

				Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII05				Naslov dokumenta: Politika upravljanja privolitev in preferenc							
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

<p>Pravno obvestilo (avtorske pravice in omejitve uporabe) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Ta dokument je intelektualna lastnina družbe Clarysec LLC. Noben del tega dokumenta se ne sme kopirati, ponovno uporabiti, distribuirati ali spreminjati za komercialne ali implementacijske namene brez predhodnega izrecnega pisnega dovoljenja.</p> <p>Nepooblaščen uporaba je strogo prepovedana in lahko povzroči pravne ukrepe.</p> <p>Za licenciranje se obrnite na: info@clarysec.com</p>
--

Usklajenost s standardi in predpisi

Standard / predpis	Klavzula / kontrola / člen	Uporabljenost	Vrsta pokritosti	Komentar
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentirane informacije in operativno obvladovanje dokazil o privolitvi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Spremljanje, neskladnost, korektivni ukrepi in izboljševanje
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Supporting	Povezava s pravno podlago
ISO/IEC 27701:2025	Annex A.1.2.4; Annex A.1.2.5	Controller	Primary	Določanje, pridobivanje in evidentiranje privolitve
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Evidence dejavnosti obdelave upravljavca
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Dogovori obdelovalca, nameni naročnika in evidence obdelovalca
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Podpora obdelovalca obveznostim upravljavca do posameznikov, na katere se nanašajo osebno določljivi podatki
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Zaščita evidenc dejavnosti obdelave PII
GDPR	Article 4(11)	Controller	Supporting	Merila za privolitev
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Zakonitost, poštenost, preglednost in odgovornost
GDPR	Article 6(1)(a); Article 6(4)	Controller	Primary	Privolitev kot pravna podlaga in povezava s

				spremenjenim namenom
GDPR	Article 7	Controller	Primary	Pogoji za privolitve in preklic
GDPR	Article 8	Conditional	Supporting	Eskalacija pri privolitvi otrok
GDPR	Article 9(2)(a)	Conditional	Supporting	Izrecna privolitve za obdelavo posebnih vrst podatkov
GDPR	Article 24	Controller	Supporting	Odgovornost upravljavca in ukrepi
GDPR	Article 28	Both	Supporting	Povezava z navodili in pomočjo obdelovalca
GDPR	Article 30	Both	Supporting	Povezava z evidencami dejavnosti obdelave
ISO/IEC 29100:2020	Clause 5.2; Clause 5.8; Clause 5.12	Both	Supporting	Načela privolitve in izbire, preglednosti ter skladnosti
ISO/IEC 29151:2022	Annex A.3	Both	Supporting	Kontrole za privolitve in izbiro
ISO/IEC TS 27560:2023	Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4	Conditional	Supporting	Struktura zapisa in potrdila o privolitvi, kadar se uporablja

1. Področje uporabe

- 1.1 Ta politika določa obvezne zahteve za ugotavljanje, kdaj je privolitev potrebna, za zahtevanje privolitve, zajemanje dokazil o privolitvi, upravljanje preferenc, obdelavo preklicev, vzdrževanje evidenc privolitev in pregled mehanizmov privolitve.
- 1.2 Ta politika se uporablja za obdelavo PII, kadar je privolitev izbrana ali zahtevana kot pravna podlaga, kadar je zahtevana izrecna privolitev, kadar se zajemajo preference glede privolitve ali kadar organizacija upravlja evidence privolitev v imenu upravljavca.
- 1.3 Ta politika se uporablja v kontekstih upravljavca, skupnega upravljavca, obdelovalca in podobdelovalca.
- 1.4 Obveznosti obdelovalca in podobdelovalca se uporabljajo samo, kadar se evidence privolitev, stanja preferenc ali navodila za preklic upravlja na podlagi dokumentiranih navodil upravljavca ali naročnika.
- 1.5 Ta politika ne določa privolitve kot privzete pravne podlage za obdelavo PII.
- 1.6 Določanje pravne podlage še naprej ureja PII03 - Politika popisa dejavnosti obdelave PII in pravne podlage.

2. Namen

- 2.1 Namen te politike je zagotoviti, da je upravljanje privolitev in preferenc zakonito, pregledno, dokazljivo, preklicljivo, tehnično izvršljivo in podprto z nadzorovanimi dokazili.
- 2.2 Ta politika zagotavlja, da se privolitev zahteva samo, kadar je to primerno, da so evidence privolitev popolne in sledljive, da se preklici upoštevajo ter da dokazila o privolitvi ostanejo na voljo za potrebe presoje, poizvedb in odgovornosti.

3. Cilji

3.1 Cilji te politike so:

- 3.1.1 Zagotoviti, da se privolitev uporablja samo, kadar je ustrezna pravna podlaga ali kadar je zahtevana za dejavnost obdelave.
- 3.1.2 Zagotoviti, da so zahteve za privolitev specifične, informirane, razločljive in povezane z veljavnim obvestilom o zasebnosti.
- 3.1.3 Zagotoviti, da se evidence privolitev in preferenc zajemajo in vzdržujejo v REG05.
- 3.1.4 Zagotoviti, da se preklici in spremembe preferenc obravnavajo v določenih operativnih rokih.
- 3.1.5 Zagotoviti, da so evidence privolitev povezane z nameni obdelave v REG02 in različicami obvestil v REG07.
- 3.1.6 Zagotoviti, da dejavnosti obdelovalcev in podobdelovalcev za podporo privolitvam sledijo dokumentiranim navodilom upravljavca ali naročnika.
- 3.1.7 Zagotoviti, da se mehanizmi privolitve spremljajo, pregledujejo, popravljajo in so primerni za presojo.

4. Izjave politike

4.1 Uporabljivost privolitve in pravna podlaga

- 4.1.1 [Controller] Process Owner / Business Owner mora v REG02 evidentirati, ali je privolitev zahtevana ali izbrana, preden se začne katera koli nova ali bistveno spremenjena dejavnost obdelave PII, ki temelji na privolitvi.
- 4.1.2 [Controller] Privacy Lead / PIMS Manager mora v REG02 in REG05 preveriti, da privolitev ni izbrana kot privzeta pravna podlaga, preden odobri novo ali bistveno spremenjeno dejavnost obdelave na podlagi privolitve.

- 4.1.3 [Controller] Data Protection Officer / Privacy Advisor mora pred uvedbo v REG04 pregledati podlago privolitve, kadar obdelava vključuje posebne vrste PII, storitve, namenjene otrokom, visoko tvegano obdelavo ali neravnovesje med organizacijo in posameznikom, na katerega se nanašajo osebno določljivi podatki.
- 4.1.4 [Joint Controller] Privacy Lead / PIMS Manager mora v REG02 in REG05 dokumentirati stranko, odgovorno za pridobivanje, evidentiranje, osveževanje in upoštevanje privolitve, preden se začne obdelava skupnih upravljavcev.
- 4.1.5 [Processor] Privacy Lead / PIMS Manager mora v REG08 in REG05 evidentirati navodila naročnika za zajem privolitve, upravljanje preferenc ali podporo pri preklicu, preden v imenu upravljavca uvede mehanizem privolitve.
- 4.1.6 [Subprocessor] Vendor / Procurement Owner mora v REG08 evidentirati obveznosti podobdelovalca v zvezi s privolitvijo, preden je podobdelovalcu dovoljeno obravnavati evidence privolitev, stanja preferenc ali navodila za preklic.

4.2 Zahtevanje in zajem privolitve

- 4.2.1 [Controller] Process Owner / Business Owner mora zagotoviti, da je vsaka zahteva za privolitev specifična glede namena in povezana z veljavno različico obvestila o zasebnosti REG07, preden se zahteva za privolitev predstavi posamezniku, na katerega se nanašajo osebno določljivi podatki.
- 4.2.2 [Controller] System Owner / Application Owner mora mehanizme privolitve konfigurirati tako, da zahtevajo pritrdilno dejanje, preden se začne obdelava, kadar je zahtevana izrecna privolitev ali privolitev z vključitvijo.
- 4.2.3 [Controller] Process Owner / Business Owner mora ob zajemu privolitve v REG05 evidentirati referenco posameznika, na katerega se nanašajo osebno določljivi podatki, namen, kategorijo PII, besedilo ali različico privolitve, različico obvestila o zasebnosti, kanal zajema, časovni žig, metodo, status in veljavno obdobje veljavnosti.
- 4.2.4 [Conditional] Privacy Lead / PIMS Manager mora v REG05 evidentirati logiko preverjanja starosti ali pooblastitve in pred uvedbo sprožiti pregled REG04, kadar se privolitev nanaša na obdelavo, namenjeno otrokom.
- 4.2.5 [Conditional] Privacy Lead / PIMS Manager mora privolitev v REG05 označiti kot izrecno, preden se začne obdelava, kadar je za izbrani namen zahtevana izrecna privolitev.
- 4.2.6 [Both] System Owner / Application Owner mora preprečiti nadaljevanje obdelave, ki temelji na privolitvi, preden REG05 za zadevni namen izkazuje aktiven status privolitve.

[... 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 izjemo pred odstopanjem od odobrene zahteve za zajem privolitve, upravljanje preferenc, preklic ali dokazila.
- 9.1.2 [All] Privacy Lead / PIMS Manager mora v REG12 odobriti ali zavrniti vsako izjemo v zvezi s privolitvijo pred izvedbo ter za vsako odobreno izjemo določiti datum poteka veljavnosti in kompenzacijsko kontrolo.
- 9.1.3 [Conditional] Data Protection Officer / Privacy Advisor mora izjemo v REG04 ali REG12 pregledati pred odobritvijo, kadar izjema vključuje izrecno privolitev, obdelavo, namenjeno otrokom, visoko tvegano obdelavo ali mehanizem preklica.
- 9.1.4 [Both] System Owner / Application Owner mora blokirati objavo v produkcijo ali onemogočiti prizadeti mehanizem privolitve, kadar izjema, zahtevana s to politiko, pred prehodom v produkcijo ni bila odobrena v REG12.

10. Uveljavljanje

- 10.1.1 [All] Privacy Lead / PIMS Manager mora v petih delovnih dneh po ugotovitvi manjkajočih, neveljavnih, nepovezanih ali nezanesljivih dokazil o privolitvi v REG12 evidentirati neskladnost v zvezi s privolitvijo.
- 10.1.2 [Controller] Process Owner / Business Owner mora začasno ustaviti ali sanirati obdelavo za prizadeti namen, preden se nadaljuje nadaljnja obdelava na podlagi privolitve, kadar je privolitev zahtevana, vendar je ni mogoče dokazati v REG05.
- 10.1.3 [Both] System Owner / Application Owner mora onemogočiti ali popraviti neskladen mehanizem zajema privolitve, preferenc ali preklica v roku, dodeljenem v REG12.
- 10.1.4 [Processor] Vendor / Procurement Owner mora napake pri navodilih naročnika, ki vključujejo evidence privolitev, stanja preferenc ali podporo pri preklicu, eskalirati v REG08 in REG12 v petih delovnih dneh od ugotovitve.
- 10.1.5 [All] Internal Audit / Compliance Reviewer mora do dodeljenega roka zapadlosti v REG12 preveriti dokazila o zaprtju korektivnih ukrepov v zvezi s privolitvijo.

11. Pregled in vzdrževanje

- 11.1.1 [All] Privacy Lead / PIMS Manager mora to politiko pregledati letno in izid pregleda evidentirati v REG12.
- 11.1.2 [All] Privacy Lead / PIMS Manager mora to politiko pregledati v 30 dneh po bistveni spremembi zakonodaje o privolitvi, tehnologije privolitev, orodij za upravljanje preferenc, strukture obvestil o zasebnosti ali zahtev za certifikacijo PIMS.
- 11.1.3 [All] Data Protection Officer / Privacy Advisor mora spremembe te politike, pomembne z vidika zasebnosti, pregledati v REG12 pred odobritvijo.
- 11.1.4 [All] Top Management mora bistvene spremembe te politike odobriti v REG12 pred objavo.
- 11.1.5 [All] Privacy Lead / PIMS Manager mora komunikacijo odobrenih sprememb politike evidentirati v REG11 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 za zasebnost
- 12.4 PII03 - Politika popisa dejavnosti obdelave PII in pravne podlage
- 12.5 PII04 - Politika obvestil o zasebnosti in preglednosti
- 12.6 PII06 - Politika upravljanja pravic posameznikov, na katere se nanašajo osebno določljivi podatki
- 12.7 PII07 - Politika ocene tveganj za zasebnost in DPIA
- 12.8 PII08 - Politika vgrajenega in privzetega varstva zasebnosti
- 12.9 PII09 - Politika zbiranja, uporabe, razkritja in deljenja PII
- 12.10 PII10 - Politika hrambe, izbrisa in odstranjevanja PII
- 12.11 PII11 - Politika točnosti in kakovosti PII
- 12.12 PII12 - Politika upravljanja zasebnosti obdelovalcev, podobdelovalcev in tretjih oseb
- 12.13 PII14 - Politika varnosti in nadzora dostopa do PII
- 12.14 PII16 - Politika usposabljanja, ozaveščanja in usposobljenosti za zasebnost
- 12.15 PII17 - Politika dokumentiranih informacij in upravljanja dokazil PIMS
- 12.16 PII18 - Politika spremljanja, presoje in izboljševanja PIMS

13. Referenčni standardi in okviri

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

13.3 ISO/IEC 27701:2025

- 13.3.1 **Clause 7.5; Clause 8.1** - Preslikano na dokumentirane informacije in operativno obvladovanje za določanje uporabljivosti privolitve, zajemanje dokazil o privolitvi, upravljanje preklica, vzdrževanje različic evidenc privolitve, testiranje mehanizmov in vzdrževanje REG05. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.2; 4.5.3; 4.5.4; 7.1.1; 7.1.2; 7.1.3; 7.1.6].
- 13.3.2 **Clause 9.1; Clause 10.2** - Preslikano na spremljanje privolitev, kazalnike, vzorčenje pri presoji, evidentiranje neskladnosti, korektivne ukrepe in preverjanje učinkovitosti. Addressed by clauses [4.5.5; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.2; 10.1.3; 10.1.4; 10.1.5].
- 13.3.3 **Annex A.1.2.3** - Preslikano na potrjevanje, kdaj je privolitev ustrezna pravna podlaga, in povezovanje evidenc privolitev z evidencami pravnih podlag REG02. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.2; 4.5.3].
- 13.3.4 **Annex A.1.2.4; Annex A.1.2.5** - Preslikano na določanje, kdaj in kako se privolitev pridobi, zajem privolitve, evidentiranje dokazil, upravljanje izrecne privolitve, preklica, osvežitve in statusa privolitve. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].
- 13.3.5 **Annex A.1.2.9** - Preslikano na evidence upravljavca za obdelavo na podlagi privolitve, zgodovino privolitve, povezavo z obvestilom, hrambo dokazil in evidence privolitev, pripravljene za presojo. Addressed by clauses [4.2.3; 4.3.6; 4.5.1; 4.5.3; 7.1.1; 8.1.1; 8.1.3].
- 13.3.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Preslikano na dogovore obdelovalca z naročniki, uskladitev namenov in navodil naročnika ter evidence obdelovalca, kadar se storitve podpore privolitvam izvajajo za upravljavca. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 8.1.4; 10.1.4].
- 13.3.7 **Annex A.2.3.2** - Preslikano na podporo obdelovalca obveznostim upravljavca do posameznikov, na katere se nanašajo osebno določljivi podatki, kadar se preklic privolitve, spremembe preferenc ali dokazila o privolitvi obravnavajo na podlagi navodila naročnika. Addressed by clauses [4.3.4; 4.3.5; 4.5.4; 6.1.4; 8.1.4].
- 13.3.8 **Annex A.3.14** - Preslikano na zaščito evidenc privolitev in preferenc pred nepooblaščenim spreminjanjem ter ohranjanje dokazil revizijske sledi. Addressed by clauses [4.5.2; 5.1.6; 7.1.2; 10.1.5].

13.4 GDPR

- 13.4.1 **Article 4(11)** - Preslikano na merila za privolitev, ki zahtevajo, da je privolitev specifična, informirana, pritrtilna, kadar je to zahtevano, in povezana z zadevnim namenom ter različico obvestila. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.5].
- 13.4.2 **Article 5(1)(a); Article 5(2)** - Preslikano na zakonitost, poštenost, preglednost, dokazila odgovornosti, vzorčenje pri presoji, korektivne ukrepe in dokazovanje obdelave na podlagi privolitve. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.5.3; 4.5.5; 8.1.1; 8.1.5; 10.1.1; 10.1.5].
- 13.4.3 **Article 6(1)(a); Article 6(4)** - Preslikano na privolitev kot pravno podlago za specifične namene ter na ponovno presojo ali osveženo privolitev, kadar se namen ali pogoji obdelave bistveno spremenijo. Addressed by clauses [4.1.1; 4.1.2; 4.4.1; 4.4.2; 4.5.3].

- 13.4.4 Article 7 - Preslikano na dokazljivost, razločljive zahteve za privolitev, preklic, enostavnost preklica, veljavnost privolitve in ohraneno zgodovino privolitve. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.4; 4.4.5; 10.1.2].
- 13.4.5 Article 8 - Preslikano na eskalacijo privolitve pri storitvah, namenjenih otrokom, logiko preverjanja starosti ali pooblastitve ter pregled tveganj za zasebnost pred uvedbo. Addressed by clauses [4.1.3; 4.2.4; 9.1.3].
- 13.4.6 **Article 9(2)(a)** - Preslikano na obravnavo izrecne privolitve, kadar je izrecna privolitev izbrana za obdelavo posebnih vrst podatkov. Addressed by clauses [4.1.3; 4.2.5; 9.1.3].
- 13.4.7 **Article 24** - Preslikano na upravljavske ukrepe upravljavca, pregled, odobritev, izjeme, korektivne ukrepe in vodstveni nadzor nad kontrolami privolitve. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.2; 6.1.3; 9.1.1; 9.1.2; 11.1.1; 11.1.4].
- 13.4.8 **Article 28** - Preslikano na obravnavo navodil obdelovalca, dokazila za podporo privolitvam, podporo pri preklicu, obveznosti podobdelovalca in eskalacijo navodil naročnika. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 10.1.4].
- 13.4.9 **Article 30** - Preslikano na povezovanje evidenc privolitev z nameni obdelave, evidence upravljavca, evidence podpore obdelovalca in sledljivost REG02/REG05. Addressed by clauses [4.1.1; 4.5.3; 4.5.4; 7.1.1; 8.1.1].

13.5 ISO/IEC 29100:2020

- 13.5.1 **Clause 5.2; Clause 5.8; Clause 5.12** - Preslikano na privolitev in izbiro, preglednost in povezavo z obvestilom, preklic, odgovornost ter dokazila o skladnosti z zasebnostjo. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.5.3; 4.5.5; 8.1.1; 10.1.1].

13.6 ISO/IEC 29151:2022

- 13.6.1 **Annex A.3** - Preslikano na kontrole za privolitev in izbiro, ki zahtevajo smiselno, informirano in nedvoumno privolitev, spremembo preferenc ter pravočasne spremembe obdelave po spremembi ali preklicu privolitve. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.4.5].

13.7 ISO/IEC TS 27560:2023

- 13.7.1 **Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4** - Preslikano na koncepte zapisa in potrdila o privolitvi, vodenje evidenc privolitev, strukturo evidence privolitve, status privolitve, povezavo z različico obvestila, strukturo potrdila in razlago potrdila o privolitvi, kadar se take evidence ali potrdila uporabljajo. Addressed by clauses [4.2.3; 4.3.2; 4.3.6; 4.4.3; 4.4.4; 4.5.2; 4.5.3; 7.1.6].

13.8 Internal Requirements

- 13.8.1 Notranja zahteva - Klavzule, ki določajo REG05 kot avtoritativni dokazni objekt, odobritev nestandardnih dokazil, blokiranje operativne objave, usposabljanje, vzdrževanje politike in podporo komuniciranju, podpirajo doslednost izvedbe, vendar niso neposredno preslikane na posamezno zunanjo klavzulo. Addressed by clauses [4.5.1; 5.1.2; 7.1.5; 9.1.4; 11.1.2; 11.1.3; 11.1.5].