					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII09					Naslov dokumenta: **Politika zbiranja, uporabe, razkritja in deljenja PII**							
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	Klavzula/kontrola/člen	Uporabljivost	Vrsta pokritosti	Komentar
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentirana operativna kontrola
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Spremljanje in korektivni ukrepi
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Nameni in evidence dejavnosti obdelave
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Povezava s pravno podlago
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Odgovornosti skupnih upravljavcev pri deljenju
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Omejitve zbiranja, obdelave in minimizacije
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Povezava z usmerjanjem prenosov
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Evidence prenosov in razkritij
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Navodila obdelovalcu in evidence
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Povezava obdelovalca z usmerjanjem prenosov
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Evidence obdelovalca o razkritjih in zahteve
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Omejitev namena, minimizacija in odgovornost
GDPR	Article 6	Controller	Referenced	Povezava s pravno podlago
GDPR	Article 24	Controller	Supporting	Odgovornost upravljavca

GDPR	Article 26	Joint Controller	Supporting	Dogovori skupnih upravljavcev
GDPR	Article 28	Both	Supporting	Navodila obdelovalcem in omejitve razkritij
GDPR	Article 30	Both	Supporting	Evidence dejavnosti obdelave in prejemnikov
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Namen, zbiranje, minimizacija in omejitev razkritja
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Odgovornost in skladnost z zahtevami glede zasebnosti
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Kontrole za namen, zbiranje, minimizacijo, uporabo in razkritje

1. Področje uporabe

1.1 Ta politika določa zahteve za zbiranje, uporabo, razkritje in deljenje PII v okviru obsega PIMS.

1.2 Ta politika se uporablja za:

1.2.1 zbiranje PII prek neposrednih, posrednih, avtomatiziranih, ročnih, notranjih, zunanjih kanalov in kanalov tretjih oseb;

1.2.2 odobreno notranjo uporabo PII v poslovnih procesih, sistemih in aplikacijah;

1.2.3 sekundarno uporabo PII za nov ali bistveno spremenjen namen;

1.2.4 zunanje razkritje PII prejemnikom, partnerjem, organom, obdelovalcem, podobdelovalcem, dobaviteljem in drugim tretjim osebam;

1.2.5 ponavljajoče se ureditve deljenja podatkov in enkratna razkritja;

1.2.6 kontekste upravljavca, skupnega upravljavca, obdelovalca in podobdelovalca;

1.2.7 REG02 - Popis dejavnosti obdelave PII / ROPA, REG08 - Register obdelovalcev, podobdelovalcev in deljenja podatkov, REG09 - Register mednarodnih prenosov ter REG12 - Register presoj, neskladnosti, korektivnih ukrepov in izboljšav.

1.3 Ta politika ne nadomešča:

1.3.1 PII03 za popis dejavnosti obdelave, pravno podlago in lastništvo ROPA;

1.3.2 PII04 za vsebino obvestila o zasebnosti, objavo in nadzor različic;

1.3.3 PII05 za delovanje privolitev in preferenc;

1.3.4 PII06 za obravnavo zahtev posameznikov, na katere se nanašajo PII, za uveljavljanje pravic;

1.3.5 PII07 za metodologijo DPIA in oceno tveganj za zasebnost;

1.3.6 PII08 za kontrolne točke vgrajenega varstva zasebnosti;

1.3.7 PII10 za izvedbo hrambe, izbrisa in odstranjevanja;

1.3.8 PII11 za upravljanje točnosti in kakovosti;

1.3.9 PII12 za upravljanje življenjskega cikla obdelovalcev, podobdelovalcev in tretjih oseb;

1.3.10 PII13 za izbiro mehanizma mednarodnega prenosa in kontrole tveganj prenosa;

1.3.11 PII14 za varnost PII in nadzor dostopa;

1.3.12 PII15 za obravnavanje incidentov in kršitev;

1.3.13 PII18 za upravljanje spremljanja, presoje, neskladnosti, korektivnih ukrepov in izboljšav na ravni PIMS.

1.4 Za namen te politike:

1.4.1 »odobrena uporaba« pomeni uporabo PII, ki je v REG02 evidentirana za določeno dejavnost obdelave, namen, kategorijo PII, kategorijo posameznikov, na katere se nanašajo PII, poslovnega lastnika in veljavno vlogo PIMS.

1.4.2 »zbiranje« pomeni pridobivanje PII neposredno od posameznika, na katerega se nanašajo PII, posredno od druge stranke, samodejno iz sistema ali naprave ali prek notranjega ali zunanjega vira podatkov.

1.4.3 »sekundarna uporaba« pomeni uporabo PII za namen, ki še ni evidentiran kot odobren namen v REG02 za zadevno dejavnost obdelave.

1.4.4 »preverjanje združljivosti« pomeni dokumentirano presojo v REG02, ki zajema prvotni namen, predlagani namen, odvisnost od pravne podlage, kategorije PII, pričakovanja posameznikov, na katere se nanašajo PII, utemeljitev minimizacije, vpliv razkritja ali prenosa ter usmerjanje na druge politike PIMS, kadar je to potrebno.

1.4.5 »zunanje razkritje« pomeni omogočanje dostopa do PII stranki zunaj organizacije ali zunaj dokumentirane verige navodil naročnika.

1.4.6 »deljenje podatkov« pomeni ponavljajočo se ali strukturirano ureditev, na podlagi katere se PII razkrijejo, prenesejo, se do njih dostopa, se izmenjajo ali se dajo na voljo drugi stranki.

1.4.7 »občutljivo ponavljajoče se deljenje« pomeni ponavljajoče se deljenje, ki vključuje posebne kategorije PII, PII o kaznivih dejanjih, PII otrok, evidence z velikim vplivom, obsežno deljenje ali zunanje deljenje, ki vključuje lokacijo prenosa, evidentirano v REG09.

2. Namen

2.1 Namen te politike je zagotoviti, da se PII zbirajo, uporabljajo, razkrivajo in delijo samo za dokumentirane, odobrene, omejene in odgovorno upravljane namene.

2.2 Ta politika organizaciji omogoča dokazati, da sta zbiranje in uporaba povezana z evidencami obdelave v REG02, da so razkritja in ureditve deljenja podatkov evidentirane v REG08, da je usmerjanje mednarodnih prenosov povezano z REG09 ter da se izjeme in neskladnosti obravnavajo prek REG12.

3. Cilji

3.1 Cilji te politike so:

3.1.1 omejiti zbiranje na PII, ki so potrebni za dokumentirane namene;

3.1.2 zagotoviti, da je notranja uporaba PII odobrena pred začetkom obdelave;

3.1.3 zahtevati preverjanje združljivosti pred sekundarno uporabo;

3.1.4 zahtevati odobritev in dokazila pred zunanjim razkritjem;

3.1.5 vzdrževati dokazila o deljenju podatkov v REG08 brez vzpostavitve ločenega registra deljenja podatkov;

3.1.6 usmeriti odvisnosti mednarodnih prenosov na REG09 in PII13 brez podvajanja kontrol mehanizmov prenosa;

3.1.7 določiti pogostost pregledov ponavljajočega se deljenja;

3.1.8 vzdrževati dokazila, primerna za revizijo, za zbiranje, uporabo, razkritje, deljenje, izjeme in korektivne ukrepe.

4. Izjave politike

4.1 Omejitev zbiranja

4.1.1 [Controller] Process Owner / Business Owner mora v REG02 evidentirati namen zbiranja, vir ali kanal, kategorije PII, kategorije posameznikov, na katere se nanašajo PII, in najmanjši obseg podatkovnih elementov, preden se začne nova dejavnost zbiranja ali bistvena sprememba zbiranja.

4.1.2 [Controller] Privacy Lead / PIMS Manager mora pred začetkom zbiranja pregledati evidenco zbiranja v REG02, kadar se doda nova kategorija PII, vir, kanal ali namen.

4.1.3 [Controller] Process Owner / Business Owner mora v REG02 evidentirati utemeljitev nujnosti za vsak podatkovni element PII, preden se ta element začne zbirati.

4.1.4 [Processor] Process Owner / Business Owner mora v REG02 evidentirati referenco navodila naročnika iz REG08, preden zbira PII v imenu naročnika.

4.1.5 [Joint Controller] Process Owner / Business Owner mora v REG08 evidentirati razporeditev odgovornosti skupnih upravljavcev za zbiranje, preden se začne skupno zbiranje.

4.2 Kontrole odobrene notranje uporabe

4.2.1 [Controller] Process Owner / Business Owner mora v REG02 evidentirati pravila odobrene notranje uporabe za vsako dejavnost obdelave, preden se uporaba začne.

4.2.2 [Controller] System Owner / Application Owner mora pred objavo v produkcijo implementirati samo tista polja delovnega toka, poročila ali izvoze za notranjo uporabo, za katere obstaja ustrezno pravilo odobrene uporabe v REG02.

4.2.3 [Processor] Process Owner / Business Owner mora v REG08 evidentirati usklajenost z navodilom naročnika, preden uporabi PII naročnika za katero koli dejavnost obdelovalca ali podobdelovalca.

4.2.4 [Controller] Privacy Lead / PIMS Manager mora pravila odobrene uporabe v REG02 pregledati vsaj enkrat letno za vsako aktivno dejavnost obdelave.

4.2.5 [All] Privacy Lead / PIMS Manager mora v REG12 evidentirati neskladnost v petih delovnih dneh, kadar se ugotovi nedokumentirana notranja uporaba PII.

[... 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 evidentirati zahtevo za izjemo, preden odstopi od odobrenega pravila zbiranja, uporabe, razkritja ali deljenja.

9.1.2 [All] Privacy Lead / PIMS Manager mora v REG12 evidentirati odločitev o odobritvi ali zavrnitvi, preden se izjema aktivira.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor mora v REG12 evidentirati mnenje pred odobritvijo izjeme, ki vključuje nezdružljivo sekundarno uporabo, občutljivo ponavljajoče se deljenje, nasprotje pri pravno zavezujočem razkritju ali usmerjanje prenosa.

9.1.4 [All] Top Management mora v REG12 evidentirati odobritev pred aktiviranjem katere koli izjeme, ki traja več kot 30 koledarskih dni ali vpliva na več kot eno dejavnost obdelave.

9.1.5 [All] Process Owner / Business Owner mora izjemo v REG12 zapreti do datuma poteka ali v petih delovnih dneh po prenehanju pogoja za izjemo.

10. Uveljavljanje

10.1.1 [All] Privacy Lead / PIMS Manager mora neodobreno zbiranje, uporabo, razkritje ali deljenje evidentirati kot neskladnost v REG12 v petih delovnih dneh po ugotovitvi.

10.1.2 [Controller] Process Owner / Business Owner mora v enem delovnem dnevu začasno ustaviti zbiranje, uporabo, razkritje ali deljenje, kadar Privacy Lead / PIMS Manager v REG12 evidentira odsotnost odobrenih dokazil iz REG02 ali REG08.

10.1.3 [Processor] Process Owner / Business Owner mora v REG08 in REG12 v enem delovnem dnevu evidentirati odločitev o ustavitvi ali eskalaciji, kadar se PII naročnika uporabijo ali razkrijejo zunaj dokumentiranega navodila.

10.1.4 [All] Top Management mora v REG12 pregledati nerešene neskladnosti z velikim vplivom pri zbiranju, uporabi, razkritju ali deljenju v 30 koledarskih dneh po eskalaciji.

10.1.5 [All] Internal Audit / Compliance Reviewer mora v REG12 preveriti dokazila o zaključku korektivnega ukrepa v 15 delovnih dneh po tem, ko Privacy Lead / PIMS Manager označi zaključek.

11. Pregled in vzdrževanje

11.1.1 [All] Privacy Lead / PIMS Manager mora to politiko pregledati vsaj enkrat letno in odločitev evidentirati v REG12.

11.1.2 [All] Privacy Lead / PIMS Manager mora to politiko pregledati v 30 koledarskih dneh po bistveni spremembi obsega PIMS, namenov obdelave, modela deljenja, usmerjanja prenosov ali veljavne obveznosti ter izid evidentirati v REG12.

11.1.3 [All] Process Owner / Business Owner mora ponovno potrditi aktivne evidence REG02 in REG08 vsaj enkrat letno in v 30 koledarskih dneh po bistveni spremembi obdelave.

11.1.4 [All] Internal Audit / Compliance Reviewer mora kontrole PII09 vključiti v letno revizijsko vzorčenje in pokritost evidentirati v REG12.

11.1.5 [All] Privacy Lead / PIMS Manager mora reference na povezane politike v REG12 posodobiti v desetih delovnih dneh, kadar PII03, PII08, PII10, PII12, PII13, PII14 ali PII18 spremeni operativno mejo te politike.

12. Povezane politike

12.1 To politiko je treba brati skupaj z:

12.1.1 PII01 - Politika sistema upravljanja informacij o zasebnosti

12.1.2 PII02 - Politika vlog, odgovornosti in odgovornosti za ravnanje na področju zasebnosti

12.1.3 PII03 - Politika popisa dejavnosti obdelave PII in pravnih podlag

12.1.4 PII04 - Politika obvestila o zasebnosti in preglednosti

12.1.5 PII05 - Politika upravljanja privolitev in preferenc

12.1.6 PII06 - Politika upravljanja pravic posameznikov, na katere se nanašajo PII

12.1.7 PII07 - Politika ocene tveganj za zasebnost in DPIA

12.1.8 PII08 - Politika vgrajenega in privzetega varstva zasebnosti

12.1.9 PII10 - Politika hrambe, izbrisa in odstranjevanja PII

12.1.10 PII11 - Politika točnosti in kakovosti PII

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

12.1.12 PII13 - Politika mednarodnega prenosa PII

12.1.13 PII14 - Politika varnosti PII in nadzora dostopa

12.1.14 PII15 - Politika upravljanja incidentov in kršitev v zvezi s PII

12.1.15 PII17 - Politika dokumentiranih informacij in upravljanja dokazil PIMS

12.1.16 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 7.5; Clause 8.1** - Preslikano na dokumentirane operativne evidence in nadzor nad dokazili o zbiranju, odobreni uporabi, sekundarni uporabi, razkritju, deljenju in usmerjanju prenosov. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Preslikano na spremljanje, merjenje, pregled, obravnavo izjem, neskladnosti in korektivne ukrepe za kontrole zbiranja, uporabe, razkritja in deljenja. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Preslikano na dokumentirane namene upravljavca, evidence odobrene uporabe in dokazila o obdelavi v REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Preslikano na povezavo s pravno podlago za zbiranje, uporabo in usmerjanje sekundarne uporabe, ne da bi nadomestilo PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Preslikano na dokazila v REG08 o odgovornosti skupnih upravljavcev za zbiranje in deljenje. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Preslikano na omejitev zbiranja, omejitev obdelave in utemeljitev minimizacije, preden se PII zbirajo ali uporabijo. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Preslikano na povezavo usmerjanja prenosov prek REG09, ne da bi nadomestilo kontrole mehanizmov prenosa po PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Preslikano na evidence prenosov, razkritij in ponavljajočih se ureditev deljenja podatkov v REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Preslikano na usklajenost obdelovalca z navodili naročnika in evidence obdelovalca za omejitve zbiranja, uporabe in sekundarne uporabe. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Preslikano na povezavo usmerjanja prenosov obdelovalca prek REG09, ne da bi nadomestilo kontrole mehanizmov prenosa po PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Preslikano na evidence obdelovalca o razkritjih, status obvestil o zahtevah za razkritje in dokazila o dovoljenju za razkritje v REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Preslikano na dokazila o omejitvi namena, minimizaciji podatkov in odgovornosti za zbiranje, uporabo, sekundarno uporabo, razkritje in deljenje. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Preslikano na povezavo s pravno podlago in usmerjanje za novo ali nezdružljivo sekundarno uporabo, ne da bi nadomestilo PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Preslikano na upravljanje upravljavca, odobritve, pregled in ukrepe odgovornosti za zbiranje, uporabo, razkritje in deljenje. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Preslikano na dokazila o odgovornosti skupnih upravljavcev za zbiranje in deljenje. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Preslikano na usklajenost obdelovalcev in podobdelovalcev z navodili, dovoljenje naročnika in omejitve razkritja. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Preslikano na evidence dejavnosti obdelave, prejemnikov, razkritij in deljenja v REG02 in REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Preslikano na določitev namena, omejitev zbiranja, minimizacijo podatkov, omejitev uporabe in omejitev razkritja. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Preslikano na odgovornost, dokazila o skladnosti, pregled, upravljanje izjem, revizijsko vzorčenje in korektivne ukrepe. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Preslikano na namen, omejitev zbiranja, minimizacijo, omejitev uporabe, omejitev razkritja in podporo evidencam razkritij. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].