					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII16					Naziv dokumenta: **Politika osposobljavanja, podizanja svijesti i kompetentnosti u području privatnosti**							
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 7.2; Clause 7.3	Both	Primary	Kompetentnost i svijest
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikacija i dokumentirani dokazi
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operativna kontrola, mjerenje i poboljšanje
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Svijest, obrazovanje i obuka o obradi PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Odgovornost, upravljanje izvršiteljima obrade, sigurnost i zadaće DPO-a
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetentnost, svijest i osposobljavanje
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Smjernice za podizanje svijesti, obrazovanje i osposobljavanje
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informacijska sigurnost i usklađenost u području privatnosti

1. Opseg

1.1 Ova politika definira zahtjeve organizacije za osposobljavanje, podizanje svijesti i kompetentnost u području privatnosti unutar sustava upravljanja informacijama o privatnosti.

1.2 Ova politika primjenjuje se na osoblje, izvođače, privremeno osoblje, relevantne treće strane, izvršitelje obrade, podizvršitelje obrade i druge zainteresirane strane čiji rad može utjecati na obradu PII, učinkovitost PIMS-a, prava ispitanika, rizik za privatnost, informacijsku sigurnost povezanu s PII, upute izvršitelju obrade, incidente u vezi s privatnošću, dokumentirane informacije ili dokaze o usklađenosti.

1.3 Ova politika primjenjuje se u kontekstima voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade.

1.4 Ova politika obuhvaća:

1.4.1 utvrđivanje ciljnih skupina obuke o privatnosti;

1.4.2 obuku pri uvođenju u posao;

1.4.3 godišnju obnovnu obuku;

1.4.4 osposobljavanje temeljeno na ulogama i obuku potaknutu događajem;

1.4.5 dokaze o završetku obuke;

1.4.6 eskalaciju nedovršavanja obuke;

1.4.7 pregled učinkovitosti obuke;

1.4.8 dokaze o provedbi obuke za izvršitelje obrade, podizvršitelje obrade i treće strane.

1.5 Ova politika ne uspostavlja zasebnu matricu obuke, nadzornu ploču obuke, registar ljudskih resursa, registar kompetentnosti, disciplinski registar ili registar obuke klijenata. Dodjele obuke, završeci, podsjetnici, dokazi o kompetentnosti i dokazi o svijesti evidentiraju se u REG11, dok se iznimke, eskalacije, nesukladnosti, korektivne radnje i dokazi o pregledu evidentiraju u REG12. Dokazi o provedbi obuke za izvršitelje obrade, podizvršitelje obrade i treće strane evidentiraju se u REG08 kada je relevantno.

1.6 Ova politika ne duplicira:

1.6.1 dodjelu odgovornosti za uloge u PII02;

1.6.2 popis aktivnosti obrade i zahtjeve za pravnu osnovu u PII03;

1.6.3 metodologiju procjene rizika za privatnost i DPIA-e u PII07;

1.6.4 kontrolne točke ugrađene zaštite privatnosti u PII08;

1.6.5 upravljanje životnim ciklusom izvršitelja obrade u PII12;

1.6.6 provedbu sigurnosti PII i kontrole pristupa u PII14;

1.6.7 radni tok za incidente u vezi s osobnim podacima i povrede osobnih podataka u PII15;

1.6.8 upravljanje dokumentiranim informacijama u PII17;

1.6.9 upravljanje praćenjem, internom revizijom i poboljšanjem u PII18.

2. Svrha

2.1 Svrha ove politike jest osigurati da osobe čiji rad utječe na obradu PII razumiju svoje odgovornosti u području privatnosti, završavaju odgovarajuću obuku prema definiranoj dinamici, održavaju kompetentnost relevantnu za svoju ulogu i stvaraju revizijski provjerljive dokaze o obuci, svijesti i eskalaciji.

2.2 Ova politika podupire dosljednu provedbu PIMS-a uporabom REG11 kao primarnog evidencijskog objekta za obuku i svijest te REG08, REG10 i REG12 kao pripadajućih evidencijskih objekata.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

3.1.1 definirati ciljne skupine obuke o privatnosti;

3.1.2 definirati zahtjeve za obuku pri uvođenju u posao;

3.1.3 definirati zahtjeve za godišnju obnovnu obuku;

3.1.4 definirati zahtjeve za osposobljavanje o privatnosti temeljeno na ulogama;

3.1.5 evidentirati dokaze o završetku u REG11;

3.1.6 eskalirati nedovršavanje obuke putem REG12;

3.1.7 održavati dokaze o provedbi obuke za izvršitelje obrade, podizvršitelje obrade i treće strane u REG08 kada je relevantno;

3.1.8 pregledavati učinkovitost obuke bez stvaranja pretjeranih metrika ili dupliciranih registara;

3.1.9 osigurati da sadržaj obuke ostane usklađen s važećim PIMS politikama i značajnim obvezama u području privatnosti.

4. Izjave politike

4.1 Ciljna skupina i dodjela obuke

4.1.1 [All] Privacy Lead / PIMS Manager MORA definirati kategorije ciljnih skupina za PIMS obuku u REG11 prije početka svakog godišnjeg ciklusa obuke.

4.1.2 [All] Process Owner / Business Owner MORA identificirati osoblje čije dužnosti uključuju obradu PII u REG11 prije uvođenja u posao, dodjele uloge ili značajne promjene dužnosti.

4.1.3 [Conditional] System Owner / Application Owner MORA identificirati korisnike kojima je potrebna obuka o privatnosti za PII sustave, pristup s povišenim ovlastima ili administrativne funkcije u REG11 prije omogućavanja ili značajne izmjene pristupa.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager MORA evidentirati raspodjelu odgovornosti za obuku zajedničkih voditelja obrade u REG11 ili REG08 prije početka ili značajne promjene zajedničke aktivnosti obrade.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor MORA identificirati potrebe za pojačanom obukom o privatnosti u REG11 prije dodjele obuke ulogama koje postupaju s obradom visokog rizika, posebnim kategorijama osobnih podataka, pravima ispitanika, DPIA-ama, međunarodnim prijenosima ili procjenom povrede.

4.1.6 [All] Privacy Lead / PIMS Manager MORA evidentirati dodijeljenu ciljnu skupinu obuke, vrstu obuke, zahtijevani datum završetka i vlasnika dokaza u REG11 prije početka svakog godišnjeg ciklusa obuke.

4.2 Dinamika obuke pri uvođenju u posao i godišnje obuke

4.2.1 [All] Privacy Lead / PIMS Manager MORA dodijeliti osnovnu obuku o podizanju svijesti o privatnosti u REG11 u roku od 10 radnih dana od uvođenja u posao za osoblje koje ima pristup PII ili odgovornosti povezane s PIMS-om.

4.2.2 [All] Process Owner / Business Owner MORA osigurati da dodijeljeno osoblje završi obuku o privatnosti pri uvođenju u posao u REG11 prije odobrenja nenadziranog pristupa PII ili u roku od 30 dana od uvođenja u posao, ovisno o tome što nastupi prije.

4.2.3 [All] Privacy Lead / PIMS Manager MORA dodijeliti godišnju obnovnu obuku o privatnosti u REG11 najmanje jednom svakih 12 mjeseci.

4.2.4 [All] Process Owner / Business Owner MORA potvrditi status završetka godišnje obnovne obuke za dodijeljeno osoblje u REG11 do objavljenog godišnjeg roka.

4.2.5 [Conditional] Privacy Lead / PIMS Manager MORA dodijeliti ciljanu obnovnu obuku u REG11 u roku od 30 dana nakon značajne promjene politike privatnosti, značajne promjene PIMS procesa, nalaza revizije, ponavljajućeg neuspjeha u obuci ili relevantne naučene lekcije iz incidenta u vezi s osobnim podacima.

[... 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 evidentirati zahtjev za iznimku od obuke o privatnosti u REG12 prije produljenja zahtijevanog roka završetka.

9.1.2 [All] Privacy Lead / PIMS Manager MORA odobriti ili odbiti zahtjeve za iznimku od obuke o privatnosti u REG12 prije nego što iznimka postane aktivna.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MORA savjetovati o iznimkama od obuke u REG12 prije odobrenja kada iznimka utječe na obradu visokog rizika, posebne kategorije osobnih podataka, postupanje s pravima, postupanje s incidentima, međunarodne prijenose ili certifikacijske dokaze.

9.1.4 [Conditional] Top Management MORA odobriti iznimke od obuke o privatnosti u REG12 prije aktivacije kada iznimka utječe na ponavljajuće nedovršavanje, privilegirani pristup PII, visokoutjecajnu obradu PII ili dokaze namijenjene regulatornim tijelima.

9.1.5 [All] Privacy Lead / PIMS Manager MORA definirati vlasnika iznimke, datum isteka, kompenzacijsku radnju i datum pregleda u REG12 prije odobravanja bilo koje iznimke od obuke o privatnosti.

9.1.6 [All] Process Owner / Business Owner MORA zatvoriti ili obnoviti odobrene iznimke od obuke o privatnosti u REG12 prije datuma isteka iznimke.

10. Provedba zahtjeva

10.1.1 [All] Privacy Lead / PIMS Manager MORA evidentirati nesukladnost u obuci u REG12 u roku od pet radnih dana kada su dokazi o obveznoj obuci o privatnosti nedostajući, nepotpuni, zakašnjeli ili nisu sljedivi do REG11.

10.1.2 [All] Process Owner / Business Owner MORA osigurati da se zakašnjela obvezna obuka o privatnosti završi ili eskalira u REG11 ili REG12 u roku od 10 radnih dana nakon evidentiranja statusa kašnjenja.

10.1.3 [Conditional] System Owner / Application Owner MORA ograničiti novi visokoutjecajni pristup PII u REG12 kada zahtijevana obuka pri uvođenju u posao ili osposobljavanje o privatnosti temeljeno na ulogama ostane nezavršeno nakon eskalacije.

10.1.4 [Processor] Vendor / Procurement Owner MORA eskalirati nedostajuće dokaze o provedbi obuke za izvršitelje obrade, podizvršitelje obrade ili vanjsku radnu snagu u REG08 i REG12 u roku od pet radnih dana nakon identifikacije.

10.1.5 [Conditional] Incident Response Coordinator MORA povezati provedbene radnje povezane s obukom s REG10 u roku od jednog radnog dana kada je neuspjeh obuke pridonio sumnji na incident u vezi s osobnim podacima ili potvrđenom incidentu u vezi s osobnim podacima.

10.1.6 [All] Internal Audit / Compliance Reviewer MORA provjeriti dokaze o zatvaranju korektivnih radnji za obuku 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 i sadržaj obuke najmanje jednom godišnje te evidentirati ishod pregleda u REG11 ili REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MORA pregledati ovu politiku u roku od 30 dana nakon značajne promjene opsega PIMS-a, zakona o privatnosti, aktivnosti obrade, modela uloga, naučenih lekcija iz incidenata, nalaza revizije ili rezultata učinkovitosti obuke.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor MORA pregledati promjene politike značajne za privatnost u REG12 prije odobrenja.

11.1.4 [All] Top Management MORA odobriti značajne promjene ove politike u REG12 prije objave.

11.1.5 [All] Privacy Lead / PIMS Manager MORA ažurirati sadržaj obuke i dokaze o dodjeli u REG11 u roku od 30 dana nakon odobrene značajne promjene politike.

12. Povezane politike

12.1 Ovu politiku treba čitati zajedno sa sljedećim politikama:

12.2 PII01 - Politika sustava upravljanja informacijama o privatnosti;

12.3 PII02 - Politika uloga, odgovornosti i odgovornosti za postupanje u području privatnosti;

12.4 PII03 - Politika popisa aktivnosti obrade PII i pravne osnove;

12.5 PII04 - Politika obavijesti o privatnosti i transparentnosti;

12.6 PII05 - Politika upravljanja privolama i preferencijama;

12.7 PII06 - Politika upravljanja pravima ispitanika;

12.8 PII07 - Politika procjene rizika za privatnost i DPIA-e;

12.9 PII08 - Politika ugrađene i zadane zaštite privatnosti;

12.10 PII09 - Politika prikupljanja, uporabe, otkrivanja i dijeljenja PII;

12.11 PII10 - Politika zadržavanja, brisanja i zbrinjavanja PII;

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

12.13 PII13 - Politika međunarodnog prijenosa PII;

12.14 PII14 - Politika sigurnosti PII i kontrole pristupa;

12.15 PII15 - Politika upravljanja incidentima i povredama u vezi s osobnim podacima;

12.16 PII17 - Politika upravljanja dokumentiranim informacijama i dokazima PIMS-a;

12.17 PII18 - Politika praćenja, revizije i poboljšanja PIMS-a.

13. Referentni standardi i 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].