					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII02					Naslov dokumenta: **Politika vlog, odgovornosti in dokazljive odgovornosti na področju zasebnosti**							
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	Točka/kontrola/člen	Uporabljivost	Vrsta pokritosti	Komentar
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Kontekst vlog PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Voditeljstvo in dokazljiva odgovornost
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Vloge, odgovornosti in pooblastila PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Usposobljenost za vlogo
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Ozaveščenost o vlogi
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Komuniciranje o vlogah
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentirane informacije o vlogah
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Lastništvo operativnih kontrol
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Vloga neodvisne presoje
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Vodstveni pregled dokazljive odgovornosti
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Neskladnost in korektivni ukrep, povezan z vlogami
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Odgovornost za pogodbo z obdelovalcem
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Vloge in odgovornosti skupnih upravljavcev
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Evidence dokazljive odgovornosti
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Dogovori s strankami in navodila za obdelovalca

ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Usklajenost namena obdelovalca
GDPR	Article 5(2)	Controller	Supporting	Dokazila o dokazljivi odgovornosti
GDPR	Article 24	Controller	Supporting	Odgovornost upravljavca in ukrepi
GDPR	Article 26	Joint Controller	Supporting	Dogovori skupnih upravljavcev
GDPR	Article 28	Both	Supporting	Upravljanje obdelovalcev in navodila
GDPR	Article 30	Both	Supporting	Evidence dejavnosti obdelave in dokazila o odgovornosti
GDPR	Article 37	Conditional	Referenced	Imenovanje DPO, kadar je ustrezno
GDPR	Article 38	Conditional	Supporting	Položaj in neodvisnost DPO, kadar je ustrezno
GDPR	Article 39	Conditional	Supporting	Naloge DPO, kadar je ustrezno
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Akterji in vloge okvira zasebnosti
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Odgovornost za skladnost zasebnosti
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Vloge za varstvo PII in ločevanje dolžnosti
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Vloge in odgovornosti informacijske varnosti
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Ločevanje dolžnosti

1. Področje uporabe

1.1 Ta politika določa model vlog PIMS, strukturo dokazljive odgovornosti, pravila dodeljevanja odgovornosti, pravila združevanja vlog, pričakovanja glede eskalacije in zahteve glede dokazil za upravljanje zasebnosti.

1.2 Ta politika se uporablja za osebje, funkcije, sisteme, dobavitelje, obdelovalce, podobdelovalce in razmerja skupnih upravljavcev, ki sodelujejo pri obdelavi PII v obsegu PIMS ali nanjo vplivajo.

1.3 Ta politika se uporablja v kontekstih upravljavca, skupnega upravljavca, obdelovalca in podobdelovalca.

1.4 Ta politika ne ustvarja novih organizacijskih nazivov delovnih mest. Določa kanonične vloge PIMS, ki se lahko dodelijo obstoječemu osebju ali funkcijam, če so zahteve glede dodelitve vlog, usposobljenosti, neodvisnosti in nasprotja interesov dokumentirane.

2. Namen

2.1 Namen te politike je zagotoviti, da so odgovornosti PIMS jasno dodeljene, razumljene, sporočene, podprte z dokazili, pregledane in izboljševane.

2.2 Ta politika organizaciji omogoča dokazovanje odgovornosti za upravljanje zasebnosti, lastništvo obdelave PII, določitev vlog upravljavca in obdelovalca, razporeditev odgovornosti skupnih upravljavcev, obravnavo navodil za obdelovalca, odgovornost dobaviteljev za zasebnost, neodvisni pregled in eskalacijo na podlagi vlog.

3. Cilji

3.1 Cilji te politike so:

3.1.1 opredeliti kanonične vloge PIMS, ki se uporabljajo v celotnem naboru politik PIMS;

3.1.2 zagotoviti, da ima vsaka bistvena odgovornost PIMS dodeljeno odgovorno vlogo;

3.1.3 podpirati odgovornost upravljavca, skupnega upravljavca, obdelovalca in podobdelovalca;

3.1.4 omogočiti praktično združevanje vlog v malih in srednje velikih organizacijah ob obvladovanju nasprotij interesov;

3.1.5 ohraniti neodvisni pregled, ki ga izvaja Internal Audit / Compliance Reviewer;

3.1.6 zagotoviti, da so dodelitve vlog in spremembe vlog evidentirane v kanoničnih dokaznih objektih;

3.1.7 zagotoviti, da nosilci vlog PIMS prejmejo ustrezno komuniciranje in ozaveščanje;

3.1.8 zagotoviti, da se vrzeli, konflikti in neskladnosti, povezani z vlogami, eskalirajo in odpravijo.

4. Izjave politike

4.1 Model vlog PIMS in dodelitev

4.1.1 [All] Top Management mora odobriti kanonični model vlog PIMS v REG01 pred začetno implementacijo PIMS in nato vsako leto.

4.1.2 [All] Privacy Lead / PIMS Manager mora vzdrževati poimenske dodelitve vlog PIMS v REG01 pred implementacijo PIMS in v 10 delovnih dneh po kadrovskih ali organizacijskih spremembah.

4.1.3 [All] Privacy Lead / PIMS Manager mora dokumentirati obseg odgovornosti in raven pooblastil za vsako dodeljeno vlogo PIMS v REG01, preden dodelitev začne učinkovati.

4.1.4 [All] Process Owner / Business Owner mora dodeliti odgovornega lastnika obdelave za vsako dejavnost obdelave PII v REG02, preden se dejavnost obdelave začne.

4.1.5 [All] System Owner / Application Owner mora dokumentirati odgovornega lastnika sistema za vsak sistem, ki obdeluje PII, v REG02 pred prehodom sistema v produkcijo.

4.1.6 [All] Vendor / Procurement Owner mora dokumentirati lastnika razmerja za vsako razmerje z obdelovalcem, podobdelovalcem, tretjo osebo pri delitvi podatkov ali skupnim upravljavcem v REG08 pred uvajanjem ali odobritvijo dogovora.

4.2 Združevanje vlog, ločevanje in neodvisnost

4.2.1 [All] Privacy Lead / PIMS Manager mora dokumentirati vsako združevanje vlog PIMS v REG01, preden združevanje vlog začne učinkovati.

4.2.2 [All] Top Management mora v REG01 pred dodelitvijo odobriti združevanja vlog, ki vključujejo Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator ali Internal Audit / Compliance Reviewer.

4.2.3 [All] Internal Audit / Compliance Reviewer mora v REG12 dokumentirati neodvisnost od procesa PIMS, ki je predmet pregleda, preden se začne vsaka presoja PIMS ali pregled skladnosti.

4.2.4 [All] Privacy Lead / PIMS Manager mora evidentirati kompenzacijske kontrole za neizogibna nasprotja pri ločevanju dolžnosti v REG12 pred odobritvijo združevanja vlog.

4.2.5 [All] Data Protection Officer / Privacy Advisor mora pomisleke glede neodvisnosti vloge ali nasprotja interesov evidentirati v REG12 v petih delovnih dneh po ugotovitvi.

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

9. Izjeme

9.1.1 [All] Process Owner / Business Owner mora zahtevati izjemo glede odgovornosti vlog v REG12, preden izvaja dejavnost obdelave PII brez zahtevane dodeljene vloge.

9.1.2 [All] Privacy Lead / PIMS Manager mora oceniti vpliv in ublažitev vsake izjeme glede odgovornosti vlog v REG12 v 10 delovnih dneh po zahtevi.

9.1.3 [All] Top Management mora v REG12 odobriti izjeme glede odgovornosti vlog, ki presegajo 30 dni ali vplivajo na visoko tvegano obdelavo, preden izjema začne učinkovati.

9.1.4 [All] Privacy Lead / PIMS Manager mora pred odobritvijo za vsako odobreno izjemo glede odgovornosti vlog v REG12 določiti datum poteka, ki ne presega 90 dni.

9.1.5 [All] Privacy Lead / PIMS Manager mora vsako izjemo glede odgovornosti vlog zapreti ali ponovno oceniti v REG12 v petih delovnih dneh po poteku.

10. Uveljavljanje

10.1.1 [All] Privacy Lead / PIMS Manager mora manjkajoče, netočne ali zastarele dodelitve vlog PIMS evidentirati kot neskladnosti v REG12 v petih delovnih dneh po ugotovitvi.

10.1.2 [All] Top Management mora za ponavljajoče se ali dolgotrajne napake pri odgovornosti zahtevati korektivni ukrep v REG12 v 15 delovnih dneh.

10.1.3 [All] Process Owner / Business Owner mora preprečiti prehod v produkcijo nove ali spremenjene obdelave PII, kadar zahtevana dokazila o vlogah in odgovornosti niso prisotna v REG02 ali REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer mora preveriti učinkovitost korektivnih ukrepov za neskladnosti glede odgovornosti vlog v REG12 ob naslednji načrtovani presoji ali v 60 dneh po zaprtju, kar nastopi prej.

11. Pregled in vzdrževanje

11.1.1 [All] Privacy Lead / PIMS Manager mora to politiko pregledati letno in v 30 dneh po bistveni spremembi modela vlog PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor mora pred odobritvijo pregledati predlagane spremembe te politike glede vpliva na vloge zasebnosti v REG12.

11.1.3 [All] Top Management mora bistvene spremembe te politike odobriti v REG12 pred objavo.

11.1.4 [All] Privacy Lead / PIMS Manager mora posodobiti REG01 in REG11 v 15 delovnih dneh po odobrenih spremembah vlog PIMS, odgovornosti ali komunikacijskih zahtev.

12. Povezane politike

12.1 To politiko podpirajo naslednje povezane politike:

12.2 PII01 - Politika sistema upravljanja informacij o zasebnosti

12.3 PII03 - Politika evidence obdelave PII in pravne podlage

12.4 PII07 - Politika ocene tveganj za zasebnost in DPIA

12.5 PII08 - Politika vgrajenega in privzetega varstva zasebnosti

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

12.7 PII14 - Politika varnosti PII in nadzora dostopa

12.8 PII15 - Politika upravljanja incidentov in kršitev PII

12.9 PII16 - Politika usposabljanja, ozaveščanja in usposobljenosti za zasebnost

12.10 PII17 - Politika dokumentiranih informacij in upravljanja dokazil PIMS

12.11 PII18 - Politika spremljanja, presoje in izboljševanja PIMS

13. Referenčni standardi in okviri

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Preslikano na določanje konteksta vlog PIMS, uporabljivosti za upravljavca in obdelovalca, lastništva obdelave ter evidenc odgovornosti za razmerja. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Preslikano na odobritev Top Management, nadzor odgovornosti, letni vodstveni pregled, kazalnike odgovornosti in korektivne ukrepe za napake vlog. 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** - Preslikano na dodelitev, dokumentiranje, komuniciranje in vzdrževanje vlog, odgovornosti in pooblastil PIMS, lastništva sistemov, lastništva obdelave, lastništva razmerij z dobavitelji, lastništva eskalacije incidentov in odgovornosti za neodvisni 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** - Preslikano na dokazila o vlogi prilagojeni usposobljenosti in ozaveščenosti za dodeljene odgovornosti PIMS. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Preslikano na ozaveščenost o dodeljenih odgovornostih PIMS, dokazila o potrditvi in letno poročanje o ozaveščenosti glede vlog. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Preslikano na komuniciranje dodelitev vlog, sprememb vlog, eskalacij in informacij o primopredaji vlog. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Preslikano na dokumentirane informacije za dodelitve vlog PIMS, obsege odgovornosti, ravni pooblastil, letno hrambo dokazil in vzdrževanje matrice vlog. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Preslikano na lastništvo operativnih kontrol za dejavnosti obdelave, sisteme, dobavitelje, obdelovalce, podobdelovalce, razmerja skupnih upravljavcev in kontrole prehoda v produkcijo. 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** - Preslikano na neodvisno presojo in pregled skladnosti dokazil o dodelitvi vlog, dokazil o združevanju vlog, dokazil o neodvisnosti, ugotovitev in zapiranja korektivnih ukrepov. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Preslikano na vodstveni pregled popolnosti dodelitve vlog PIMS, konfliktov vlog, izjem, kazalnikov odgovornosti in rezultatov pregleda odgovornosti. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Preslikano na eskalacijo, evidentiranje neskladnosti, korektivne ukrepe, zapiranje izjem in preverjanje učinkovitosti za vprašanja odgovornosti vlog. 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** - Preslikano na dodelitev in dokumentiranje odgovornosti za pogodbo z obdelovalcem ter eskalacijo odgovornosti tretjih oseb pred odobritvijo ali podaljšanjem pogodbe. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Preslikano na dokumentiranje razporeditve odgovornosti skupnih upravljavcev in dokazil o odgovornosti za razmerje pred začetkom obdelave v vlogi skupnega upravljavca. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Preslikano na vzdrževanje evidenc odgovornosti za lastništvo obdelave pri upravljavcu, razvrstitev vlog in lastništvo dokazil. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Preslikano na odgovornost za pogodbe s strankami obdelovalca, lastništvo navodil strank in dokazila o razmerju z obdelovalcem. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Preslikano na uskladitev namena in navodil obdelovalca prek lastništva navodil stranke in preverjanja vlog upravljavca/obdelovalca. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Preslikano na dokazila o odgovornosti za dodelitve vlog, lastništvo obdelave, preglede vlog, neskladnosti in ugotovitve presoje. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Preslikano na odgovornost upravljavca, odgovorno lastništvo obdelave, nadzor Top Management, letni pregled in ukrepe odgovornosti. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Preslikano na dokumentiranje razporeditve odgovornosti skupnih upravljavcev in dokazil o odgovornosti za razmerje pred začetkom obdelave v vlogi skupnega upravljavca. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Preslikano na razporeditev odgovornosti obdelovalca in podobdelovalca, lastništvo navodil stranke, odgovornost za pogodbo in eskalacijske poti tretjih oseb. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Preslikano na evidence dejavnosti obdelave, lastništvo obdelave, razvrstitev vlog PIMS in preverjanje vlog upravljavca/obdelovalca. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Preslikano na dokumentiranje vloge Data Protection Officer / Privacy Advisor, kadar je imenovanje ustrezno ali prostovoljno dodeljeno. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Preslikano na položaj, neodvisnost, vključenost in obravnavo nasprotij interesov vloge Data Protection Officer / Privacy Advisor, kadar je ustrezno. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Preslikano na nasvete glede zasebnosti, opažanja spremljanja, svetovalni pregled in pregled vpliva na zasebnost, povezan z vlogami, ki ga izvaja Data Protection Officer / Privacy Advisor, kadar je ustrezno. 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** - Preslikano na akterje okvira zasebnosti in dodelitev vlog za posameznike, na katere se nanašajo PII, upravljavce PII, obdelovalce PII, tretje osebe in razvrstitev vlog PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Preslikano na odgovornost za skladnost zasebnosti, dokazila o vlogah, pregled, ugotovitve presoje in preverjanje korektivnih ukrepov. 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** - Preslikano na opredelitev vlog za varstvo PII, dokumentiranje vlog, komuniciranje vlog, usklajevanje varnosti in zasebnosti ter ločevanje dolžnosti za varstvo 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 - Preslikano na opredelitev, dodelitev, dokumentiranje, komuniciranje in vzdrževanje odgovornosti PIMS in informacijske varnosti. 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 - Preslikano na ločevanje dolžnosti, odobritev združevanja vlog, neodvisni pregled, kontrole konfliktov in preverjanje korektivnih ukrepov za konflikte vlog. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].