					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII07					Naslov dokumenta: **Politika ocenjevanja tveganj za zasebnost in DPIA**							
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**

Usklajenost s standardi in predpisi

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Tveganja in priložnosti PIMS
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Ocena tveganj za zasebnost
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Obravnava tveganj za zasebnost in povezava z SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Načrtovane spremembe PIMS in ponovna ocena tveganj
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentirane informacije o tveganjih za zasebnost in DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operativno načrtovanje in nadzor
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operativna ocena tveganj za zasebnost
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operativna obravnava tveganj za zasebnost
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Spremljanje in merjenje tveganj za zasebnost
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Pregled tveganj za zasebnost s strani vodstva
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Neskladnosti in korektivni ukrepi, povezani s tveganji
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Ocena vpliva na zasebnost
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Evidence dejavnosti obdelave, ki podpirajo oceno tveganj
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Pogodba z naročnikom

				obdelovalca in pomoč pri DPIA
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informacije obdelovalca za podporo skladnosti naročnika
GDPR	Article 5(2)	Controller	Supporting	Dokazila odgovornosti
GDPR	Article 24	Controller	Supporting	Odgovornost in ukrepi upravljavca
GDPR	Article 25	Controller	Supporting	Varstvo podatkov že pri načrtovanju in privzeto
GDPR	Article 28	Both	Supporting	Pomoč obdelovalca in navodila
GDPR	Article 30	Both	Supporting	Evidence dejavnosti obdelave, ki podpirajo DPIA
GDPR	Article 32	Both	Supporting	Varnostno tveganje in varovalni ukrepi
GDPR	Article 35	Controller	Primary	Ocena učinka v zvezi z varstvom podatkov
GDPR	Article 36	Controller	Primary	Predhodno posvetovanje
GDPR	Article 39	Conditional	Supporting	Svetovanje in spremljanje DPO, kadar je relevantno
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Kontrole zasebnosti, informacijska varnost in skladnost zasebnosti
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Obseg, koristi, sprožilec in priprava PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Program varovanja PII in identifikacija zahtev
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause	Both	Supporting	Integracija organizacijskega upravljanja tveganj za zasebnost

	6.5; Clause 6.6; Clause 6.7			

1. Področje uporabe

1.1 Ta politika določa zahteve za ocenjevanje tveganj za zasebnost, preverjanje potrebe po DPIA, izvedbo celovite DPIA, obravnavo tveganj, sprejem preostalega tveganja, posvetovanje, pregled in upravljanje dokazil za obdelavo PII v obsegu PIMS.

1.2 Ta politika se uporablja za:

1.2.1 nove in bistveno spremenjene dejavnosti obdelave PII;

1.2.2 kontekste obdelave pri upravljavcu, skupnem upravljavcu, obdelovalcu in podobdelovalcu;

1.2.3 sisteme, aplikacije, storitve, poslovne procese, dobavitelje, obdelovalce, podobdelovalce, mednarodne prenose in ureditve deljenja podatkov, ki vplivajo na obdelavo PII;

1.2.4 dokazila o tveganjih za zasebnost in DPIA, ki se vodijo v REG04, ter podporna dokazila, ki se vodijo v REG02, REG03, REG08, REG09, REG10, REG11 in REG12.

1.3 Ta politika ne nadomešča kontrol popisa dejavnosti obdelave, kontrol obvestil o zasebnosti, kontrol privolitve, kontrol pravic posameznikov, na katere se nanašajo osebno določljivi podatki, kontrol varstva zasebnosti že pri načrtovanju, kontrol dobaviteljev, kontrol mednarodnih prenosov, varnostnih kontrol PII, kontrol incidentov, kontrol dokumentiranih informacij ali kontrol spremljanja/presoje/izboljševanja. Te zahteve so opredeljene v povezanih politikah, navedenih v razdelku 12.

1.4 Za namene te politike ocena tveganj za zasebnost pomeni dokumentirano identifikacijo, analizo, vrednotenje, obravnavo, pregled in spremljanje morebitnih škodljivih vplivov na zasebnost, ki izhajajo iz obdelave PII.

1.5 Za namene te politike DPIA pomeni dokumentirano oceno, ki se uporablja pri obdelavi upravljavca, za katero je verjetno, da bo povzročila visoko tveganje za posameznike, na katere se nanašajo osebno določljivi podatki, in ki ocenjuje nujnost obdelave, sorazmernost, tveganja, varovalne ukrepe, preostalo tveganje, potrebe po posvetovanju in pogoje odobritve.

1.6 Za namene te politike visoko preostalo tveganje za zasebnost pomeni tveganje za zasebnost, ki po predlagani ali izvedeni obravnavi tveganja ostane nad odobrenim pragom sprejemljivosti.

1.7 Za namene te politike bistvena sprememba pomeni vsako spremembo, ki vpliva na obseg PIMS, namen obdelave, pravno podlago, kategorije PII, kategorije posameznikov, na katere se nanašajo osebno določljivi podatki, obseg obdelave, tehnologijo obdelave, spremljanje ali profiliranje, avtomatizirano sprejemanje odločitev, ranljive posameznike, na katere se nanašajo osebno določljivi podatki, prejemnike, obdelovalce, podobdelovalce, mednarodne prenose, hrambo, varnostne kontrole, profil tveganja, navodila naročnika ali obseg certifikacije.

2. Namen

2.1 Namen te politike je zagotoviti, da se tveganja za zasebnost in obveznosti glede DPIA identificirajo, ocenijo, obravnavajo, odobrijo, pregledajo in dokazujejo, preden obdelava PII povzroči nesprejemljivo tveganje za posameznike, na katere se nanašajo osebno določljivi podatki, ali za PIMS.

2.2 Ta politika organizaciji omogoča dokazovanje upravljanja zasebnosti na podlagi tveganj, odgovornosti upravljavca za DPIA, pomoči obdelovalca pri DPIA, dokumentirane obravnave tveganj, odobritve preostalega tveganja, odločanja o predhodnem posvetovanju in nenehnega izboljševanja kontrol zasebnosti.

3. Cilji

3.1 Cilji te politike so:

3.1.1 določiti obvezne sprožilce za preverjanje tveganj za zasebnost;

3.1.2 določiti, kdaj je zahtevana celovita DPIA;

3.1.3 zagotoviti, da so odločitve upravljavca glede DPIA dokumentirane in pregledljive;

3.1.4 zagotoviti, da je pomoč obdelovalca in podobdelovalca pri DPIA dokumentirana, kadar jo zahtevajo navodilo naročnika ali pogodba;

3.1.5 zagotoviti, da se tveganja za zasebnost ocenijo pred začetkom nove ali bistveno spremenjene obdelave PII;

3.1.6 zagotoviti, da so obravnave tveganj za zasebnost dodeljene, izvedene in preverjene;

3.1.7 zagotoviti, da se visoka preostala tveganja za zasebnost eskalirajo in odobrijo pred začetkom ali nadaljevanjem obdelave;

3.1.8 zagotoviti, da so odločitve o predhodnem posvetovanju dokumentirane, kadar ostane visoko preostalo tveganje;

3.1.9 zagotoviti, da se dokazila o tveganjih za zasebnost in DPIA vodijo v REG04 ter povežejo s povezanimi dokaznimi objekti;

3.1.10 preprečiti vzpostavitev ločenih registrov DPIA, tveganj ali posvetovanj zunaj REG04.

4. Izjave politike

4.1 Preverjanje tveganj za zasebnost

4.1.1 [Both] Process Owner / Business Owner mora v REG04 začeti preverjanje tveganj za zasebnost pred začetkom nove ali bistveno spremenjene obdelave PII, evidentirane v REG02.

4.1.2 [Both] Privacy Lead / PIMS Manager mora vzdrževati merila za preverjanje tveganj za zasebnost v REG04 pred začetnim delovanjem PIMS in nato vsako leto.

4.1.3 [Controller] Process Owner / Business Owner mora v REG04 opraviti preverjanje potrebe po DPIA pred začetkom obdelave upravljavca, ki izpolnjuje merila za preverjanje tveganj za zasebnost.

4.1.4 [Processor] Vendor / Procurement Owner mora v REG08 evidentirati zahteve naročnika glede pomoči pri DPIA pred začetkom obdelave obdelovalca, kadar pogodba z naročnikom ali dokumentirano navodilo zahteva podporo pri DPIA.

4.1.5 [Both] System Owner / Application Owner mora v REG04 zagotoviti dokazila o zasnovi sistema, dostopu, varnosti, beleženju in tokovih podatkov pred odobritvijo ocene tveganj za zasebnost za nove ali bistveno spremenjene sisteme, ki obdelujejo PII.

4.1.6 [Both] Privacy Lead / PIMS Manager mora v REG04 evidentirati rezultat preverjanja in utemeljitev odločitve o celoviti DPIA pred nadaljevanjem dejavnosti obdelave.

4.2 Sprožilci DPIA in določitev zahteve

4.2.1 [Controller] Privacy Lead / PIMS Manager mora v REG04 zahtevati celovito DPIA pred začetkom obdelave upravljavca, za katero je verjetno, da bo povzročila visoko tveganje.

4.2.2 [Controller] Process Owner / Business Owner mora obdelavo, ki vključuje velik obseg, sistematično spremljanje, profiliranje, avtomatizirano sprejemanje odločitev, posebne kategorije PII, podatke o kazenskih obsodbah ali prekrških, ranljive posameznike, na katere se nanašajo osebno določljivi podatki, inovativno tehnologijo ali bistveno spremenjeno obdelavo, pred začetkom obdelave napotiti na Privacy Lead / PIMS Manager v REG04.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor mora v REG04 evidentirati nasvet pred odobritvijo odločitve o zahtevi za celovito DPIA za visoko tvegano obdelavo upravljavca.

4.2.4 [Both] Process Owner / Business Owner mora v REG04 ponovno preveriti tveganje za zasebnost pred uporabo PII za nov namen, dodajanjem novega prejemnika, uvedbo novega obdelovalca ali podobdelovalca, spremembo arhitekture sistema ali začetkom novega mednarodnega prenosa.

4.2.5 [Processor] Privacy Lead / PIMS Manager mora v REG08 dokumentirati, ali je podpora obdelovalca pri DPIA potrebna, v 10 delovnih dneh po prejemu zahteve naročnika za pomoč pri DPIA.

4.2.6 [Subprocessor] Vendor / Procurement Owner mora v REG08 dokumentirati zahteve glede pomoči pri DPIA navzgor po pogodbeni verigi pred začetkom podobdelave, kadar tako pomoč zahteva pogodba z naročnikom ali obdelovalcem navzgor po pogodbeni verigi.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Izjeme

9.1 Izjeme glede tveganj za zasebnost in DPIA

9.1.1 [All] Process Owner / Business Owner mora vsako izjemo od te politike zahtevati v REG12, preden pride do odstopanja.

9.1.2 [All] Privacy Lead / PIMS Manager mora v REG04 ali REG12 oceniti vpliv vsake zahtevane izjeme na zasebnost, pravne zahteve, certifikacijo, poslovanje in posameznike, na katere se nanašajo osebno določljivi podatki, v 10 delovnih dneh od zahteve.

9.1.3 [All] Data Protection Officer / Privacy Advisor mora v REG12 evidentirati nasvet pred odobritvijo vsake izjeme, ki vpliva na visoko tvegano obdelavo, dokončanje celovite DPIA, predhodno posvetovanje, visoko preostalo tveganje za zasebnost ali pomoč naročniku pri DPIA.

9.1.4 [All] Top Management mora v REG12 odobriti izjeme glede tveganj za zasebnost ali DPIA, ki vplivajo na visoko tvegano obdelavo, obseg certifikacije, predhodno posvetovanje ali nerešeno visoko preostalo tveganje za zasebnost, preden izjema začne učinkovati.

9.1.5 [All] Privacy Lead / PIMS Manager mora pred odobritvijo za vsako odobreno izjemo glede tveganj za zasebnost ali DPIA v REG12 določiti datum izteka, ki ne presega 90 dni.

9.1.6 [All] Process Owner / Business Owner mora vsako izjemo glede tveganj za zasebnost ali DPIA v REG12 zapreti ali ponovno oceniti v petih delovnih dneh po izteku.

10. Uveljavljanje

10.1 Uveljavljanje zahtev glede tveganj za zasebnost in DPIA

10.1.1 [All] Privacy Lead / PIMS Manager mora manjkajoča, netočna, nepopolna, zapadla ali neodobrena dokazila REG04 o tveganjih za zasebnost ali DPIA evidentirati kot neskladnost v REG12 v petih delovnih dneh po identifikaciji.

10.1.2 [Controller] Process Owner / Business Owner mora začasno ustaviti novo visoko tvegano obdelavo upravljavca, kadar pred uvedbo manjkajo zahtevana dokazila REG04 o odobritvi DPIA.

10.1.3 [Both] System Owner / Application Owner mora blokirati prehod v produkcijo sistemov, ki obdelujejo PII, kadar pred odobritvijo prehoda v produkcijo manjkajo zahtevana dokazila REG04 o obravnavi tveganj.

10.1.4 [Both] Vendor / Procurement Owner mora blokirati uvajanje dobavitelja, obdelovalca, podobdelovalca ali ureditve deljenja podatkov, kadar pred odobritvijo pogodbe manjkajo zahtevana dokazila REG04 o tveganjih za zasebnost ali pomoči pri DPIA.

10.1.5 [All] Top Management mora med pregledom vodstva v REG12 pregledati nerešene večje neskladnosti glede tveganj za zasebnost ali DPIA.

10.1.6 [All] Privacy Lead / PIMS Manager mora ponavljajoče se zamude rokov za preverjanje REG04, pregled DPIA ali obravnavo tveganj eskalirati Top Management v REG12 v petih delovnih dneh po drugi pojavitvi v 12-mesečnem obdobju.

10.1.7 [All] Internal Audit / Compliance Reviewer mora v REG12 preveriti učinkovitost korektivnih ukrepov za neskladnosti glede tveganj za zasebnost in DPIA ob naslednji načrtovani presoji ali v 60 dneh po zaprtju, kar nastopi prej.

11. Pregled in vzdrževanje

11.1 Pregled in vzdrževanje politike

11.1.1 [All] Privacy Lead / PIMS Manager mora to politiko v REG12 pregledati letno in v 30 dneh po bistveni spremembi zahtev glede tveganj za zasebnost, DPIA, predhodnega posvetovanja, pomoči obdelovalca ali certifikacije.

11.1.2 [All] Privacy Lead / PIMS Manager mora v REG12 letno pregledati merila preverjanja REG04, merila sprožilcev DPIA, merila ocenjevanja tveganj in merila sprejema preostalega tveganja.

11.1.3 [All] Data Protection Officer / Privacy Advisor mora v REG12 pred odobritvijo pregledati spremembe te politike, ki so pomembne z vidika zasebnosti.

11.1.4 [All] Top Management mora v REG12 odobriti bistvene spremembe te politike pred objavo.

11.1.5 [All] Privacy Lead / PIMS Manager mora posodobiti REG03 in REG04 v 15 delovnih dneh po odobrenih spremembah politike, ki spremenijo uporabljivost kontrol, merila tveganj ali zahteve za preverjanje potrebe po DPIA.

11.1.6 [All] Privacy Lead / PIMS Manager mora evidentirati komunikacijo odobrenih sprememb te politike v REG11 v 30 dneh po objavi.

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 obdelave PII in pravne podlage

12.5 PII04 - Politika obvestil o zasebnosti in preglednosti

12.6 PII05 - Politika upravljanja privolitev in preferenc

12.7 PII06 - Politika upravljanja pravic posameznikov, na katere se nanašajo osebno določljivi podatki

12.8 PII08 - Politika varstva zasebnosti že pri načrtovanju 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 PII13 - Politika mednarodnih prenosov PII

12.14 PII14 - Politika varnosti PII in nadzora dostopa

12.15 PII15 - Politika upravljanja incidentov in kršitev PII

12.16 PII17 - Politika dokumentiranih informacij in upravljanja dokazil PIMS

12.17 PII18 - Politika spremljanja, presoje in izboljševanja PIMS

13. Referenčni standardi in okviri

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Preslikano na identifikacijo in načrtovanje ukrepov za tveganja in priložnosti zasebnosti z uporabo meril preverjanja, pragov tveganj, eskalacije in vhodnih informacij za pregled vodstva. 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** - Preslikano na izvajanje preverjanja tveganj za zasebnost, ocene tveganj za zasebnost, ocenjevanja tveganj, ponovne ocene in vrednotenja sprožilcev DPIA pred

nadaljevanjem nove ali bistveno spremenjene obdelave. 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** - Preslikano na načrtovanje obravnave tveganj za zasebnost, posodobitve uporabljivosti kontrol, izvedbo obravnave, sprejem preostalega tveganja in povezavo z 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** - Preslikano na načrtovane spremembe PIMS in obdelave, ki sprožijo ponovno oceno tveganj za zasebnost in pregled DPIA. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Preslikano na nadzorovane dokumentirane informacije za preverjanje tveganj za zasebnost, dokazila DPIA, obravnavo tveganj, sprejem preostalega tveganja, odločitve o predhodnem posvetovanju, izjeme, neskladnosti in dokazila 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** - Preslikano na izvajanje kontrol tveganj za zasebnost in DPIA pred prehodom v produkcijo, uvajanjem, odobritvijo obdelave, zaprtjem obravnave in povezavo s korektivnimi ukrepi. 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** - Preslikano na operativno oceno tveganj za zasebnost za nove, spremenjene, sistemske, dobaviteljske, prenosne in z incidenti sprožene spremembe obdelave. 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** - Preslikano na operativno obravnavo tveganj za zasebnost, dodelitev obravnave, izvedbo obravnave, eskalacijo zapadle obravnave in preverjanje učinkovitosti. 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** - Preslikano na spremljanje in merjenje pokritosti preverjanja, statusa DPIA, odprtih tveganj, zapadlih ukrepov obravnave, ukrepov dobaviteljev, varnostnih ukrepov obravnave, ukrepov ponovne ocene po incidentih in ugotovitev presoje. 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** - Preslikano na pregled vodstva glede visokih preostalih tveganj za zasebnost, zapadlih ukrepov obravnave, statusa celovitih DPIA, odločitev o predhodnem posvetovanju in pomembnih izjem glede tveganj za zasebnost. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Preslikano na neskladnosti, izjeme, odpiranje korektivnih ukrepov, eskalacijo in preverjanje učinkovitosti v zvezi s tveganji za zasebnost in DPIA. 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** - Preslikano na ocenjevanje potrebe po oceni vpliva na zasebnost za novo ali spremenjeno obdelavo upravljavca ter njeno izvedbo, kadar je to ustrezno. 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** - Preslikano na evidence dejavnosti obdelave, ki podpirajo vhodne informacije za oceno tveganj za zasebnost in DPIA, vključno z namenom, kategorijami, sistemi, prejemniki, prenosi in dobavitelji. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Preslikano na pogodbe obdelovalca z naročniki in obveznosti pomoči naročniku pri DPIA. 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** - Preslikano na zagotavljanje informacij obdelovalca, potrebnih za skladnost naročnika, vključno s pomočjo pri DPIA in dokazili o podpori naročniku. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Preslikano na dokazila odgovornosti za preverjanje DPIA, odločitve o celoviti DPIA, obravnavo tveganj, sprejem preostalega tveganja, odločitve o predhodnem

posvetovanju, izjeme, ugotovitve presoje in korektivne ukrepe. 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** - Preslikano na odgovornost upravljavca za ustrezne ukrepe glede tveganj za zasebnost, pregled visokega preostalega tveganja, odobritev vodstva in vzdrževanje politike. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Preslikano na dokazila o varstvu zasebnosti že pri načrtovanju in privzetem varstvu zasebnosti, uporabljena pri oceni tveganj in pred odobritvijo prehoda v produkcijo. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Preslikano na pomoč obdelovalcev in podobdelovalcev pri DPIA, obravnavo navodil naročnika in dokazila o obravnavi tveganj dobaviteljev. 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** - Preslikano na evidence dejavnosti obdelave, ki podpirajo vhodne informacije za oceno tveganj za zasebnost in DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Preslikano na vhodne informacije o varnostnih tveganjih PII, izbiro varovalnih ukrepov, obravnavo varnostnih tveganj in posodobitve statusa varnostnih kontrol. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Preslikano na preverjanje potrebe po DPIA, določanje zahteve za celovito DPIA, vsebino DPIA, nasvet DPO, pregled in blokiranje visoko tvegane obdelave brez zahtevane odobritve DPIA. 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** - Preslikano na odločanje o predhodnem posvetovanju, nasvet DPO, odobritev Top Management in ukrepe nadaljevanja, začasne ustavitve, preoblikovanja ali posvetovanja, kadar ostane visoko preostalo tveganje. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Preslikano na svetovanje in spremljanje Data Protection Officer / Privacy Advisor, kadar je relevantno za odločitve o DPIA, visoko tvegano obdelavo, predhodno posvetovanje in spremembe 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** - Preslikano na identifikacijo kontrol zasebnosti, varnostne varovalne ukrepe, skladnost zasebnosti, dokazila o tveganjih za zasebnost, spremljanje in 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** - Preslikano na obseg procesa PIA, koristi, določanje sprožilcev, pripravo, vhodne informacije za oceno, dokazila deležnikov in strukturo poročila DPIA, ki se vodi v 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** - Preslikano na zahteve programa varovanja PII, identifikacijo zahtev za varovanje PII, izbiro kontrol na podlagi tveganj in povezavo z obravnavo tveganj za zasebnost. 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** - Preslikano na organizacijska načela tveganj za zasebnost, voditeljstvo, integracijo, oceno tveganj, obravnavo tveganj, spremljanje in pregled ter evidentiranje in poročanje. 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].