					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII07					Documenttitel: **Beleid inzake privacyrisicobeoordeling en DPIA**							
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**

Juridische kennisgeving (auteursrecht en gebruiksbeperkingen)

(C) 2025 Clarysec LLC. All rights reserved.

Dit document is intellectueel eigendom van Clarysec LLC. Geen enkel deel van dit document mag zonder voorafgaande uitdrukkelijke schriftelijke toestemming worden gekopieerd, hergebruikt, verspreid of gewijzigd voor commerciële of implementatiedoeleinden.
Ongeautoriseerd gebruik is strikt verboden en kan leiden tot juridische stappen.
Neem voor licentiëring contact op via: info@clarysec.com

Afgestemd op normen en regelgeving

Norm / Regelgeving	Clausule / Beheersmaatregel / Artikel	Toepasselijkheid	Dekkingssoort	Opmerking
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	PIMS-risico's en kansen
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Privacyrisicobeoordeling
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Behandeling van privacyrisico's en koppeling met de SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Geplande PIMS-wijzigingen en herbeoordeling van risico's
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Gedocumenteerde informatie over privacyrisico's en DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operationele planning en beheersing
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operationele privacyrisicobeoordeling
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operationele behandeling van privacyrisico's
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Monitoring en meting van privacyrisico's
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Directiebeoordeling van privacyrisico's
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Risicogerelateerde non-conformiteit en corrigerende maatregel
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Privacy-impactbeoordeling
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Verwerkingsregistraties ter ondersteuning van risicobeoordeling
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Klantovereenkomst van de verwerker en DPIA-ondersteuning
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informatie van de verwerker ter ondersteuning van klantnaleving
GDPR	Article 5(2)	Controller	Supporting	Bewijsmateriaal voor verantwoordingsplicht
GDPR	Article 24	Controller	Supporting	Verantwoordelijkheid en maatregelen van de verwerkingsverantwoordelijke
GDPR	Article 25	Controller	Supporting	Gegevensbescherming door ontwerp en standaardinstellingen
GDPR	Article 28	Both	Supporting	Ondersteuning en instructies van verwerkers

GDPR	Article 30	Both	Supporting	Verwerkingsregistraties ter ondersteuning van DPIA
GDPR	Article 32	Both	Supporting	Beveiligingsrisico en waarborgen
GDPR	Article 35	Controller	Primary	Gegevensbeschermingseffectbeoordeling
GDPR	Article 36	Controller	Primary	Voorafgaande raadpleging
GDPR	Article 39	Conditional	Supporting	DPO-advies en monitoring waar van toepassing
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Privacybeheersmaatregelen, informatiebeveiliging en naleving van privacyvereisten
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Reikwijdte, voordelen, trigger en voorbereiding van PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	PII-beschermingsprogramma en identificatie van vereisten
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Integratie van organisatorisch privacyrisicobeheer

1. Reikwijdte

1.1 Dit beleid definieert de vereisten voor privacyrisicobeoordeling, DPIA-screening, uitvoering van volledige DPIA's, risicobehandeling, acceptatie van resterend risico, raadpleging, beoordeling en beheer van bewijsmateriaal voor PII-verwerking binnen het PIMS-toepassingsgebied.

1.2 Dit beleid is van toepassing op het volgende:

1.2.1 nieuwe en wezenlijk gewijzigde PII-verwerkingsactiviteiten;

1.2.2 verwerkingscontexten als verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker;

1.2.3 systemen, applicaties, diensten, bedrijfsprocessen, leveranciers, verwerkers, subverwerkers, internationale doorgiften en regelingen voor gegevensdeling die PII-verwerking beïnvloeden;

1.2.4 bewijsmateriaal over privacyrisico's en DPIA's dat wordt bijgehouden in REG04 en ondersteunend bewijsmateriaal dat wordt bijgehouden in REG02, REG03, REG08, REG09, REG10, REG11 en REG12.

1.3 Dit beleid vervangt geen beheersmaatregelen voor de verwerkingsinventaris, privacyverklaring, toestemming, rechten van betrokkenen, privacy by design, leveranciers, internationale doorgiften, PII-beveiliging, incidenten, gedocumenteerde informatie of monitoring/audit/verbetering. Die vereisten zijn gedefinieerd in de gerelateerde beleidslijnen die in Sectie 12 zijn vermeld.

1.4 Voor dit beleid betekent privacyrisicobeoordeling de gedocumenteerde identificatie, analyse, evaluatie, behandeling, beoordeling en monitoring van mogelijke negatieve privacy-impact die voortvloeit uit PII-verwerking.

1.5 Voor dit beleid betekent DPIA een gedocumenteerde beoordeling die wordt gebruikt voor verwerking door een verwerkingsverantwoordelijke die waarschijnlijk een hoog risico voor betrokkenen oplevert en waarin de noodzaak, proportionaliteit, risico's, waarborgen, resterende risico's, raadplegingsbehoeften en goedkeuringsvoorwaarden van de verwerking worden geëvalueerd.

1.6 Voor dit beleid betekent hoog resterend privacyrisico een privacyrisico dat na voorgestelde of geïmplementeerde risicobehandeling boven de goedgekeurde acceptatiedrempel blijft.

1.7 Voor dit beleid betekent een wezenlijke wijziging elke wijziging die gevolgen heeft voor het PIMS-toepassingsgebied, het verwerkingsdoel, de rechtsgrondslag, PII-categorieën, categorieën betrokkenen, verwerkingsschaal, verwerkingstechnologie, monitoring of profilering, geautomatiseerde besluitvorming, kwetsbare betrokkenen, ontvangers, verwerkers, subverwerkers, internationale doorgiften, bewaring, beveiligingsbeheersmaatregelen, risicoprofiel, klantinstructies of certificeringstoepassingsgebied.

2. Doel

2.1 Het doel van dit beleid is te waarborgen dat privacyrisico's en DPIA-verplichtingen worden geïdentificeerd, beoordeeld, behandeld, goedgekeurd, beoordeeld en met bewijsmateriaal onderbouwd voordat PII-verwerking onaanvaardbare risico's voor betrokkenen of voor het PIMS veroorzaakt.

2.2 Dit beleid stelt de organisatie in staat risicogebaseerde privacygovernance, DPIA-verantwoordingsplicht van de verwerkingsverantwoordelijke, DPIA-ondersteuning door de verwerker, gedocumenteerde risicobehandeling, goedkeuring van resterend risico, besluitvorming over voorafgaande raadpleging en voortdurende verbetering van privacybeheersmaatregelen aan te tonen.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn:

3.1.1 verplichte triggers voor privacyrisicoscreening definiëren;

3.1.2 definiëren wanneer een volledige DPIA vereist is;

3.1.3 waarborgen dat DPIA-besluiten van de verwerkingsverantwoordelijke worden gedocumenteerd en beoordeelbaar zijn;

3.1.4 waarborgen dat DPIA-ondersteuning door verwerkers en subverwerkers wordt gedocumenteerd wanneer dit op grond van klantinstructie of overeenkomst vereist is;

3.1.5 waarborgen dat privacyrisico's worden beoordeeld voordat nieuwe of wezenlijk gewijzigde PII-verwerking doorgaat;

3.1.6 waarborgen dat behandelingen van privacyrisico's worden toegewezen, geïmplementeerd en geverifieerd;

3.1.7 waarborgen dat hoge resterende privacyrisico's worden geëscaleerd en goedgekeurd voordat de verwerking begint of wordt voortgezet;

3.1.8 waarborgen dat besluiten over voorafgaande raadpleging worden gedocumenteerd wanneer een hoog resterend risico blijft bestaan;

3.1.9 waarborgen dat bewijsmateriaal over privacyrisico's en DPIA's wordt bijgehouden in REG04 en wordt gekoppeld aan gerelateerde bewijsobjecten;

3.1.10 voorkomen dat afzonderlijke DPIA-, risico- of raadplegingsregisters buiten REG04 worden aangemaakt.

4. Beleidsverklaringen

4.1 Privacyrisicoscreening

4.1.1 [Both] The Process Owner / Business Owner MUST privacyrisicoscreening in REG04 initiëren voordat nieuwe of wezenlijk gewijzigde PII-verwerking die in REG02 is geregistreerd, begint.

4.1.2 [Both] The Privacy Lead / PIMS Manager MUST criteria voor privacyrisicoscreening in REG04 bijhouden vóór de initiële PIMS-werking en daarna jaarlijks.

4.1.3 [Controller] The Process Owner / Business Owner MUST DPIA-screening in REG04 voltooien voordat verwerking door de verwerkingsverantwoordelijke die aan de criteria voor privacyrisicoscreening voldoet, begint.

4.1.4 [Processor] The Vendor / Procurement Owner MUST vereisten voor DPIA-ondersteuning aan klanten in REG08 registreren voordat verwerking door de verwerker begint wanneer de klantovereenkomst of gedocumenteerde instructie DPIA-ondersteuning vereist.

4.1.5 [Both] The System Owner / Application Owner MUST bewijsmateriaal over systeemontwerp, toegang, beveiliging, logging en gegevensstromen in REG04 verstrekken vóór goedkeuring van de privacyrisicobeoordeling voor nieuwe of wezenlijk gewijzigde systemen die PII verwerken.

4.1.6 [Both] The Privacy Lead / PIMS Manager MUST de screeninguitkomst en de motivering voor het volledige-DPIA-besluit in REG04 registreren voordat de verwerkingsactiviteit doorgaat.

4.2 DPIA-triggers en bepaling van vereisten

4.2.1 [Controller] The Privacy Lead / PIMS Manager MUST een volledige DPIA in REG04 vereisen voordat verwerking door de verwerkingsverantwoordelijke die waarschijnlijk een hoog risico oplevert, begint.

4.2.2 [Controller] The Process Owner / Business Owner MUST verwerking waarbij sprake is van grootschaligheid, systematische monitoring, profilering, geautomatiseerde besluiten, bijzondere categorieën PII, gegevens over strafrechtelijke veroordelingen of strafbare feiten,

kwetsbare betrokkenen, innovatieve technologie of wezenlijk gewijzigde verwerking, in REG04 voorleggen aan The Privacy Lead / PIMS Manager voordat de verwerking begint.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST advies in REG04 registreren vóór goedkeuring van een besluit over de vereiste van een volledige DPIA voor verwerking met hoog risico door de verwerkingsverantwoordelijke.

4.2.4 [Both] The Process Owner / Business Owner MUST het privacyrisico opnieuw screenen in REG04 voordat PII voor een nieuw doel wordt gebruikt, een nieuwe ontvanger wordt toegevoegd, een nieuwe verwerker of subverwerker wordt geïntroduceerd, de systeemarchitectuur wordt gewijzigd of een nieuwe internationale doorgifte wordt gestart.

4.2.5 [Processor] The Privacy Lead / PIMS Manager MUST binnen 10 werkdagen na ontvangst van een verzoek van een klant om DPIA-ondersteuning in REG08 documenteren of DPIA-ondersteuning door de verwerker vereist is.

4.2.6 [Subprocessor] The Vendor / Procurement Owner MUST upstreamvereisten voor DPIA-ondersteuning in REG08 documenteren voordat subverwerking begint wanneer de upstreamklant of verwerkersovereenkomst dergelijke ondersteuning vereist.

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

9. Uitzonderingen

9.1 Uitzonderingen inzake privacyrisico's en DPIA's

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

9.1.2 [All] The Privacy Lead / PIMS Manager MUST de impact op privacy, juridische aspecten, certificering, operatie en betrokkenen van elke aangevraagde uitzondering in REG04 of REG12 beoordelen binnen 10 werkdagen na het verzoek.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST advies in REG12 registreren vóór goedkeuring van elke uitzondering die gevolgen heeft voor verwerking met hoog risico, voltooiing van een volledige DPIA, voorafgaande raadpleging, hoog resterend privacyrisico of DPIA-ondersteuning aan klanten.

9.1.4 [All] Top Management MUST privacyrisico- of DPIA-uitzonderingen die gevolgen hebben voor verwerking met hoog risico, certificeringstoepassingsgebied, voorafgaande raadpleging of onopgelost hoog resterend privacyrisico in REG12 goedkeuren voordat de uitzondering van kracht wordt.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST vóór goedkeuring voor elke goedgekeurde privacyrisico- of DPIA-uitzondering in REG12 een vervaldatum instellen die niet langer is dan 90 dagen.

9.1.6 [All] The Process Owner / Business Owner MUST elke privacyrisico- of DPIA-uitzondering in REG12 binnen vijf werkdagen na verval sluiten of herbeoordelen.

10. Handhaving

10.1 Handhaving inzake privacyrisico's en DPIA's

10.1.1 [All] The Privacy Lead / PIMS Manager MUST ontbrekend, onjuist, onvolledig, achterstallig of niet-goedgekeurd REG04-bewijsmateriaal over privacyrisico's of DPIA's binnen vijf werkdagen na identificatie als non-conformiteit in REG12 registreren.

10.1.2 [Controller] The Process Owner / Business Owner MUST nieuwe verwerking met hoog risico door de verwerkingsverantwoordelijke opschorten wanneer vereist REG04-bewijsmateriaal voor DPIA-goedkeuring vóór lancering ontbreekt.

10.1.3 [Both] The System Owner / Application Owner MUST livegang van systemen die PII verwerken blokkeren wanneer vereist REG04-bewijsmateriaal voor risicobehandeling vóór goedkeuring van livegang ontbreekt.

10.1.4 [Both] The Vendor / Procurement Owner MUST onboarding van leveranciers, verwerkers, subverwerkers of gegevensdeling blokkeren wanneer vereist REG04-bewijsmateriaal over privacyrisico's of DPIA-ondersteuning vóór goedkeuring van de overeenkomst ontbreekt.

10.1.5 [All] Top Management MUST onopgeloste grote non-conformiteiten inzake privacyrisico's of DPIA's in REG12 beoordelen tijdens de directiebeoordeling.

10.1.6 [All] The Privacy Lead / PIMS Manager MUST herhaald gemiste deadlines voor REG04-screening, DPIA-beoordeling of risicobehandeling binnen vijf werkdagen na de tweede gebeurtenis in een periode van 12 maanden in REG12 escaleren naar Top Management.

10.1.7 [All] The Internal Audit / Compliance Reviewer MUST de doeltreffendheid van corrigerende maatregelen voor non-conformiteiten inzake privacyrisico's en DPIA's in REG12 verifiëren bij de eerstvolgende geplande audit of binnen 60 dagen na afsluiting, afhankelijk van wat zich het eerst voordoet.

11. Beoordeling en onderhoud

11.1 Beleidsbeoordeling en onderhoud

11.1.1 [All] The Privacy Lead / PIMS Manager MUST dit beleid jaarlijks en binnen 30 dagen na een wezenlijke wijziging in privacyrisico-, DPIA-, voorafgaande-raadplegings-, verwerkersondersteunings- of certificeringsvereisten in REG12 beoordelen.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST REG04-screeningcriteria, DPIA-triggercriteria, risicoclassificatiecriteria en acceptatiecriteria voor resterend risico jaarlijks in REG12 beoordelen.

11.1.3 [All] The Data Protection Officer / Privacy Advisor MUST privacy-significante wijzigingen in dit beleid in REG12 beoordelen vóór goedkeuring.

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

11.1.5 [All] The Privacy Lead / PIMS Manager MUST REG03 en REG04 binnen 15 werkdagen bijwerken na goedgekeurde beleidswijzigingen die de toepasselijkheid van beheersmaatregelen, risicocriteria of DPIA-screeningvereisten wijzigen.

11.1.6 [All] The Privacy Lead / PIMS Manager MUST communicatie over goedgekeurde wijzigingen in dit beleid binnen 30 dagen na publicatie registreren in REG11.

12. Gerelateerde beleidslijnen

12.1 Dit beleid wordt ondersteund door de volgende gerelateerde beleidslijnen:

12.2 PII01 - Beleid inzake privacy-informatiemanagementsysteem

12.3 PII02 - Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht

12.4 PII03 - Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag

12.5 PII04 - Beleid inzake privacyverklaring en transparantie

12.6 PII05 - Beleid inzake toestemming en voorkeurenbeheer

12.7 PII06 - Beleid inzake beheer van rechten van betrokkenen

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

12.9 PII09 - Beleid inzake verzameling, gebruik, openbaarmaking en deling van PII

12.10 PII10 - Beleid inzake bewaring, verwijdering en vernietiging van PII

12.11 PII11 - Beleid inzake nauwkeurigheid en kwaliteit van PII

12.12 PII12 - Beleid inzake privacybeheer voor verwerkers, subverwerkers en derde partijen

12.13 PII13 - Beleid inzake internationale doorgifte van PII

12.14 PII14 - Beleid inzake PII-beveiliging en toegangscontrole

12.15 PII15 - Beleid inzake PII-incidenten en inbreukbeheer

12.16 PII17 - Beleid inzake gedocumenteerde informatie en bewijsmateriaalbeheer voor PIMS

12.17 PII18 - Beleid inzake monitoring, audit en verbetering van PIMS

13. Referentienormen en -raamwerken

13.1 Dit beleid is gekoppeld aan de volgende normen en regelgeving. De koppeling 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 6.1.1** - Gekoppeld aan het identificeren en plannen van acties voor privacyrisico's en kansen met behulp van screeningcriteria, risicodrempels, escalatie en input voor directiebeoordeling. 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** - Gekoppeld aan het uitvoeren van privacyrisicoscreening, privacyrisicobeoordeling, risicoclassificatie, herbeoordeling en evaluatie van DPIA-triggers voordat nieuwe of wezenlijk gewijzigde verwerking doorgaat. 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** - Gekoppeld aan planning van behandeling van privacyrisico's, updates van toepasselijkheid van beheersmaatregelen, implementatie van behandeling, acceptatie van resterend risico en koppeling met de 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** - Gekoppeld aan geplande PIMS- en verwerkingswijzigingen die herbeoordeling van privacyrisico's en DPIA-beoordeling triggeren. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Gekoppeld aan beheerste gedocumenteerde informatie voor privacyrisicoscreening, DPIA-bewijsmateriaal, risicobehandeling, acceptatie van resterend risico, besluiten over voorafgaande raadpleging, uitzonderingen, non-conformiteiten en bewijsmateriaal voor beleidsbeoordeling. 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** - Gekoppeld aan het uitvoeren van privacyrisico- en DPIA-beheersmaatregelen vóór livegang, onboarding, verwerkingsgoedkeuring, afsluiting van behandeling en koppeling aan corrigerende maatregelen. 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** - Gekoppeld aan operationele privacyrisicobeoordeling voor nieuwe, gewijzigde, systeem-, leveranciers-, doorgifte- en incidentgedreven verwerkingswijzigingen. 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** - Gekoppeld aan operationele behandeling van privacyrisico's, toewijzing van behandeling, implementatie van behandeling, escalatie van achterstallige behandeling en verificatie van doeltreffendheid. 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** - Gekoppeld aan monitoring en meting van screeningdekking, DPIA-status, openstaande risico's, achterstallige behandelingsacties, leveranciersacties, beveiligingsbehandelingsacties, incidentherbeoordelingsacties en auditbevindingen. 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** - Gekoppeld aan directiebeoordeling van hoge resterende privacyrisico's, achterstallige behandelingsacties, status van volledige DPIA's, besluiten over voorafgaande

raadpleging en grote uitzonderingen op privacyrisico's. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Gekoppeld aan non-conformiteiten inzake privacyrisico's en DPIA's, uitzonderingen, openen van corrigerende maatregelen, escalatie en verificatie van doeltreffendheid. 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** - Gekoppeld aan het beoordelen van de noodzaak van, en waar passend implementeren van, privacy-impactbeoordeling voor nieuwe of gewijzigde verwerking door de verwerkingsverantwoordelijke. 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** - Gekoppeld aan verwerkingsregistraties ter ondersteuning van input voor privacyrisico- en DPIA-beoordelingen, waaronder doel, categorieën, systemen, ontvangers, doorgiften en leveranciers. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Gekoppeld aan klantovereenkomsten van verwerkers en verplichtingen tot DPIA-ondersteuning aan klanten. 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** - Gekoppeld aan het verstrekken door de verwerker van informatie die nodig is voor klantnaleving, waaronder DPIA-ondersteuning en bewijsmateriaal voor klantondersteuning. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Gekoppeld aan verantwoordingsbewijsmateriaal voor DPIA-screening, besluiten over volledige DPIA's, risicobehandeling, acceptatie van resterend risico, besluiten over voorafgaande raadpleging, uitzonderingen, auditbevindingen en corrigerende maatregelen. 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** - Gekoppeld aan verantwoordelijkheid van de verwerkingsverantwoordelijke voor passende privacyrisicomaatregelen, beoordeling van hoog resterend risico, goedkeuring door management en onderhoud van beleid. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Gekoppeld aan bewijsmateriaal voor privacy-by-design en privacy-by-default dat wordt gebruikt bij risicobeoordeling en vóór goedkeuring van livegang. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Gekoppeld aan DPIA-ondersteuning door verwerkers en subverwerkers, afhandeling van klantinstructies en bewijsmateriaal voor behandeling van leveranciersrisico's. 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** - Gekoppeld aan verwerkingsregistraties ter ondersteuning van input voor privacyrisicobeoordelingen en DPIA's. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Gekoppeld aan input voor PII-beveiligingsrisico's, selectie van waarborgen, behandeling van beveiligingsrisico's en updates van de status van beveiligingsbeheersmaatregelen. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Gekoppeld aan DPIA-screening, bepaling van de vereiste voor een volledige DPIA, DPIA-inhoud, DPO-advies, beoordeling en het blokkeren van verwerking met hoog risico zonder vereiste DPIA-goedkeuring. 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** - Gekoppeld aan besluitvorming over voorafgaande raadpleging, DPO-advies, goedkeuring door Top Management en acties voor voortzetting, opschorting, herontwerp of raadpleging wanneer hoog resterend risico blijft bestaan. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Gekoppeld aan advies en monitoring door Data Protection Officer / Privacy Advisor waar van toepassing voor DPIA-besluiten, verwerking met hoog risico, voorafgaande raadpleging en beleidswijzigingen. 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** - Gekoppeld aan identificatie van privacybeheersmaatregelen, beveiligingswaarborgen, naleving van privacyvereisten, privacyrisicobewijsmateriaal, monitoring en beoordeling. 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** - Gekoppeld aan de reikwijdte, voordelen, triggerbepaling, voorbereiding, beoordelingsinput, stakeholderbewijsmateriaal en DPIA-rapportstructuur van het PIA-proces die in REG04 worden bijgehouden. 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** - Gekoppeld aan vereisten voor het PII-beschermingsprogramma, identificatie van PII-beschermingsvereisten, risicogebaseerde selectie van beheersmaatregelen en koppeling met behandeling van privacyrisico's. 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** - Gekoppeld aan organisatorische privacyrisicoprincipes, leiderschap, integratie, risicobeoordeling, risicobehandeling, monitoring en beoordeling, en registratie en rapportage. 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].