					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII16					Naslov dokumenta: **Politika usposabljanja, ozaveščanja in kompetenc 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	Klavzula/kontrola/člen	Uporabljivost	Vrsta pokritosti	Komentar
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Kompetence in ozaveščenost
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikacija in dokumentirana dokazila
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operativno obvladovanje, merjenje in izboljševanje
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Ozaveščanje, izobraževanje in usposabljanje o obdelavi PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Odgovornost, upravljanje obdelovalcev, varnost in naloge DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetence, ozaveščenost in usposabljanje
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Smernice za ozaveščanje, izobraževanje in usposabljanje
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informacijska varnost in skladnost z zahtevami zasebnosti

1. Področje uporabe

1.1 Ta politika določa zahteve organizacije za usposabljanje, ozaveščanje in kompetence na področju zasebnosti v okviru sistema upravljanja informacij o zasebnosti.

1.2 Ta politika se uporablja za osebje, pogodbene izvajalce, začasno osebje, relevantne tretje osebe, obdelovalce, podobdelovalce in druge zainteresirane strani, katerih delo lahko vpliva na obdelavo PII, uspešnost PIMS, pravice posameznikov, na katere se nanaša PII, tveganje za zasebnost, informacijsko varnost v zvezi s PII, navodila obdelovalcem, incidente na področju zasebnosti, dokumentirane informacije ali dokazila o skladnosti.

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

1.4 Ta politika zajema:

1.4.1 identifikacijo ciljnih skupin za usposabljanje na področju zasebnosti;

1.4.2 uvajalno usposabljanje;

1.4.3 letno obnovitveno usposabljanje;

1.4.4 usposabljanje na podlagi vlog in usposabljanje, sproženo z dogodki;

1.4.5 dokazila o dokončanju usposabljanja;

1.4.6 eskalacijo nedokončanja;

1.4.7 pregled učinkovitosti usposabljanja;

1.4.8 dokazila o zagotovilih glede usposabljanja obdelovalcev, podobdelovalcev in tretjih oseb.

1.5 Ta politika ne vzpostavlja ločene matrike usposabljanj, nadzorne plošče usposabljanj, kadrovske evidence, evidence kompetenc, disciplinske evidence ali evidence usposabljanj za stranke. Dodelitve usposabljanj, dokončanja, opomniki, dokazila o kompetencah in dokazila o ozaveščanju se evidentirajo v REG11, izjeme, eskalacije, neskladnosti, korektivni ukrepi in dokazila o pregledu pa v REG12. Dokazila o zagotovilih glede usposabljanja obdelovalcev, podobdelovalcev in tretjih oseb se, kadar je relevantno, evidentirajo v REG08.

1.6 Ta politika ne podvaja:

1.6.1 dodelitve odgovornosti po vlogah v PII02;

1.6.2 zahtev glede popisa dejavnosti obdelave in pravne podlage v PII03;

1.6.3 metodologije za tveganja za zasebnost in DPIA v PII07;

1.6.4 kontrolnih točk vgrajenega varstva zasebnosti v PII08;

1.6.5 upravljanja življenjskega cikla obdelovalcev v PII12;

1.6.6 delovanja varnosti PII in nadzora dostopa v PII14;

1.6.7 delovnega toka za incidente in kršitve v zvezi s PII v PII15;

1.6.8 upravljanja dokumentiranih informacij v PII17;

1.6.9 upravljanja spremljanja, notranje presoje in izboljševanja v PII18.

2. Namen

2.1 Namen te politike je zagotoviti, da osebe, katerih delo vpliva na obdelavo PII, razumejo svoje odgovornosti glede zasebnosti, opravijo ustrezno usposabljanje v določenih časovnih intervalih, vzdržujejo kompetence, relevantne za vlogo, ter ustvarjajo preverljiva dokazila o usposabljanju, ozaveščenosti in eskalaciji.

2.2 Ta politika podpira dosledno izvajanje PIMS z uporabo REG11 kot primarnega dokaznega objekta za usposabljanje in ozaveščanje ter REG08, REG10 in REG12 kot podpornih dokaznih objektov.

3. Cilji

3.1 Cilji te politike so:

3.1.1 določiti ciljne skupine za usposabljanje na področju zasebnosti;

3.1.2 določiti zahteve za uvajalno usposabljanje;

3.1.3 določiti zahteve za letno obnovitveno usposabljanje;

3.1.4 določiti zahteve za usposabljanje na področju zasebnosti na podlagi vlog;

3.1.5 evidentirati dokazila o dokončanju v REG11;

3.1.6 eskalirati nedokončanje prek REG12;

3.1.7 kadar je relevantno, vzdrževati dokazila o zagotovilih glede usposabljanja obdelovalcev, podobdelovalcev in tretjih oseb v REG08;

3.1.8 pregledovati učinkovitost usposabljanja brez ustvarjanja pretiranih metrik ali podvojenih evidenc;

3.1.9 zagotoviti, da vsebina usposabljanja ostane usklajena z veljavnimi politikami PIMS in bistvenimi obveznostmi glede zasebnosti.

4. Izjave politike

4.1 Ciljna skupina in dodelitev usposabljanja

4.1.1 [All] Privacy Lead / PIMS Manager mora pred začetkom vsakega letnega cikla usposabljanja v REG11 določiti kategorije ciljnih skupin za usposabljanje PIMS.

4.1.2 [All] Process Owner / Business Owner mora pred uvajanjem, dodelitvijo vloge ali bistveno spremembo delovnih nalog v REG11 opredeliti osebje, katerega naloge vključujejo obdelavo PII.

4.1.3 [Conditional] System Owner / Application Owner mora pred omogočitvijo ali bistveno spremembo dostopa v REG11 opredeliti uporabnike, ki potrebujejo usposabljanje na področju zasebnosti za sisteme PII, privilegirani dostop ali administrativne naloge.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager mora pred začetkom ali bistveno spremembo skupne dejavnosti obdelave v REG11 ali REG08 evidentirati razdelitev odgovornosti za usposabljanje med skupnimi upravljavci.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor mora pred dodelitvijo usposabljanja vlogam, ki obravnavajo visoko tvegano obdelavo, posebne vrste PII, pravice posameznikov, na katere se nanaša PII, DPIA, mednarodne prenose ali oceno kršitve, v REG11 opredeliti potrebe po okrepljenem usposabljanju na področju zasebnosti.

4.1.6 [All] Privacy Lead / PIMS Manager mora pred začetkom vsakega letnega cikla usposabljanja v REG11 evidentirati dodeljeno ciljno skupino usposabljanja, vrsto usposabljanja, zahtevani datum dokončanja in lastnika dokazil.

4.2 Uvajalna in letna časovna dinamika usposabljanja

4.2.1 [All] Privacy Lead / PIMS Manager mora v REG11 dodeliti osnovno usposabljanje za ozaveščanje o zasebnosti v 10 delovnih dneh po uvajanju za osebje z dostopom do PII ali odgovornostmi v okviru PIMS.

4.2.2 [All] Process Owner / Business Owner mora zagotoviti, da dodeljeno osebje v REG11 opravi uvajalno usposabljanje na področju zasebnosti pred odobritvijo nenadzorovanega dostopa do PII ali v 30 dneh po uvajanju, kar nastopi prej.

4.2.3 [All] Privacy Lead / PIMS Manager mora v REG11 dodeliti letno obnovitveno usposabljanje na področju zasebnosti vsaj enkrat na 12 mesecev.

4.2.4 [All] Process Owner / Business Owner mora do objavljenega letnega roka v REG11 potrditi status dokončanja letnega obnovitvenega usposabljanja za dodeljeno osebje.

4.2.5 [Conditional] Privacy Lead / PIMS Manager mora v REG11 dodeliti ciljno obnovitveno usposabljanje v 30 dneh po bistveni spremembi politike zasebnosti, bistveni spremembi

procesa PIMS, ugotovitvi presoje, ponavljajočem se neuspehu pri usposabljanju ali relevantni izkušnji iz incidenta v zvezi s 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 pred podaljšanjem zahtevanega roka za dokončanje v REG12 evidentirati zahtevo za izjemo pri usposabljanju na področju zasebnosti.

9.1.2 [All] Privacy Lead / PIMS Manager mora pred aktivacijo izjeme v REG12 odobriti ali zavrniti zahteve za izjeme pri usposabljanju na področju zasebnosti.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor mora pred odobritvijo svetovati glede izjem pri usposabljanju v REG12, kadar izjema vpliva na visoko tvegano obdelavo, posebne vrste PII, obravnavo zahtev za uveljavljanje pravic, obravnavanje incidentov, mednarodne prenose ali certifikacijska dokazila.

9.1.4 [Conditional] Top Management mora pred aktivacijo odobriti izjeme pri usposabljanju na področju zasebnosti v REG12, kadar izjema vpliva na ponavljajoče se nedokončanje, privilegirani dostop do PII, obdelavo PII z velikim vplivom ali dokazila za regulatorje.

9.1.5 [All] Privacy Lead / PIMS Manager mora pred odobritvijo katere koli izjeme pri usposabljanju na področju zasebnosti v REG12 določiti lastnika izjeme, datum poteka, kompenzacijski ukrep in datum pregleda.

9.1.6 [All] Process Owner / Business Owner mora pred datumom poteka izjeme v REG12 zapreti ali obnoviti odobrene izjeme pri usposabljanju na področju zasebnosti.

10. Uveljavljanje

10.1.1 [All] Privacy Lead / PIMS Manager mora v REG12 evidentirati neskladnost pri usposabljanju v petih delovnih dneh, kadar dokazila o obveznem usposabljanju na področju zasebnosti manjkajo, so nepopolna, zapadla ali niso sledljiva do REG11.

10.1.2 [All] Process Owner / Business Owner mora zagotoviti, da je zapadlo obvezno usposabljanje na področju zasebnosti dokončano ali eskalirano v REG11 ali REG12 v 10 delovnih dneh po evidentiranju statusa zapadlosti.

10.1.3 [Conditional] System Owner / Application Owner mora v REG12 omejiti nov dostop z velikim vplivom do PII, kadar zahtevano uvajalno usposabljanje ali usposabljanje na področju zasebnosti na podlagi vlog po eskalaciji ostane nedokončano.

10.1.4 [Processor] Vendor / Procurement Owner mora manjkajoča dokazila o zagotovilih glede usposabljanja obdelovalca, podobdelovalca ali zunanje delovne sile eskalirati v REG08 in REG12 v petih delovnih dneh po identifikaciji.

10.1.5 [Conditional] Incident Response Coordinator mora ukrepe uveljavljanja, povezane z usposabljanjem, povezati z REG10 v enem delovnem dnevu, kadar je neuspeh pri usposabljanju prispeval k domnevnemu ali potrjenemu incidentu v zvezi s PII.

10.1.6 [All] Internal Audit / Compliance Reviewer mora preveriti dokazila o zaključku korektivnih ukrepov v zvezi z usposabljanjem v REG12 ob naslednji načrtovani presoji ali v 60 dneh po zaključku, kar nastopi prej.

11. Pregled in vzdrževanje

11.1.1 [All] Privacy Lead / PIMS Manager mora vsaj letno pregledati to politiko in vsebino usposabljanja ter rezultat pregleda evidentirati v REG11 ali REG12.

11.1.2 [All] Privacy Lead / PIMS Manager mora to politiko pregledati v 30 dneh po bistveni spremembi obsega PIMS, zakonodaje o zasebnosti, dejavnosti obdelave, modela vlog, izkušenj iz incidentov, ugotovitev presoje ali rezultatov učinkovitosti usposabljanja.

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

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

11.1.5 [All] Privacy Lead / PIMS Manager mora posodobiti vsebino usposabljanja in dokazila o dodelitvah v REG11 v 30 dneh po odobreni bistveni spremembi politike.

12. Povezane politike

12.1 To politiko je treba brati skupaj z:

12.2 PII01 - Politika sistema upravljanja informacij o zasebnosti;

12.3 PII02 - Politika vlog, odgovornosti in odgovornosti za ravnanje 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 posameznikov, na katere se nanaša PII;

12.8 PII07 - Politika ocene tveganj za zasebnost in DPIA;

12.9 PII08 - Politika vgrajenega in privzetega varstva zasebnosti;

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

12.11 PII10 - Politika hrambe, izbrisa in odstranjevanja PII;

12.12 PII12 - Politika upravljanja zasebnosti obdelovalcev, podobdelovalcev in tretjih oseb;

12.13 PII13 - Politika mednarodnih prenosov PII;

12.14 PII14 - Politika varnosti PII in nadzora dostopa;

12.15 PII15 - Politika upravljanja incidentov in kršitev v zvezi s PII;

12.16 PII17 - Politika upravljanja dokumentiranih informacij in dokazil PIMS;

12.17 PII18 - Politika spremljanja, presoje in izboljševanja PIMS.

13. Referenčni standardi in okviri

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].