					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: PII01					Documenttitel: **Beleid inzake privacy-informatiemanagementsysteem**						
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	Dekkingstype	Opmerking
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Context en bepaling van de PIMS-rol
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Belanghebbenden en vereisten
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	PIMS-toepassingsgebied
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Vaststelling en verbetering van het PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Leiderschap en betrokkenheid
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Privacybeleid
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Rollen en bevoegdheden
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Risico's en kansen
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Beoordeling van privacyrisico's
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Behandeling van privacyrisico's en SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Privacydoelstellingen
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Geplande PIMS-wijzigingen
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Middelen
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competentie
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Bewustwording
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Communicatie
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Gedocumenteerde informatie
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operationele planning en beheersing
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operationele beoordeling van privacyrisico's

ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operationele behandeling van privacyrisico's
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitoring en evaluatie
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Interne audit
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Directiebeoordeling
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Voortdurende verbetering
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Non-conformiteit en corrigerende maatregel
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Governanceregistraties voor de verwerkingsverantwoordelijke
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Verwerkersovereenkomst en doeleinden
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Koppeling met PII-beveiligingsbeleid
GDPR	Article 5(2)	Controller	Supporting	Bewijsmateriaal voor verantwoordingsplicht
GDPR	Article 24	Controller	Supporting	Maatregelen en beleid van de verwerkingsverantwoordelijke
GDPR	Article 26	Joint Controller	Supporting	Regelingen tussen gezamenlijke verwerkingsverantwoordelijken
GDPR	Article 28	Both	Supporting	Governance van verwerkers
GDPR	Article 30	Both	Supporting	Verwerkingsregistraties
GDPR	Article 32	Both	Supporting	Beveiliging van de verwerking
GDPR	Article 35	Controller	Supporting	DPIA-governance
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Privacybeheersmaatregelen en -principes
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA-proces en voorbereiding
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	PII-beschermingsprogramma en beleid

ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integratie van organisatorische privacyrisico's

1. Reikwijdte

1.1 Dit beleid stelt het privacy-informatiemanagementsysteem van de organisatie vast voor de verwerking van PII in contexten van verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker.

1.2 Dit beleid is van toepassing op:

1.2.1 PIMS-toepassingsgebied, context, belanghebbenden en organisatorische grenzen;

1.2.2 bepaling van de PIMS-rol voor PII-verwerkingsactiviteiten;

1.2.3 privacybeleid, privacydoelstellingen, beoordeling van privacyrisico's, behandeling van privacyrisico's en de PIMS-Verklaring van Toepasselijkheid;

1.2.4 PIMS-governance, monitoring, interne audit, directiebeoordeling, non-conformiteit, corrigerende maatregelen en voortdurende verbetering;

1.2.5 gedocumenteerde informatie en bewijsmateriaal die nodig zijn om PIMS-conformiteit en verantwoordingsplicht aan te tonen.

1.3 Voor dit beleid betekent een wezenlijke wijziging elke wijziging die gevolgen heeft voor het PIMS-toepassingsgebied, PII-verwerkingsdoeleinden, PII-categorieën, categorieën betrokkenen, verwerkingslocaties, roltoewijzing als verwerkingsverantwoordelijke of verwerker, systeemarchitectuur, regelingen met leveranciers of subverwerkers, het privacyrisicoprofiel, toepasselijke wettelijke of contractuele verplichtingen, of het certificeringstoepassingsgebied.

2. Doel

2.1 Dit beleid definieert de verplichte governancevereisten voor het vaststellen, implementeren, onderhouden, monitoren en voortdurend verbeteren van het PIMS.

2.2 Het doel van dit beleid is te waarborgen dat de organisatie verantwoordingsplichtig, risicogebaseerd en door bewijsmateriaal onderbouwd beheer van PII-verwerking kan aantonen voor alle toepasselijke PIMS-rollen.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn om:

3.1.1 het PIMS-toepassingsgebied, de context, grenzen en roltoepasselijkheid te definiëren;

3.1.2 governanceverantwoordingsplicht voor het PIMS toe te wijzen met gebruikmaking van canonieke PIMS-rollen;

3.1.3 privacydoelstellingen en meetbare verwachtingen voor PIMS-prestaties vast te stellen;

3.1.4 een PIMS-Verklaring van Toepasselijkheid te onderhouden voor geselecteerde en uitgesloten beheersmaatregelen;

3.1.5 beoordeling van privacyrisico's, behandeling van privacyrisico's en DPIA-governance te integreren in de PIMS-werking;

3.1.6 te waarborgen dat verplichtingen voor verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker worden geïdentificeerd voordat de verwerking begint;

3.1.7 auditgereed bewijsmateriaal te onderhouden ten behoeve van gereedheid voor certificering en voortdurende verbetering;

3.1.8 onnodige rollen, registers, formulieren en dubbele operationele beheersmaatregelen te vermijden.

4. Beleidsverklaringen

4.1 Vaststelling, context en toepassingsgebied van het PIMS

4.1.1 [Both] Top Management MUST het PIMS-toepassingsgebied in REG01 goedkeuren vóór de initiële PIMS-implementatie en binnen 30 dagen na elke wezenlijke wijziging.

4.1.2 [Both] De Privacy Lead / PIMS Manager MUST externe en interne privacycontextkwesties jaarlijks in REG01 documenteren en binnen 30 dagen na elke wezenlijke wijziging.

4.1.3 [Both] De Privacy Lead / PIMS Manager MUST relevante belanghebbenden en hun PIMS-vereisten jaarlijks in REG01 documenteren en binnen 30 dagen na elke wezenlijke wijziging.

4.1.4 [Both] De Privacy Lead / PIMS Manager MUST de samenvatting van de interactie tussen PIMS-processen in REG01 onderhouden vóór elke directiebeoordeling.

4.2 Bepaling van de PIMS-rol

4.2.1 [Both] De Process Owner / Business Owner MUST de PIMS-rol van de organisatie voor elke PII-verwerkingsactiviteit in REG02 classificeren voordat de verwerkingsactiviteit begint.

4.2.2 [Joint Controller] De Vendor / Procurement Owner MUST de toewijzing van verantwoordelijkheden tussen gezamenlijke verwerkingsverantwoordelijken in REG08 documenteren voordat gezamenlijke verwerking begint.

4.2.3 [Processor] De Vendor / Procurement Owner MUST klantinstructies voor verwerking voor verwerkersactiviteiten in REG08 documenteren vóór service-onboarding.

4.2.4 [Subprocessor] De Vendor / Procurement Owner MUST upstream-klantinstructies en goedgekeurde subverwerkingsregelingen in REG08 documenteren voordat subverwerking begint.

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

9. Uitzonderingen

9.1 Verzoek om uitzondering en goedkeuring

9.1.1 [All] De Process Owner / Business Owner MUST elke aangevraagde uitzondering op dit beleid in REG12 documenteren voordat de afwijking plaatsvindt.

9.1.2 [Both] De Privacy Lead / PIMS Manager MUST het privacyrisico van elke aangevraagde uitzondering in REG04 beoordelen vóór goedkeuring.

9.1.3 [Both] Top Management MUST uitzonderingen die geaccepteerde drempels voor privacyrisico overschrijden in REG12 goedkeuren vóór implementatie.

9.1.4 [Both] De Privacy Lead / PIMS Manager MUST actieve PIMS-uitzonderingen per kwartaal in REG12 beoordelen totdat deze zijn afgesloten.

9.2 Afsluiting van uitzonderingen

9.2.1 [All] De Process Owner / Business Owner MUST bewijsmateriaal voor afsluiting van uitzonderingen in REG12 documenteren uiterlijk op de goedgekeurde vervaldatum van de uitzondering.

9.2.2 [Both] De Internal Audit / Compliance Reviewer MUST bewijsmateriaal voor afsluiting van verlopen uitzonderingen in REG12 verifiëren tijdens de volgende geplande interne audit.

10. Handhaving

10.1 Afhandeling van non-conformiteiten

10.1.1 [All] De Privacy Lead / PIMS Manager MUST vermoedelijke non-conformiteiten met dit beleid in REG12 vastleggen binnen vijf werkdagen na identificatie.

10.1.2 [All] De Process Owner / Business Owner MUST goedgekeurde corrigerende maatregelen in REG12 implementeren uiterlijk op de toegewezen vervaldatum na goedkeuring van de non-conformiteit.

10.1.3 [All] Top Management MUST onopgeloste majeure PIMS-non-conformiteiten in REG12 beoordelen bij elke directiebeoordeling.

10.1.4 [All] De Internal Audit / Compliance Reviewer MUST de doeltreffendheid van corrigerende maatregelen in REG12 verifiëren binnen 30 dagen na gerapporteerde afsluiting.

10.2 Escalatie

10.2.1 [All] De Privacy Lead / PIMS Manager MUST achterstallige majeure corrigerende maatregelen binnen vijf werkdagen na de vervaldatum escaleren naar Top Management in REG12.

10.2.2 [All] Top Management MUST besluiten over achterstallige majeure corrigerende maatregelen in REG12 vastleggen binnen 15 werkdagen na escalatie.

11. Beoordeling en onderhoud

11.1 Beleidsbeoordeling

11.1.1 [All] De Privacy Lead / PIMS Manager MUST dit beleid jaarlijks in REG12 beoordelen en binnen 30 dagen na elke wezenlijke juridische, organisatorische, verwerkings-, technologische of certificeringstoepassingsgebiedgerelateerde wijziging.

11.1.2 [All] De Data Protection Officer / Privacy Advisor MUST gedocumenteerd advies in REG12 verstrekken vóór goedkeuring van het beleid wanneer wezenlijke privacyverplichtingen wijzigen.

11.1.3 [All] Top Management MUST wezenlijke wijzigingen in dit beleid in REG12 goedkeuren vóór publicatie.

11.1.4 [All] De Privacy Lead / PIMS Manager MUST REG01 en REG03 binnen 15 werkdagen bijwerken na goedgekeurde beleidswijzigingen die het PIMS-toepassingsgebied of de toepasselijkheid van beheersmaatregelen wijzigen.

11.1.5 [All] De Privacy Lead / PIMS Manager MUST communicatie over goedgekeurde beleidswijzigingen in REG11 vastleggen binnen 30 dagen na publicatie.

12. Gerelateerde beleidslijnen

12.1 Dit beleid wordt ondersteund door de volgende gerelateerde beleidslijnen:

12.2 PII02 - Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht

12.3 PII03 - Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag

12.4 PII07 - Beleid inzake beoordeling van privacyrisico's en DPIA

12.5 PII08 - Beleid inzake privacy by design en privacy by default

12.6 PII12 - Beleid inzake verwerkers, subverwerkers en gegevensdeling

12.7 PII14 - Beleid inzake PII-beveiliging en toegangscontrole

12.8 PII15 - Beleid inzake PII-incidenten en inbreukbeheer

12.9 PII16 - Beleid inzake privacytraining, bewustwording en competentie

12.10 PII17 - Beleid inzake PIMS-gedocumenteerde informatie en bewijsmateriaalbeheer

12.11 PII18 - Beleid inzake PIMS-monitoring, audit en verbetering

13. Referentienormen en -raamwerken

13.1 Dit beleid is gekoppeld aan de volgende normen en regelgeving. De mapping licht toe hoe het beleid de aangehaalde vereisten ondersteunt en identificeert de interne clausules die deze implementeren of ondersteunen.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Gekoppeld aan het bepalen van de organisatorische context, privacycontextkwesties en de toepasselijkheid van de rol als verwerkingsverantwoordelijke of verwerker voor PIMS-activiteiten. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Gekoppeld aan het identificeren van belanghebbenden, betrokkenen, klanten, toezichthoudende autoriteiten, verwerkers, subverwerkers en hun relevante PIMS-vereisten. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Gekoppeld aan het definiëren, goedkeuren, onderhouden en wijzigen van het gedocumenteerde PIMS-toepassingsgebied. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Gekoppeld aan het vaststellen, implementeren, onderhouden en verbeteren van PIMS-processen en hun interacties. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Gekoppeld aan goedkeuring door Top Management, middelen, governancebeoordeling en leiderschap over PIMS-doeltreffendheid en verbetering. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Gekoppeld aan het onderhouden van dit privacybeleid als goedgekeurde gedocumenteerde informatie en het communiceren van beleidswijzigingen. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Gekoppeld aan het toewijzen en communiceren van PIMS-rollen, verantwoordelijkheden en bevoegdheden. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Gekoppeld aan het plannen van acties voor PIMS-risico's en -kansen op basis van context, vereisten van belanghebbenden, doelstellingen en verbeterinputs. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Gekoppeld aan de vereiste om privacyrisico's te beoordelen vóór nieuwe of wezenlijk gewijzigde verwerking en bewijsmateriaal over privacyrisico's te onderhouden. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Gekoppeld aan behandeling van privacyrisico's, selectie van beheersmaatregelen, koppeling met het informatiebeveiligingsprogramma en onderhoud van de Verklaring van Toepasselijkheid. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Gekoppeld aan het vaststellen, meten, monitoren, communiceren en bijwerken van PIMS-doelstellingen. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Gekoppeld aan geplande PIMS-wijzigingen en beheersing van wijzigingen die toepassingsgebied, rollen, beheersmaatregelen en gedocumenteerde informatie beïnvloeden. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Gekoppeld aan het bepalen en verschaffen van middelen voor vaststelling, werking, onderhoud en verbetering van het PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Gekoppeld aan competentieverwachtingen en bewijsmateriaal ter ondersteuning van PIMS-verantwoordelijkheden en rolprestaties. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Gekoppeld aan bewustwording van het privacybeleid, bijdrage aan PIMS-doeltreffendheid en gevolgen van non-conformiteit. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Gekoppeld aan interne en externe communicatie die relevant is voor PIMS-governance, beleidswijzigingen en escalatie. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Gekoppeld aan het creëren, onderhouden, beheersen, auditgereed houden en bewaren van gedocumenteerde informatie. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Gekoppeld aan het plannen, implementeren en beheersen van PIMS-operationele processen en extern geleverde processen. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Gekoppeld aan het uitvoeren van beoordelingen van privacyrisico's met geplande tussenpozen en wanneer significante wijzigingen worden voorgesteld of plaatsvinden. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Gekoppeld aan het implementeren van plannen voor behandeling van privacyrisico's en het bewaren van bewijsmateriaal van behandelingsresultaten. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Gekoppeld aan monitoring, meting, analyse, evaluatie, metrieken en rapportage over PIMS-doeltreffendheid. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Gekoppeld aan planning van interne audits, steekproeven van bewijsmateriaal, auditresultaten en onafhankelijke beoordeling. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Gekoppeld aan inputs voor directiebeoordeling, prestatiebeoordeling, outputs van directiebeoordeling en verbeterbesluiten. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Gekoppeld aan voortdurende verbetering via directiebeoordeling, metrieken, opvolging van corrigerende maatregelen en beleidsonderhoud. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Gekoppeld aan afhandeling van non-conformiteiten, corrigerende maatregelen, escalatie, afsluiting en verificatie van doeltreffendheid. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Gekoppeld aan registraties aan de kant van de verwerkingsverantwoordelijke van verwerkingsdoeleinden, koppeling met rechtsgrondslag, bepaling van DPIA-noodzaak, toewijzing van verantwoordelijkheden tussen gezamenlijke verwerkingsverantwoordelijken en bewijsregistraties van verwerking. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Gekoppeld aan klantovereenkomsten van verwerkers, gedocumenteerde klantinstructies en doelbindingsbeperkingen voor verwerkers. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Gekoppeld aan de koppeling met PII-beveiligingsbeleid, eigenaarschap van de baseline voor PII-beveiligingsmaatregelen en status van informatiebeveiligingsmaatregelen in de PIMS-Verklaring van Toepasselijkheid. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Gekoppeld aan bewijsmateriaal voor verantwoordingsplicht, goedkeuring van beleid, classificatie van verwerkingsrollen, toepasselijkheid van beheersmaatregelen, monitoring, audit en registraties van corrigerende maatregelen. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Gekoppeld aan governancemaatregelen van de verwerkingsverantwoordelijke, goedkeuring van beleid, PIMS-doelstellingen, beoordeling van doeltreffendheid en gedocumenteerd bewijsmateriaal van verantwoordingsplicht van de verwerkingsverantwoordelijke. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Gekoppeld aan het bepalen en documenteren van de toewijzing van verantwoordelijkheden tussen gezamenlijke verwerkingsverantwoordelijken voordat gezamenlijke verwerking begint. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Gekoppeld aan governanceregistraties voor verwerkers en subverwerkers, klantinstructies voor verwerking en beheersing van extern geleverde processen. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Gekoppeld aan registraties van verwerkingsactiviteiten, rolclassificatie, verantwoordingsregistraties voor verwerking en bewijsmateriaal dat wordt bewaard ten behoeve van auditeerbaarheid. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Gekoppeld aan governance van de PII-beveiligingsbaseline, eigenaarschap van beveiligingsmaatregelen, implementatiestatus van beveiliging en bevestiging van operationele beheersing. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Gekoppeld aan bepaling van DPIA-noodzaak en beoordeling van privacyrisico's voordat verwerking door een verwerkingsverantwoordelijke met hoog risico of wezenlijk gewijzigde verwerking wordt voortgezet. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Gekoppeld aan identificatie van privacybeheersmaatregelen, privacyprincipes, informatiebeveiliging, privacynaleving, audit, bewijsmateriaal en risicogebaseerde privacygovernance. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Gekoppeld aan PIA-governance, bepaling van DPIA-triggers, PIA-voorbereiding, criteria voor privacyrisico's en gedocumenteerd bewijsmateriaal van beoordeling van privacyrisico's. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Gekoppeld aan vereisten voor het PII-beschermingsprogramma, identificatie van PII-beschermingsvereisten, risicogebaseerde selectie van privacybeheersmaatregelen en beleidsrichting voor PII-bescherming. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Gekoppeld aan organisatorische privacyrisicoprincipes, leiderschapsbetrokkenheid, integratie van privacyrisico in PIMS-governance en inzicht in de rol van de organisatie bij PII-verwerking. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].