					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII16					Documenttitel: **Beleid voor privacytraining, bewustwording en competentie**							
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 7.2; Clause 7.3	Both	Primary	Competentie en bewustwording
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Communicatie en gedocumenteerd bewijsmateriaal
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operationele beheersing, meting en verbetering
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Bewustwording, opleiding en training inzake verwerking van PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Verantwoordingsplicht, governance van verwerkers, beveiliging en DPO-taken
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Competentie, bewustwording en training
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Richtsnoeren voor bewustwording, opleiding en training
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informatiebeveiliging en naleving van privacyvereisten

1. Reikwijdte

1.1 Dit beleid definieert de eisen van de organisatie voor privacytraining, bewustwording en competentie binnen het privacy-informatiemanagementsysteem.

1.2 Dit beleid is van toepassing op personeel, contractanten, tijdelijke krachten, relevante derde partijen, verwerkers, subverwerkers en andere belanghebbenden van wie de werkzaamheden invloed kunnen hebben op de verwerking van PII, PIMS-prestaties, rechten van betrokkenen, privacyrisico, informatiebeveiliging met betrekking tot PII, instructies aan verwerkers, privacy-incidenten, gedocumenteerde informatie of nalevingsbewijsmateriaal.

1.3 Dit beleid is van toepassing in contexten van verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker.

1.4 Dit beleid omvat:

1.4.1 identificatie van trainingsdoelgroepen voor privacytraining;

1.4.2 onboardingtraining;

1.4.3 jaarlijkse opfriscursus;

1.4.4 rolgebaseerde en door gebeurtenissen getriggerde training;

1.4.5 bewijsmateriaal van voltooiing van training;

1.4.6 escalatie bij niet-voltooiing;

1.4.7 beoordeling van trainingseffectiviteit;

1.4.8 assurance-bewijsmateriaal inzake training voor verwerkers, subverwerkers en derde partijen.

1.5 Dit beleid creëert geen afzonderlijke trainingsmatrix, trainingsdashboard, HR-register, competentieregister, disciplinair register of klanttrainingsregister. Trainingstoewijzingen, voltooiingen, herinneringen, competentiebewijsmateriaal en bewustwordingsbewijsmateriaal worden vastgelegd in REG11, waarbij uitzonderingen, escalaties, non-conformiteiten, corrigerende maatregelen en beoordelingsbewijsmateriaal worden vastgelegd in REG12. Assurance-bewijsmateriaal inzake training voor verwerkers, subverwerkers en derde partijen wordt, waar relevant, vastgelegd in REG08.

1.6 Dit beleid dupliceert niet:

1.6.1 toewijzing van rolverantwoordelijkheid in PII02;

1.6.2 verwerkingsinventaris en eisen inzake rechtsgrondslag in PII03;

1.6.3 privacyrisico- en DPIA-methodologie in PII07;

1.6.4 privacy-by-design-gates in PII08;

1.6.5 governance van de levenscyclus van verwerkers in PII12;

1.6.6 werking van PII-beveiliging en toegangscontrole in PII14;

1.6.7 workflow voor incidenten met betrekking tot PII en inbreuken in PII15;

1.6.8 governance van gedocumenteerde informatie in PII17;

1.6.9 governance voor monitoring, interne audit en verbetering in PII18.

2. Doel

2.1 Het doel van dit beleid is te waarborgen dat personen van wie het werk invloed heeft op de verwerking van PII hun privacyverantwoordelijkheden begrijpen, passende training volgens een vastgestelde frequentie voltooien, rolrelevante competentie behouden en auditeerbaar bewijsmateriaal genereren van training, bewustwording en escalatie.

2.2 Dit beleid ondersteunt consistente implementatie van het PIMS door REG11 te gebruiken als primair bewijsobject voor training en bewustwording, en REG08, REG10 en REG12 als ondersteunende bewijsobjecten.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn om:

3.1.1 trainingsdoelgroepen voor privacytraining te definiëren;

3.1.2 eisen voor onboardingtraining te definiëren;

3.1.3 eisen voor jaarlijkse opfristraining te definiëren;

3.1.4 eisen voor rolgebaseerde privacytraining te definiëren;

3.1.5 bewijsmateriaal van voltooiing vast te leggen in REG11;

3.1.6 niet-voltooiing te escaleren via REG12;

3.1.7 assurance-bewijsmateriaal inzake training voor verwerkers, subverwerkers en derde partijen te onderhouden in REG08 waar relevant;

3.1.8 trainingseffectiviteit te beoordelen zonder buitensporige metrieken of dubbele registers te creëren;

3.1.9 te waarborgen dat trainingsinhoud afgestemd blijft op actuele PIMS-beleidslijnen en wezenlijke privacyverplichtingen.

4. Beleidsverklaringen

4.1 Trainingsdoelgroep en toewijzing

4.1.1 [All] Privacy Lead / PIMS Manager MOET vóór aanvang van elke jaarlijkse trainingscyclus de PIMS-trainingsdoelgroepcategorieën definiëren in REG11.

4.1.2 [All] Process Owner / Business Owner MOET vóór onboarding, roltoewijzing of een wezenlijke wijziging van taken in REG11 vaststellen welke personeelsleden taken hebben waarbij PII wordt verwerkt.

4.1.3 [Conditional] System Owner / Application Owner MOET vóórdat toegang wordt geactiveerd of wezenlijk wordt gewijzigd in REG11 gebruikers identificeren die PII-systeemtraining, training voor geprivilegieerde toegang of administratieve privacytraining nodig hebben.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager MOET vóórdat gezamenlijke verwerkingsactiviteiten beginnen of wezenlijk wijzigen de verdeling van trainingsverantwoordelijkheden voor gezamenlijke verwerkingsverantwoordelijken vastleggen in REG11 of REG08.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor MOET vóórdat training wordt toegewezen aan rollen die verwerking met een hoog risico, speciale categorieën PII, rechten van betrokkenen, DPIAs, internationale doorgiften of datalekbeoordeling behandelen, de behoefte aan verdiepende privacytraining vaststellen in REG11.

4.1.6 [All] Privacy Lead / PIMS Manager MOET vóór aanvang van elke jaarlijkse trainingscyclus de toegewezen trainingsdoelgroep, het trainingstype, de vereiste voltooiingsdatum en de eigenaar van het bewijsmateriaal vastleggen in REG11.

4.2 Onboarding en jaarlijkse trainingsfrequentie

4.2.1 [All] Privacy Lead / PIMS Manager MOET binnen 10 werkdagen na onboarding basistraining voor privacybewustwording toewijzen in REG11 voor personeel met toegang tot PII of PIMS-verantwoordelijkheden.

4.2.2 [All] Process Owner / Business Owner MOET waarborgen dat toegewezen personeel onboardingtraining inzake privacy voltooit in REG11 voordat toegang tot PII zonder toezicht wordt goedgekeurd of binnen 30 dagen na onboarding, afhankelijk van wat zich het eerst voordoet.

4.2.3 [All] Privacy Lead / PIMS Manager MOET ten minste eenmaal per 12 maanden jaarlijkse opfristraining inzake privacy toewijzen in REG11.

4.2.4 [All] Process Owner / Business Owner MOET uiterlijk op de gepubliceerde jaarlijkse vervaldatum de voltooiingsstatus van de jaarlijkse opfriscursus voor toegewezen personeel bevestigen in REG11.

4.2.5 [Conditional] Privacy Lead / PIMS Manager MOET binnen 30 dagen na een wezenlijke wijziging van privacybeleid, een wezenlijke wijziging van een PIMS-proces, een auditbevinding, herhaald falen bij training of een relevante les uit een PII-incident gerichte opfristraining toewijzen in REG11.

[... 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 [All] Process Owner / Business Owner MOET vóór verlenging van een vereiste voltooiingsdeadline een verzoek om een uitzondering op privacytraining vastleggen in REG12.

9.1.2 [All] Privacy Lead / PIMS Manager MOET verzoeken om uitzonderingen op privacytraining goedkeuren of afwijzen in REG12 voordat de uitzondering actief wordt.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MOET vóór goedkeuring adviseren over trainingsuitzonderingen in REG12 wanneer de uitzondering verwerking met een hoog risico, speciale categorieën PII, rechtenafhandeling, incidentafhandeling, internationale doorgiften of certificeringsbewijsmateriaal raakt.

9.1.4 [Conditional] Top Management MOET vóór activering privacytrainingsuitzonderingen goedkeuren in REG12 wanneer de uitzondering herhaalde niet-voltooiing, geprivilegieerde PII-toegang, PII-verwerking met hoge impact of bewijsmateriaal richting toezichthouders raakt.

9.1.5 [All] Privacy Lead / PIMS Manager MOET vóór goedkeuring van enige privacytrainingsuitzondering de eigenaar van de uitzondering, de vervaldatum, de compenserende actie en de beoordelingsdatum definiëren in REG12.

9.1.6 [All] Process Owner / Business Owner MOET goedgekeurde privacytrainingsuitzonderingen vóór de vervaldatum van de uitzondering afsluiten of verlengen in REG12.

10. Handhaving

10.1.1 [All] Privacy Lead / PIMS Manager MOET binnen vijf werkdagen een trainingsnon-conformiteit vastleggen in REG12 wanneer verplicht privacytrainingsbewijsmateriaal ontbreekt, onvolledig is, achterstallig is of niet herleidbaar is tot REG11.

10.1.2 [All] Process Owner / Business Owner MOET waarborgen dat achterstallige verplichte privacytraining binnen 10 werkdagen nadat de achterstallige status is vastgelegd wordt voltooid of geëscaleerd in REG11 of REG12.

10.1.3 [Conditional] System Owner / Application Owner MOET nieuwe PII-toegang met hoge impact beperken in REG12 wanneer vereiste onboarding- of rolgebaseerde privacytraining na escalatie onvoltooid blijft.

10.1.4 [Processor] Vendor / Procurement Owner MOET ontbrekend assurance-bewijsmateriaal inzake training voor verwerkers, subverwerkers of extern personeel binnen vijf werkdagen na identificatie escaleren in REG08 en REG12.

10.1.5 [Conditional] Incident Response Coordinator MOET trainingsgerelateerde handhavingsacties binnen één werkdag koppelen aan REG10 wanneer het trainingsfalen heeft bijgedragen aan een vermoedelijk of bevestigd PII-incident.

10.1.6 [All] Internal Audit / Compliance Reviewer MOET afsluitingsbewijsmateriaal voor corrigerende trainingsmaatregelen verifiëren in REG12 bij de eerstvolgende geplande audit of binnen 60 dagen na afsluiting, afhankelijk van wat zich het eerst voordoet.

11. Beoordeling en onderhoud

11.1.1 [All] Privacy Lead / PIMS Manager MOET dit beleid en de trainingsinhoud ten minste jaarlijks beoordelen en de beoordelingsuitkomst vastleggen in REG11 of REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MOET dit beleid binnen 30 dagen beoordelen na een wezenlijke wijziging van PIMS-reikwijdte, privacywetgeving, verwerkingsactiviteiten, rolmodel, incidentlessen, auditbevindingen of resultaten inzake trainingseffectiviteit.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor MOET privacy-significante beleidswijzigingen beoordelen in REG12 vóór goedkeuring.

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

11.1.5 [All] Privacy Lead / PIMS Manager MOET binnen 30 dagen na een goedgekeurde wezenlijke beleidswijziging de trainingsinhoud en het toewijzingsbewijsmateriaal in REG11 bijwerken.

12. Gerelateerde beleidslijnen

12.1 Dit beleid moet worden gelezen in samenhang met:

12.2 PII01 - Beleid voor het privacy-informatiemanagementsysteem;

12.3 PII02 - Beleid voor privacyrollen, verantwoordelijkheden en verantwoordingsplicht;

12.4 PII03 - Beleid voor PII-verwerkingsinventaris en rechtsgrondslag;

12.5 PII04 - Beleid voor privacyverklaring en transparantie;

12.6 PII05 - Beleid voor toestemmings- en voorkeurenbeheer;

12.7 PII06 - Beleid voor beheer van rechten van betrokkenen;

12.8 PII07 - Beleid voor privacyrisicobeoordeling en DPIA;

12.9 PII08 - Beleid voor privacy by design en privacy by default;

12.10 PII09 - Beleid voor verzameling, gebruik, verstrekking en delen van PII;

12.11 PII10 - Beleid voor bewaring, verwijdering en vernietiging van PII;

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

12.13 PII13 - Beleid voor internationale doorgifte van PII;

12.14 PII14 - Beleid voor PII-beveiliging en toegangscontrole;

12.15 PII15 - Beleid voor beheer van PII-incidenten en inbreuken;

12.16 PII17 - Beleid voor PIMS-gedocumenteerde informatie en bewijsmateriaalbeheer;

12.17 PII18 - Beleid voor PIMS-monitoring, audit en verbetering.

13. Referentienormen en -raamwerken

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].