					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII17					Naslov dokumenta: **Politika upravljanja dokumentiranih informacij in dokazil PIMS**							
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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Dokumentirane informacije SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentirane informacije PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Nadzor operativnih dokazil
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Dokazila o spremljanju
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Revizijski dokazi
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Dokazila o pregledu vodstva
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Dokazila o neskladnostih in korektivnih ukrepih
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Evidence dejavnosti obdelave upravljavca
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Dokazila o pogodbi in navodilih obdelovalca
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Varovanje evidenc
GDPR	Article 5(2)	Controller	Supporting	Dokazila o odgovornosti
GDPR	Article 24	Controller	Supporting	Ukrepi in dokazila upravljavca
GDPR	Article 28	Both	Supporting	Dokumentacija obdelovalca
GDPR	Article 30	Both	Supporting	Evidence dejavnosti obdelave
GDPR	Article 32	Both	Supporting	Varovanje dokazil
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Dokazila o skladnosti na področju zasebnosti
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Varovanje evidenc

ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Nadzor dokumentiranih informacij
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Varovanje evidenc
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Varstvo zasebnosti in PII

1. Področje uporabe

1.1 Ta politika določa obvezne zahteve za ustvarjanje, odobritev, nadzor različic, varovanje, hrambo, pridobivanje, prevajanje, umik in dokazovanje PIMS dokumentiranih informacij.

1.2 Ta politika se uporablja za politike PIMS, registre, dokumentirane odobritve, evidence dokazil, revizijske dokaze, zapise pregledov vodstva, dokazila o korektivnih ukrepih in nadzorovane prevode, ki se uporabljajo za dokazovanje skladnosti PIMS.

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

1.4 Ta politika ne vzpostavlja ločenega registra za nadzor dokumentov. Dokazila o nadzoru dokumentiranih informacij se vodijo prek kanoničnih dokaznih objektov PIMS REG01 do REG12, pri čemer se REG03 in REG12 uporabljata za dokazila o uporabljivosti kontrol, presoji, neskladnostih, korektivnih ukrepih in izboljšavah.

2. Namen

2.1 Namen te politike je zagotoviti, da so PIMS dokumentirane informacije točne, nadzorovane, dostopne pooblaščenim uporabnikom, zaščitene pred nepooblaščeno spremembo ali razkritjem, hranjene za potrebe preverljivosti ter umaknjene, ko zastarajo.

2.2 Ta politika podpira pripravljenost na certifikacijo z zagotavljanjem, da je dokazila, potrebna za dokazovanje skladnosti PIMS, mogoče najti, preveriti, pridobiti in povezati z veljavnimi politikami, kontrolami, dejavnostmi obdelave, tveganji, presojami in korektivnimi ukrepi.

3. Cilji

3.1 Cilji te politike so:

3.1.1 določiti zahteve za nadzor PIMS dokumentiranih informacij;

3.1.2 vzdrževati celovitost dokazov v REG01 do REG12;

3.1.3 zagotoviti sledljivost odobritev politik in dokazil;

3.1.4 zagotoviti dokumentiranje evidence različic in odločitev o umiku;

3.1.5 povezati dokazila PIMS z Izjavo o uporabnosti in preslikavami politik;

3.1.6 nadzorovati dostop do dokumentov PIMS in evidenc dokazil;

3.1.7 podpirati nadzor različic večjezičnih politik in dokazil;

3.1.8 omogočiti pravočasno pridobivanje revizijskih dokazov;

3.1.9 preprečiti nepotrebno birokracijo pri nadzoru dokumentov;

3.1.10 ohraniti evidence, pripravljene za revizijo, za certifikacijo, zagotavljanje zaupanja naročnikov in nenehno izboljševanje.

4. Izjave politike

4.1 Nadzor PIMS dokumentiranih informacij

4.1.1 [All] Privacy Lead / PIMS Manager mora vzdrževati indeks PIMS dokumentiranih informacij v REG12 pred prvo objavo PIMS in nato četrtletno.

4.1.2 [All] Process Owner / Business Owner mora v REG02 opredeliti dokumentirane informacije, potrebne za vsako dejavnost obdelave PII, ki jo ima v lasti, pred začetkom dejavnosti obdelave in nato letno.

4.1.3 [All] Privacy Lead / PIMS Manager mora povezati veljavne politike PIMS, kontrole in obveznosti glede dokazil z REG03 pred vsako izdajo politike in v 15 delovnih dneh po vsaki bistveni spremembi uporabljivosti kontrol.

4.1.4 [All] Privacy Lead / PIMS Manager mora vsaki kategoriji PIMS dokumentiranih informacij v REG12 dodeliti raven dostopa in razvrstitev občutljivosti dokazil, preden se kategorija začne uporabljati.

4.2 Ustvarjanje, odobritev, nadzor različic in objava

4.2.1 [All] Privacy Lead / PIMS Manager mora dokumentiranim informacijam PIMS pred objavo v REG12 dodeliti identifikator dokumenta, lastnika, številko različice, status odobritve, datum začetka veljavnosti in datum pregleda.

4.2.2 [All] Top Management mora v REG12 odobriti temeljne politike PIMS in bistvene spremembe politik pred objavo.

4.2.3 [All] Privacy Lead / PIMS Manager mora v REG12 odobriti predloge dokazil PIMS ali vdelane razdelke registra pred operativno uporabo.

4.2.4 [All] Privacy Lead / PIMS Manager mora v REG12 evidentirati evidenco različic in utemeljitev spremembe pred izdajo posodobljenih PIMS dokumentiranih informacij.

4.2.5 [All] Privacy Lead / PIMS Manager mora v REG11 evidentirati obveščanje o odobrenih spremembah PIMS dokumentiranih informacij v 30 dneh od objave.

[... 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 v REG12 zahtevati izjeme glede dokumentiranih informacij ali nadzora dokazil pred odstopanjem od te politike.

9.1.2 [All] Privacy Lead / PIMS Manager mora v REG12 oceniti vsako izjemo glede dokumentiranih informacij ali nadzora dokazil v 10 delovnih dneh od zahteve.

9.1.3 [All] Data Protection Officer / Privacy Advisor mora v REG12 evidentirati nasvet pred odobritvijo katere koli izjeme, ki vključuje razkritje dokazil PII, prevajalsko neskladje, konflikt hrambe ali omejitev revizijskih dokazov.

9.1.4 [All] Top Management mora v REG12 odobriti izjeme glede dokumentiranih informacij, ki presegajo 30 dni ali vplivajo na certifikacijo, visoko tvegano obdelavo ali zunanje zagotavljanje zaupanja, preden izjema začne veljati.

9.1.5 [All] Privacy Lead / PIMS Manager mora za vsako odobreno izjemo glede dokumentiranih informacij ali nadzora dokazil v REG12 določiti datum poteka, ki ne presega 90 dni.

9.1.6 [All] Privacy Lead / PIMS Manager mora v REG12 zapreti ali ponovno oceniti vsako izjemo glede dokumentiranih informacij ali nadzora dokazil v petih delovnih dneh po poteku.

10. Uveljavljanje

10.1.1 [All] Privacy Lead / PIMS Manager mora manjkajoče, netočne, nenadzorovane, zastarele ali nepridobljive PIMS dokumentirane informacije evidentirati kot neskladnost v REG12 v petih delovnih dneh od ugotovitve.

10.1.2 [All] Privacy Lead / PIMS Manager mora preprečiti objavo PIMS dokumentiranih informacij, kadar v REG12 manjkajo zahtevana dokazila o odobritvi, različici, lastniku ali datumu začetka veljavnosti.

10.1.3 [All] Process Owner / Business Owner mora preprečiti predložitev dokazil o obdelavi za presojo, kadar v REG02 manjkajo zahtevana dokazila o lastniku, datumu, statusu ali odobritvi.

10.1.4 [All] System Owner / Application Owner mora odstraniti nepooblaščen dostop do repozitorijev PIMS dokumentiranih informacij in odstranitev evidentirati v REG12 v enem delovnem dnevu od ugotovitve.

10.1.5 [All] Internal Audit / Compliance Reviewer mora ob naslednji načrtovani presoji ali v 60 dneh od zaprtja, kar nastopi prej, v REG12 preveriti učinkovitost korektivnih ukrepov za neskladnosti dokumentiranih informacij.

11. Pregled in vzdrževanje

11.1.1 [All] Privacy Lead / PIMS Manager mora to politiko pregledati letno in v 30 dneh po bistveni spremembi zahtev glede PIMS dokumentiranih informacij.

11.1.2 [All] Privacy Lead / PIMS Manager mora to politiko pregledati v 30 dneh po pomembni revizijski ugotovitvi, certifikacijski neskladnosti, spremembi platforme repozitorija ali spremembi postopka večjezične objave.

11.1.3 [All] Data Protection Officer / Privacy Advisor mora v REG12 pred odobritvijo pregledati spremembe te politike, ki so pomembne z vidika zasebnosti.

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

11.1.5 [All] Privacy Lead / PIMS Manager mora v REG11 evidentirati obveščanje o odobrenih spremembah te politike v 30 dneh od objave.

12. Povezane politike

12.1 To politiko podpirajo naslednje povezane politike:

12.2 PII01 - Politika sistema upravljanja informacij o zasebnosti

12.3 PII02 - Politika vlog, odgovornosti in odgovornosti na področju zasebnosti

12.4 PII03 - Politika popisa obdelave PII in pravne podlage

12.5 PII04 - Politika obvestil o zasebnosti in preglednosti

12.6 PII05 - Politika upravljanja privolitev in preferenc

12.7 PII06 - Politika upravljanja pravic PII principal

12.8 PII07 - Politika ocenjevanja tveganj za zasebnost in DPIA

12.9 PII08 - Politika varstva zasebnosti že pri načrtovanju in privzetih nastavitvah

12.10 PII09 - Politika zbiranja, uporabe, razkritja in deljenja PII

12.11 PII10 - Politika hrambe, izbrisa in odstranjevanja PII

12.12 PII11 - Politika točnosti in kakovosti PII

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

12.14 PII13 - Politika mednarodnih prenosov PII

12.15 PII14 - Politika varnosti PII in nadzora dostopa

12.16 PII15 - Politika upravljanja incidentov in kršitev PII

12.17 PII16 - Politika usposabljanja, ozaveščanja in kompetenc na področju zasebnosti

12.18 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, in opredeljuje notranje klavzule, ki jih izvajajo ali podpirajo.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Preslikano na vzdrževanje Izjave o uporabnosti PIMS, evidenc uporabljivosti kontrol in povezav med politikami in dokazili. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Preslikano na identifikacijo dokumentiranih informacij, odobritev, nadzor različic, dostop, pridobivanje, ohranjanje, umik, povezavo prevodnih različic in metapodatke o hrambi. 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** - Preslikano na operativno načrtovanje in kontrolna dokazila za evidence dejavnosti obdelave, predloge dokazil, kakovost operativnih dokazil in zunanje zagotovljena dokazila. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Preslikano na vzdrževanje dokumentiranih dokazil o merjenju, učinkovitosti pridobivanja, vrzelih v dokazilih, neskladjih prevodov in dokončanju pregleda dostopa do repozitorija. 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** - Preslikano na pridobivanje revizijskih dokazov, revizijsko vzorčenje, sledljivost revizijskih dokazov in revizijske ugotovitve v zvezi z nadzorom dokumentiranih informacij. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Preslikano na dokazila o pregledu vodstva, obravnavo nadzora dokumentiranih informacij pri pregledu vodstva in pregled uspešnosti nadzora dokazil, ki ga izvede Top Management. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Preslikano na neskladnosti dokumentiranih informacij, korektivne ukrepe, obravnavo izjem, zapiranje in preverjanje učinkovitosti. 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** - Preslikano na evidence dejavnosti obdelave upravljavca, evidence odgovornosti, kakovost dokazil o obdelavi in hrambo dokazil, ki podpirajo obveznosti upravljavca. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Preslikano na pogodbo obdelovalca, navodilo naročnika, zunanje zagotovljena dokazila in nadzor dokazil o razmerju z obdelovalcem. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Preslikano na varovanje evidenc PIMS pred izgubo, nepooblaščeno spremembo, nepooblaščenim dostopom, nepooblaščenim razkritjem in neustreznim odstranjevanjem. 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)** - Preslikano na dokazila o odgovornosti, sledljivost dokazil, pridobivanje dokazil, evidence neskladnosti in evidence, pripravljene za revizijo, ki dokazujejo skladnost. 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** - Preslikano na dokazila o upravljanju s strani upravljavca, evidence odobritev, nadzor politik, ukrepe odgovornosti, dokumentirani pregled in nadzor, ki ga izvaja 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** - Preslikano na dokumentacijo obdelovalcev in podobdelovalcev, dokazila o navodilih naročnika, zunanje zagotovljena dokazila o procesu in nadzor razkritja dokazil. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Preslikano na dokazila evidenc dejavnosti obdelave, zahteve glede kakovosti dokazil, sklice na dejavnosti obdelave in metapodatke o lastniku/statusu dokazil o obdelavi. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Preslikano na varovanje repozitorijev dokazil, omejitve dostopa, odobritve dostopa, pregled varovanja repozitorija in odstranitev nepooblaščenega dostopa. 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** - Preslikano na dokazila o skladnosti na področju zasebnosti, pridobivanje revizijskih dokazov, sledljivost dokazil, podporo neodvisnemu pregledu in dokazila o korektivnih ukrepih. 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** - Preslikano na varovanje evidenc, povezanih s PII, ohranjanje evidenc ter kontrole dostopa do repozitorijev dokazil in brisanja. 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** - Preslikano na identifikacijo dokumentiranih informacij, odobritev, razpoložljivost, varovanje, nadzor različic, hrambo, odstranjevanje in nadzor dokumentiranih informacij, ki so zahtevane od zunaj. 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 - Preslikano na varovanje evidenc PIMS pred izgubo, uničenjem, ponarejanjem, nepooblaščenim dostopom, nepooblaščenim razkritjem in neustreznim odstranjevanjem. 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 - Preslikano na varovanje zasebnosti in PII v dokumentiranih informacijah, repozitorijih dokazil, razkritjih in evidencah z nadzorovanim dostopom. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].