					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII07					Naziv dokumenta: **Politika procjene rizika za privatnost i DPIA-e**							
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 6.1.1	Both	Primary	Rizici i prilike za PIMS
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 poveznica sa SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Planirane promjene PIMS-a i ponovna procjena rizika
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentirane informacije o riziku za privatnost i DPIA-i
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operativno planiranje i kontrola
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	Supporting	Praćenje i mjerenje rizika za privatnost
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Preispitivanje rizika za privatnost od strane uprave
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Nesukladnost povezana s rizikom i korektivna radnja
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Procjena učinka na privatnost
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Evidencije obrade koje podupiru procjenu rizika
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Ugovor s klijentom izvršitelja obrade i pomoć pri DPIA-i
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informacije izvršitelja obrade koje podupiru usklađenost klijenta

GDPR	Article 5(2)	Controller	Supporting	Dokazi o odgovornosti
GDPR	Article 24	Controller	Supporting	Odgovornost voditelja obrade i mjere
GDPR	Article 25	Controller	Supporting	Zaštita podataka u fazi projektiranja i prema zadanim postavkama
GDPR	Article 28	Both	Supporting	Pomoć izvršitelja obrade i upute
GDPR	Article 30	Both	Supporting	Evidencije obrade koje podupiru DPIA-u
GDPR	Article 32	Both	Supporting	Sigurnosni rizik i zaštitne mjere
GDPR	Article 35	Controller	Primary	Procjena učinka na zaštitu podataka
GDPR	Article 36	Controller	Primary	Prethodno savjetovanje
GDPR	Article 39	Conditional	Supporting	Savjeti i praćenje DPO-a gdje je primjenjivo
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Kontrole privatnosti, informacijska sigurnost i usklađenost u području privatnosti
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Opseg, koristi, okidač i priprema PIA-e
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Program zaštite osobnih podataka (PII) i utvrđivanje zahtjeva
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Integracija organizacijskog upravljanja rizicima za privatnost

1. Opseg

1.1 Ova politika definira zahtjeve za procjenu rizika za privatnost, provjeru potrebe za DPIA-om, provedbu cjelovite DPIA-e, obradu rizika, prihvaćanje preostalog rizika, savjetovanje, pregled i upravljanje dokazima za obradu osobnih podataka (PII) unutar opsega PIMS-a.

1.2 Ova se politika primjenjuje na:

1.2.1 nove i značajno izmijenjene aktivnosti obrade osobnih podataka (PII);

1.2.2 kontekste obrade u ulozi voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade;

1.2.3 sustave, aplikacije, usluge, poslovne procese, dobavljače, izvršitelje obrade, podizvršitelje obrade, međunarodne prijenose i aranžmane dijeljenja podataka koji utječu na obradu osobnih podataka (PII);

1.2.4 dokaze o riziku za privatnost i DPIA-i koji se održavaju u REG04 te pripadajuće dokaze koji se održavaju u REG02, REG03, REG08, REG09, REG10, REG11 i REG12.

1.3 Ova politika ne zamjenjuje kontrole popisa obrade, kontrole obavijesti o privatnosti, kontrole privole, kontrole prava ispitanika, kontrole ugrađene zaštite privatnosti, kontrole dobavljača, kontrole međunarodnih prijenosa, kontrole sigurnosti osobnih podataka (PII), kontrole incidenata, kontrole dokumentiranih informacija ni kontrole praćenja/revizije/poboljšanja. Ti su zahtjevi definirani u povezanim politikama navedenima u odjeljku 12.

1.4 Za potrebe ove politike, procjena rizika za privatnost znači dokumentiranu identifikaciju, analizu, vrednovanje, obradu, pregled i praćenje mogućih štetnih učinaka na privatnost koji proizlaze iz obrade osobnih podataka (PII).

1.5 Za potrebe ove politike, DPIA znači dokumentirana procjena koja se koristi za obradu u svojstvu voditelja obrade koja će vjerojatno prouzročiti visok rizik za ispitanike te kojom se vrednuju nužnost obrade, proporcionalnost, rizici, zaštitne mjere, preostali rizik, potrebe za savjetovanjem i uvjeti odobrenja.

1.6 Za potrebe ove politike, visok preostali rizik za privatnost znači rizik za privatnost koji nakon predložene ili provedene obrade rizika ostaje iznad odobrenog praga prihvaćanja.

1.7 Za potrebe ove politike, značajna promjena znači svaka promjena koja utječe na opseg PIMS-a, svrhu obrade, pravnu osnovu, kategorije osobnih podataka (PII), kategorije ispitanika, opseg obrade, tehnologiju obrade, praćenje ili profiliranje, automatizirano donošenje odluka, ranjive ispitanike, primatelje, izvršitelje obrade, podizvršitelje obrade, međunarodne prijenose, zadržavanje, sigurnosne kontrole, profil rizika, upute klijenta ili opseg certifikacije.

2. Svrha

2.1 Svrha ove politike jest osigurati da se rizici za privatnost i obveze DPIA-e identificiraju, procijene, obrade, odobre, pregledaju i dokažu prije nego što obrada osobnih podataka (PII) stvori neprihvatljiv rizik za ispitanike ili za PIMS.

2.2 Ova politika organizaciji omogućuje dokazivanje upravljanja privatnošću temeljenog na riziku, odgovornosti voditelja obrade za DPIA-u, pomoći izvršitelja obrade pri DPIA-i, dokumentirane obrade rizika, odobravanja preostalog rizika, odlučivanja o prethodnom savjetovanju i kontinuiranog poboljšanja kontrola privatnosti.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

3.1.1 definirati obvezne okidače za provjeru rizika za privatnost;

3.1.2 definirati kada je potrebna cjelovita DPIA;

3.1.3 osigurati da su odluke voditelja obrade o DPIA-i dokumentirane i dostupne za pregled;

3.1.4 osigurati da je pomoć izvršitelja obrade i podizvršitelja obrade pri DPIA-i dokumentirana kada je potrebna prema uputi klijenta ili ugovoru;

3.1.5 osigurati da se rizici za privatnost procijene prije početka nove ili značajno izmijenjene obrade osobnih podataka (PII);

3.1.6 osigurati da se obrade rizika za privatnost dodijele, provedu i provjere;

3.1.7 osigurati da se visoki preostali rizici za privatnost eskaliraju i odobre prije početka ili nastavka obrade;

3.1.8 osigurati da se odluke o prethodnom savjetovanju dokumentiraju kada visok preostali rizik ostaje;

3.1.9 osigurati da se dokazi o riziku za privatnost i DPIA-i održavaju u REG04 i povezuju s povezanim dokaznim objektima;

3.1.10 izbjeći stvaranje zasebnih registara DPIA-e, rizika ili savjetovanja izvan REG04.

4. Izjave politike

4.1 Provjera rizika za privatnost

4.1.1 [Both] Process Owner / Business Owner mora pokrenuti provjeru rizika za privatnost u REG04 prije početka nove ili značajno izmijenjene obrade osobnih podataka (PII) evidentirane u REG02.

4.1.2 [Both] Privacy Lead / PIMS Manager mora održavati kriterije za provjeru rizika za privatnost u REG04 prije početnog rada PIMS-a i nakon toga jednom godišnje.

4.1.3 [Controller] Process Owner / Business Owner mora dovršiti provjeru potrebe za DPIA-om u REG04 prije početka obrade u svojstvu voditelja obrade koja ispunjava kriterije za provjeru rizika za privatnost.

4.1.4 [Processor] Vendor / Procurement Owner mora evidentirati zahtjeve klijenta za pomoć pri DPIA-i u REG08 prije početka obrade u svojstvu izvršitelja obrade kada ugovor s klijentom ili dokumentirana uputa zahtijeva podršku pri DPIA-i.

4.1.5 [Both] System Owner / Application Owner mora dostaviti dokaze o dizajnu sustava, pristupu, sigurnosti, zapisivanju događaja i tokovima podataka u REG04 prije odobrenja procjene rizika za privatnost za nove ili značajno izmijenjene sustave koji obrađuju osobne podatke (PII).

4.1.6 [Both] Privacy Lead / PIMS Manager mora evidentirati ishod provjere i obrazloženje odluke o cjelovitoj DPIA-i u REG04 prije nastavka aktivnosti obrade.

4.2 Okidači DPIA-e i utvrđivanje zahtjeva

4.2.1 [Controller] Privacy Lead / PIMS Manager mora zahtijevati cjelovitu DPIA-u u REG04 prije početka obrade u svojstvu voditelja obrade koja će vjerojatno prouzročiti visok rizik.

4.2.2 [Controller] Process Owner / Business Owner mora u REG04 uputiti obradu koja uključuje veliki opseg, sustavno praćenje, profiliranje, automatizirane odluke, posebne kategorije osobnih podataka, podatke o kaznenim osudama ili kažnjivim djelima, ranjive ispitanike, inovativnu tehnologiju ili značajno izmijenjenu obradu na Privacy Lead / PIMS Manager prije početka obrade.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor mora evidentirati savjet u REG04 prije odobrenja odluke o zahtjevu za cjelovitu DPIA-u za visokorizičnu obradu u svojstvu voditelja obrade.

4.2.4 [Both] Process Owner / Business Owner mora ponovno provjeriti rizik za privatnost u REG04 prije uporabe osobnih podataka (PII) za novu svrhu, dodavanja novog primatelja, uvođenja novog izvršitelja obrade ili podizvršitelja obrade, promjene arhitekture sustava ili početka novog međunarodnog prijenosa.

4.2.5 [Processor] Privacy Lead / PIMS Manager mora u REG08 dokumentirati je li potrebna podrška izvršitelja obrade pri DPIA-i u roku od 10 radnih dana od primitka zahtjeva klijenta za pomoć pri DPIA-i.

4.2.6 [Subprocessor] Vendor / Procurement Owner mora dokumentirati zahtjeve nadređene strane za pomoć pri DPIA-i u REG08 prije početka podizvršavanja obrade kada takvu pomoć zahtijeva ugovor s nadređenim klijentom ili izvršiteljem obrade.

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

9. Iznimke

9.1 Iznimke za rizik za privatnost i DPIA-u

9.1.1 [All] Process Owner / Business Owner mora zatražiti svaku iznimku od ove politike u REG12 prije nastanka odstupanja.

9.1.2 [All] Privacy Lead / PIMS Manager mora procijeniti učinak svake zatražene iznimke na privatnost, pravne zahtjeve, certifikaciju, poslovanje i ispitanike u REG04 ili REG12 u roku od 10 radnih dana od zahtjeva.

9.1.3 [All] Data Protection Officer / Privacy Advisor mora evidentirati savjet u REG12 prije odobrenja svake iznimke koja utječe na visokorizičnu obradu, dovršetak cjelovite DPIA-e, prethodno savjetovanje, visok preostali rizik za privatnost ili pomoć klijentu pri DPIA-i.

9.1.4 [All] Top Management mora odobriti iznimke za rizik za privatnost ili DPIA-u koje utječu na visokorizičnu obradu, opseg certifikacije, prethodno savjetovanje ili neriješeni visok preostali rizik za privatnost u REG12 prije nego što iznimka stupi na snagu.

9.1.5 [All] Privacy Lead / PIMS Manager mora u REG12 odrediti datum isteka koji ne premašuje 90 dana za svaku odobrenu iznimku za rizik za privatnost ili DPIA-u prije odobrenja.

9.1.6 [All] Process Owner / Business Owner mora zatvoriti ili ponovno procijeniti svaku iznimku za rizik za privatnost ili DPIA-u u REG12 u roku od pet radnih dana od isteka.

10. Provedba politike

10.1 Provedba zahtjeva za rizik za privatnost i DPIA-u

10.1.1 [All] Privacy Lead / PIMS Manager mora evidentirati nedostajuće, netočne, nepotpune, zakašnjele ili neodobrene dokaze o riziku za privatnost ili DPIA-i u REG04 kao nesukladnost u REG12 u roku od pet radnih dana od identifikacije.

10.1.2 [Controller] Process Owner / Business Owner mora obustaviti novu visokorizičnu obradu u svojstvu voditelja obrade kada prije pokretanja nedostaju potrebni dokazi o odobrenju DPIA-e u REG04.

10.1.3 [Both] System Owner / Application Owner mora blokirati puštanje u produkcijski rad sustava koji obrađuju osobne podatke (PII) kada prije odobrenja puštanja u produkcijski rad nedostaju potrebni dokazi o obradi rizika u REG04.

10.1.4 [Both] Vendor / Procurement Owner mora blokirati uvođenje dobavljača, izvršitelja obrade, podizvršitelja obrade ili aranžmana dijeljenja podataka kada prije odobrenja ugovora nedostaju potrebni dokazi o riziku za privatnost ili pomoći pri DPIA-i u REG04.

10.1.5 [All] Top Management mora tijekom preispitivanja od strane uprave pregledati neriješene veće nesukladnosti povezane s rizikom za privatnost ili DPIA-om u REG12.

10.1.6 [All] Privacy Lead / PIMS Manager mora eskalirati ponovljena propuštanja rokova za provjeru u REG04, pregled DPIA-e ili obradu rizika Top Management u REG12 u roku od pet radnih dana nakon drugog pojavljivanja u razdoblju od 12 mjeseci.

10.1.7 [All] Internal Audit / Compliance Reviewer mora provjeriti djelotvornost korektivnih radnji za nesukladnosti povezane s rizikom za privatnost i DPIA-om 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 Pregled i održavanje politike

11.1.1 [All] Privacy Lead / PIMS Manager mora ovu politiku pregledati u REG12 jednom godišnje i u roku od 30 dana od značajne promjene zahtjeva za rizik za privatnost, DPIA-u, prethodno savjetovanje, pomoć izvršitelja obrade ili certifikaciju.

11.1.2 [All] Privacy Lead / PIMS Manager mora jednom godišnje u REG12 pregledati kriterije provjere u REG04, kriterije okidača za DPIA-u, kriterije ocjenjivanja rizika i kriterije prihvaćanja preostalog rizika.

11.1.3 [All] Data Protection Officer / Privacy Advisor mora pregledati promjene ove politike koje su 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 REG03 i REG04 u roku od 15 radnih dana nakon odobrenih promjena politike koje mijenjaju primjenjivost kontrola, kriterije rizika ili zahtjeve provjere potrebe za DPIA-om.

11.1.6 [All] Privacy Lead / PIMS Manager mora evidentirati komunikaciju odobrenih promjena ove 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 upravljanja informacijama o privatnosti

12.3 PII02 - Politika uloga, odgovornosti i odgovornosti za privatnost

12.4 PII03 - Politika popisa obrade osobnih podataka (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 PII08 - Politika zaštite privatnosti u fazi projektiranja i prema zadanim postavkama

12.9 PII09 - Politika prikupljanja, uporabe, otkrivanja i dijeljenja osobnih podataka (PII)

12.10 PII10 - Politika zadržavanja, brisanja i zbrinjavanja osobnih podataka (PII)

12.11 PII11 - Politika točnosti i kvalitete osobnih podataka (PII)

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

12.13 PII13 - Politika međunarodnog prijenosa osobnih podataka (PII)

12.14 PII14 - Politika sigurnosti i kontrole pristupa osobnim podacima (PII)

12.15 PII15 - Politika upravljanja incidentima i povredama osobnih podataka (PII)

12.16 PII17 - Politika dokumentiranih informacija i upravljanja dokazima PIMS-a

12.17 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 navedene zahtjeve i utvrđuje interne točke koje ih provode ili podupiru.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Mapirano na identificiranje i planiranje radnji za rizike i prilike u području privatnosti primjenom kriterija provjere, pragova rizika, eskalacije i ulaznih podataka za preispitivanje od strane uprave. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Mapirano na provođenje provjere rizika za privatnost, procjene rizika za privatnost, ocjenjivanja rizika, ponovne procjene i vrednovanja okidača za DPIA-u prije

nastavka nove ili značajno izmijenjene obrade. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Mapirano na planiranje obrade rizika za privatnost, ažuriranja primjenjivosti kontrola, provedbu obrade rizika, prihvaćanje preostalog rizika i poveznicu sa SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Mapirano na planirane promjene PIMS-a i obrade koje pokreću ponovnu procjenu rizika za privatnost i pregled DPIA-e. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mapirano na kontrolirane dokumentirane informacije za provjeru rizika za privatnost, dokaze o DPIA-i, obradu rizika, prihvaćanje preostalog rizika, odluke o prethodnom savjetovanju, iznimke, nesukladnosti i dokaze o pregledu politike. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Mapirano na provedbu kontrola rizika za privatnost i DPIA-e prije puštanja u produkcijski rad, uvođenja, odobrenja obrade, zatvaranja obrade rizika i povezivanja s korektivnim radnjama. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Mapirano na operativnu procjenu rizika za privatnost za nove i izmijenjene obrade te promjene povezane sa sustavima, dobavljačima, prijenosima i incidentima. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Mapirano na operativnu obradu rizika za privatnost, dodjelu obrade rizika, provedbu obrade rizika, eskalaciju zakašnjele obrade rizika i provjeru djelotvornosti. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Mapirano na praćenje i mjerenje pokrivenosti provjerom, statusa DPIA-e, otvorenih rizika, zakašnjelih radnji obrade rizika, radnji dobavljača, radnji obrade sigurnosnih rizika, radnji ponovne procjene nakon incidenata i nalaza revizije. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Mapirano na preispitivanje visokih preostalih rizika za privatnost, zakašnjelih radnji obrade rizika, statusa cjelovite DPIA-e, odluka o prethodnom savjetovanju i većih iznimaka rizika za privatnost od strane uprave. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mapirano na nesukladnosti i iznimke povezane s rizikom za privatnost i DPIA-om, otvaranje korektivnih radnji, eskalaciju i provjeru djelotvornosti. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Mapirano na procjenu potrebe za procjenom učinka na privatnost i njezinu provedbu, gdje je primjereno, za novu ili izmijenjenu obradu u svojstvu voditelja obrade. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Mapirano na evidencije obrade koje podupiru ulazne podatke za procjenu rizika za privatnost i DPIA-u, uključujući svrhu, kategorije, sustave, primatelje, prijenose i dobavljače. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mapirano na ugovore izvršitelja obrade s klijentima i obveze pomoći klijentu pri DPIA-i. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Mapirano na pružanje informacija od strane izvršitelja obrade potrebnih za usklađenost klijenta, uključujući pomoć pri DPIA-i i dokaze o podršci klijentu. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapirano na dokaze o odgovornosti za provjeru potrebe za DPIA-om, odluke o cjelovitoj DPIA-i, obradu rizika, prihvaćanje preostalog rizika, odluke o prethodnom

savjetovanju, iznimke, nalaze revizije i korektivne radnje. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Mapirano na odgovornost voditelja obrade za odgovarajuće mjere rizika za privatnost, pregled visokog preostalog rizika, odobrenje uprave i održavanje politike. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Mapirano na dokaze o zaštiti privatnosti u fazi projektiranja i prema zadanim postavkama koji se koriste u procjeni rizika i prije odobrenja puštanja u produkcijski rad. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mapirano na pomoć izvršitelja obrade i podizvršitelja obrade pri DPIA-i, postupanje prema uputama klijenta i dokaze o obradi rizika dobavljača. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Mapirano na evidencije obrade koje podupiru ulazne podatke za procjenu rizika za privatnost i DPIA-u. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mapirano na ulazne podatke o sigurnosnom riziku za osobne podatke (PII), odabir zaštitnih mjera, obradu sigurnosnog rizika i ažuriranja statusa sigurnosnih kontrola. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mapirano na provjeru potrebe za DPIA-om, utvrđivanje zahtjeva za cjelovitu DPIA-u, sadržaj DPIA-e, savjet DPO-a, pregled i blokiranje visokorizične obrade bez potrebnog odobrenja DPIA-e. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Mapirano na odlučivanje o prethodnom savjetovanju, savjet DPO-a, odobrenje Top Management i radnje nastavka, obustave, redizajna ili savjetovanja kada visok preostali rizik ostaje. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mapirano na savjetovanje i praćenje Data Protection Officer / Privacy Advisor gdje je primjenjivo za odluke o DPIA-i, visokorizičnu obradu, prethodno savjetovanje i promjene politike. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Mapirano na identifikaciju kontrola privatnosti, sigurnosne zaštitne mjere, usklađenost u području privatnosti, dokaze o riziku za privatnost, praćenje i pregled. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapirano na opseg procesa PIA-e, koristi, utvrđivanje okidača, pripremu, ulazne podatke procjene, dokaze dionika i strukturu izvješća DPIA-e koja se održava u REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Mapirano na zahtjeve programa zaštite osobnih podataka (PII), identifikaciju zahtjeva za zaštitu osobnih podataka (PII), odabir kontrola temeljen na riziku i poveznicu s obradom rizika za privatnost. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Mapirano na organizacijska načela rizika za privatnost, vodstvo, integraciju, procjenu rizika, obradu rizika, praćenje i pregled te evidentiranje i izvješćivanje. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].