					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII15					Naziv dokumenta: **Politika upravljanja incidentima u vezi s osobnim podacima i povredama osobnih podataka**							
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 7.4; Clause 7.5	Both	Supporting	Komunikacije PIMS-a i dokumentirani dokazi o povredama
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operativna kontrola te povezanost s procjenom rizika za privatnost i obradom rizika za privatnost
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Praćenje, vrednovanje, nesukladnost, korektivna radnja i poboljšanje
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planiranje upravljanja incidentima i priprema za obradu PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Odgovor na incidente informacijske sigurnosti koji uključuju PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Pravni, zakonski, regulatorni i ugovorni zahtjevi te zaštita zapisa
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Sporazum izvršitelja obrade s klijentom i podrška obvezama klijenta
GDPR	Article 5(2); Article 24	Controller	Supporting	Odgovornost i odgovornost voditelja obrade
GDPR	Article 26	Joint Controller	Supporting	Koordinacija odgovornosti zajedničkih voditelja obrade za povrede
GDPR	Article 28	Both	Supporting	Pomoć izvršitelja obrade i ugovorne

				obveze izvršitelja obrade
GDPR	Article 32	Both	Supporting	Sigurnost obrade i sposobnost otkrivanja povreda
GDPR	Article 33	Both	Primary	Prijava povrede osobnih podataka i dokumentiranje povreda
GDPR	Article 34	Controller	Primary	Komunikacija o povredama osobnih podataka prema pogođenim ispitanicima
GDPR	Article 39	Conditional	Supporting	Savjetovanje DPO-a, praćenje, suradnja i podrška kontaktnoj točki
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Načela informacijske sigurnosti i usklađenosti privatnosti
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Odgovornosti za odgovor na incidente u vezi s PII i prijavljivanje događaja
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Planiranje incidenata, procjena, odgovor, naučene lekcije i prikupljanje dokaza
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Životni ciklus procesa upravljanja incidentima
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politika, plan, podizanje svijesti, testiranje i naučene lekcije u vezi s incidentima
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operacije otkrivanja, obavješćivanja, trijaže, analize, odgovora i izvješćivanja

ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Očekivanja u pogledu obavješćivanja izvršitelja obrade u oblaku i zapisa o povredama
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Prijavljivanje značajnih incidenata gdje je primjenjivo
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Upravljanje IKT incidentima, klasifikacija i izvješćivanje gdje je primjenjivo

1. Opseg

1.1 Ova politika utvrđuje zahtjeve za identificiranje, prijavljivanje, trijažu, procjenu, ograničavanje, obavješćivanje, dokumentiranje, zatvaranje i poboljšavanje na temelju incidenata u vezi s osobnim podacima i povreda osobnih podataka unutar opsega PIMS-a.

1.2 Ova se politika primjenjuje na sljedeće:

1.2.1 organizaciju kada djeluje kao voditelj obrade PII;

1.2.2 organizaciju kada djeluje kao zajednički voditelj obrade, ako je potrebna koordinacija odgovornosti za povredu;

1.2.3 organizaciju kada djeluje kao izvršitelj obrade PII;

1.2.4 organizaciju kada djeluje kao podizvršitelj obrade;

1.2.5 sustave, aplikacije, usluge, procese, dobavljače, izvršitelje obrade, podizvršitelje obrade i treće strane koje obrađuju, pohranjuju, prenose, podržavaju, pristupaju ili na drugi način utječu na PII unutar opsega PIMS-a.

1.3 Ova politika koristi REG10 - Registar incidenata u vezi s osobnim podacima i povreda osobnih podataka kao primarni dokazni objekt za upravljanje incidentima u vezi s osobnim podacima i povredama osobnih podataka.

1.4 Ova politika koristi potporne dokazne objekte kako slijedi:

1.4.1 REG01 za opseg PIMS-a te primjenjivi kontekst zainteresiranih strana, pravni, ugovorni, sektorski i klijentski kontekst izvješćivanja.

1.4.2 REG02 za pogođene aktivnosti obrade, kategorije PII, kategorije ispitanika, svrhe i sustave.

1.4.3 REG03 za Izjavu o primjenjivosti i ažuriranja primjenjivosti kontrola.

1.4.4 REG04 za povezanost s rizikom za privatnost, DPIA-om i preostalim rizikom.

1.4.5 REG08 za dokaze o sučelju za incidente s izvršiteljima obrade, podizvršiteljima obrade, klijentima, dobavljačima i trećim stranama.

1.4.6 REG09 za povezanost s međunarodnim prijenosima kada incident utječe na prekograničnu obradu.

1.4.7 REG11 za dokaze o osposobljavanju, podizanju svijesti i kompetenciji za odgovor na incidente.

1.4.8 REG12 za dokaze o reviziji, nesukladnosti, korektivnim radnjama i poboljšanjima.

1.5 Ova politika oslanja se na povezane politike PIMS-a za specijalističke kontrole:

1.5.1 PII03 uređuje popis aktivnosti obrade i zapise o pravnoj osnovi.

1.5.2 PII04 uređuje obavijest o privatnosti i kontrole transparentnosti izvan komunikacija specifičnih za povredu.

1.5.3 PII06 uređuje zahtjeve ispitanika za ostvarivanje prava koji nastanu prije, tijekom ili nakon incidenta.

1.5.4 PII07 uređuje metodologiju procjene rizika za privatnost i DPIA-e.

1.5.5 PII08 uređuje kontrole ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama.

1.5.6 PII10 uređuje kontrole zadržavanja, brisanja i zbrinjavanja.

1.5.7 PII12 uređuje kontrole odnosa u području privatnosti s izvršiteljima obrade, podizvršiteljima obrade, dobavljačima i trećim stranama.

1.5.8 PII13 uređuje mehanizme međunarodnog prijenosa PII i zapise o riziku prijenosa.

1.5.9 PII14 uređuje preventivne i detektivne sigurnosne kontrole te kontrole pristupa za PII.

1.5.10 PII16 uređuje osposobljavanje, podizanje svijesti i kompetenciju u području privatnosti.

1.5.11 PII17 uređuje dokumentirane informacije i upravljanje dokazima.

1.5.12 PII18 uređuje praćenje, internu reviziju, preispitivanje od strane uprave, nesukladnost, korektivne radnje i kontinuirano poboljšanje.

1.6 Za potrebe ove politike:

1.6.1 „Incident u vezi s osobnim podacima" znači sumnjivi ili potvrđeni događaj koji je utjecao, mogao utjecati ili bi razumno mogao utjecati na povjerljivost, cjelovitost, dostupnost, zakonitu obradu ili ovlašteno postupanje s PII.

1.6.2 „Povreda osobnih podataka" znači potvrđeni incident u vezi s osobnim podacima koji uključuje neovlašteno, nezakonito, slučajno ili nenamjerno uništenje, gubitak, izmjenu, otkrivanje, pristup, nedostupnost ili kompromitaciju PII.

1.6.3 „Procjena povrede" znači dokumentirano vrednovanje toga je li incident u vezi s osobnim podacima povreda osobnih podataka, koji su PII i ispitanici pogođeni, koji rizici mogu nastati, koje su obavijesti ili komunikacije potrebne te koje su korektivne mjere potrebne.

1.6.4 „Saznanje" znači trenutak u kojem organizacija ima razuman stupanj sigurnosti da se dogodio sigurnosni incident ili incident u području privatnosti te da je PII kompromitiran ili je mogao biti kompromitiran.

1.6.5 „Incident visokog utjecaja u vezi s osobnim podacima" znači incident u vezi s osobnim podacima koji uključuje obradu visokog rizika, posebne kategorije osobnih podataka ili izrazito osjetljiv PII, PII velikog opsega, ranjive pojedince, regulirane klijente, višejurisdikcijski utjecaj, značajan utjecaj na klijente, kompromitaciju privilegiranog pristupa, javnu izloženost, ransomware, nedostupnost usluge ili značajan operativni ili reputacijski utjecaj.

1.6.6 „Značajna promjena u vezi s incidentom" znači nova ili promijenjena informacija koja utječe na opseg incidenta, ozbiljnost, kategorije PII, utjecaj na ispitanike, odluku o obavješćivanju, utjecaj na klijente, temeljni uzrok, ograničavanje, oporavak, korektivnu radnju ili vanjske obveze izvješćivanja.

2. Svrha

2.1 Svrha ove politike jest osigurati da se incidentima u vezi s osobnim podacima i povredama osobnih podataka postupa dosljedno, pravodobno, zakonito, sigurno i uz dokaze spremne za reviziju.

2.2 Ova politika podupire odgovornost zahtijevajući da se incidenti u vezi s osobnim podacima i povrede osobnih podataka evidentiraju u REG10 te povežu s pogođenim zapisima o obradi, rizicima za privatnost, odnosima s izvršiteljima i podizvršiteljima obrade, zapisima o prijenosima, korektivnim radnjama i zapisima o osposobljavanju kada je to potaknuto činjenicama.

2.3 Ova politika osigurava da se obveze voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade rješavaju kroz zasebna pravila primjenjivosti, uz održavanje jednog integriranog modela dokaza o incidentima i povredama.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

3.1.1 osigurati da se sumnjivi incidenti u vezi s osobnim podacima pravodobno prijavljuju i evidentiraju;

3.1.2 osigurati da se incidenti u vezi s osobnim podacima trijažiraju i klasificiraju prema dosljednim kriterijima;

3.1.3 osigurati da procjene povreda razmatraju pogođeni PII, ispitanike, sustave, aktivnosti obrade, izvršitelje obrade, podizvršitelje obrade, prijenose, rizike i korektivne mjere;

3.1.4 osigurati dokumentiranje odluka voditelja obrade o prijavi povrede i odluka o komunikaciji s ispitanicima;

3.1.5 osigurati da se obavijesti izvršitelja obrade i podizvršitelja obrade o povredi prema klijentima ili nadređenim stranama dostavljaju bez nepotrebnog odgađanja i u skladu s primjenjivim sporazumima;

3.1.6 osigurati da se dokazi čuvaju i štite tijekom postupanja s incidentom;

3.1.7 osigurati da se ograničavanje, uklanjanje prijetnje, oporavak i validacija prate kroz REG10;

3.1.8 osigurati vrednovanje okidača za regulirano, ugovorno, klijentsko i sektorsko izvješćivanje gdje je primjenjivo;

3.1.9 osigurati da naučene lekcije iz incidenata rezultiraju korektivnim radnjama i kontinuiranim poboljšanjem;

3.1.10 osigurati da su zapisi o incidentima i povredama dostupni za reviziju, preispitivanje od strane uprave, pružanje potvrda klijentima i regulatorni pregled gdje je primjenjivo.

4. Izjave politike

4.1 Spremnost za incidente i zaprimanje prijava

4.1.1 [Both] Privacy Lead / PIMS Manager MUST održavati kriterije za postupanje s incidentima u vezi s osobnim podacima i povredama osobnih podataka u REG10 najmanje jednom godišnje i nakon svake značajne promjene opsega PIMS-a, pravnog konteksta, ugovornih obveza ili obrade visokog rizika.

4.1.2 [All] Incident Response Coordinator MUST evidentirati svaki prijavljeni ili otkriveni sumnjivi incident u vezi s osobnim podacima u REG10 u roku od jednog radnog dana od primitka, ili ranije kada se može pokrenuti primjenjivi rok za obavješćivanje ili izvješćivanje klijenta.

4.1.3 [Both] System Owner / Application Owner MUST sačuvati relevantne zapise dnevnika sustava, upozorenja, evidencije pristupa, konfiguracijske dokaze i dokaze o oporavku povezane s REG10 kada sumnjivi incident utječe na sustav ili aplikaciju koja obrađuje PII.

4.1.4 [Both] Information Security Lead MUST dovršiti početnu tehničku trijažu svakog sigurnosnog događaja koji uključuje PII u roku od 24 sata od otkrivanja te evidentirati početnu ozbiljnost, pogođenu imovinu i status ograničavanja u REG10.

4.2 Klasifikacija i procjena povrede

4.2.1 [Both] Incident Response Coordinator MUST klasificirati svaki unos u REG10 kao događaj koji nije povezan s PII, sumnjivi incident u vezi s osobnim podacima, potvrđeni incident u vezi s osobnim podacima ili potvrđenu povredu osobnih podataka u roku od 24 sata od zaprimanja ili ažurirati zapis u REG10 razlogom zbog kojeg klasifikacija ostaje na čekanju.

4.2.2 [Both] Privacy Lead / PIMS Manager MUST identificirati pogođenu aktivnost obrade, kategorije PII, kategorije ispitanika, sustave, izvršitelje obrade, podizvršitelje obrade, lokacije prijenosa i rizike za privatnost u REG02, REG04, REG08, REG09 i REG10 prije konačne odluke o prijavi povrede.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUST procijeniti rizik za pogođene ispitanike za svaku potvrđenu ili razumno sumnjivu povredu osobnih podataka te evidentirati preporuku o obavješćivanju, obrazloženje rizika i savjet u REG10 prije donošenja odluke o vanjskom obavješćivanju.

4.2.4 [Processor] Privacy Lead / PIMS Manager MUST identificirati pogođenog voditelja obrade ili klijenta i primjenjive ugovorne zahtjeve za obavješćivanje čim organizacija sazna za povredu osobnih podataka koja utječe na PII klijenta, te MUST evidentirati ishod u REG08 i REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUST provjeriti dogovorenu odgovornost za povredu, vodeću odgovornost za komunikaciju i koordinacijski aranžman prije bilo kakvog vanjskog obavješćivanja ili komunikacije od strane zajedničkog voditelja obrade, te MUST evidentirati odluku u REG08 i REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager MUST procijeniti primjenjive pravne, sektorske, financijsko-sektorske, kibernetičko-sigurnosne, ugovorne, klijentske i primateljske okidače izvješćivanja za svaki incident visokog utjecaja u vezi s osobnim podacima te evidentirati ishod primjenjivosti u REG01, REG08 i REG10.

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

9. Iznimke

9.1.1 [Both] Privacy Lead / PIMS Manager MUST evidentirati svaku iznimku od ove politike u REG12 prije provedbe ili u roku od 24 sata nakon hitne radnje kada prethodno odobrenje nije bilo izvedivo.

9.1.2 [Both] Top Management MUST odobriti svaku iznimku koja značajno utječe na rok prijave povrede, javnu komunikaciju, obvezu prema klijentu, očuvanje dokaza ili rizik za ispitanika prije zatvaranja incidenta, uz zadržavanje dokaza o odobrenju u REG10 i REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST dokumentirati savjet za svako odgođeno obavješćivanje, odluku o neobavješćivanju ili izniman pristup komunikaciji prije zatvaranja incidenta, uz zadržavanje savjeta u REG10.

9.1.4 [Both] Vendor / Procurement Owner MUST evidentirati iznimke koje potječu od dobavljača, izvršitelja obrade, podizvršitelja obrade ili klijenta i utječu na odgovor na incident u REG08 i REG12 u roku od pet radnih dana od identificiranja iznimke.

10. Provedba politike

10.1.1 [All] Process Owner / Business Owner MUST eskalirati propust prijavljivanja sumnjivog incidenta u vezi s osobnim podacima, očuvanja dokaza, postupanja po dodijeljenim radnjama ili suradnje u procjeni povrede prema Privacy Lead / PIMS Manager u roku od dva radna dana od otkrivanja, uz zadržavanje dokaza u REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager MUST evidentirati nesukladnost u REG12 kada kršenje ove politike utječe na zaprimanje incidenta, trijažu, ograničavanje, obavješćivanje, cjelovitost dokaza, komunikaciju ili korektivnu radnju.

10.1.3 [Both] Vendor / Procurement Owner MUST pokrenuti otklanjanje nedostataka dobavljača ili izvršitelja obrade kroz REG08 i REG12 u roku od pet radnih dana kada izvršitelj obrade, podizvršitelj obrade, dobavljač ili druga treća strana ne ispuni dogovorene obveze u vezi s incidentom ili povredom.

10.1.4 [Both] Top Management MUST pregledati značajne ili ponavljajuće nesukladnosti u upravljanju incidentima na sljedećem planiranom preispitivanju od strane uprave, uz zadržavanje odluka i potrebnih radnji u REG12.

11. Pregled i održavanje

11.1.1 [Both] Privacy Lead / PIMS Manager MUST pregledati ovu politiku najmanje jednom godišnje te evidentirati ishod pregleda, potrebne izmjene i status odobrenja u REG12.

11.1.2 [Both] Incident Response Coordinator MUST pokrenuti pregled ove politike nakon incidenta u roku od 30 kalendarskih dana nakon zatvaranja svakog incidenta visokog utjecaja u vezi s osobnim podacima ili potvrđene povrede osobnih podataka, uz zadržavanje dokaza o pregledu u REG10 i REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUST pregledati ovu politiku u roku od 30 kalendarskih dana od saznanja za značajnu promjenu primjenjivih pravnih, sektorskih, klijentskih, ugovornih zahtjeva, zahtjeva izvršitelja obrade, podizvršitelja obrade ili zahtjeva izvješćivanja o incidentima povezanih s prijenosom, uz zadržavanje dokaza o pregledu u REG01, REG08, REG09 i REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUST najmanje jednom godišnje pregledati provedbu ove politike kroz program interne revizije PIMS-a, uz zadržavanje nalaza revizije i korektivnih radnji u REG12.

11.1.5 [Both] Top Management MUST pregledati trendove incidenata, značajne povrede, učinkovitost obavješćivanja, zakašnjele korektivne radnje i djelotvornost politike tijekom planiranog preispitivanja od strane uprave, uz zadržavanje izlaznih rezultata u REG12.

12. Povezane politike

12.1 Ovu politiku treba čitati zajedno sa sljedećim politikama:

12.1.1 PII01 - Politika sustava upravljanja informacijama o privatnosti

12.1.2 PII02 - Politika uloga, odgovornosti i odgovornosti u području privatnosti

12.1.3 PII03 - Politika popisa obrade PII i pravne osnove

12.1.4 PII04 - Politika obavijesti o privatnosti i transparentnosti

12.1.5 PII06 - Politika upravljanja pravima ispitanika

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

12.1.7 PII08 - Politika ugrađene zaštite privatnosti i zaštite privatnosti prema zadanim postavkama

12.1.8 PII10 - Politika zadržavanja, brisanja i zbrinjavanja PII

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

12.1.10 PII13 - Politika međunarodnog prijenosa PII

12.1.11 PII14 - Politika sigurnosti i kontrole pristupa za PII

12.1.12 PII16 - Politika osposobljavanja, podizanja svijesti i kompetencije u području privatnosti

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

12.1.14 PII18 - Politika praćenja, revizije i poboljšanja PIMS-a

13. Referentni standardi i 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].