					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII02					Naziv dokumenta: **Politika uloga, odgovornosti i dokazive odgovornosti za privatnost**							
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 4.1	Both	Primary	Kontekst PIMS uloge
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Vodstvo i dokaziva odgovornost
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	PIMS uloge, odgovornosti i ovlasti
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetentnost uloge
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Svijest o ulozi
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Komunikacija o ulozi
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentirane informacije o ulozi
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Vlasništvo nad operativnim kontrolama
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Uloga neovisne revizije
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Preispitivanje dokazive odgovornosti od strane uprave
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Nesukladnost i korektivna radnja povezane s ulogom
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Odgovornost za ugovor s izvršiteljem obrade
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Uloge i odgovornosti zajedničkih voditelja obrade
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Zapisi za dokazivanje odgovornosti
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Ugovori s korisnicima i upute za izvršitelja obrade

ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Usklađenost svrhe izvršitelja obrade
GDPR	Article 5(2)	Controller	Supporting	Dokazi o odgovornosti
GDPR	Article 24	Controller	Supporting	Odgovornost voditelja obrade i mjere
GDPR	Article 26	Joint Controller	Supporting	Aranžmani zajedničkih voditelja obrade
GDPR	Article 28	Both	Supporting	Upravljanje izvršiteljima obrade i upute
GDPR	Article 30	Both	Supporting	Zapisi o obradi i dokazi o odgovornosti
GDPR	Article 37	Conditional	Referenced	Imenovanje DPO-a gdje je primjenjivo
GDPR	Article 38	Conditional	Supporting	Položaj i neovisnost DPO-a gdje je primjenjivo
GDPR	Article 39	Conditional	Supporting	Zadaće DPO-a gdje je primjenjivo
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Akteri i uloge okvira privatnosti
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Odgovornost za usklađenost privatnosti
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Uloge za zaštitu PII i razdvajanje dužnosti
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Uloge i odgovornosti informacijske sigurnosti
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Razdvajanje dužnosti

1. Opseg

1.1 Ova politika definira model PIMS uloga, strukturu dokazive odgovornosti, pravila dodjele odgovornosti, pravila kombiniranja uloga, očekivanja u vezi s eskalacijom i zahtjeve za dokaze za upravljanje privatnošću.

1.2 Ova politika primjenjuje se na osoblje, funkcije, sustave, dobavljače, izvršitelje obrade, podizvršitelje obrade i odnose zajedničkih voditelja obrade koji sudjeluju u obradi PII ili utječu na nju unutar opsega 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 nove organizacijske nazive radnih mjesta. Ona definira kanonske PIMS uloge koje se mogu dodijeliti postojećem osoblju ili funkcijama, pod uvjetom da su dodjela uloga, kompetentnost, neovisnost i zahtjevi u vezi sa sukobom interesa dokumentirani.

2. Svrha

2.1 Svrha ove politike jest osigurati da su PIMS odgovornosti jasno dodijeljene, shvaćene, komunicirane, potkrijepljene dokazima, pregledane i poboljšavane.

2.2 Ova politika omogućuje organizaciji da dokaže odgovornost za upravljanje privatnošću, vlasništvo nad obradom PII, utvrđivanje uloga voditelja obrade i izvršitelja obrade, raspodjelu odgovornosti zajedničkih voditelja obrade, postupanje s uputama za izvršitelje obrade, odgovornost dobavljača za privatnost, neovisni pregled i eskalaciju temeljenu na ulogama.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

3.1.1 definirati kanonske PIMS uloge koje se koriste u cijelom skupu PIMS politika;

3.1.2 osigurati da svaka značajna PIMS odgovornost ima dodijeljenu odgovornu ulogu;

3.1.3 podržati odgovornost voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade;

3.1.4 omogućiti praktično kombiniranje uloga za male i srednje organizacije uz kontrolu sukoba interesa;

3.1.5 očuvati neovisni pregled koji provodi Internal Audit / Compliance Reviewer;

3.1.6 osigurati da se dodjele uloga i promjene uloga evidentiraju u kanonskim objektima dokaza;

3.1.7 osigurati da nositelji PIMS uloga prime odgovarajuću komunikaciju i podizanje svijesti;

3.1.8 osigurati da se praznine, sukobi i nesukladnosti povezani s ulogama eskaliraju i isprave.

4. Izjave politike

4.1 Model i dodjela PIMS uloga

4.1.1 [All] Top Management mora odobriti kanonski model PIMS uloga u REG01 prije početne implementacije PIMS-a i zatim jednom godišnje.

4.1.2 [All] Privacy Lead / PIMS Manager mora održavati imenovane dodjele PIMS uloga u REG01 prije implementacije PIMS-a i u roku od 10 radnih dana od promjena osoblja ili organizacijskih promjena.

4.1.3 [All] Privacy Lead / PIMS Manager mora dokumentirati opseg odgovornosti i razinu ovlasti za svaku dodijeljenu PIMS ulogu u REG01 prije nego što dodjela stupi na snagu.

4.1.4 [All] Process Owner / Business Owner mora dodijeliti odgovornog vlasnika aktivnosti obrade za svaku aktivnost obrade PII u REG02 prije početka aktivnosti obrade.

4.1.5 [All] System Owner / Application Owner mora dokumentirati odgovornog vlasnika sustava za svaki sustav koji obrađuje PII u REG02 prije puštanja sustava u produkcijski rad.

4.1.6 [All] Vendor / Procurement Owner mora dokumentirati vlasnika odnosa za svakog izvršitelja obrade, podizvršitelja obrade, dijeljenje podataka s trećom stranom ili odnos zajedničkog voditelja obrade u REG08 prije uvođenja ili odobrenja ugovora.

4.2 Kombiniranje uloga, razdvajanje i neovisnost

4.2.1 [All] Privacy Lead / PIMS Manager mora dokumentirati svaku kombinaciju PIMS uloga u REG01 prije nego što kombinacija uloga stupi na snagu.

4.2.2 [All] Top Management mora odobriti kombinacije uloga koje uključuju Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator ili Internal Audit / Compliance Reviewer u REG01 prije dodjele.

4.2.3 [All] Internal Audit / Compliance Reviewer mora dokumentirati neovisnost od PIMS procesa koji se pregledava u REG12 prije početka svake PIMS revizije ili pregleda usklađenosti.

4.2.4 [All] Privacy Lead / PIMS Manager mora evidentirati kompenzacijske kontrole za neizbježne sukobe razdvajanja dužnosti u REG12 prije odobrenja kombinacije uloga.

4.2.5 [All] Data Protection Officer / Privacy Advisor mora evidentirati pitanja u vezi s neovisnošću uloge ili pitanja u vezi sa sukobom interesa u REG12 u roku od pet radnih dana od utvrđivanja.

[... 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 iznimku od odgovornosti uloge u REG12 prije rada aktivnosti obrade PII bez potrebne dodijeljene uloge.

9.1.2 [All] Privacy Lead / PIMS Manager mora procijeniti učinak i ublažavanje svake iznimke od odgovornosti uloge u REG12 u roku od 10 radnih dana od zahtjeva.

9.1.3 [All] Top Management mora odobriti iznimke od odgovornosti uloge koje premašuju 30 dana ili utječu na obradu visokog rizika u REG12 prije nego što iznimka stupi na snagu.

9.1.4 [All] Privacy Lead / PIMS Manager mora za svaku odobrenu iznimku od odgovornosti uloge prije odobrenja odrediti datum isteka koji ne premašuje 90 dana u REG12.

9.1.5 [All] Privacy Lead / PIMS Manager mora zatvoriti ili ponovno procijeniti svaku iznimku od odgovornosti uloge u REG12 u roku od pet radnih dana od isteka.

10. Provedba

10.1.1 [All] Privacy Lead / PIMS Manager mora evidentirati nedostajuće, netočne ili zastarjele dodjele PIMS uloga kao nesukladnosti u REG12 u roku od pet radnih dana od utvrđivanja.

10.1.2 [All] Top Management mora zahtijevati korektivnu radnju u REG12 u roku od 15 radnih dana za ponovljene ili produljene neuspjehe u odgovornosti.

10.1.3 [All] Process Owner / Business Owner mora spriječiti puštanje u produkcijski rad nove ili izmijenjene obrade PII ako u REG02 ili REG08 nedostaju potrebni dokazi o ulozi i odgovornosti.

10.1.4 [All] Internal Audit / Compliance Reviewer mora provjeriti djelotvornost korektivnih radnji za nesukladnosti povezane s odgovornošću uloga 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 modela PIMS uloga.

11.1.2 [All] Data Protection Officer / Privacy Advisor mora pregledati predložene izmjene ove politike u pogledu utjecaja na uloge privatnosti u REG12 prije odobrenja.

11.1.3 [All] Top Management mora odobriti značajne izmjene ove politike u REG12 prije objave.

11.1.4 [All] Privacy Lead / PIMS Manager mora ažurirati REG01 i REG11 u roku od 15 radnih dana nakon odobrenih izmjena PIMS uloga, odgovornosti ili komunikacijskih zahtjeva.

12. Povezane politike

12.1 Ovu politiku podržavaju sljedeće povezane politike:

12.2 PII01 - Politika sustava upravljanja informacijama o privatnosti

12.3 PII03 - Politika popisa obrade PII i pravne osnove

12.4 PII07 - Politika procjene rizika za privatnost i DPIA

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

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

12.7 PII14 - Politika sigurnosti PII i kontrole pristupa

12.8 PII15 - Politika upravljanja incidentima i povredama PII

12.9 PII16 - Politika osposobljavanja, podizanja svijesti i kompetentnosti za privatnost

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

12.11 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 podržava navedene zahtjeve i identificira interne točke koje ih provode ili podržavaju.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Mapirano na utvrđivanje konteksta PIMS uloga, primjenjivosti voditelja obrade i izvršitelja obrade, vlasništva nad obradom i zapisa o odgovornosti za odnose. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Mapirano na odobrenje Top Management, nadzor odgovornosti, godišnje preispitivanje od strane uprave, metrike odgovornosti i korektivne radnje za neuspjehe uloga. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Mapirano na dodjelu, dokumentiranje, komunikaciju i održavanje PIMS uloga, odgovornosti, ovlasti, vlasništva nad sustavima, vlasništva nad obradom, vlasništva nad odnosima s dobavljačima, vlasništva nad eskalacijom incidenata i odgovornosti za neovisni pregled. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Mapirano na dokaze o kompetentnosti i svijesti specifične za ulogu za dodijeljene PIMS odgovornosti. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Mapirano na svijest o dodijeljenim PIMS odgovornostima, dokaze o potvrdi prihvaćanja i godišnje izvješćivanje o svijesti o ulozi. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Mapirano na komunikaciju dodjele uloga, promjena uloga, eskalacija i informacija o primopredaji uloga. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Mapirano na dokumentirane informacije za dodjele PIMS uloga, opsege odgovornosti, razine ovlasti, godišnje zadržavanje dokaza i održavanje matrice uloga. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Mapirano na vlasništvo nad operativnim kontrolama za aktivnosti obrade, sustave, dobavljače, izvršitelje obrade, podizvršitelje obrade, odnose zajedničkih voditelja obrade i kontrole puštanja u produkcijski rad. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Mapirano na neovisnu reviziju i pregled usklađenosti dokaza o dodjeli uloga, dokaza o kombiniranju uloga, dokaza o neovisnosti, nalaza i zatvaranja korektivnih radnji. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Mapirano na preispitivanje potpunosti dodjele PIMS uloga, sukoba uloga, iznimaka, metrika odgovornosti i rezultata pregleda odgovornosti od strane uprave. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Mapirano na eskalaciju, evidentiranje nesukladnosti, korektivne radnje, zatvaranje iznimaka i provjeru djelotvornosti za pitanja odgovornosti uloga. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Mapirano na dodjelu i dokumentiranje odgovornosti za ugovor s izvršiteljem obrade i eskalaciju odgovornosti trećih strana prije odobrenja ili obnove ugovora. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Mapirano na dokumentiranje raspodjele odgovornosti zajedničkih voditelja obrade i dokaza o odgovornosti za odnos prije početka obrade u svojstvu zajedničkog voditelja obrade. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Mapirano na održavanje zapisa za dokazivanje odgovornosti za vlasništvo nad obradom u svojstvu voditelja obrade, klasifikaciju uloga i vlasništvo nad dokazima. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Mapirano na odgovornost za korisnički ugovor izvršitelja obrade, vlasništvo nad uputama korisnika i dokaze o odnosu s izvršiteljem obrade. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Mapirano na usklađivanje svrhe i uputa izvršitelja obrade putem vlasništva nad uputama korisnika i provjere uloga voditelja obrade/izvršitelja obrade. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapirano na dokaze o odgovornosti za dodjele uloga, vlasništvo nad obradom, preglede uloga, nesukladnosti i nalaze revizije. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mapirano na odgovornost voditelja obrade, odgovorno vlasništvo nad obradom, nadzor Top Management, godišnji pregled i mjere odgovornosti. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Mapirano na dokumentiranje raspodjele odgovornosti zajedničkih voditelja obrade i dokaza o odgovornosti za odnos prije početka obrade u svojstvu zajedničkog voditelja obrade. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Mapirano na raspodjelu odgovornosti izvršitelja obrade i podizvršitelja obrade, vlasništvo nad uputama korisnika, odgovornost za ugovor i putove eskalacije trećih strana. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Mapirano na zapise o obradi, vlasništvo nad obradom, klasifikaciju PIMS uloga i provjeru uloga voditelja obrade/izvršitelja obrade. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Mapirano na dokumentiranje uloge Data Protection Officer / Privacy Advisor kada je imenovanje primjenjivo ili dobrovoljno dodijeljeno. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Mapirano na položaj, neovisnost, uključenost i postupanje sa sukobom interesa za Data Protection Officer / Privacy Advisor gdje je primjenjivo. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Mapirano na savjet o privatnosti, opažanja iz praćenja, savjetodavni pregled i pregled utjecaja na privatnost povezan s ulogom koji provodi Data Protection Officer / Privacy Advisor gdje je primjenjivo. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Mapirano na aktere okvira privatnosti i raspodjelu uloga za ispitanike, voditelje obrade PII, izvršitelje obrade PII, treće strane i klasifikaciju PIMS uloga. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Mapirano na odgovornost za usklađenost privatnosti, dokaze o ulogama, pregled, nalaze revizije i provjeru korektivnih radnji. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Mapirano na definiciju uloga za zaštitu PII, dokumentiranje uloga, komunikaciju o ulogama, koordinaciju sigurnosti/privatnosti i razdvajanje dužnosti za zaštitu PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Mapirano na definiranje, dodjelu, dokumentiranje, komunikaciju i održavanje PIMS odgovornosti i odgovornosti informacijske sigurnosti. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Mapirano na razdvajanje dužnosti, odobrenje kombiniranja uloga, neovisni pregled, kontrole sukoba interesa i provjeru korektivnih radnji za sukobe uloga. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].