

				Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII01				Naziv dokumenta: Politika sustava upravljanja informacijama o 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

<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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Kontekst i utvrđivanje uloge PIMS-a
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Zainteresirane strane i zahtjevi
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	Opseg PIMS-a
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Uspostava i poboljšavanje PIMS-a
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Vodstvo i predanost
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Politika privatnosti
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Uloge i ovlasti
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Rizici i prilike
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Procjena rizika za privatnost
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Obrada rizika za privatnost i SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Ciljevi privatnosti
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Planirane promjene PIMS-a
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Resursi
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetencije
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Svijest
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Komunikacije
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentirane informacije
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operativno planiranje i nadzor

ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operativna procjena rizika za privatnost
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operativna obrada rizika za privatnost
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Praćenje i vrednovanje
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Interna revizija
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Preispitivanje od strane uprave
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Kontinuirano poboljšanje
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Nesukladnost i korektivna radnja
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Zapisi upravljanja za voditelja obrade
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Sporazum izvršitelja obrade i svrhe
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Povezanost s politikom sigurnosti PII-a
GDPR	Article 5(2)	Controller	Supporting	Dokazi odgovornosti
GDPR	Article 24	Controller	Supporting	Mjere i politika voditelja obrade
GDPR	Article 26	Joint Controller	Supporting	Aranžmani zajedničkih voditelja obrade
GDPR	Article 28	Both	Supporting	Upravljanje izvršiteljima obrade
GDPR	Article 30	Both	Supporting	Evidencije obrade
GDPR	Article 32	Both	Supporting	Sigurnost obrade
GDPR	Article 35	Controller	Supporting	Upravljanje DPIA-om
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Kontrole i načela privatnosti

ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Proces i priprema PIA-e
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	Program i politika zaštite PII-a
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integracija organizacijskog rizika za privatnost

1. Opseg

1.1 Ovom se politikom uspostavlja organizacijski sustav upravljanja informacijama o privatnosti za obradu PII-a u kontekstima voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade.

1.2 Ova se politika primjenjuje na:

1.2.1 opseg, kontekst, zainteresirane strane i organizacijske granice PIMS-a;

1.2.2 utvrđivanje uloge PIMS-a za aktivnosti obrade PII-a;

1.2.3 politiku privatnosti, ciljeve privatnosti, procjenu rizika za privatnost, obradu rizika za privatnost i Izjavu o primjenjivosti PIMS-a;

1.2.4 upravljanje PIMS-om, praćenje, internu reviziju, preispitivanje od strane uprave, nesukladnost, korektivne radnje i kontinuirano poboljšanje;

1.2.5 dokumentirane informacije i dokaze potrebne za dokazivanje sukladnosti PIMS-a i odgovornosti.

1.3 Za potrebe ove politike, značajna promjena znači svaku promjenu koja utječe na opseg PIMS-a, svrhe obrade PII-a, kategorije PII-a, kategorije ispitanika, lokacije obrade, raspodjelu uloga voditelja obrade ili izvršitelja obrade, arhitekturu sustava, aranžmane s dobavljačima ili podizvršiteljima obrade, profil rizika za privatnost, primjenjive pravne ili ugovorne obveze ili opseg certifikacije.

2. Svrha

2.1 Ova politika definira obvezne zahtjeve upravljanja za uspostavu, implementaciju, održavanje, praćenje i kontinuirano poboljšavanje PIMS-a.

2.2 Svrha ove politike jest osigurati da organizacija može dokazati odgovorno, na riziku utemeljeno i dokazima vođeno upravljanje obradom PII-a u svim primjenjivim ulogama PIMS-a.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

3.1.1 definirati opseg, kontekst, granice i primjenjivost uloga PIMS-a;

3.1.2 dodijeliti odgovornost za upravljanje PIMS-om upotrebom kanonskih uloga PIMS-a;

3.1.3 uspostaviti ciljeve privatnosti i mjerljiva očekivanja učinkovitosti PIMS-a;

3.1.4 održavati Izjavu o primjenjivosti PIMS-a za odabrane i isključene kontrole;

3.1.5 integrirati procjenu rizika za privatnost, obradu rizika za privatnost i upravljanje DPIA-om u rad PIMS-a;

3.1.6 osigurati da se obveze voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade utvrde prije početka obrade;

3.1.7 održavati dokaze spremne za reviziju radi spremnosti za certifikaciju i kontinuiranog poboljšanja;

3.1.8 izbjegavati nepotrebne uloge, registre, obrasce i duplicirane operativne kontrole.

4. Izjave politike

4.1 Uspostava, kontekst i opseg PIMS-a

4.1.1 [Both] Top Management MORA odobriti opseg PIMS-a u REG01 prije početne implementacije PIMS-a i u roku od 30 dana od svake značajne promjene.

4.1.2 [Both] Privacy Lead / PIMS Manager MORA dokumentirati vanjska i unutarnja pitanja konteksta privatnosti u REG01 jednom godišnje i u roku od 30 dana od svake značajne promjene.

- 4.1.3 [Both] Privacy Lead / PIMS Manager MORA dokumentirati relevantne zainteresirane strane i njihove zahtjeve za PIMS u REG01 jednom godišnje i u roku od 30 dana od svake značajne promjene.
- 4.1.4 [Both] Privacy Lead / PIMS Manager MORA održavati sažetak interakcija procesa PIMS-a u REG01 prije svakog preispitivanja od strane uprave.

4.2 Utvrđivanje uloge PIMS-a

- 4.2.1 [Both] Process Owner / Business Owner MORA klasificirati organizacijsku ulogu PIMS-a za svaku aktivnost obrade PII-a u REG02 prije početka aktivnosti obrade.
- 4.2.2 [Joint Controller] Vendor / Procurement Owner MORA dokumentirati raspodjelu odgovornosti zajedničkih voditelja obrade u REG08 prije početka zajedničke obrade.
- 4.2.3 [Processor] Vendor / Procurement Owner MORA dokumentirati upute klijenta za obradu u aktivnostima izvršitelja obrade u REG08 prije uvođenja usluge.
- 4.2.4 [Subprocessor] Vendor / Procurement Owner MORA dokumentirati upute nadređenog klijenta i odobrene aranžmane podizvršitelja obrade u REG08 prije početka podizvršavanja obrade.

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

9. Iznimke

9.1 Zahtjev za iznimku i odobrenje

- 9.1.1 [All] Process Owner / Business Owner MORA dokumentirati svaku zatraženu iznimku od ove politike u REG12 prije nastanka odstupanja.
- 9.1.2 [Both] Privacy Lead / PIMS Manager MORA procijeniti rizik za privatnost svake zatražene iznimke u REG04 prije odobrenja.
- 9.1.3 [Both] Top Management MORA odobriti iznimke koje prelaze prihvaćene pragove rizika za privatnost u REG12 prije implementacije.
- 9.1.4 [Both] Privacy Lead / PIMS Manager MORA tromjesečno pregledavati aktivne iznimke PIMS-a u REG12 do zatvaranja.

9.2 Zatvaranje iznimke

- 9.2.1 [All] Process Owner / Business Owner MORA dokumentirati dokaze zatvaranja iznimke u REG12 do odobrenog datuma isteka iznimke.
- 9.2.2 [Both] Internal Audit / Compliance Reviewer MORA tijekom sljedeće planirane interne revizije provjeriti dokaze zatvaranja isteklih iznimki u REG12.

10. Provedba

10.1 Postupanje s nesukladnostima

- 10.1.1 [All] Privacy Lead / PIMS Manager MORA zabilježiti sumnje na nesukladnosti s ovom politikom u REG12 u roku od pet radnih dana od utvrđivanja.
- 10.1.2 [All] Process Owner / Business Owner MORA implementirati odobrene korektivne radnje u REG12 do dodijeljenog roka nakon odobrenja nesukladnosti.
- 10.1.3 [All] Top Management MORA pri svakom preispitivanju od strane uprave pregledati neriješene veće nesukladnosti PIMS-a u REG12.
- 10.1.4 [All] Internal Audit / Compliance Reviewer MORA potvrditi djelotvornost korektivnih radnji u REG12 u roku od 30 dana od prijavljenog zatvaranja.

10.2 Eskalacija

- 10.2.1 [All] Privacy Lead / PIMS Manager MORA eskalirati zakašnjele veće korektivne radnje prema Top Management u REG12 u roku od pet radnih dana nakon roka dospjeća.

10.2.2 [All] Top Management MORA zabilježiti odluke o zakašnjelim većim korektivnim radnjama u REG12 u roku od 15 radnih dana od eskalacije.

11. Pregled i održavanje

11.1 Pregled politike

11.1.1 [All] Privacy Lead / PIMS Manager MORA pregledati ovu politiku u REG12 jednom godišnje i u roku od 30 dana od svake značajne promjene pravnog, organizacijskog, obradnog, tehnološkog ili certifikacijskog opsega.

11.1.2 [All] Data Protection Officer / Privacy Advisor MORA pružiti dokumentirani savjet u REG12 prije odobrenja politike kada se značajno promijene obveze u području privatnosti.

11.1.3 [All] Top Management MORA odobriti značajne izmjene ove politike u REG12 prije objave.

11.1.4 [All] Privacy Lead / PIMS Manager MORA ažurirati REG01 i REG03 u roku od 15 radnih dana nakon odobrenih izmjena politike koje mijenjaju opseg PIMS-a ili primjenjivost kontrola.

11.1.5 [All] Privacy Lead / PIMS Manager MORA zabilježiti komunikaciju odobrenih izmjena politike u REG11 u roku od 30 dana od objave.

12. Povezane politike

12.1 Ovu politiku podržavaju sljedeće povezane politike:

12.2 PII02 - Politika uloga, zaduženja i odgovornosti u području privatnosti

12.3 PII03 - Politika inventara obrade PII-a i pravne osnove

12.4 PII07 - Politika procjene rizika za privatnost i DPIA-e

12.5 PII08 - Politika ugrađene i zadane zaštite privatnosti

12.6 PII12 - Politika izvršitelja obrade, podizvršitelja obrade i dijeljenja podataka

12.7 PII14 - Politika sigurnosti PII-a i kontrole pristupa

12.8 PII15 - Politika upravljanja incidentima i povredama PII-a

12.9 PII16 - Politika osposobljavanja, podizanja svijesti i kompetencija u području privatnosti

12.10 PII17 - Politika upravljanja dokumentiranim informacijama i dokazima PIMS-a

12.11 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 podržava navedene zahtjeve i utvrđuje interne točke koje ih implementiraju ili podržavaju.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Mapirano na utvrđivanje organizacijskog konteksta, pitanja konteksta privatnosti i primjenjivosti uloge voditelja obrade ili izvršitelja obrade za aktivnosti PIMS-a. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Mapirano na utvrđivanje zainteresiranih strana, ispitanika, klijenata, nadzornih tijela, izvršitelja obrade, podizvršitelja obrade i njihovih relevantnih zahtjeva za PIMS. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Mapirano na definiranje, odobravanje, održavanje i izmjenu dokumentiranog opsega PIMS-a. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Mapirano na uspostavu, implementaciju, održavanje i poboljšavanje procesa PIMS-a i njihovih interakcija. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Mapirano na odobrenje Top Management, resurse, preispitivanje od strane uprave i vodstvo nad djelotvornošću i poboljšanjem PIMS-a. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

- 13.2.6 **Clause 5.2** - Mapirano na održavanje ove politike privatnosti kao odobrene dokumentirane informacije i komunikaciju izmjena politike. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].
- 13.2.7 **Clause 5.3** - Mapirano na dodjelu i komunikaciju uloga, odgovornosti i ovlasti PIMS-a. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].
- 13.2.8 **Clause 6.1.1** - Mapirano na planiranje radnji za rizike i prilike PIMS-a upotrebom konteksta, zahtjeva zainteresiranih strana, ciljeva i ulaznih informacija za poboljšanje. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].
- 13.2.9 **Clause 6.1.2** - Mapirano na zahtijevanje procjene rizika za privatnost prije nove ili značajno izmijenjene obrade i održavanje dokaza o riziku za privatnost. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].
- 13.2.10 **Clause 6.1.3** - Mapirano na obradu rizika za privatnost, odabir kontrola, povezanost s programom informacijske sigurnosti i održavanje Izjave o primjenjivosti. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].
- 13.2.11 **Clause 6.2** - Mapirano na uspostavu, mjerenje, praćenje, komunikaciju i ažuriranje ciljeva PIMS-a. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].
- 13.2.12 **Clause 6.3** - Mapirano na planirane promjene PIMS-a i kontrolu promjena koje utječu na opseg, uloge, kontrole i dokumentirane informacije. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].
- 13.2.13 **Clause 7.1** - Mapirano na utvrđivanje i osiguravanje resursa za uspostavu, rad, održavanje i poboljšavanje PIMS-a. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].
- 13.2.14 **Clause 7.2** - Mapirano na očekivanja u pogledu kompetencija i dokaze koji podržavaju odgovornosti PIMS-a i obavljanje uloga. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].
- 13.2.15 **Clause 7.3** - Mapirano na svijest o politici privatnosti, doprinos djelotvornosti PIMS-a i posljedice nesukladnosti. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].
- 13.2.16 **Clause 7.4** - Mapirano na interne i vanjske komunikacije relevantne za upravljanje PIMS-om, izmjene politike i eskalaciju. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].
- 13.2.17 **Clause 7.5** - Mapirano na izradu, održavanje, kontrolu, spremnost dokaza i zadržavanje dokumentiranih informacija. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].
- 13.2.18 **Clause 8.1** - Mapirano na planiranje, implementaciju i nadzor operativnih procesa PIMS-a i eksterno pruženih procesa. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].
- 13.2.19 **Clause 8.2** - Mapirano na provedbu procjena rizika za privatnost u planiranim intervalima i kada se predlažu ili nastanu značajne promjene. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].
- 13.2.20 **Clause 8.3** - Mapirano na implementaciju planova obrade rizika za privatnost i zadržavanje dokaza o rezultatima obrade rizika. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].
- 13.2.21 **Clause 9.1** - Mapirano na praćenje, mjerenje, analizu, vrednovanje, metrike i izvješćivanje o djelotvornosti PIMS-a. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].
- 13.2.22 **Clause 9.2** - Mapirano na planiranje interne revizije, uzorkovanje dokaza, rezultate revizije i neovisni pregled. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].
- 13.2.23 **Clause 9.3** - Mapirano na ulazne informacije za preispitivanje od strane uprave, pregled učinkovitosti, izlazne rezultate preispitivanja od strane uprave i odluke o poboljšanju. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].
- 13.2.24 **Clause 10.1** - Mapirano na kontinuirano poboljšanje kroz preispitivanje od strane uprave, metrike, praćenje korektivnih radnji i održavanje politike. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

- 13.2.25 **Clause 10.2** - Mapirano na postupanje s nesukladnostima, korektivne radnje, eskalaciju, zatvaranje i potvrdu djelotvornosti. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].
- 13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mapirano na zapise o svrhama obrade na strani voditelja obrade, povezanost s pravnom osnovom, utvrđivanje potrebe za DPIA-om, raspodjelu odgovornosti zajedničkih voditelja obrade i zapise dokaza o obradi. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].
- 13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Mapirano na ugovore izvršitelja obrade s klijentima, dokumentirane upute klijentima i ograničenja svrhe izvršitelja obrade. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].
- 13.2.28 **Annex A.3.3** - Mapirano na povezanost s politikom sigurnosti PII-a, vlasništvo nad polaznom osnovom sigurnosnih kontrola za PII i status kontrola informacijske sigurnosti u Izjavi o primjenjivosti PIMS-a. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

- 13.3.1 **Article 5(2)** - Mapirano na dokaze odgovornosti, odobrenje politike, klasifikaciju uloga u obradi, primjenjivost kontrola, praćenje, reviziju i zapise korektivnih radnji. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].
- 13.3.2 **Article 24** - Mapirano na mjere upravljanja voditelja obrade, odobrenje politike, ciljeve PIMS-a, pregled djelotvornosti i dokumentirane dokaze odgovornosti voditelja obrade. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].
- 13.3.3 **Article 26** - Mapirano na utvrđivanje i dokumentiranje raspodjele odgovornosti zajedničkih voditelja obrade prije početka zajedničke obrade. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].
- 13.3.4 **Article 28** - Mapirano na zapise upravljanja izvršiteljima obrade i podizvršiteljima obrade, upute klijenta za obradu i kontrolu eksterno pruženih procesa. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].
- 13.3.5 **Article 30** - Mapirano na evidencije aktivnosti obrade, klasifikaciju uloga, zapise odgovornosti za obradu i dokaze zadržane radi revizivnosti. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].
- 13.3.6 **Article 32** - Mapirano na upravljanje polaznom osnovom sigurnosti PII-a, vlasništvo nad sigurnosnim kontrolama, status implementacije sigurnosti i potvrdu operativnih kontrola. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].
- 13.3.7 **Article 35** - Mapirano na utvrđivanje potrebe za DPIA-om i procjenu rizika za privatnost prije nastavka visokorizične ili značajno izmijenjene obrade koju provodi voditelj obrade. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Mapirano na identifikaciju kontrola privatnosti, načela privatnosti, informacijsku sigurnost, usklađenost u području privatnosti, reviziju, dokaze i na riziku utemeljeno upravljanje privatnošću. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

- 13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapirano na upravljanje PIA-om, utvrđivanje okidača za DPIA-u, pripremu PIA-e, kriterije rizika za privatnost i dokumentirane dokaze procjene rizika za privatnost. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Mapirano na zahtjeve programa zaštite PII-a, utvrđivanje zahtjeva zaštite PII-a, odabir kontrola temeljen na riziku za privatnost i smjernice politike zaštite PII-a. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapirano na načela organizacijskog rizika za privatnost, predanost vodstva, integraciju rizika za privatnost u upravljanje PIMS-om i razumijevanje uloge organizacije u obradi PII-a. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].