

1.4 Ova politika ne uspostavlja zaseban registar kontrole dokumenata. Dokazi kontrole dokumentiranih informacija održavaju se kroz kanonske objekte dokaza PIMS-a od REG01 do REG12, pri čemu se REG03 i REG12 koriste za dokaze o primjenjivosti kontrola, reviziji, nesukladnosti, korektivnim radnjama i poboljšanju.

2. Svrha

2.1 Svrha ove politike jest osigurati da su dokumentirane informacije PIMS-a točne, kontrolirane, dostupne ovlaštenim korisnicima, zaštićene od neovlaštene izmjene ili otkrivanja, zadržane radi revizijske provjerljivosti i povučene kada zastare.

2.2 Ova politika podupire spremnost za certifikaciju tako što osigurava da se dokazi potrebni za dokazivanje usklađenosti PIMS-a mogu pronaći, provjeriti, dohvatiti i povezati s primjenjivim politikama, kontrolama, aktivnostima obrade, rizicima, revizijama i korektivnim radnjama.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

3.1.1 definirati zahtjeve kontrole dokumentiranih informacija PIMS-a;

3.1.2 održavati cjelovitost dokaza od REG01 do REG12;

3.1.3 osigurati sljedivost odobravanja politika i dokaza;

3.1.4 osigurati dokumentiranje povijesti verzija i odluka o povlačenju;

3.1.5 povezati dokaze PIMS-a s Izjavom o primjenjivosti i mapiranjem politika;

3.1.6 kontrolirati pristup dokumentima PIMS-a i zapisima o dokazima;

3.1.7 podržati upravljanje verzijama višejezičnih politika i dokaza;

3.1.8 omogućiti pravodoban dohvat revizijskih dokaza;

3.1.9 spriječiti nepotrebnu birokraciju u kontroli dokumenata;

3.1.10 očuvati zapise spremne za reviziju radi certifikacije, dokazivanja usklađenosti prema klijentima i kontinuiranog poboljšanja.

4. Izjave politike

4.1 Kontrola dokumentiranih informacija PIMS-a

4.1.1 [All] Privacy Lead / PIMS Manager mora održavati indeks dokumentiranih informacija PIMS-a u REG12 prije prve objave PIMS-a i nakon toga tromjesečno.

4.1.2 [All] Process Owner / Business Owner mora identificirati dokumentirane informacije potrebne za svaku aktivnost obrade PII koju posjeduje u REG02 prije početka aktivnosti obrade i nakon toga jednom godišnje.

4.1.3 [All] Privacy Lead / PIMS Manager mora povezati primjenjive politike PIMS-a, kontrole i obveze dokazivanja s REG03 prije svake objave politike i u roku od 15 radnih dana od svake značajne promjene primjenjivosti kontrola.

4.1.4 [All] Privacy Lead / PIMS Manager mora dodijeliti razinu pristupa i klasifikaciju osjetljivosti dokaza svakoj kategoriji dokumentiranih informacija PIMS-a u REG12 prije uporabe te kategorije.

4.2 Izrada, odobravanje, verzioniranje i objava

4.2.1 [All] Privacy Lead / PIMS Manager mora dodijeliti identifikator dokumenta, vlasnika, broj verzije, status odobrenja, datum stupanja na snagu i datum pregleda u REG12 prije objave dokumentiranih informacija PIMS-a.

4.2.2 [All] Top Management mora odobriti temeljne politike PIMS-a i značajne izmjene politike u REG12 prije objave.

4.2.3 [All] Privacy Lead / PIMS Manager mora odobriti predloške dokaza PIMS-a ili ugrađene odjeljke registra u REG12 prije operativne uporabe.

4.2.4 [All] Privacy Lead / PIMS Manager mora evidentirati povijest verzija i obrazloženje promjene u REG12 prije objave ažuriranih dokumentiranih informacija PIMS-a.

4.2.5 [All] Privacy Lead / PIMS Manager mora evidentirati komunikaciju odobrenih izmjena dokumentiranih informacija PIMS-a u REG11 u roku od 30 dana od objave.

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

9. Iznimke

9.1.1 [All] Process Owner / Business Owner mora zatražiti iznimke u vezi s dokumentiranim informacijama ili kontrolom dokaza u REG12 prije odstupanja od ove politike.

9.1.2 [All] Privacy Lead / PIMS Manager mora procijeniti svaku iznimku u vezi s dokumentiranim informacijama ili kontrolom dokaza u REG12 u roku od 10 radnih dana od zahtjeva.

9.1.3 [All] Data Protection Officer / Privacy Advisor mora evidentirati savjet u REG12 prije odobrenja svake iznimke koja uključuje otkrivanje dokaza koji sadržavaju PII, odstupanje u prijevodu, sukob u vezi sa zadržavanjem ili ograničenje revizijskih dokaza.

9.1.4 [All] Top Management mora odobriti iznimke dokumentiranih informacija koje traju dulje od 30 dana ili utječu na certifikaciju, obradu visokog rizika ili vanjsko dokazivanje usklađenosti u REG12 prije nego što iznimka stupi na snagu.

9.1.5 [All] Privacy Lead / PIMS Manager mora za svaku odobrenu iznimku u vezi s dokumentiranim informacijama ili kontrolom dokaza odrediti datum isteka koji ne prelazi 90 dana u REG12.

9.1.6 [All] Privacy Lead / PIMS Manager mora zatvoriti ili ponovno procijeniti svaku iznimku u vezi s dokumentiranim informacijama ili kontrolom dokaza u REG12 u roku od pet radnih dana od isteka.

10. Provedba

10.1.1 [All] Privacy Lead / PIMS Manager mora evidentirati nedostajuće, netočne, nekontrolirane, zastarjele ili nedohvatljive dokumentirane informacije PIMS-a kao nesukladnost u REG12 u roku od pet radnih dana od utvrđivanja.

10.1.2 [All] Privacy Lead / PIMS Manager mora spriječiti objavu dokumentiranih informacija PIMS-a kada u REG12 nedostaju potrebni dokazi o odobrenju, verziji, vlasniku ili datumu stupanja na snagu.

10.1.3 [All] Process Owner / Business Owner mora spriječiti podnošenje dokaza o obradi za reviziju kada u REG02 nedostaju potrebni dokazi o vlasniku, datumu, statusu ili odobrenju.

10.1.4 [All] System Owner / Application Owner mora ukloniti neovlašteni pristup repozitorijima dokumentiranih informacija PIMS-a i evidentirati uklanjanje u REG12 u roku od jednog radnog dana od utvrđivanja.

10.1.5 [All] Internal Audit / Compliance Reviewer mora provjeriti djelotvornost korektivnih radnji za nesukladnosti dokumentiranih informacija u REG12 pri sljedećoj planiranoj reviziji ili u roku od 60 dana od zatvaranja, ovisno o tome što nastupi prije.

11. Pregled i održavanje

11.1.1 [All] Privacy Lead / PIMS Manager mora pregledati ovu politiku jednom godišnje i u roku od 30 dana od značajne promjene zahtjeva za dokumentirane informacije PIMS-a.

11.1.2 [All] Privacy Lead / PIMS Manager mora pregledati ovu politiku u roku od 30 dana nakon velikog nalaza revizije, certifikacijske nesukladnosti, promjene platforme repozitorija ili promjene postupka višejezične objave.

11.1.3 [All] Data Protection Officer / Privacy Advisor mora pregledati promjene ove politike značajne za privatnost u REG12 prije odobrenja.

11.1.4 [All] Top Management mora odobriti značajne promjene ove politike u REG12 prije objave.

11.1.5 [All] Privacy Lead / PIMS Manager mora evidentirati komunikaciju odobrenih promjena ove politike u REG11 u roku od 30 dana od objave.

12. Povezane politike

12.1 Ovu politiku podupiru sljedeće povezane politike:

12.2 PII01 - Politika sustava upravljanja informacijama o privatnosti

12.3 PII02 - Politika uloga, odgovornosti i odgovornosti za privatnost

12.4 PII03 - Politika inventara obrade PII i pravne osnove

12.5 PII04 - Politika obavijesti o privatnosti i transparentnosti

12.6 PII05 - Politika upravljanja privolama i preferencijama

12.7 PII06 - Politika upravljanja pravima ispitanika

12.8 PII07 - Politika procjene rizika za privatnost i DPIA

12.9 PII08 - Politika ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama

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

12.11 PII10 - Politika zadržavanja, brisanja i zbrinjavanja PII

12.12 PII11 - Politika točnosti i kvalitete PII

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

12.14 PII13 - Politika međunarodnog prijenosa PII

12.15 PII14 - Politika sigurnosti PII i kontrole pristupa

12.16 PII15 - Politika upravljanja incidentima i povredama PII

12.17 PII16 - Politika obuke, podizanja svijesti i kompetencija u području privatnosti

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

13. Referentni standardi i okviri

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Mapirano na održavanje Izjave o primjenjivosti PIMS-a, zapisa o primjenjivosti kontrola i povezivanja politike s dokazima. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Mapirano na identifikaciju dokumentiranih informacija, odobravanje, upravljanje verzijama, pristup, dohvat, očuvanje, povlačenje, povezivanje verzija prijevoda i metapodatke o zadržavanju. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Mapirano na dokaze operativnog planiranja i kontrole za zapise o obradi, predloške dokaza, kvalitetu operativnih dokaza i dokaze koje dostavljaju vanjske strane. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Mapirano na održavanje dokumentiranih dokaza o mjerenju, učinkovitosti dohvata, prazninama u dokazima, nepodudarnostima prijevoda i dovršetku pregleda pristupa repozitoriju. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Mapirano na dohvat revizijskih dokaza, revizijsko uzorkovanje, sljedivost revizijskih dokaza i revizijske nalaze povezane s kontrolom dokumentiranih informacija. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Mapirano na dokaze preispitivanja od strane uprave, razmatranje kontrole dokumentiranih informacija tijekom preispitivanja od strane uprave i pregled učinkovitosti kontrole dokaza koji provodi Top Management. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Mapirano na nesukladnosti dokumentiranih informacija, korektivne radnje, postupanje s iznimkama, zatvaranje i provjeru djelotvornosti. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Mapirano na zapise voditelja obrade o obradi, zapise odgovornosti, kvalitetu dokaza o obradi i zadržavanje dokaza koji podupiru obveze voditelja obrade. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Mapirano na ugovor s izvršiteljem obrade, upute klijenta, dokaze koje dostavljaju vanjske strane i kontrolu dokaza o odnosu s izvršiteljem obrade. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Mapirano na zaštitu zapisa PIMS-a od gubitka, neovlaštene izmjene, neovlaštenog pristupa, neovlaštenog ustupanja i neprimjerenog zbrinjavanja. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapirano na dokaze o odgovornosti, sljedivost dokaza, dohvat dokaza, zapise o nesukladnosti i zapise spremne za reviziju kojima se dokazuje usklađenost. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Mapirano na dokaze upravljanja za voditelja obrade, zapise odobrenja, kontrolu politika, mjere odgovornosti, dokumentirani pregled i nadzor koji provodi Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Mapirano na dokumentaciju izvršitelja obrade i podizvršitelja obrade, dokaze o uputama klijenta, dokaze o postupku koje dostavljaju vanjske strane i kontrolu otkrivanja dokaza. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Mapirano na dokaze zapisa o obradi, zahtjeve kvalitete dokaza, reference aktivnosti obrade i metapodatke o vlasniku/statusu dokaza o obradi. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Mapirano na zaštitu repozitorija dokaza, ograničenja pristupa, odobrenja pristupa, pregled zaštite repozitorija i uklanjanje neovlaštenog pristupa. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapirano na dokaze usklađenosti privatnosti, dohvat revizijskih dokaza, sljedivost dokaza, podršku neovisnom pregledu i dokaze o korektivnim radnjama. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Mapirano na zaštitu zapisa povezanih s PII, očuvanje zapisa te kontrole pristupa i brisanja za repozitorij dokaza. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Mapirano na identifikaciju dokumentiranih informacija, odobravanje, dostupnost, zaštitu, upravljanje verzijama, zadržavanje, raspolaganje i kontrolu dokumentiranih informacija koje se zahtijevaju izvana. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Mapirano na zaštitu zapisa PIMS-a od gubitka, uništenja, krivotvorenja, neovlaštenog pristupa, neovlaštenog ustupanja i neprimjerenog zbrinjavanja. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Mapirano na zaštitu privatnosti i PII u dokumentiranim informacijama, repozitorijima dokaza, otkrivanjima i zapisima s kontroliranim pristupom. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].