

				Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII05				Naziv dokumenta: Politika upravljanja privolama i preferencijama							
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

<p>Pravna napomena (autorska prava i ograničenja uporabe) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Ovaj dokument intelektualno je vlasništvo društva Clarysec LLC. Nijedan dio ovog dokumenta ne smije se kopirati, ponovno upotrebljavati, distribuirati niti mijenjati u komercijalne svrhe ili svrhe implementacije bez izričitog prethodnog pisanog odobrenja.</p> <p>Neovlaštena uporaba strogo je zabranjena i može rezultirati pravnim postupkom.</p> <p>Za licenciranje kontaktirajte: info@clarysec.com</p>

Usklađeno sa standardima i propisima

Standard / propis	Točka / kontrola / članak	Primjenjivost	Vrsta pokrivenosti	Napomena
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentirane informacije i operativna kontrola za dokaze o privoli
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Praćenje, nesukladnost, korektivna radnja i poboljšanje
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Supporting	Povezivanje s pravnom osnovom
ISO/IEC 27701:2025	Annex A.1.2.4; Annex A.1.2.5	Controller	Primary	Utvrđivanje, pribavljanje i evidentiranje privole
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Zapisi obrade voditelja obrade
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Sporazumi izvršitelja obrade, svrhe klijenta i zapisi izvršitelja obrade
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Podrška izvršitelja obrade obvezama voditelja obrade prema ispitanicima
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Zaštita zapisa o obradi osobnih podataka (PII)
GDPR	Article 4(11)	Controller	Supporting	Kriteriji privole
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Zakonitost, poštenost, transparentnost i odgovornost
GDPR	Article 6(1)(a); Article 6(4)	Controller	Primary	Privola kao pravna osnova i poveznica s promijenjenom svrhom
GDPR	Article 7	Controller	Primary	Uvjeti privole i povlačenje
GDPR	Article 8	Conditional	Supporting	Eskalacija privole djeteta

GDPR	Article 9(2)(a)	Conditional	Supporting	Izričita privola za obradu posebnih kategorija podataka
GDPR	Article 24	Controller	Supporting	Odgovornost i mjere voditelja obrade
GDPR	Article 28	Both	Supporting	Povezanost uputa i pomoći izvršitelja obrade
GDPR	Article 30	Both	Supporting	Povezanost sa zapisima obrade
ISO/IEC 29100:2020	Clause 5.2; Clause 5.8; Clause 5.12	Both	Supporting	Načela privole i izbora, transparentnosti i usklađenosti
ISO/IEC 29151:2022	Annex A.3	Both	Supporting	Kontrole privole i izbora
ISO/IEC TS 27560:2023	Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4	Conditional	Supporting	Struktura zapisa i potvrde o privoli kada se upotrebljavaju

1. Opseg

- 1.1 Ova politika definira obvezne zahtjeve za utvrđivanje kada je privola potrebna, traženje privole, prikupljanje dokaza o privoli, upravljanje preferencijama, obradu povlačenja, održavanje zapisa o privoli i pregled mehanizama privole.
- 1.2 Ova se politika primjenjuje na obradu osobnih podataka (PII) kada je privola odabrana ili potrebna kao pravna osnova, kada je potrebna izričita privola, kada se prikupljaju preferencije privole ili kada organizacija upravlja zapisima o privoli u ime voditelja obrade.
- 1.3 Ova se politika primjenjuje u kontekstima voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade.
- 1.4 Obveze izvršitelja obrade i podizvršitelja obrade primjenjuju se samo kada se zapisima o privoli, stanjima preferencija ili uputama za povlačenje upravlja prema dokumentiranim uputama voditelja obrade ili klijenta.
- 1.5 Ova politika ne čini privolu zadanom pravnom osnovom za obradu osobnih podataka (PII).
- 1.6 Utvrđivanje pravne osnove i dalje je uređeno politikom PII03 - Politika popisa aktivnosti obrade PII i pravne osnove.

2. Svrha

- 2.1 Svrha ove politike jest osigurati da upravljanje privolama i preferencijama bude zakonito, transparentno, dokazivo, opozivo, tehnički provedivo i potkrijepljeno kontroliranim dokazima.
- 2.2 Ova politika osigurava da se privola traži samo kada je to primjereno, da su zapisi o privoli potpuni i sljedivi, da se povlačenja poštuju te da dokazi o privoli ostanu dostupni za potrebe revizije, upita i odgovornosti.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

- 3.1.1 Osigurati da se privola upotrebljava samo kada je odgovarajuća pravna osnova ili kada je potrebna za aktivnost obrade.
- 3.1.2 Osigurati da su zahtjevi za privolu specifični, informirani, jasno odvojivi i povezani s primjenjivom obavijesti o privatnosti.
- 3.1.3 Osigurati da se zapisi o privoli i preferencijama prikupljaju i održavaju u REG05.
- 3.1.4 Osigurati da se po povlačenjima i promjenama preferencija postupa unutar definiranih operativnih rokova.
- 3.1.5 Osigurati da su zapisi o privoli povezani sa svrhama obrade u REG02 i verzijama obavijesti u REG07.
- 3.1.6 Osigurati da aktivnosti izvršitelja obrade i podizvršitelja obrade koje pružaju podršku privoli slijede dokumentirane upute voditelja obrade ili klijenta.
- 3.1.7 Osigurati da se mehanizmi privole prate, pregledavaju, ispravljaju i da su revizijski provjerljivi.

4. Izjave politike

4.1 Primjenjivost privole i pravna osnova

- 4.1.1 [Controller] Process Owner / Business Owner MORA u REG02 evidentirati je li privola potrebna ili odabrana prije početka bilo koje nove ili značajno izmijenjene aktivnosti obrade osobnih podataka (PII) koja se oslanja na privolu.
- 4.1.2 [Controller] Privacy Lead / PIMS Manager MORA u REG02 i REG05 provjeriti da privola nije odabrana kao zadana pravna osnova prije odobravanja nove ili značajno izmijenjene aktivnosti obrade koja se temelji na privoli.

- 4.1.3 [Controller] Data Protection Officer / Privacy Advisor MORA pregledati osnovu privole u REG04 prije pokretanja kada obrada uključuje posebne kategorije osobnih podataka (PII), usluge namijenjene djeci, obradu visokog rizika ili neravnotežu između organizacije i ispitanika.
- 4.1.4 [Joint Controller] Privacy Lead / PIMS Manager MORA u REG02 i REG05 dokumentirati stranu odgovornu za pribavljanje, evidentiranje, obnavljanje i poštivanje privole prije početka obrade u okviru zajedničkog voditeljstva obrade.
- 4.1.5 [Processor] Privacy Lead / PIMS Manager MORA evidentirati upute klijenta za prikupljanje privole, upravljanje preferencijama ili podršku povlačenju u REG08 i REG05 prije implementacije mehanizma privole u ime voditelja obrade.
- 4.1.6 [Subprocessor] Vendor / Procurement Owner MORA evidentirati obveze podizvršitelja obrade povezane s privolom u REG08 prije nego što se podizvršitelju obrade dopusti rukovanje zapisima o privoli, stanjima preferencija ili uputama za povlačenje.

4.2 Zahtjev za privolu i prikupljanje privole

- 4.2.1 [Controller] Process Owner / Business Owner MORA osigurati da je svaki zahtjev za privolu specifičan za svrhu i povezan s primjenjivom verzijom obavijesti o privatnosti u REG07 prije nego što se zahtjev za privolu predstavi ispitaniku.
- 4.2.2 [Controller] System Owner / Application Owner MORA konfigurirati mehanizme privole tako da zahtijevaju potvrđenu radnju prije početka obrade kada je potrebna izričita privola ili privola na temelju uključivanja.
- 4.2.3 [Controller] Process Owner / Business Owner MORA u REG05 evidentirati referencu ispitanika, svrhu, kategoriju osobnih podataka (PII), tekst ili verziju privole, verziju obavijesti o privatnosti, kanal prikupljanja, vremensku oznaku, metodu, status i primjenjivo razdoblje valjanosti kada se privola prikupi.
- 4.2.4 [Conditional] Privacy Lead / PIMS Manager MORA u REG05 evidentirati logiku provjere dobi ili autorizacije i pokrenuti pregled u REG04 prije pokretanja kada se privola odnosi na obradu namijenjenu djeci.
- 4.2.5 [Conditional] Privacy Lead / PIMS Manager MORA u REG05 označiti privolu kao izričitu prije početka obrade kada je za odabranu svrhu potrebna izričita privola.
- 4.2.6 [Both] System Owner / Application Owner MORA spriječiti nastavak obrade koja se oslanja na privolu prije nego što REG05 pokaže aktivan status privole za relevantnu svrhu.

[... 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 zatražiti iznimku u REG12 prije odstupanja od odobrenog zahtjeva za prikupljanje privole, upravljanje preferencijama, povlačenje ili dokaze.
- 9.1.2 [All] Privacy Lead / PIMS Manager MORA odobriti ili odbiti svaku iznimku povezanu s privolom u REG12 prije implementacije te dodijeliti datum isteka i kompenzacijsku kontrolu za svaku odobrenu iznimku.
- 9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MORA pregledati iznimku u REG04 ili REG12 prije odobrenja kada iznimka uključuje izričitu privolu, obradu namijenjenu djeci, obradu visokog rizika ili mehanizam povlačenja.
- 9.1.4 [Both] System Owner / Application Owner MORA blokirati produkcijsko izdanje ili onemogućiti zahvaćeni mehanizam privole kada iznimka koju zahtijeva ova politika nije odobrena u REG12 prije puštanja u produkcijski rad.

10. Provedba

- 10.1.1 [All] Privacy Lead / PIMS Manager MORA evidentirati nesukladnost povezanu s privolom u REG12 u roku od pet radnih dana od utvrđivanja nedostajućih, nevaljanih, nepovezanih ili nepouzdanih dokaza o privoli.
- 10.1.2 [Controller] Process Owner / Business Owner MORA obustaviti ili ispraviti obradu za zahvaćenu svrhu prije nastavka daljnje obrade koja se temelji na privoli kada je privola potrebna, ali se ne može dokazati u REG05.
- 10.1.3 [Both] System Owner / Application Owner MORA onemogućiti ili ispraviti nesukladan mehanizam za prikupljanje privole, preferencije ili povlačenje u roku dodijeljenom u REG12.
- 10.1.4 [Processor] Vendor / Procurement Owner MORA eskalirati neuspjeh uputa klijenta koji uključuju zapise o privoli, stanja preferencija ili podršku povlačenju u REG08 i REG12 u roku od pet radnih dana od utvrđivanja.
- 10.1.5 [All] Internal Audit / Compliance Reviewer MORA provjeriti dokaze o zatvaranju korektivnih radnji povezanih s privolom u REG12 do dodijeljenog krajnjeg roka.

11. Pregled i održavanje

- 11.1.1 [All] Privacy Lead / PIMS Manager MORA pregledati ovu politiku jednom godišnje i evidentirati ishod pregleda u REG12.
- 11.1.2 [All] Privacy Lead / PIMS Manager MORA pregledati ovu politiku u roku od 30 dana od značajne promjene propisa o privoli, tehnologije privole, alata za upravljanje preferencijama, strukture obavijesti o privatnosti ili zahtjeva za PIMS certifikaciju.
- 11.1.3 [All] Data Protection Officer / Privacy Advisor MORA pregledati promjene ove 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 evidentirati komunikaciju odobrenih promjena politike u REG11 u roku od 30 dana od objave.

12. Povezane politike

- 12.1 Ovu politiku podupiru sljedeće povezane politike:
- 12.2 PII01 - Politika sustava za upravljanje informacijama o privatnosti
- 12.3 PII02 - Politika uloga, odgovornosti i odgovornosti za privatnost
- 12.4 PII03 - Politika popisa aktivnosti obrade PII i pravne osnove
- 12.5 PII04 - Politika obavijesti o privatnosti i transparentnosti
- 12.6 PII06 - Politika upravljanja pravima ispitanika
- 12.7 PII07 - Politika procjene rizika za privatnost i DPIA
- 12.8 PII08 - Politika ugrađene i zadane zaštite privatnosti
- 12.9 PII09 - Politika prikupljanja, uporabe, otkrivanja i dijeljenja PII
- 12.10 PII10 - Politika zadržavanja, brisanja i zbrinjavanja PII
- 12.11 PII11 - Politika točnosti i kvalitete PII
- 12.12 PII12 - Politika upravljanja privatnošću izvršitelja obrade, podizvršitelja obrade i trećih strana
- 12.13 PII14 - Politika sigurnosti i kontrole pristupa PII
- 12.14 PII16 - Politika osposobljavanja, podizanja svijesti i kompetencija u području privatnosti
- 12.15 PII17 - Politika dokumentiranih informacija i upravljanja dokazima PIMS
- 12.16 PII18 - Politika praćenja, revizije i poboljšanja PIMS

13. Referentni standardi i okviri

13.1 Ova je politika mapirana na sljedeće standarde i propise. Mapiranje objašnjava kako politika podupire navedene zahtjeve i identificira interne odredbe koje ih provode ili podupiru.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapirano na dokumentirane informacije i operativnu kontrolu za utvrđivanje primjenjivosti privole, prikupljanje dokaza o privoli, upravljanje povlačenjem, verzioniranje zapisa o privoli, testiranje mehanizama i održavanje 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].

13.2.2 **Clause 9.1; Clause 10.2** - Mapirano na praćenje privole, metrike, revizijsko uzorkovanje, evidentiranje nesukladnosti, korektivnu radnju i provjeru 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].

13.2.3 **Annex A.1.2.3** - Mapirano na potvrđivanje kada je privola odgovarajuća pravna osnova i povezivanje zapisa o privoli sa zapisima o pravnoj osnovi u REG02. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.2; 4.5.3].

13.2.4 **Annex A.1.2.4; Annex A.1.2.5** - Mapirano na utvrđivanje kada i kako se privola pribavlja, prikupljanje privole, evidentiranje dokaza, upravljanje izričitom privolom, povlačenjem, obnavljanjem i statusom privole. 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].

13.2.5 **Annex A.1.2.9** - Mapirano na zapise voditelja obrade za obradu koja se temelji na privoli, povijest privole, povezivanje obavijesti, zadržavanje dokaza i zapise o privoli spremne za reviziju. Addressed by clauses [4.2.3; 4.3.6; 4.5.1; 4.5.3; 7.1.1; 8.1.1; 8.1.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapirano na ugovore izvršitelja obrade s klijentima, usklađivanje svrhe i uputa klijenta te zapise izvršitelja obrade kada se usluge podrške privoli obavljaju za voditelja obrade. 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].

13.2.7 **Annex A.2.3.2** - Mapirano na podršku izvršitelja obrade obvezama voditelja obrade prema ispitanicima kada se povlačenje privole, promjene preferencija ili dokazi o privoli obrađuju prema uputi klijenta. Addressed by clauses [4.3.4; 4.3.5; 4.5.4; 6.1.4; 8.1.4].

13.2.8 **Annex A.3.14** - Mapirano na zaštitu zapisa o privoli i preferencijama od neovlaštene izmjene te na očuvanje dokaza revizijskog traga. Addressed by clauses [4.5.2; 5.1.6; 7.1.2; 10.1.5].

13.3 GDPR

13.3.1 **Article 4(11)** - Mapirano na kriterije privole koji zahtijevaju da privola bude specifična, informirana, potvrdna kada je potrebno te povezana s relevantnom svrhom i verzijom obavijesti. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.5].

13.3.2 **Article 5(1)(a); Article 5(2)** - Mapirano na zakonitost, poštenost, transparentnost, dokaze o odgovornosti, revizijsko uzorkovanje, korektivnu radnju i dokaz obrade koja se temelji na privoli. 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].

13.3.3 **Article 6(1)(a); Article 6(4)** - Mapirano na privolu kao pravnu osnovu za specifične svrhe te na ponovnu procjenu ili obnovljenu privolu kada se svrha ili uvjeti obrade značajno promijene. Addressed by clauses [4.1.1; 4.1.2; 4.4.1; 4.4.2; 4.5.3].

13.3.4 **Article 7** - Mapirano na dokazivost, odvojive zahtjeve za privolu, povlačenje, jednostavnost povlačenja, valjanost privole i zadržanu povijest privole. 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].

- 13.3.5 **Article 8** - Mapirano na eskalaciju privole u uslugama namijenjenima djeci, logiku provjere dobi ili autorizacije te pregled rizika za privatnost prije pokretanja. Addressed by clauses [4.1.3; 4.2.4; 9.1.3].
- 13.3.6 **Article 9(2)(a)** - Mapirano na postupanje s izričitom privolom kada je izričita privola odabrana za obradu posebnih kategorija podataka. Addressed by clauses [4.1.3; 4.2.5; 9.1.3].
- 13.3.7 **Article 24** - Mapirano na upravljačke mjere voditelja obrade, pregled, odobrenje, iznimke, korektivnu radnju i nadzor uprave nad kontrolama privole. 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].
- 13.3.8 **Article 28** - Mapirano na postupanje prema uputama izvršitelja obrade, dokaze o podršci privoli, podršku povlačenju, obveze podizvršitelja obrade i eskalaciju uputa klijenta. 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].
- 13.3.9 **Article 30** - Mapirano na povezivanje zapisa o privoli sa svrhama obrade, zapise voditelja obrade, zapise podrške izvršitelja obrade i sljedivost REG02/REG05. Addressed by clauses [4.1.1; 4.5.3; 4.5.4; 7.1.1; 8.1.1].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.2; Clause 5.8; Clause 5.12** - Mapirano na privolu i izbor, transparentnost i povezanost s obavijesti, povlačenje, odgovornost i dokaze usklađenosti privatnosti. 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].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Annex A.3** - Mapirano na kontrole privole i izbora koje zahtijevaju smislen, informiran i nedvosmislen pristanak, izmjenu preferencija i pravodobne promjene obrade nakon izmjene ili povlačenja privole. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.4.5].

13.6 ISO/IEC TS 27560:2023

- 13.6.1 **Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4** - Mapirano na koncepte zapisa i potvrde o privoli, vođenje zapisa o privoli, strukturu zapisa o privoli, status privole, povezanost s verzijom obavijesti, strukturu potvrde i tumačenje potvrde o privoli kada se takvi zapisi ili potvrde upotrebljavaju. 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].

13.7 Interni zahtjevi

- 13.7.1 **Interni zahtjev** - Odredbe koje definiraju REG05 kao mjerodavni dokazni objekt, odobrenje nestandardnih dokaza, blokiranje operativnog izdanja, osposobljavanje, održavanje politike i komunikaciju podupiru dosljednost implementacije, ali nisu izravno mapirane na jednu vanjsku odredbu. Addressed by clauses [4.5.1; 5.1.2; 7.1.5; 9.1.4; 11.1.2; 11.1.3; 11.1.5].