

				Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII08				Naziv dokumenta: Politika ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama							
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

Pravna napomena (autorska prava i ograničenja uporabe)
(C) 2025 Clarysec LLC. All rights reserved.

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.

Neovlaštena uporaba strogo je zabranjena i može rezultirati pravnim postupkom.

Za licenciranje kontaktirajte: info@clarysec.com

Usklađeno sa standardima i propisima

Standard / regulativa	Točka / kontrola / članak	Primjenjivost	Vrsta pokrivenosti	Napomena
ISO/IEC 27701:2025	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Poveznica s procjenom rizika za privatnost i obradom rizika za privatnost
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Planirane promjene i operativna kontrola
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Dokumentirani dokazi o ugrađenoj zaštiti privatnosti
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Praćenje i korektivne radnje
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9	Controller	Supporting	Svrhe, okidač za PIA-u i zapisi
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Ograničenje prikupljanja i obrade
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Ciljevi točnosti i minimizacije
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Projektiranje deidentifikacije, brisanja i privremenih datoteka
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Ugovor s klijentom, podrška i zapisi izvršitelja obrade
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Projektne mogućnosti izvršitelja obrade
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Životni ciklus razvoja i inženjerska načela
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Ograničenje svrhe, minimizacija i odgovornost
GDPR	Article 24	Controller	Supporting	Mjere voditelja obrade
GDPR	Article 25	Controller	Primary	Zaštita podataka u fazi projektiranja i

				prema zadanim postavkama
GDPR	Article 28	Both	Supporting	Upute izvršitelju obrade i pomoć
GDPR	Article 30	Both	Supporting	Evidencije obrade
GDPR	Article 35	Controller	Supporting	Poveznica s okidačem za DPIA
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Kontrole privatnosti u fazi projektiranja
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Svrha, prikupljanje, minimizacija i ograničenje uporabe
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Točnost, odgovornost i usklađenost
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Načela i kontrole zaštite osobnih podataka (PII)

1. Opseg

1.1 Ova politika definira zahtjeve za ugradnju ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama u nove i izmijenjene aktivnosti obrade osobnih podataka (PII), projekte, proizvode, usluge, sustave, aplikacije, integracije, aktivnosti nabave i promjene poslovnih procesa unutar opsega PIMS-a.

1.2 Ova politika primjenjuje se na kontekste voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade. Obveze izvršitelja obrade i podizvršitelja obrade primjenjuju se kada organizacija projektira, konfigurira, mijenja ili provodi obradu u ime klijenta, voditelja obrade ili nadređenog izvršitelja obrade prema dokumentiranim uputama.

1.3 Ova politika obuhvaća:

- 1.3.1 zahtjeve privatnosti pri pokretanju projekta;
- 1.3.2 kontrole projektiranja za svrhu, minimizaciju podataka i zadane postavke;
- 1.3.3 pregled ugrađene zaštite privatnosti prije puštanja u produkcijski rad;
- 1.3.4 pregled ugrađene zaštite privatnosti potaknut promjenom;
- 1.3.5 provjere zaštite privatnosti u fazi projektiranja pri nabavi;
- 1.3.6 poveznicu s rizikom za privatnost, provjerom potrebe za DPIA-om i dokazima o korektivnim radnjama.

1.4 Ova politika ne zamjenjuje:

- 1.4.1 PII03 za popis obrade, svrhe, pravnu osnovu i ROPA zapise;
- 1.4.2 PII04 za sadržaj i objavu obavijesti o privatnosti;
- 1.4.3 PII05 za kontrole privole i preferencija;
- 1.4.4 PII06 za postupanje sa zahtjevima ispitanika;
- 1.4.5 PII07 za metodologiju procjene rizika za privatnost i DPIA-e;
- 1.4.6 PII09 za kontrole prikupljanja, uporabe, otkrivanja i dijeljenja;
- 1.4.7 PII10 za provedbu zadržavanja, brisanja i zbrinjavanja;
- 1.4.8 PII11 za operativno osiguravanje točnosti i kvalitete;
- 1.4.9 PII12 za upravljanje životnim ciklusom izvršitelja obrade, podizvršitelja obrade i trećih strana;
- 1.4.10 PII13 za mehanizme međunarodnog prijenosa;
- 1.4.11 PII14 za sigurnost osobnih podataka (PII) i operativnu kontrolu pristupa;
- 1.4.12 PII18 za upravljanje praćenjem, revizijom, korektivnim radnjama i poboljšanjima na razini PIMS-a.

2. Svrha

2.1 Svrha je ove politike osigurati da se zahtjevi privatnosti utvrde, provedu i potkrijepe dokazima prije početka ili značajne promjene obrade osobnih podataka (PII), te da su sustavi i procesi prema zadanim postavkama konfigurirani tako da ograničavaju prikupljanje, uporabu, izloženost, ovisnost o zadržavanju, ovisnost o otkrivanju i mogućnost identifikacije osobnih podataka (PII) na ono što je nužno za dokumentiranu svrhu.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

- 3.1.1 ugraditi zahtjeve privatnosti u odluke o pokretanju projekta, projektiranju, nabavi, promjenama i puštanju u produkcijski rad;
- 3.1.2 osigurati da su projekti obrade osobnih podataka (PII) povezani s dokumentiranim svrhama i zapisima obrade u REG02;

- 3.1.3 provesti minimizaciju podataka i zadane postavke koje štite privatnost prije početka obrade;
- 3.1.4 osigurati pokretanje procjene rizika za privatnost i provjere potrebe za DPIA-om bez dupliciranja metodologije iz PII07;
- 3.1.5 osigurati evidentiranje zahtjeva projektiranja za nabavu i izvršitelje obrade bez dupliciranja upravljanja životnim ciklusom iz PII12;
- 3.1.6 osigurati eskalaciju neriješenih pitanja projektiranja putem REG12;
- 3.1.7 održavati dokaze o ugrađenoj zaštiti privatnosti spremne za reviziju u REG02, REG04, REG08 i REG12.

4. Izjave politike

4.1 Pokretanje projekta i zahtjevi privatnosti

- 4.1.1 [Both] Process Owner / Business Owner mora evidentirati unos o ugrađenoj zaštiti privatnosti u REG04 prije pokretanja bilo kojeg projekta, proizvoda, usluge, sustava, aplikacije, integracije ili promjene poslovnog procesa koji uključuje osobne podatke (PII).
- 4.1.2 [Both] Process Owner / Business Owner mora povezati svaki unos o ugrađenoj zaštiti privatnosti u REG04 s postojećom ili nacrtnom aktivnosti obrade u REG02 prije odobrenja funkcionalnih zahtjeva.
- 4.1.3 [Controller] Privacy Lead / PIMS Manager mora evidentirati zahtjeve voditelja obrade za zaštitu privatnosti u fazi projektiranja u REG04 prije odobrenja funkcionalnog projekta voditelja obrade.
- 4.1.4 [Processor] Vendor / Procurement Owner mora evidentirati upute klijenta za ugrađenu zaštitu privatnosti i ugovorna ograničenja projektiranja u REG08 prije odobrenja projekta usluge izvršitelja obrade ili značajne promjene usluge.
- 4.1.5 [Conditional] Data Protection Officer / Privacy Advisor mora evidentirati savjet u REG04 prije odobrenja visokorizičnog, novog, osjetljivog, automatiziranog, opsežnog ili značajno izmijenjenog projekta obrade osobnih podataka (PII).
- 4.1.6 [Both] Information Security Lead mora evidentirati ovisnosti o sigurnosnim kontrolama osobnih podataka (PII) koje podupiru ugrađenu zaštitu privatnosti u REG04 prije odobrenja arhitekture.

4.2 Minimizacija podataka i zaštita privatnosti prema zadanim postavkama

- 4.2.1 [Controller] Process Owner / Business Owner mora dokumentirati minimalne kategorije osobnih podataka (PII), kategorije ispitanika, izvore i svrhe u REG02 i REG04 prije odobrenja projekta prikupljanja ili uvoza.
- 4.2.2 [Both] System Owner / Application Owner mora konfigurirati zadane postavke obrade na najmanji opseg prikupljanja i obrade osobnih podataka (PII) potreban za dokumentiranu svrhu te evidentirati dokaze u REG04 prije puštanja u produkcijski rad.
- 4.2.3 [Controller] Process Owner / Business Owner mora dokumentirati neobvezna polja osobnih podataka (PII), neobvezne izbore obrade i postavke koje su prema zadanim postavkama isključene u REG02 i REG04 prije odobrenja korisničkog sučelja, obrasca ili tijeka rada.
- 4.2.4 [Both] System Owner / Application Owner mora dokumentirati zadane postavke izloženosti privatnosti za prikaze, izvješća, izvoze, sučelja i automatizirane tijekove rada u REG04 prije puštanja u produkcijski rad.
- 4.2.5 [Both] Process Owner / Business Owner mora dokumentirati izvedivost deidentifikacije, pseudonimizacije, agregiranja ili obrade bez mogućnosti identifikacije u REG04 prije odobrenja

uporabe osobnih podataka (PII) koji omogućuju identifikaciju za testiranje, analitiku, izvješćivanje ili sekundarnu operativnu uporabu.

4.2.6 [Both] System Owner / Application Owner mora dokumentirati postupanje s privremenim artefaktima osobnih podataka (PII), uključujući privremene datoteke, predmemorije, zapise dnevnika ili pripreme zapise, u REG04 prije puštanja u produkcijski rad.

4.2.7 [Both] Process Owner / Business Owner mora usmjeriti zahtjeve projektiranja koji su u nadležnosti PII10, PII11, PII13 ili PII14 na povezani put dokazivanja politike u REG04 u roku od pet radnih dana od utvrđivanja ovisnosti.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Iznimke

9.1 Iznimke ugrađene zaštite privatnosti

9.1.1 [Both] Process Owner / Business Owner mora zatražiti iznimku ugrađene zaštite privatnosti u REG12 prije odobrenja projekta ili promjene koja ne može ispuniti primjenjivi zahtjev ugrađene zaštite privatnosti.

9.1.2 [Both] Privacy Lead / PIMS Manager mora procijeniti utjecaj, kompenzacijske kontrole i istek svake iznimke ugrađene zaštite privatnosti u REG12 u roku od pet radnih dana od zahtjeva.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor mora evidentirati savjet u REG12 prije odobrenja iznimke ugrađene zaštite privatnosti koja uključuje visokorizičnu, osjetljivu, automatiziranu, opsežnu, spornu ili pravno značajnu obradu.

9.1.4 [All] Top Management mora odobriti iznimku ugrađene zaštite privatnosti koja utječe na obradu s visokim utjecajem, certifikacijski opseg, neriješeni veliki rizik ili pravnu obvezu u REG12 prije nego što iznimka stupi na snagu.

9.1.5 [Both] Privacy Lead / PIMS Manager mora za svaku odobrenu iznimku ugrađene zaštite privatnosti u REG12 odrediti datum isteka koji ne prelazi 90 dana prije odobrenja.

9.1.6 [Both] Privacy Lead / PIMS Manager mora zatvoriti ili ponovno procijeniti svaku iznimku ugrađene zaštite privatnosti u REG12 u roku od pet radnih dana od isteka.

10. Provedba

10.1 Provedba i postupanje s nesukladnostima

10.1.1 [Both] Privacy Lead / PIMS Manager mora evidentirati izostanak pregleda ugrađene zaštite privatnosti, izostanak dokaza o minimizaciji, neriješen neuspjeh zadane postavke ili neovlašteno puštanje u produkcijski rad kao nesukladnost u REG12 u roku od pet radnih dana od identifikacije.

10.1.2 [Both] System Owner / Application Owner mora spriječiti puštanje u produkcijski rad sustava za obradu osobnih podataka (PII) kada pregled ugrađene zaštite privatnosti u REG04 nije dovršen te evidentirati odluku u REG12 prije puštanja u produkcijski rad.

10.1.3 [Both] Vendor / Procurement Owner mora spriječiti uvođenje dobavljača ili potpisivanje ugovora kada nedostaju potrebni dokazi o ugrađenoj zaštiti privatnosti u REG08 te evidentirati odluku u REG12 prije uvođenja ili potpisivanja.

10.1.4 [Both] Process Owner / Business Owner mora obustaviti uporabu novog ili izmijenjenog projekta obrade osobnih podataka (PII) dok pregled u REG04, ažuriranja u REG02 i potrebne iznimke u REG12 ne budu dovršeni.

10.1.5 [All] Top Management mora zahtijevati korektivnu radnju u REG12 u roku od 10 radnih dana za ponovljeni, produljeni ili visokoutjecajni neuspjeh ugrađene zaštite privatnosti.

- 10.1.6 [All] Internal Audit / Compliance Reviewer mora provjeriti djelotvornost korektivnih radnji za nesukladnosti ugrađene zaštite privatnosti u REG12 pri sljedećoj planiranoj PIMS reviziji ili u roku od 60 dana od zatvaranja, ovisno o tome što nastupi ranije.

11. Pregled i održavanje

11.1 Pregled politike i kontrola projektiranja

- 11.1.1 [All] Privacy Lead / PIMS Manager mora pregledati ovu politiku u REG12 godišnje i u roku od 30 dana od značajne promjene pravnih zahtjeva, obrade, tehnologije, certifikacijskog opsega ili PIMS kontrole.
- 11.1.2 [Both] Process Owner / Business Owner mora pregledati aktivne aktivnosti obrade u REG02 radi promjena ovisnosti ugrađene zaštite privatnosti godišnje i u roku od 30 dana od značajne promjene obrade.
- 11.1.3 [Both] System Owner / Application Owner mora pregledati dokaze o konfiguraciji privatnosti prema zadanim postavkama u REG04 godišnje i u roku od 30 dana od značajne promjene sustava.
- 11.1.4 [Both] Vendor / Procurement Owner mora pregledati obveze ugrađene zaštite privatnosti dobavljača, izvršitelja obrade, podizvršitelja obrade i trećih strana u REG08 prije obnove i u roku od 30 dana od značajne promjene odnosa.
- 11.1.5 [Conditional] Data Protection Officer / Privacy Advisor mora pregledati utjecaj značajnih promjena politike na privatnost u REG12 prije odobrenja.
- 11.1.6 [All] Top Management mora odobriti značajne promjene ove politike u REG12 prije objave.

12. Povezane politike

- 12.1 PII01 - Politika sustava upravljanja privatnim informacijama
- 12.2 PII02 - Politika uloga, odgovornosti i odgovornosti za privatnost
- 12.3 PII03 - Politika popisa obrade osobnih podataka (PII) i pravne osnove
- 12.4 PII04 - Politika obavijesti o privatnosti i transparentnosti
- 12.5 PII05 - Politika upravljanja privolama i preferencijama
- 12.6 PII06 - Politika upravljanja pravima ispitanika
- 12.7 PII07 - Politika procjene rizika za privatnost i DPIA-e
- 12.8 PII09 - Politika prikupljanja, uporabe, otkrivanja i dijeljenja osobnih podataka (PII)
- 12.9 PII10 - Politika zadržavanja, brisanja i zbrinjavanja osobnih podataka (PII)
- 12.10 PII11 - Politika točnosti i kvalitete osobnih podataka (PII)
- 12.11 PII12 - Politika upravljanja privatnošću izvršitelja obrade, podizvršitelja obrade i trećih strana
- 12.12 PII13 - Politika međunarodnog prijenosa osobnih podataka (PII)
- 12.13 PII14 - Politika sigurnosti osobnih podataka (PII) i kontrole pristupa
- 12.14 PII17 - Politika dokumentiranih informacija i upravljanja dokazima PIMS-a
- 12.15 PII18 - Politika praćenja, revizije i poboljšanja PIMS-a

13. Referentni standardi i okviri

- 13.1 Ova je politika mapirana na sljedeće standarde i propise. Mapiranje objašnjava kako politika podupire citirane zahtjeve i utvrđuje interne točke koje ih provode ili podupiru.

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 6.1.2; Clause 6.1.3** - Mapirano na provjeru rizika za privatnost, poveznicu s radnjama obrade rizika, analizu ovisnosti projekta, eskalaciju i korektivne radnje bez

- dupliciranja cjelovite metodologije procjene rizika za privatnost i DPIA-e. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].
- 13.2.2 **Clause 6.3; Clause 8.1** - Mapirano na planirane promjene privatnosti, pokretanje projekta, operativni pregled ugrađene zaštite privatnosti, kontrolu puštanja u produkcijski rad i pregled značajnih promjena. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].
- 13.2.3 **Clause 7.5** - Mapirano na dokumentirane dokaze o ugrađenoj zaštiti privatnosti koji se čuvaju u REG02, REG04, REG08 i REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].
- 13.2.4 **Clause 9.1; Clause 10.2** - Mapirano na metrike ugrađene zaštite privatnosti, uzorkovanje dokaza, evidentiranje nesukladnosti, korektivne radnje i provjeru djelotvornosti. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].
- 13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Mapirano na dokumentiranje svrha obrade, evidencije obrade, poveznicu s ugrađenom zaštitom privatnosti i okidače za procjenu rizika za privatnost ili provjeru potrebe za DPIA-om za obradu voditelja obrade. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].
- 13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Mapirano na ograničavanje prikupljanja i obrade osobnih podataka (PII) putem minimalnih zahtjeva za podatke temeljenih na svrsi, neobvezne obrade koja je prema zadanim postavkama isključena i minimalnih zadanih postavki obrade. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].
- 13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Mapirano na usmjeravanje ovisnosti o točnosti, ciljeve minimizacije, izvedivost deidentifikacije i dokaze projekta za minimiziranje osobnih podataka (PII) koji omogućuju identifikaciju. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].
- 13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Mapirano na identifikaciju deidentifikacije u fazi projektiranja, ovisnosti o brisanju, privremenih artefakata osobnih podataka (PII) i usmjeravanje na kontrole životnog ciklusa bez dupliciranja provedbe zadržavanja ili zbrinjavanja. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].
- 13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapirano na upute klijenta izvršitelju obrade, informacije za podršku klijentu, zapise projekta izvršitelja obrade i promjene projekta usluge koje je odobrio klijent. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].
- 13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Mapirano na projektne mogućnosti izvršitelja obrade za privremene datoteke, ovisnost o povratu ili zbrinjavanju te ovisnost o kontroli prijenosa, evidentirane kao dokazi projekta bez dupliciranja operativnih postupaka brisanja ili sigurnosnih kontrola. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].
- 13.2.11 **Annex A.3.27; Annex A.3.29** - Mapirano na zahtjeve privatnosti u životnom ciklusu razvoja, inženjerska načela, kontrolne točke zaštite osobnih podataka (PII) i dokaze o konfiguraciji privatnosti prema zadanim postavkama. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 **GDPR**

- 13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapirano na ograničenje svrhe, projekt minimalnih osobnih podataka (PII), poveznicu sa zapisima obrade, zadanu minimizaciju, dokaze i odgovornost. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

- 13.3.2 **Article 24** - Mapirano na mjere voditelja obrade, pregled upravljanja, odobrenje iznimaka, korektivne radnje i održavanje politike za provedbu zaštite privatnosti u fazi projektiranja. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].
- 13.3.3 **Article 25** - Mapirano na pokretanje projekta, zahtjeve privatnosti u fazi projektiranja, postavke privatnosti prema zadanim postavkama, minimizaciju, provjere projektiranja pri nabavi, pregled prije puštanja u produkcijski rad i pregled potaknut promjenom. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].
- 13.3.4 **Article 28** - Mapirano na upute izvršitelju obrade, podršku projektu izvršitelja obrade, dokaze ugrađene zaštite privatnosti dobavljača i promjene projekta koje je odobrio klijent. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].
- 13.3.5 **Article 30** - Mapirano na poveznicu sa zapisima obrade, ažuriranja REG02, ovisnosti projekta aktivnosti obrade i dokaze zapisa obrade. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].
- 13.3.6 **Article 35** - Mapirano na okidače za procjenu rizika za privatnost i provjeru potrebe za DPIA-om u fazi projektiranja, savjete za visoki rizik i postimplementacijske provjere bez dupliciranja metodologije DPIA-e. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 4.7** - Mapirano na utvrđivanje kontrola privatnosti u fazi projektiranja, poveznicu s rizikom za privatnost i dokaze projekta za provedbu kontrola. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].
- 13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapirano na određivanje svrhe, ograničenje prikupljanja, minimizaciju podataka, ograničenu uporabu i zadane postavke obrade. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].
- 13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Mapirano na usmjeravanje ovisnosti o točnosti, dokaze o odgovornosti, praćenje ugrađene zaštite privatnosti, reviziju i korektivne radnje. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Mapirano na legitimnost svrhe, ograničenje prikupljanja, minimizaciju podataka, ograničenje uporabe i otkrivanja, ovisnost o zadržavanju, postupanje s privremenim datotekama i kontrole projektiranja ovisnosti o točnosti. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].