

				Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII03				Documenttitel: <b>Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag</b>							
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](mailto:info@clarysec.com)

## Afgestemd op normen en regelgeving

Norm / regelgeving	Clausule / beheersmaatregel / artikel	Toepasselijkheid	Dekkingssoort	Opmerking
ISO/IEC 27701:2025	Clause 4.1	Both	Supporting	Bepaling van de PIMS-rol voor verwerkingsactiviteiten
ISO/IEC 27701:2025	Clause 6.1.2	Both	Supporting	Koppeling met triggers voor privacyrisicobeoordeling
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Koppeling met toepasselijkheid van beheersmaatregelen en SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Gedocumenteerde informatie over de verwerkingsinventaris
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operationele planning en beheersing voor verwerkingsregistraties
ISO/IEC 27701:2025	Clause 8.2	Both	Supporting	Koppeling met operationele privacyrisicobeoordeling
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Monitoring en meting van de inventaris
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Non-conformiteit van de inventaris en corrigerende maatregelen
ISO/IEC 27701:2025	Annex A.1.2.2	Controller	Primary	Identificatie van verwerkingsdoeleinden door de verwerkingsverantwoordelijke
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Primary	Identificatie van de rechtsgrondslag door de verwerkingsverantwoordelijke
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Supporting	Koppeling met DPIA-screening
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Registraties van verwerkingsverantwoordelijkheden van gezamenlijke verwerkingsverantwoordelijken
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registraties van de verwerkingsverantwoordelijke met betrekking tot PII-verwerking
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Registraties van klantovereenkomsten en instructies van de verwerker
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Primary	Afstemming van het verwerkingsdoel van de verwerker op klantinstructies
ISO/IEC 27701:2025	Annex A.2.2.7	Processor	Supporting	Registraties van de verwerker met betrekking tot PII-verwerking

GDPR	Article 5(1)(a)	Controller	Supporting	Koppeling met rechtmatigheid, behoorlijkheid en transparantie
GDPR	Article 5(1)(b)	Controller	Supporting	Doelbinding
GDPR	Article 5(1)(c)	Controller	Supporting	Gegevensminimalisatie
GDPR	Article 5(1)(e)	Controller	Supporting	Koppeling met opslagbeperking
GDPR	Article 5(2)	Controller	Supporting	Bewijsmateriaal voor verantwoordingsplicht
GDPR	Article 6	Controller	Primary	Rechtmatigheid van verwerking
GDPR	Article 9	Conditional	Supporting	Voorwaarde voor verwerking van bijzondere categorieën
GDPR	Article 10	Conditional	Supporting	Voorwaarde voor gegevens over strafrechtelijke veroordelingen en strafbare feiten
GDPR	Article 24	Controller	Supporting	Verantwoordelijkheid en maatregelen van de verwerkingsverantwoordelijke
GDPR	Article 26	Joint Controller	Supporting	Registraties van de regeling tussen gezamenlijke verwerkingsverantwoordelijken
GDPR	Article 28	Both	Supporting	Registraties van verwerkersinstructies en overeenkomsten
GDPR	Article 30	Both	Primary	Registraties van verwerkingsactiviteiten
GDPR	Article 35	Controller	Supporting	Koppeling met DPIA-screening
ISO/IEC 29100:2020	Clause 5.3	Both	Supporting	Rechtmatigheid en specificatie van doeleinden
ISO/IEC 29100:2020	Clause 5.4	Both	Supporting	Beperking van verzameling
ISO/IEC 29100:2020	Clause 5.5	Both	Supporting	Gegevensminimalisatie
ISO/IEC 29100:2020	Clause 5.6	Both	Supporting	Beperking van gebruik, bewaring en verstrekking
ISO/IEC 29100:2020	Clause 5.10	Both	Supporting	Verantwoordingsplicht
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Controller	Supporting	Beheersmaatregelen voor bescherming van PII inzake doel, verzameling, minimalisatie, gebruik, bewaring en verstrekking
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Both	Supporting	Koppeling met PIA-voordeel en triggers



## 1. Reikwijdte

1.1 Dit beleid definieert de vereisten voor het onderhouden van de PII-verwerkingsinventaris / ROPA en het documenteren van rechtsgrondslag, verwerkingsdoeleinden, verwerkingsrollen, PII-categorieën, categorieën betrokkenen, ontvangers, bewaartermijnreferenties, overdrachtsreferenties, verwerkersinstructies, registraties van gezamenlijke verwerkingsverantwoordelijken en koppelingen met privacyrisicoscreening.

### 1.2 Dit beleid is van toepassing op:

1.2.1 alle PII-verwerkingsactiviteiten binnen de PIMS-reikwijdte;

1.2.2 verwerking die wordt uitgevoerd als verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker of subverwerker;

1.2.3 verwerking die wordt uitgevoerd door bedrijfsprocessen, systemen, toepassingen, leveranciers, verwerkers, subverwerkers en ontvangers bij gegevensdeling;

1.2.4 nieuwe verwerking, wezenlijk gewijzigde verwerking en beëindigde verwerking;

1.2.5 bewijsmateriaal dat wordt onderhouden in REG02 en ondersteunend bewijsmateriaal in REG01, REG03, REG04, REG05, REG07, REG08, REG09 en REG12.

1.3 Dit beleid vervangt geen gedetailleerde beheersmaatregelen voor privacyverklaringen, toestemmingsbeheersmaatregelen, DPIA-methodologie, uitvoering van bewaartermijnen, selectie van mechanismen voor internationale doorgifte, beheersmaatregelen voor verwerkerscontractering, PII-beveiligingsmaatregelen of beheersmaatregelen voor gedocumenteerde informatie. Die vereisten zijn gedefinieerd in de gerelateerde beleidslijnen die in sectie 12 zijn vermeld.

1.4 Voor dit beleid betekent een verwerkingsinventarisregistratie een REG02-vermelding die een afzonderlijke PII-verwerkingsactiviteit beschrijft, met inbegrip van het doel, de rol, de eigenaar, PII-categorieën, categorieën betrokkenen, rechtsgrondslag of verwijzing naar klantinstructies, systemen, ontvangers, bewaartermijnreferentie, overdrachtsreferentie, privacyrisicostatus en beoordelingsstatus.

1.5 Voor dit beleid betekent een wezenlijke wijziging in verwerking elke wijziging in verwerkingsdoel, rechtsgrondslag, PIMS-rol, PII-categorie, categorie betrokkenen, ontvanger, systeem, leverancier, subverwerker, verwerkingslocatie, overdracht, bewaarregel, beveiligingsclassificatie, privacyverklaring, afhankelijkheid van toestemming, DPIA-status, klantinstructie of certificeringsscope.

## 2. Doel

2.1 Het doel van dit beleid is te waarborgen dat de organisatie de PII-verwerkingsactiviteiten binnen de PIMS-reikwijdte kan identificeren, documenteren, rechtvaardigen, beoordelen en aantonen.

2.2 Dit beleid stelt de organisatie in staat een volledige, actuele en auditgereed PII-verwerkingsinventaris te onderhouden die rechtmatige verwerking, verantwoordingsplicht, privacyverklaringen, toestemmingsbeheer, privacyrisicobeoordeling, DPIA-screening, bewaring, governance van overdrachten, governance van verwerkers en PIMS-monitoring ondersteunt.

## 3. Doelstellingen

### 3.1 De doelstellingen van dit beleid zijn om:

3.1.1 REG02 vast te stellen als de gezaghebbende PII-verwerkingsinventaris en het bewijsmateriaalobject voor ROPA;

3.1.2 te waarborgen dat elke PII-verwerkingsactiviteit een verantwoordelijke eigenaar heeft;

3.1.3 onderscheid te maken tussen verwerkingsregistraties als verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker;

3.1.4 specifieke verwerkingsdoeleinden te documenteren voordat de verwerking begint;

- 3.1.5 de rechtsgrondslag voor verwerking door de verwerkingsverantwoordelijke te documenteren voordat de verwerking begint;
- 3.1.6 klantinstructies voor verwerking door verwerkers en subverwerkers te documenteren voordat de verwerking begint;
- 3.1.7 PII-categorieën, categorieën betrokkenen, ontvangers, bewaartermijnreferenties, overdrachtsreferenties, systemen en leveranciersrelaties te documenteren;
- 3.1.8 inventarisregistraties te koppelen aan privacyverklaringen, toestemming, DPIA, risico-, leveranciers-, overdrachts-, beheersmaatregel- en auditbewijsmateriaal waar van toepassing;
- 3.1.9 te waarborgen dat verwerkingsinventarisregistraties worden beoordeeld, bijgewerkt en gecorrigeerd wanneer de verwerking wijzigt;
- 3.1.10 te voorkomen dat afzonderlijke registers voor rechtsgrondslagen of verwerkingsinventarissen buiten REG02 worden aangemaakt.

#### **4. Beleidsverklaringen**

##### **4.1 Baseline voor de verwerkingsinventaris**

- 4.1.1 [Both] Process Owner / Business Owner moet een REG02-verwerkingsinventarisregistratie aanmaken voordat een nieuwe PII-verwerkingsactiviteit begint.
- 4.1.2 [Both] Process Owner / Business Owner moet de vereiste REG02-velden voor elke verwerkingsactiviteit registreren voordat de activiteit begint.
- 4.1.3 [Both] Privacy Lead / PIMS Manager moet de vereiste REG02-veldenset in REG12 goedkeuren vóór de eerste PIMS-werking en daarna jaarlijks.
- 4.1.4 [Both] Process Owner / Business Owner moet de PIMS-rol van de organisatie voor elke verwerkingsactiviteit in REG02 classificeren voordat de activiteit begint.
- 4.1.5 [Both] System Owner / Application Owner moet elk systeem of elke toepassing die PII verwerkt koppelen aan de relevante REG02-verwerkingsactiviteit vóór de livegang van het systeem.
- 4.1.6 [Both] Vendor / Procurement Owner moet elke relatie met een verwerker, subverwerker, derde partij voor gegevensdeling of gezamenlijke verwerkingsverantwoordelijke in REG08 koppelen aan de relevante REG02-verwerkingsactiviteit vóór goedkeuring van de overeenkomst of onboarding.

##### **4.2 Registraties van doel en rechtsgrondslag voor de verwerkingsverantwoordelijke**

- 4.2.1 [Controller] Process Owner / Business Owner moet het specifieke verwerkingsdoel in REG02 documenteren voordat PII wordt verzameld, gebruikt, verstrekt of anderszins verwerkt.
- 4.2.2 [Controller] Privacy Lead / PIMS Manager moet de in REG02 geregistreerde rechtsgrondslag valideren voordat verwerking door de verwerkingsverantwoordelijke begint en voordat een doelwijziging van kracht wordt.
- 4.2.3 [Controller] Data Protection Officer / Privacy Advisor moet advies vastleggen in REG12 vóór goedkeuring van een nieuwe rechtsgrondslag voor verwerking met hoog risico, bijzondere categorieën PII, gegevens over strafrechtelijke veroordelingen of strafbare feiten, of wezenlijk gewijzigde verwerking door de verwerkingsverantwoordelijke.
- 4.2.4 [Controller] Process Owner / Business Owner moet REG02 koppelen aan REG05 voordat verwerking door de verwerkingsverantwoordelijke op toestemming als rechtsgrondslag berust.
- 4.2.5 [Controller] Process Owner / Business Owner moet de referentie naar de gerechtvaardigd-belangbeoordeling in REG04 registreren voordat verwerking door de verwerkingsverantwoordelijke op gerechtvaardigde belangen berust.

- 4.2.6 [Conditional] Process Owner / Business Owner moet de voorwaarde voor verwerking van bijzondere categorieën in REG02 registreren voordat bijzondere categorieën PII worden verwerkt.
- 4.2.7 [Conditional] Privacy Lead / PIMS Manager moet de autorisatiegrondslag voor gegevens over strafrechtelijke veroordelingen of strafbare feiten in REG02 registreren voordat gegevens over strafrechtelijke veroordelingen of strafbare feiten worden verwerkt.
- 4.2.8 [Controller] Process Owner / Business Owner moet doelverenigbaarheid en privacyrisicoscreening in REG02 en REG04 documenteren voordat PII wordt gebruikt voor een nieuw doel dat niet eerder is geregistreerd.

[ ... 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 voor verwerkingsinventaris en rechtsgrondslag**

- 9.1.1 [All] Process Owner / Business Owner moet een uitzondering in REG12 aanvragen voordat een PII-verwerkingsactiviteit wordt uitgevoerd zonder vereist REG02-veld, registratie van rechtsgrondslag, verwijzing naar klantinstructies of beoordelingsstatus.
- 9.1.2 [All] Privacy Lead / PIMS Manager moet de privacy-, certificerings- en operationele impact van elke uitzondering op de verwerkingsinventaris binnen 10 werkdagen na het verzoek in REG12 beoordelen.
- 9.1.3 [All] Data Protection Officer / Privacy Advisor moet advies in REG12 vastleggen vóór goedkeuring van een uitzondering die betrekking heeft op rechtsgrondslag, bijzondere categorieën PII, gegevens over strafrechtelijke veroordelingen of strafbare feiten, verwerking met hoog risico, koppeling met internationale overdracht of beperking van klantinstructies.
- 9.1.4 [All] Top Management moet uitzonderingen op de verwerkingsinventaris die langer duren dan 30 dagen, verwerking met hoog risico beïnvloeden of de certificeringsscope beïnvloeden in REG12 goedkeuren voordat de uitzondering van kracht wordt.
- 9.1.5 [All] Privacy Lead / PIMS Manager moet voor elke goedgekeurde uitzondering op de verwerkingsinventaris vóór goedkeuring in REG12 een vervaldatum instellen die niet langer is dan 90 dagen.
- 9.1.6 [All] Process Owner / Business Owner moet elke uitzondering op de verwerkingsinventaris binnen vijf werkdagen na afloop sluiten of opnieuw beoordelen in REG12.

## **10. Handhaving**

### **10.1 Handhaving van verwerkingsinventaris en rechtsgrondslag**

- 10.1.1 [All] Privacy Lead / PIMS Manager moet ontbrekend, onnauwkeurig, verouderd of niet-goedgekeurd REG02-bewijsmateriaal voor de verwerkingsinventaris binnen vijf werkdagen na identificatie als non-conformiteit in REG12 registreren.
- 10.1.2 [Controller] Process Owner / Business Owner moet nieuwe verwerking door de verwerkingsverantwoordelijke opschorten wanneer het vereiste bewijsmateriaal voor doel of rechtsgrondslag vóór lancering ontbreekt in REG02.
- 10.1.3 [Processor] Process Owner / Business Owner moet nieuwe verwerking door de verwerker opschorten wanneer vereist bewijsmateriaal voor klantinstructies vóór service-onboarding ontbreekt in REG02 of REG08.
- 10.1.4 [Both] System Owner / Application Owner moet de livegang van systemen voor PII-verwerking blokkeren wanneer de vereiste REG02-inventariskoppeling ontbreekt vóór goedkeuring van livegang.

- 10.1.5 [Both] Vendor / Procurement Owner moet onboarding van leveranciers, verwerkers, subverwerkers, derde ontvangers of gezamenlijke verwerkingsverantwoordelijken blokkeren wanneer vereist bewijsmateriaal voor REG02- en REG08-koppeling ontbreekt vóór goedkeuring van de overeenkomst.
- 10.1.6 [All] Top Management moet onopgeloste majeure non-conformiteiten inzake verwerkingsinventaris of rechtsgrondslag in REG12 beoordelen tijdens de directiebeoordeling.
- 10.1.7 [All] Internal Audit / Compliance Reviewer moet de doeltreffendheid van corrigerende maatregelen voor non-conformiteiten in de verwerkingsinventaris verifiëren in REG12 bij de volgende geplande audit of binnen 60 dagen na afsluiting, afhankelijk van wat zich het eerst voordoet.

## **11. Beoordeling en onderhoud**

### **11.1 Beoordeling en onderhoud van beleid**

- 11.1.1 [All] Privacy Lead / PIMS Manager moet dit beleid jaarlijks en binnen 30 dagen na een wezenlijke wijziging in verwerkingsinventaris, rechtsgrondslag, verwerkersinstructie, ROPA of certificeringsvereisten in REG12 beoordelen.
- 11.1.2 [All] Privacy Lead / PIMS Manager moet de minimale veldvereisten van REG02 jaarlijks en binnen 30 dagen na een wezenlijke juridische, regelgevende, contractuele of verwerkingswijziging in REG12 beoordelen.
- 11.1.3 [All] Data Protection Officer / Privacy Advisor moet wijzigingen aan dit beleid met significante privacy-impact in REG12 beoordelen vóór goedkeuring.
- 11.1.4 [All] Top Management moet wezenlijke wijzigingen aan dit beleid in REG12 goedkeuren vóór publicatie.
- 11.1.5 [All] Privacy Lead / PIMS Manager moet REG03 en REG04 binnen 15 werkdagen na goedgekeurde beleidswijzigingen bijwerken wanneer die wijzigingen de toepasselijkheid van beheersmaatregelen of de vereisten voor privacyrisicoscreening wijzigen.
- 11.1.6 [All] Privacy Lead / PIMS Manager moet de communicatie over goedgekeurde wijzigingen aan dit beleid binnen 30 dagen na publicatie in REG11 registreren.

## **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 PII04 - Beleid inzake privacyverklaringen en transparantie
- 12.5 PII05 - Beleid inzake toestemmings- en voorkeurenbeheer
- 12.6 PII07 - Beleid inzake privacyrisicobeoordeling en DPIA
- 12.7 PII08 - Beleid inzake privacy by design en privacy by default
- 12.8 PII09 - Beleid inzake verzameling, gebruik, verstrekking en delen van PII
- 12.9 PII10 - Beleid inzake bewaring, verwijdering en vernietiging van PII
- 12.10 PII11 - Beleid inzake nauwkeurigheid en kwaliteit van PII
- 12.11 PII12 - Beleid inzake privacybeheer van verwerkers, subverwerkers en derde partijen
- 12.12 PII13 - Beleid inzake internationale PII-overdracht
- 12.13 PII14 - Beleid inzake PII-beveiliging en toegangscontrole
- 12.14 PII17 - Beleid inzake gedocumenteerde PIMS-informatie en bewijsmateriaalbeheer
- 12.15 PII18 - Beleid inzake PIMS-monitoring, audits en verbetering

## **13. Referentienormen en -raamwerken**

13.1 Dit beleid is in kaart gebracht ten opzichte van de volgende normen en regelgeving. De mapping legt uit 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** - Gemapt op het bepalen van de PIMS-rol van de organisatie voor elke verwerkingsactiviteit en het onderscheiden van contexten als verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker. Addressed by clauses [4.1.4; 4.3.1; 4.3.4; 4.3.5].

13.2.2 **Clause 6.1.2** - Gemapt op koppeling met triggers voor privacyrisicobeoordeling voor nieuwe en wezenlijk gewijzigde PII-verwerkingsactiviteiten. Addressed by clauses [4.2.8; 4.5.2; 4.5.3].

13.2.3 **Clause 6.1.3** - Gemapt op het koppelen van verwerkingsactiviteiten aan toepasselijkheid van beheersmaatregelen en bewijsmateriaal voor de PIMS-Verklaring van Toepasselijkheid. Addressed by clauses [4.5.4; 7.1.5; 11.1.5].

13.2.4 **Clause 7.5** - Gemapt op het onderhouden van registraties van verwerkingsinventaris, rechtsgrondslag, werkersinstructies, beoordelingen, uitzonderingen en corrigerende maatregelen als beheerste gedocumenteerde informatie. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.2; 4.3.1; 4.4.1; 4.5.1; 7.1.1; 7.1.3; 9.1.1; 10.1.1].

13.2.5 **Clause 8.1** - Gemapt op operationele planning en beheersing voor het aanmaken, valideren, bijwerken, beoordelen en beëindigen van verwerkingsinventarisregistraties voordat verwerking begint of wijzigt. Addressed by clauses [4.1.1; 4.1.5; 4.1.6; 4.5.1; 4.5.6; 7.1.2; 7.1.6; 7.1.7; 7.1.8].

13.2.6 **Clause 8.2** - Gemapt op koppeling met operationele privacyrisicobeoordeling vanuit verwerkingsinventarisregistraties en triggers voor wezenlijke wijzigingen in verwerking. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.2.7 **Clause 9.1** - Gemapt op het monitoren en meten van volledigheid van de verwerkingsinventaris, validatie van rechtsgrondslagen, koppeling met instructies, beoordelingsstatus, koppeling met DPIA-screening en afstemmingsuitzonderingen. Addressed by clauses [4.5.4; 4.5.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.8 **Clause 10.2** - Gemapt op de behandeling van non-conformiteiten, uitzonderingen, corrigerende maatregelen, handhaving en verificatie van doeltreffendheid met betrekking tot inventaris en rechtsgrondslag. Addressed by clauses [9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.6; 10.1.7].

13.2.9 **Annex A.1.2.2** - Gemapt op het identificeren en documenteren van verwerkingsdoeleinden van de verwerkingsverantwoordelijke voordat PII wordt verzameld, gebruikt, verstrekt of anderszins verwerkt. Addressed by clauses [4.1.2; 4.2.1; 4.2.8; 4.3.5].

13.2.10 **Annex A.1.2.3** - Gemapt op het bepalen, documenteren, valideren en aantonen van de rechtsgrondslag voor verwerking door de verwerkingsverantwoordelijke. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7].

13.2.11 **Annex A.1.2.6** - Gemapt op het screenen van nieuwe en wezenlijk gewijzigde verwerkingsactiviteiten van de verwerkingsverantwoordelijke op de noodzaak van een DPIA. Addressed by clauses [4.5.2; 4.5.3; 8.1.5].

13.2.12 **Annex A.1.2.8** - Gemapt op het registreren van verwerkingsdoeleinden van gezamenlijke verwerkingsverantwoordelijken en referenties naar de verdeling van verantwoordelijkheden. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.2.13 **Annex A.1.2.9** - Gemapt op het onderhouden van registraties van de verwerkingsverantwoordelijke met betrekking tot PII-verwerking, waaronder doeleinden,

- categorieën, ontvangers, bewaartermijnreferenties, overdrachten, rechtsgrondslag, risicoscreening, eigenaar, status en beoordelingsbewijsmateriaal. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.4.6; 4.5.1; 4.5.6; 7.1.2; 7.1.8].
- 13.2.14 **Annex A.2.2.2** - Gemapt op bewijsmateriaal voor klantovereenkomsten en gedocumenteerde instructies van verwerkers, met inbegrip van onderwerp, duur, doel, PII-categorieën en categorieën betrokkenen. Addressed by clauses [4.3.1; 4.3.2; 5.1.7; 10.1.3].
- 13.2.15 **Annex A.2.2.3** - Gemapt op het waarborgen dat verwerkingsdoeleinden van verwerkers afgestemd blijven op gedocumenteerde klantinstructies. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 10.1.3].
- 13.2.16 **Annex A.2.2.7** - Gemapt op het onderhouden van verwerkersregistraties met betrekking tot verwerking van PII namens klanten. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 8.1.3].

### 13.3 **GDPR**

- 13.3.1 **Article 5(1)(a)** - Gemapt op verwerkingsdoel van de verwerkingsverantwoordelijke, validatie van rechtsgrondslag en bewijsmateriaal voor verantwoordingsplicht voordat verwerking begint. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.8].
- 13.3.2 **Article 5(1)(b)** - Gemapt op doelspecificatie, beoordeling van doelverenigbaarheid en het voorkomen van verwerking voor niet-gedocumenteerde nieuwe doelen. Addressed by clauses [4.2.1; 4.2.8; 4.3.3].
- 13.3.3 **Article 5(1)(c)** - Gemapt op het registreren van PII-categorieën, categorieën betrokkenen en brongegevens vóór verwerking ter ondersteuning van de beoordeling van minimalisatie. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].
- 13.3.4 **Article 5(1)(e)** - Gemapt op het registreren van de bewaarregel of bewaartermijnreferentie voor elke verwerkingsactiviteit. Addressed by clauses [4.4.4; 8.1.6].
- 13.3.5 **Article 5(2)** - Gemapt op bewijsmateriaal voor verantwoordingsplicht inzake verwerkingsinventaris, validatie van rechtsgrondslag, beoordeling, afstemming, auditsteekproeven en corrigerende maatregelen. Addressed by clauses [4.1.1; 4.2.2; 4.5.4; 4.5.5; 6.1.2; 10.1.1; 10.1.7].
- 13.3.6 **Article 6** - Gemapt op het documenteren en valideren van de rechtsgrondslag voor verwerking door de verwerkingsverantwoordelijke, waaronder koppeling met toestemming, referentie naar gerechtvaardigd-belangbeoordeling en doelverenigbaarheid. Addressed by clauses [4.2.2; 4.2.4; 4.2.5; 4.2.8].
- 13.3.7 **Article 9** - Gemapt op het registreren van de voorwaarde voor verwerking van bijzondere categorieën en privacyadvies vóór verwerking van bijzondere categorieën PII. Addressed by clauses [4.2.3; 4.2.6; 9.1.3].
- 13.3.8 **Article 10** - Gemapt op het registreren van de autorisatiegrondslag voor gegevens over strafrechtelijke veroordelingen of strafbare feiten vóór verwerking. Addressed by clauses [4.2.3; 4.2.7; 9.1.3].
- 13.3.9 **Article 24** - Gemapt op governance, beoordeling, verantwoordingsplicht en managementtoezicht van de verwerkingsverantwoordelijke op verwerkingsinventaris en registraties van rechtsgrondslagen. Addressed by clauses [4.2.2; 5.1.1; 6.1.2; 10.1.6; 11.1.4].
- 13.3.10 **Article 26** - Gemapt op verwerkingsdoel van gezamenlijke verwerkingsverantwoordelijken en bewijsmateriaal voor verdeling van verantwoordelijkheden. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].
- 13.3.11 **Article 28** - Gemapt op instructies, overeenkomsten, relatiekoppelingen en onboardingbeheersmaatregelen voor verwerkers en subverwerkers. Addressed by clauses [4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 5.1.7; 7.1.7; 10.1.3; 10.1.5].

13.3.12 **Article 30** - Gemapt op registraties van verwerkingsactiviteiten van verwerkingsverantwoordelijken en verwerkers, waaronder verwerkingsdoeleinden, PII-categorieën, categorieën betrokkenen, ontvangers, overdrachten, bewaartermijnreferenties en registraties van klantinstructies. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.3.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.6; 7.1.2].

13.3.13 **Article 35** - Gemapt op koppeling met DPIA-screening voor nieuwe, wezenlijk gewijzigde of hoog-risico verwerkingsactiviteiten van de verwerkingsverantwoordelijke. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

#### **13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.3** - Gemapt op rechtmatigheid van doeleinden, doelspecificatie, koppeling met rechtsgrondslag en bewijsmateriaal voor doelverenigbaarheid. Addressed by clauses [4.2.1; 4.2.2; 4.2.8; 4.3.1; 4.3.3].

13.4.2 **Clause 5.4** - Gemapt op beperking van verzameling door PII-categorieën, categorieën betrokkenen, bronnen en rechtvaardiging te documenteren voordat verwerking begint. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.4.3 **Clause 5.5** - Gemapt op gegevensminimalisatie door veldvereisten voor de inventaris, documentatie van categorieën, documentatie van ontvangers en beoordeling van actuele verwerkingsregistraties. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.5.4; 8.1.6].

13.4.4 **Clause 5.6** - Gemapt op beperking van gebruik, bewaring, verstrekking en overdracht door gedocumenteerde doeleinden, categorieën ontvangers, bewaartermijnreferenties, overdrachtkoppeling en beheersmaatregelen voor doelwijziging. Addressed by clauses [4.2.1; 4.2.8; 4.4.2; 4.4.4; 4.4.5].

13.4.5 **Clause 5.10** - Gemapt op verantwoordingsplicht door eigenaarschap, governance van de inventaris, beoordeling, afstemming, auditssteekproeven, uitzonderingsafhandeling en bewijsmateriaal voor corrigerende maatregelen. Addressed by clauses [4.1.1; 4.1.3; 4.5.4; 4.5.5; 5.1.5; 6.1.1; 8.1.1; 10.1.1].

#### **13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Gemapt op PII-beschermingsmaatregelen voor rechtmatigheid van doeleinden, beperking van verzameling, gegevensminimalisatie en beperking van gebruik, bewaring en verstrekking. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.4; 4.4.6; 4.5.4; 8.1.6].

#### **13.6 ISO/IEC 29134:2020**

13.6.1 **Clause 5.1; Clause 6.2** - Gemapt op het gebruiken van wijzigingen in de verwerkingsinventaris om privacyrisicobeoordeling en DPIA-screening te triggeren voordat nieuwe of wezenlijk gewijzigde verwerking doorgaat. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].