					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: PII15					Documenttitel: **Beleid voor beheer van PII-incidenten en inbreuken**						
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:						
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm / Regelgeving	Clausule / Beheersmaatregel / Artikel	Toepasselijkheid	Dekkingssoort	Opmerking
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS-communicatie en gedocumenteerd bewijsmateriaal van inbreuken
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operationele beheersing, privacyrisicobeoordeling en koppeling met risicobehandeling
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, evaluatie, non-conformiteit, corrigerende maatregelen en verbetering
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planning van en voorbereiding op incidentbeheer voor PII-verwerking
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Respons op informatiebeveiligingsincidenten waarbij PII betrokken is
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Juridische, wettelijke, regelgevende en contractuele eisen en bescherming van registraties
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Ondersteuning voor klantovereenkomsten van verwerkers en klantverplichtingen
GDPR	Article 5(2); Article 24	Controller	Supporting	Verantwoordingsplicht en verantwoordelijkheid van de verwerkingsverantwoordelijke
GDPR	Article 26	Joint Controller	Supporting	Coördinatie van inbreukverantwoordelijkheid tussen gezamenlijke verwerkingsverantwoordelijken
GDPR	Article 28	Both	Supporting	Bijstand door verwerkers en contractuele verplichtingen van verwerkers
GDPR	Article 32	Both	Supporting	Beveiliging van de verwerking en vermogen tot detectie van inbreuken
GDPR	Article 33	Both	Primary	Melding van inbreuken in verband met persoonsgegevens en documentatie van inbreuken

GDPR	Article 34	Controller	Primary	Communicatie over inbreuken in verband met persoonsgegevens aan getroffen betrokkenen
GDPR	Article 39	Conditional	Supporting	Advies, monitoring, samenwerking en ondersteuning als contactpunt door de DPO
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Beginselen voor informatiebeveiliging en privacynaleving
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Verantwoordelijkheden voor incidentrespons met betrekking tot PII en melding van gebeurtenissen
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incidentplanning, beoordeling, respons, geleerde lessen en verzameling van bewijsmateriaal
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Levenscyclus van het incidentbeheerproces
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incidentbeleid, plan, bewustwording, testen en geleerde lessen
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Detectie, melding, triage, analyse, respons en rapportageactiviteiten
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Verwachtingen inzake kennisgeving en inbreukregistraties voor cloudverwerkers
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Rapportage van significante incidenten waar van toepassing
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	ICT-incidentbeheer, classificatie en rapportage waar van toepassing

1. Reikwijdte

1.1 Dit beleid definieert de eisen voor het identificeren, melden, triëren, beoordelen, indammen, kennisgeven, documenteren, afsluiten en verbeteren naar aanleiding van PII-incidenten en PII-inbreuken binnen de PIMS-reikwijdte.

1.2 Dit beleid is van toepassing op:

1.2.1 de organisatie die optreedt als PII-verwerkingsverantwoordelijke;

1.2.2 de organisatie die optreedt als gezamenlijke verwerkingsverantwoordelijke wanneer coördinatie van inbreukverantwoordelijkheid vereist is;

1.2.3 de organisatie die optreedt als PII-verwerker;

1.2.4 de organisatie die optreedt als subverwerker;

1.2.5 systemen, toepassingen, diensten, processen, leveranciers, verwerkers, subverwerkers en derde partijen die PII binnen de PIMS-reikwijdte verwerken, opslaan, verzenden, ondersteunen, benaderen of anderszins beïnvloeden.

1.3 Dit beleid gebruikt REG10 - Register van PII-incidenten en PII-inbreuken als primair bewijsmateriaalobject voor beheer van PII-incidenten en PII-inbreuken.

1.4 Dit beleid gebruikt ondersteunende bewijsmateriaalobjecten als volgt:

1.4.1 REG01 voor de PIMS-reikwijdte en de toepasselijke context van belanghebbenden, wettelijke, contractuele, sectorale en klantrapportageverplichtingen.

1.4.2 REG02 voor getroffen verwerkingsactiviteiten, PII-categorieën, categorieën betrokkenen, doeleinden en systemen.

1.4.3 REG03 voor de Verklaring van Toepasselijkheid en actualiseringen van toepasselijkheid van beheersmaatregelen.

1.4.4 REG04 voor koppeling met privacyrisico's, DPIA en resterend privacyrisico.

1.4.5 REG08 voor bewijsmateriaal van incidentinterfaces met verwerkers, subverwerkers, klanten, leveranciers en derde partijen.

1.4.6 REG09 voor koppeling met internationale doorgifte wanneer een incident grensoverschrijdende verwerking raakt.

1.4.7 REG11 voor bewijsmateriaal van training, bewustwording en competentie voor incidentrespons.

1.4.8 REG12 voor bewijsmateriaal van audit, non-conformiteit, corrigerende maatregelen en verbetering.

1.5 Dit beleid steunt op gerelateerde PIMS-beleidslijnen voor specialistische beheersmaatregelen:

1.5.1 PII03 regelt de verwerkingsinventaris en registraties van rechtsgronden.

1.5.2 PII04 regelt privacyverklaringen en transparantiebeheersmaatregelen buiten inbreukspecifieke communicatie.

1.5.3 PII06 regelt verzoeken tot uitoefening van rechten door betrokkenen die vóór, tijdens of na een incident ontstaan.

1.5.4 PII07 regelt de methodologie voor privacyrisicobeoordeling en DPIA.

1.5.5 PII08 regelt privacy by design- en privacy by default-beheersmaatregelen.

1.5.6 PII10 regelt beheersmaatregelen voor bewaring, verwijdering en afvoer.

1.5.7 PII12 regelt privacyrelaties met verwerkers, subverwerkers, leveranciers en derde partijen.

1.5.8 PII13 regelt mechanismen voor internationale doorgifte van PII en registraties van doorgifterisico's.

1.5.9 PII14 regelt preventieve en detectieve beveiligings- en toegangsbeheersmaatregelen voor PII.

1.5.10 PII16 regelt privacytraining, bewustwording en competentie.

1.5.11 PII17 regelt gedocumenteerde informatie en beheer van bewijsmateriaal.

1.5.12 PII18 regelt monitoring, interne audit, directiebeoordeling, non-conformiteit, corrigerende maatregelen en voortdurende verbetering.

1.6 Voor dit beleid geldt:

1.6.1 "PII incident" betekent een vermoedelijke of bevestigde gebeurtenis die de vertrouwelijkheid, integriteit, beschikbaarheid, rechtmatige verwerking of geautoriseerde behandeling van PII heeft beïnvloed, mogelijk heeft beïnvloed of redelijkerwijs kan beïnvloeden.

1.6.2 "PII breach" betekent een bevestigd PII-incident waarbij sprake is van ongeoorloofde, onrechtmatige, accidentele of onbedoelde vernietiging, verlies, wijziging, openbaarmaking van, toegang tot, onbeschikbaarheid van of compromittering van PII.

1.6.3 "Breach assessment" betekent de gedocumenteerde beoordeling of een PII-incident een PII-inbreuk is, welke PII en betrokkenen zijn getroffen, welke risico's kunnen ontstaan, welke kennisgevingen of communicaties vereist zijn en welke herstelmaatregelen nodig zijn.

1.6.4 "Awareness" betekent het moment waarop de organisatie een redelijke mate van zekerheid heeft dat zich een beveiligings- of privacyincident heeft voorgedaan en dat PII is of mogelijk is gecompromitteerd.

1.6.5 "High-impact PII incident" betekent een PII-incident waarbij sprake is van hoogrisicoverwerking, bijzondere categorieën of zeer gevoelige PII, grootschalige PII, kwetsbare personen, gereguleerde klanten, impact in meerdere jurisdicties, wezenlijke klantimpact, compromittering van geprivilegieerde toegang, openbare blootstelling, ransomware, onbeschikbaarheid van diensten of significante operationele of reputatie-impact.

1.6.6 "Material incident change" betekent nieuwe of gewijzigde informatie die van invloed is op de incidentreikwijdte, ernst, PII-categorieën, impact op betrokkenen, kennisgevingsbesluit, klantimpact, oorzaak, indamming, herstel, corrigerende maatregelen of externe rapportageverplichtingen.

2. Doel

2.1 Het doel van dit beleid is te waarborgen dat PII-incidenten en PII-inbreuken consistent, tijdig, rechtmatig, veilig en met auditgereed bewijsmateriaal worden afgehandeld.

2.2 Dit beleid ondersteunt verantwoordingsplicht door te vereisen dat PII-incidenten en PII-inbreuken in REG10 worden geregistreerd en, waar geactiveerd, worden gekoppeld aan getroffen verwerkingsregistraties, privacyrisico's, verwerkers- en subverwerkersrelaties, doorgifteregistraties, corrigerende maatregelen en trainingsregistraties.

2.3 Dit beleid waarborgt dat verplichtingen van verwerkingsverantwoordelijken, gezamenlijke verwerkingsverantwoordelijken, verwerkers en subverwerkers worden afgehandeld via afzonderlijke toepasselijkheidsregels, terwijl één geïntegreerd bewijsmodel voor incidenten en inbreuken wordt gehandhaafd.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn:

3.1.1 waarborgen dat vermoedelijke PII-incidenten tijdig worden gemeld en geregistreerd;

3.1.2 waarborgen dat PII-incidenten worden getrieerd en geclassificeerd aan de hand van consistente criteria;

3.1.3 waarborgen dat datalekbeoordelingen rekening houden met getroffen PII, betrokkenen, systemen, verwerkingsactiviteiten, verwerkers, subverwerkers, doorgiften, risico's en herstelmaatregelen;

3.1.4 waarborgen dat besluiten over kennisgeving door de verwerkingsverantwoordelijke en communicatie aan betrokkenen worden gedocumenteerd;

3.1.5 waarborgen dat kennisgevingen van inbreuken door verwerkers en subverwerkers aan klanten of bovenliggende partijen zonder onredelijke vertraging en overeenkomstig toepasselijke overeenkomsten plaatsvinden;

3.1.6 waarborgen dat bewijsmateriaal tijdens incidentafhandeling wordt bewaard en beschermd;

3.1.7 waarborgen dat indamming, verwijdering, herstel en validatie via REG10 worden gevolgd;

3.1.8 waarborgen dat gereguleerde, contractuele, klant- en sectorale rapportagetriggers worden geëvalueerd waar van toepassing;

3.1.9 waarborgen dat uit incidenten geleerde lessen leiden tot corrigerende maatregelen en voortdurende verbetering;

3.1.10 waarborgen dat incident- en inbreukregistraties beschikbaar zijn voor audit, directiebeoordeling, klantassurance en toetsing door toezichthouders waar van toepassing.

4. Beleidsverklaringen

4.1 Paraatheid voor incidenten en intake

4.1.1 [Both] The Privacy Lead / PIMS Manager MUST criteria voor de afhandeling van PII-incidenten en PII-inbreuken in REG10 ten minste jaarlijks onderhouden en na elke wezenlijke wijziging in de PIMS-reikwijdte, juridische context, contractuele verplichtingen of hoogrisicoverwerking.

4.1.2 [All] The Incident Response Coordinator MUST elk gemeld of gedetecteerd vermoedelijk PII-incident binnen één werkdag na ontvangst in REG10 registreren, of eerder wanneer een toepasselijke kennisgevings- of klantrapportagetermijn kan worden geactiveerd.

4.1.3 [Both] The System Owner / Application Owner MUST relevante systeemlogboeken, waarschuwingen, toegangsregistraties, configuratiebewijsmateriaal en herstelbewijsmateriaal die aan REG10 zijn gekoppeld bewaren wanneer een vermoedelijk incident een systeem of toepassing raakt waarin PII wordt verwerkt.

4.1.4 [Both] The Information Security Lead MUST de initiële technische triage van elke beveiligingsgebeurtenis waarbij PII betrokken is binnen 24 uur na detectie voltooien en de initiële ernst, getroffen activa en indammingsstatus in REG10 registreren.

4.2 Classificatie en datalekbeoordeling

4.2.1 [Both] The Incident Response Coordinator MUST elke REG10-registratie binnen 24 uur na intake classificeren als een niet-PII-gebeurtenis, vermoedelijk PII-incident, bevestigd PII-incident of bevestigde PII-inbreuk, of de REG10-registratie bijwerken met de reden waarom de classificatie nog in afwachting is.

4.2.2 [Both] The Privacy Lead / PIMS Manager MUST de getroffen verwerkingsactiviteit, PII-categorieën, categorieën betrokkenen, systemen, verwerkers, subverwerkers, doorgiftelocaties en privacyrisico's in REG02, REG04, REG08, REG09 en REG10 identificeren voordat het besluit over kennisgeving van de inbreuk definitief wordt gemaakt.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST het risico voor getroffen betrokkenen beoordelen voor elke bevestigde of redelijkerwijs vermoede PII-inbreuk en de aanbeveling voor kennisgeving, risicorationale en het advies in REG10 registreren voordat het externe kennisgevingsbesluit wordt genomen.

4.2.4 [Processor] The Privacy Lead / PIMS Manager MUST de getroffen verwerkingsverantwoordelijke of klant en toepasselijke contractuele kennisgevingseisen identificeren zodra de organisatie zich bewust wordt van een PII-inbreuk die klant-PII raakt, en MUST het resultaat in REG08 en REG10 registreren.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST de overeengekomen inbreukverantwoordelijkheid, leidende communicatieverantwoordelijkheid en coördinatieregeling verifiëren vóór enige externe kennisgeving of communicatie door een gezamenlijke verwerkingsverantwoordelijke, en MUST het besluit in REG08 en REG10 registreren.

4.2.6 [Conditional] The Privacy Lead / PIMS Manager MUST toepasselijke wettelijke, sectorale, financiële-sector-, cyberbeveiligings-, contractuele, klant- en dienstenontvangergerichte rapportagetriggers evalueren voor elk PII-incident met hoge impact en het toepasselijkheidsresultaat in REG01, REG08 en REG10 registreren.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Uitzonderingen

9.1.1 [Both] The Privacy Lead / PIMS Manager MUST elke uitzondering op dit beleid vóór implementatie in REG12 registreren, of binnen 24 uur na een noodactie wanneer voorafgaande goedkeuring niet haalbaar was.

9.1.2 [Both] Top Management MUST elke uitzondering goedkeuren die wezenlijke gevolgen heeft voor de timing van inbreukkennisgeving, publieke communicatie, klantverplichtingen, bewaring van bewijsmateriaal of risico voor betrokkenen voordat het incident wordt afgesloten, waarbij goedkeuringsbewijsmateriaal in REG10 en REG12 wordt bewaard.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST advies documenteren voor elke vertraagde kennisgeving, elk besluit tot niet-kennisgeving of elke uitzonderlijke communicatieaanpak vóór incidentafsluiting, waarbij het advies in REG10 wordt bewaard.

9.1.4 [Both] The Vendor / Procurement Owner MUST door leveranciers, verwerkers, subverwerkers of klanten gedreven uitzonderingen die incidentrespons beïnvloeden binnen vijf werkdagen na identificatie van de uitzondering in REG08 en REG12 registreren.

10. Handhaving

10.1.1 [All] The Process Owner / Business Owner MUST het niet melden van een vermoedelijk PII-incident, het niet bewaren van bewijsmateriaal, het niet volgen van toegewezen acties of het niet meewerken aan datalekbeoordeling binnen twee werkdagen na ontdekking escaleren naar Privacy Lead / PIMS Manager, waarbij bewijsmateriaal in REG12 wordt bewaard.

10.1.2 [Both] The Privacy Lead / PIMS Manager MUST een REG12-non-conformiteit registreren wanneer een schending van dit beleid gevolgen heeft voor incidentintake, triage, indamming, kennisgeving, integriteit van bewijsmateriaal, communicatie of corrigerende maatregelen.

10.1.3 [Both] The Vendor / Procurement Owner MUST binnen vijf werkdagen remediatie door leveranciers of verwerkers initiëren via REG08 en REG12 wanneer een verwerker, subverwerker, leverancier of andere derde partij overeengekomen incident- of inbreukverplichtingen niet nakomt.

10.1.4 [Both] Top Management MUST wezenlijke of terugkerende non-conformiteiten in incidentbeheer beoordelen tijdens de eerstvolgende geplande directiebeoordeling, waarbij besluiten en vereiste acties in REG12 worden bewaard.

11. Beoordeling en onderhoud

11.1.1 [Both] The Privacy Lead / PIMS Manager MUST dit beleid ten minste jaarlijks beoordelen en de beoordelingsuitkomst, vereiste wijzigingen en goedkeuringsstatus in REG12 registreren.

11.1.2 [Both] The Incident Response Coordinator MUST binnen 30 kalenderdagen na afsluiting van elk PII-incident met hoge impact of elke bevestigde PII-inbreuk een post-incidentbeoordeling van dit beleid starten, waarbij beoordelingsbewijsmateriaal in REG10 en REG12 wordt bewaard.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUST dit beleid binnen 30 kalenderdagen beoordelen nadat hij kennis heeft gekregen van een wezenlijke wijziging in toepasselijke wettelijke, sectorale, klant-, contractuele, verwerker-, subverwerker- of doorgiftegerelateerde incidentrapportage-eisen, waarbij beoordelingsbewijsmateriaal in REG01, REG08, REG09 en REG12 wordt bewaard.

11.1.4 [Both] The Internal Audit / Compliance Reviewer MUST de implementatie van dit beleid ten minste jaarlijks beoordelen via het interne PIMS-auditprogramma, waarbij auditbevindingen en corrigerende maatregelen in REG12 worden bewaard.

11.1.5 [Both] Top Management MUST incidenttrends, significante inbreuken, kennisgevingsprestaties, achterstallige corrigerende maatregelen en beleidseffectiviteit beoordelen tijdens geplande directiebeoordeling, waarbij uitkomsten in REG12 worden bewaard.

12. Gerelateerde beleidslijnen

12.1 Dit beleid moet worden gelezen in samenhang met:

12.1.1 PII01 - Beleid voor het privacy-informatiemanagementsysteem

12.1.2 PII02 - Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht

12.1.3 PII03 - Beleid voor PII-verwerkingsinventaris en rechtsgrondslag

12.1.4 PII04 - Beleid inzake privacyverklaring en transparantie

12.1.5 PII06 - Beleid voor beheer van rechten van betrokkenen

12.1.6 PII07 - Beleid voor privacyrisicobeoordeling en DPIA

12.1.7 PII08 - Beleid voor privacy by design en privacy by default

12.1.8 PII10 - Beleid voor bewaring, verwijdering en afvoer van PII

12.1.9 PII12 - Beleid voor privacybeheer van verwerkers, subverwerkers en derde partijen

12.1.10 PII13 - Beleid voor internationale doorgifte van PII

12.1.11 PII14 - Beleid voor beveiliging en toegangscontrole van PII

12.1.12 PII16 - Beleid voor privacytraining, bewustwording en competentie

12.1.13 PII17 - Beleid voor gedocumenteerde PIMS-informatie en beheer van bewijsmateriaal

12.1.14 PII18 - Beleid voor PIMS-monitoring, audit en verbetering

13. Referentienormen en -raamwerken

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].