					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII15					Naslov dokumenta: **Politika upravljanja incidentov in kršitev varnosti osebnih podatkov**							
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 7.4; Clause 7.5	Both	Supporting	Komunikacije PIMS in dokumentirana dokazila o kršitvah
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operativna kontrola ter povezava z oceno in obravnavo tveganj za zasebnost
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Spremljanje, vrednotenje, neskladnost, korektivni ukrepi in izboljševanje
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Načrtovanje upravljanja incidentov in priprava na obdelavo PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Odziv na incidente informacijske varnosti, ki vključujejo PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Zakonske, statutarne, regulativne in pogodbene zahteve ter varstvo zapisov
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Pogodba obdelovalca z naročnikom in podpora obveznostim naročnika
GDPR	Article 5(2); Article 24	Controller	Supporting	Odgovornost in odgovornost upravljavca
GDPR	Article 26	Joint Controller	Supporting	Usklajevanje odgovornosti skupnih upravljavcev pri kršitvah
GDPR	Article 28	Both	Supporting	Pomoč obdelovalca in pogodbene

				obveznosti obdelovalca
GDPR	Article 32	Both	Supporting	Varnost obdelave in zmožnost zaznavanja kršitev
GDPR	Article 33	Both	Primary	Obveščanje o kršitvah varnosti osebnih podatkov in dokumentiranje kršitev
GDPR	Article 34	Controller	Primary	Sporočanje kršitev varnosti osebnih podatkov prizadetim posameznikom, na katere se nanašajo osebno določljivi podatki
GDPR	Article 39	Conditional	Supporting	Svetovanje DPO, spremljanje, sodelovanje in podpora kontaktne točke
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Načeli informacijske varnosti in skladnosti zasebnosti
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Odgovornosti odzivanja na incidente v zvezi s PII in poročanje o dogodkih
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Načrtovanje incidentov, ocenjevanje, odziv, pridobljene izkušnje in zbiranje dokazov
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Življenjski cikel procesa upravljanja incidentov
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politika, načrt, ozaveščanje, testiranje in pridobljene

				izkušnje na področju incidentov
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operacije zaznavanja, obveščanja, triaže, analize, odzivanja in poročanja
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Pričakovanja glede obveščanja obdelovalca v oblaku in zapisov o kršitvah
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Poročanje o pomembnih incidentih, kadar je primerno
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Upravljanje, razvrščanje in poročanje o ICT incidentih, kadar je primerno

1. Področje uporabe

1.1 Ta politika določa zahteve za prepoznavanje, poročanje, triažo, ocenjevanje, zajezitev, obveščanje, dokumentiranje, zaključevanje in izboljševanje na podlagi incidentov v zvezi z osebno določljivimi podatki in kršitev varnosti osebnih podatkov v obsegu PIMS.

1.2 Ta politika se uporablja za:

1.2.1 organizacijo, kadar deluje kot upravljavec PII;

1.2.2 organizacijo, kadar deluje kot skupni upravljavec in je potrebno usklajevanje odgovornosti za kršitve;

1.2.3 organizacijo, kadar deluje kot obdelovalec PII;

1.2.4 organizacijo, kadar deluje kot podobdelovalec;

1.2.5 sisteme, aplikacije, storitve, procese, dobavitelje, obdelovalce, podobdelovalce in tretje osebe, ki obdelujejo, hranijo, prenašajo, podpirajo, dostopajo do PII ali kako drugače vplivajo na PII v obsegu PIMS.

1.3 Ta politika uporablja REG10 - register incidentov v zvezi z osebno določljivimi podatki in kršitev varnosti osebnih podatkov kot primarni dokazni objekt za upravljanje incidentov in kršitev v zvezi s PII.

1.4 Ta politika uporablja podporne dokazne objekte, kot sledi:

1.4.1 REG01 za obseg PIMS ter kontekst veljavnih zainteresiranih strani, pravnih, pogodbenih, sektorskih zahtev in zahtev naročnikov glede poročanja.

1.4.2 REG02 za prizadete dejavnosti obdelave, kategorije PII, kategorije posameznikov, na katere se nanašajo osebno določljivi podatki, namene in sisteme.

1.4.3 REG03 za Izjavo o uporabnosti in posodobitve uporabljivosti kontrol.

1.4.4 REG04 za povezavo s tveganji za zasebnost, DPIA in preostalim tveganjem.

1.4.5 REG08 za dokazila o stičnih točkah za obravnavo incidentov pri obdelovalcih, podobdelovalcih, naročnikih, dobaviteljih in tretjih osebah.

1.4.6 REG09 za povezavo z mednarodnimi prenosi, kadar incident vpliva na čezmejno obdelavo.

1.4.7 REG11 za dokazila o usposabljanju, ozaveščanju in usposobljenosti za odzivanje na incidente.

1.4.8 REG12 za dokazila o presoji, neskladnosti, korektivnih ukrepih in izboljševanju.

1.5 Ta politika se za specialistične kontrole opira na povezane politike PIMS:

1.5.1 PII03 ureja popis dejavnosti obdelave in evidence pravnih podlag.

1.5.2 PII04 ureja obvestilo o zasebnosti in kontrole preglednosti zunaj komunikacij, specifičnih za kršitve.

1.5.3 PII06 ureja zahteve za uveljavljanje pravic posameznikov, na katere se nanašajo osebno določljivi podatki, ki nastanejo pred incidentom, med njim ali po njem.

1.5.4 PII07 ureja metodologijo ocenjevanja tveganj za zasebnost in DPIA.

1.5.5 PII08 ureja kontrole varstva zasebnosti že pri načrtovanju in privzeto.

1.5.6 PII10 ureja kontrole hrambe, izbrisa in odstranjevanja.

1.5.7 PII12 ureja kontrole zasebnostnih razmerij z obdelovalci, podobdelovalci, dobavitelji in tretjimi osebami.

1.5.8 PII13 ureja mehanizme mednarodnega prenosa PII in zapise o tveganjih prenosa.

1.5.9 PII14 ureja preventivne in odkrivalne kontrole varnosti in dostopa do PII.

1.5.10 PII16 ureja usposabljanje, ozaveščanje in usposobljenost na področju zasebnosti.

1.5.11 PII17 ureja dokumentirane informacije in upravljanje dokazil.

1.5.12 PII18 ureja spremljanje, notranjo presojo, vodstveni pregled, neskladnost, korektivne ukrepe in nenehno izboljševanje.

1.6 Za namene te politike:

1.6.1 »incident v zvezi z osebno določljivimi podatki« pomeni domnevni ali potrjeni dogodek, ki je vplival, bi lahko vplival ali bi lahko razumno vplival na zaupnost, celovitost, razpoložljivost, zakonito obdelavo ali pooblaščeno ravnanje s PII.

1.6.2 »kršitev varnosti osebnih podatkov« pomeni potrjeni incident v zvezi z osebno določljivimi podatki, ki vključuje nepooblaščeno, nezakonito, nenamerno ali neželeno uničenje, izgubo, spremembo, razkritje, dostop, nerazpoložljivost ali kompromitacijo PII.

1.6.3 »ocena kršitve« pomeni dokumentirano vrednotenje, ali je incident v zvezi z osebno določljivimi podatki kršitev varnosti osebnih podatkov, kateri PII in kateri posamezniki, na katere se nanašajo osebno določljivi podatki, so prizadeti, katera tveganja lahko nastanejo, katera obvestila ali komunikacije so potrebne in kateri sanacijski ukrepi so potrebni.

1.6.4 »seznanjenost« pomeni trenutek, ko ima organizacija razumno stopnjo gotovosti, da je prišlo do varnostnega incidenta ali incidenta zasebnosti ter da so bili PII kompromitirani ali so morda bili kompromitirani.

1.6.5 »incident v zvezi z osebno določljivimi podatki z velikim vplivom« pomeni incident v zvezi z osebno določljivimi podatki, ki vključuje visoko tvegano obdelavo, posebne vrste ali zelo občutljive PII, obsežno količino PII, ranljive posameznike, regulirane naročnike, vpliv v več jurisdikcijah, bistven vpliv na naročnika, kompromitacijo privilegiranega dostopa, javno izpostavljenost, izsiljevalsko programsko opremo, nerazpoložljivost storitve ali pomemben operativni ali ugledni vpliv.

1.6.6 »bistvena sprememba okoliščin incidenta« pomeni nove ali spremenjene informacije, ki vplivajo na obseg incidenta, resnost, kategorije PII, vpliv na posameznike, na katere se nanašajo osebno določljivi podatki, odločitev o obveščanju, vpliv na naročnika, temeljni vzrok, zajezitev, obnovitev, korektivni ukrep ali obveznosti zunanjega poročanja.

2. Namen

2.1 Namen te politike je zagotoviti, da se incidenti in kršitve v zvezi s PII obravnavajo dosledno, pravočasno, zakonito, varno in z dokazili, pripravljenimi za presojo.

2.2 Ta politika podpira odgovornost tako, da zahteva evidentiranje incidentov in kršitev v zvezi s PII v REG10 ter povezavo s prizadetimi zapisi o obdelavi, tveganji za zasebnost, razmerji z obdelovalci in podobdelovalci, zapisi o prenosih, korektivnimi ukrepi in zapisi o usposabljanju, kadar se sprožijo.

2.3 Ta politika zagotavlja, da se obveznosti upravljavca, skupnega upravljavca, obdelovalca in podobdelovalca obravnavajo z ločenimi pravili uporabljivosti, hkrati pa se ohranja enoten model dokazil za incidente in kršitve.

3. Cilji

3.1 Cilji te politike so:

3.1.1 zagotoviti, da se domnevni incidenti v zvezi z osebno določljivimi podatki poročajo in evidentirajo pravočasno;

3.1.2 zagotoviti, da se incidenti v zvezi z osebno določljivimi podatki triažirajo in razvrščajo po doslednih merilih;

3.1.3 zagotoviti, da ocene kršitev upoštevajo prizadete PII, posameznike, na katere se nanašajo osebno določljivi podatki, sisteme, dejavnosti obdelave, obdelovalce, podobdelovalce, prenose, tveganja in sanacijske ukrepe;

3.1.4 zagotoviti, da so odločitve o obveščanju upravljavca in komunikaciji s posamezniki, na katere se nanašajo osebno določljivi podatki, dokumentirane;

3.1.5 zagotoviti, da obdelovalci in podobdelovalci obvestila o kršitvah naročnikom ali nadrejenim strankam podajo brez nepotrebnega odlašanja in v skladu z veljavnimi pogodbami;

3.1.6 zagotoviti, da se dokazila med obravnavo incidenta ohranijo in zaščitijo;

3.1.7 zagotoviti, da se zajezitev, odstranitev, obnovitev in validacija spremljajo prek REG10;

3.1.8 zagotoviti, da se sprožilci reguliranega, pogodbenega, naročniškega in sektorskega poročanja ocenijo, kadar je primerno;

3.1.9 zagotoviti, da pridobljene izkušnje iz incidentov vodijo v korektivne ukrepe in nenehno izboljševanje;

3.1.10 zagotoviti, da so zapisi o incidentih in kršitvah na voljo za presojo, vodstveni pregled, zagotavljanje zaupanja naročnikov in regulativni pregled, kadar je primerno.

4. Izjave politike

4.1 Pripravljenost na incidente in sprejem prijav

4.1.1 [Both] Privacy Lead / PIMS Manager mora v REG10 najmanj enkrat letno in po vsaki bistveni spremembi obsega PIMS, pravnega konteksta, pogodbenih obveznosti ali visoko tvegane obdelave vzdrževati merila za obravnavo incidentov in kršitev v zvezi s PII.

4.1.2 [All] Incident Response Coordinator mora vsak prijavljeni ali zaznani domnevni incident v zvezi z osebno določljivimi podatki evidentirati v REG10 v enem delovnem dnevu po prejemu ali prej, kadar se lahko sproži veljavni rok za obveščanje ali poročanje naročniku.

4.1.3 [Both] System Owner / Application Owner mora ohraniti relevantne sistemske dnevnike, opozorila, evidence dostopa, konfiguracijska dokazila in dokazila o obnovitvi, povezana z REG10, kadar domnevni incident vpliva na sistem ali aplikacijo, ki obdeluje PII.

4.1.4 [Both] Information Security Lead mora v 24 urah po zaznavi izvesti začetno tehnično triažo vsakega varnostnega dogodka, ki vključuje PII, ter v REG10 evidentirati začetno resnost, prizadeta sredstva in status zajezitve.

4.2 Razvrščanje in ocena kršitve

4.2.1 [Both] Incident Response Coordinator mora vsak vnos v REG10 v 24 urah po sprejemu razvrstiti kot dogodek, ki ni povezan s PII, domnevni incident v zvezi z osebno določljivimi podatki, potrjeni incident v zvezi z osebno določljivimi podatki ali potrjeno kršitev varnosti osebnih podatkov, ali pa mora zapis REG10 posodobiti z razlogom, zakaj razvrstitev ostaja odprta.

4.2.2 [Both] Privacy Lead / PIMS Manager mora pred dokončno odločitvijo o obveščanju o kršitvi v REG02, REG04, REG08, REG09 in REG10 opredeliti prizadeto dejavnost obdelave, kategorije PII, kategorije posameznikov, na katere se nanašajo osebno določljivi podatki, sisteme, obdelovalce, podobdelovalce, lokacije prenosa in tveganja za zasebnost.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor mora za vsako potrjeno ali razumno domnevno kršitev varnosti osebnih podatkov oceniti tveganje za prizadete posameznike, na katere se nanašajo osebno določljivi podatki, ter v REG10 evidentirati priporočilo glede obveščanja, utemeljitev tveganja in nasvet, preden se sprejme odločitev o zunanjem obveščanju.

4.2.4 [Processor] Privacy Lead / PIMS Manager mora opredeliti prizadetega upravljavca ali naročnika in veljavne pogodbene zahteve glede obveščanja takoj, ko se organizacija seznani s kršitvijo varnosti osebnih podatkov, ki vpliva na PII naročnika, ter mora rezultat evidentirati v REG08 in REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager mora pred vsakim zunanjim obvestilom ali komunikacijo skupnega upravljavca preveriti dogovorjeno odgovornost za kršitev, odgovornost za vodenje komunikacije in ureditev usklajevanja ter mora odločitev evidentirati v REG08 in REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager mora za vsak incident v zvezi z osebno določljivimi podatki z velikim vplivom oceniti veljavne pravne, sektorske, finančnosektorske, kibernetskovarnostne, pogodbene, naročniške in prejemniške sprožilce poročanja ter rezultat uporabljivosti evidentirati v REG01, REG08 in REG10.

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

9. Izjeme

9.1.1 [Both] Privacy Lead / PIMS Manager mora vsako izjemo od te politike evidentirati v REG12 pred izvedbo ali v 24 urah po nujnem ukrepanju, kadar predhodna odobritev ni bila izvedljiva.

9.1.2 [Both] Top Management mora pred zaključkom incidenta odobriti vsako izjemo, ki bistveno vpliva na čas obvestila o kršitvi, javno komunikacijo, zavezo naročniku, ohranitev dokazil ali tveganje za posameznika, na katerega se nanašajo osebno določljivi podatki, pri čemer se dokazila o odobritvi hranijo v REG10 in REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor mora pred zaključkom incidenta dokumentirati nasvet za vsako zakasnjeno obvestilo, odločitev o neobveščanju ali izjemen pristop k komunikaciji, pri čemer se nasvet hrani v REG10.

9.1.4 [Both] Vendor / Procurement Owner mora izjeme, ki jih povzročijo dobavitelj, obdelovalec, podobdelovalec ali naročnik in vplivajo na odziv na incident, evidentirati v REG08 in REG12 v petih delovnih dneh po prepoznavi izjeme.

10. Uveljavljanje

10.1.1 [All] Process Owner / Business Owner mora neuspeh pri prijavi domnevnega incidenta v zvezi z osebno določljivimi podatki, ohranitvi dokazil, izvajanju dodeljenih ukrepov ali sodelovanju pri oceni kršitve eskalirati Privacy Lead / PIMS Manager v dveh delovnih dneh po odkritju, pri čemer se dokazila hranijo v REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager mora evidentirati neskladnost REG12, kadar kršitev te politike vpliva na sprejem incidenta, triažo, zajezitev, obveščanje, celovitost dokazil, komunikacijo ali korektivni ukrep.

10.1.3 [Both] Vendor / Procurement Owner mora v petih delovnih dneh prek REG08 in REG12 začeti sanacijo dobavitelja ali obdelovalca, kadar obdelovalec, podobdelovalec, dobavitelj ali druga tretja oseba ne izpolni dogovorjenih obveznosti glede incidentov ali kršitev.

10.1.4 [Both] Top Management mora bistvene ali ponavljajoče se neskladnosti pri upravljanju incidentov pregledati ob naslednjem načrtovanem vodstvenem pregledu, pri čemer se odločitve in zahtevani ukrepi hranijo v REG12.

11. Pregled in vzdrževanje

11.1.1 [Both] Privacy Lead / PIMS Manager mora to politiko pregledati najmanj enkrat letno ter rezultat pregleda, zahtevane spremembe in status odobritve evidentirati v REG12.

11.1.2 [Both] Incident Response Coordinator mora v 30 koledarskih dneh po zaključku vsakega incidenta v zvezi z osebno določljivimi podatki z velikim vplivom ali potrjene kršitve varnosti osebnih podatkov sprožiti pregled te politike po incidentu, pri čemer se dokazila o pregledu hranijo v REG10 in REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager mora to politiko pregledati v 30 koledarskih dneh po seznanitvi z bistveno spremembo veljavnih pravnih, sektorskih, naročniških,

pogodbenih zahtev ali zahtev obdelovalcev, podobdelovalcev ali zahtev glede poročanja o incidentih, povezanih s prenosi, pri čemer se dokazila o pregledu hranijo v REG01, REG08, REG09 in REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer mora izvajanje te politike pregledati najmanj enkrat letno v okviru programa notranje presoje PIMS, pri čemer se ugotovitve presoje in korektivni ukrepi hranijo v REG12.

11.1.5 [Both] Top Management mora med načrtovanim vodstvenim pregledom pregledati trende incidentov, pomembne kršitve, uspešnost obveščanja, zapadle korektivne ukrepe in učinkovitost politike, pri čemer se rezultati hranijo v REG12.

12. Povezane politike

12.1 To politiko je treba brati skupaj z:

12.1.1 PII01 - Politika sistema upravljanja informacij o zasebnosti

12.1.2 PII02 - Politika vlog, odgovornosti in odgovornosti na področju zasebnosti

12.1.3 PII03 - Politika popisa obdelave PII in pravnih podlag

12.1.4 PII04 - Politika obvestil o zasebnosti in preglednosti

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

12.1.6 PII07 - Politika ocenjevanja tveganj za zasebnost in DPIA

12.1.7 PII08 - Politika varstva zasebnosti že pri načrtovanju in privzeto

12.1.8 PII10 - Politika hrambe, izbrisa in odstranjevanja PII

12.1.9 PII12 - Politika upravljanja zasebnosti obdelovalcev, podobdelovalcev in tretjih oseb

12.1.10 PII13 - Politika mednarodnih prenosov PII

12.1.11 PII14 - Politika varnosti PII in nadzora dostopa

12.1.12 PII16 - Politika usposabljanja, ozaveščanja in usposobljenosti na področju zasebnosti

12.1.13 PII17 - Politika dokumentiranih informacij in upravljanja dokazil PIMS

12.1.14 PII18 - Politika spremljanja, presoje in izboljševanja PIMS

13. Referenčni standardi in okviri

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].