					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII15-FS					Documenttitel: **Beleid voor incident- en inbreukbeheer rond persoonlijk identificeerbare informatie (PII) in de financiële sector**							
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 7.4; Clause 7.5	Both	Supporting	PIMS-communicatie en gedocumenteerd incidentbewijsmateriaal
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 maatregel en verbetering
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planning en voorbereiding van incidentbeheer voor verwerking van persoonlijk identificeerbare informatie (PII)
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Respons op informatiebeveiligingsincidenten waarbij persoonlijk identificeerbare informatie (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 verwerkersovereenkomst met de klant en klantverplichtingen
GDPR	Article 5(2); Article 24	Controller	Supporting	Verantwoordingsplicht en verantwoordelijkheid van de verwerkingsverantwoordelijke
GDPR	Article 26	Joint Controller	Supporting	Coördinatie van incidentverantwoordelijkheid 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 FG
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Proces voor beheer van ICT-gerelateerde incidenten voor financiële entiteiten binnen de reikwijdte
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Classificatiecriteria voor ICT-gerelateerde incidenten en significante cyberdreigingen
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Rapportage van ernstige ICT-gerelateerde incidenten en melding van significante cyberdreigingen
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Rapportage-inhoud, termijnen, sjablonen en procedures
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Rapportage van significante incidenten waar van toepassing
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Beginselen voor informatiebeveiliging en naleving van privacyvereisten
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Verantwoordelijkheden voor incidentrespons rond persoonlijk identificeerbare informatie (PII) en gebeurtenismelding
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 bewijsverzameling
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 voor melding door publieke-cloudverwerkers en registratie van inbreuken

1. Reikwijdte

1.1 Dit beleid definieert de vereisten voor het identificeren, melden, triëren, classificeren, beoordelen, indammen, melden aan externe partijen, documenteren, afsluiten en verbeteren naar aanleiding van incidenten met betrekking tot persoonsgegevens en inbreuken in verband met persoonsgegevens binnen PIMS-reikwijdten in de financiële sector.

1.2 **Implementatiekennisgeving:** Dit beleid is een vervangende variant voor de financiële sector voor PII15. Het mag niet gelijktijdig met PII15 worden geïmplementeerd voor dezelfde PIMS-reikwijdte, bedrijfseenheid, product, klantomgeving, gereguleerde dienst of bewijsgrens. Organisaties moeten voor dezelfde reikwijdte hetzij PII15 hetzij PII15-FS selecteren om dubbele verplichtingen voor incidentbeheer, dubbele registers en dubbel werk voor auditbewijsmateriaal te vermijden.

1.3 Dit beleid is van toepassing op:

1.3.1 de organisatie die optreedt als PII controller in een context van de financiële sector;

1.3.2 de organisatie die optreedt als gezamenlijke verwerkingsverantwoordelijke wanneer coördinatie van incident- of inbreukverantwoordelijkheid vereist is;

1.3.3 de organisatie die optreedt als PII processor voor klanten in de financiële sector;

1.3.4 de organisatie die optreedt als subverwerker voor klanten in de financiële sector of upstream verwerkers;

1.3.5 systemen, toepassingen, diensten, processen, leveranciers, verwerkers, subverwerkers en derde partijen die persoonlijk identificeerbare informatie (PII) verwerken, opslaan, verzenden, ondersteunen, raadplegen of anderszins beïnvloeden binnen de PIMS-reikwijdte voor de financiële sector.

1.4 Dit beleid gebruikt REG10 - Register voor PII-incidenten en inbreuken als primair bewijsobject voor incident- en inbreukbeheer rond persoonlijk identificeerbare informatie (PII) in de financiële sector.

1.5 Dit beleid gebruikt ondersteunende bewijsobjecten als volgt:

1.5.1 REG01 voor PIMS-reikwijdte en toepasselijke context van belanghebbenden, sector, klanten, contracten en rapportage.

1.5.2 REG02 voor getroffen verwerkingsactiviteiten, categorieën persoonlijk identificeerbare informatie (PII), categorieën betrokkenen, doeleinden, systemen en diensten.

1.5.3 REG03 voor Verklaring van Toepasselijkheid en updates van de toepasselijkheid van beheersmaatregelen, inclusief vervanging van PII15 door PII15-FS voor dezelfde reikwijdte.

1.5.4 REG04 voor privacyrisico, DPIA, resterend risico en koppeling met risicobehandeling.

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

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

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

1.5.8 REG12 voor bewijsmateriaal van audit, non-conformiteit, corrigerende maatregel, directiebeoordeling en verbetering.

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

1.6.1 PII03 regelt de verwerkingsinventaris en registraties van rechtsgronden.

1.6.2 PII04 regelt privacyverklaringen en transparantiebeheersmaatregelen buiten inbreukspecifieke communicatie.

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

1.6.4 PII07 regelt de methodologie voor privacyrisicobeoordeling en DPIA.

1.6.5 PII08 regelt privacy by design en privacy by default.

1.6.6 PII10 regelt beheersmaatregelen voor bewaring, verwijdering en vernietiging.

1.6.7 PII12 regelt beheersmaatregelen voor privacyrelaties met verwerkers, subverwerkers, leveranciers en derde partijen.

1.6.8 PII13 regelt mechanismen voor internationale doorgifte van persoonlijk identificeerbare informatie (PII) en registraties van doorgifterisico's.

1.6.9 PII14 regelt preventieve en detectieve beheersmaatregelen voor beveiliging en toegangscontrole van persoonlijk identificeerbare informatie (PII).

1.6.10 PII16 regelt privacytraining, bewustwording en competentie.

1.6.11 PII17 regelt gedocumenteerde informatie en bewijsbeheer.

1.6.12 PII18 regelt monitoring, interne audit, directiebeoordeling, non-conformiteit, corrigerende maatregel en voortdurende verbetering.

1.6.13 PII23 regelt beheersmaatregelen voor cloudverwerkers van persoonlijk identificeerbare informatie (PII) wanneer verplichtingen voor cloudverwerkers binnen de reikwijdte vallen.

1.7 Voor dit beleid geldt:

1.7.1 "Incident met betrekking tot persoonsgegevens" betekent een vermoedelijke of bevestigde gebeurtenis die de vertrouwelijkheid, integriteit, beschikbaarheid, rechtmatige verwerking of geautoriseerde behandeling van persoonlijk identificeerbare informatie (PII) heeft geraakt, mogelijk heeft geraakt of redelijkerwijs kan raken.

1.7.2 "Inbreuk in verband met persoonsgegevens" betekent een bevestigd incident met betrekking tot persoonsgegevens waarbij sprake is van ongeoorloofde, onrechtmatige, accidentele of onbedoelde vernietiging, verlies, wijziging, verstrekking van, toegang tot, onbeschikbaarheid van of compromittering van persoonlijk identificeerbare informatie (PII).

1.7.3 "Incident met betrekking tot persoonsgegevens in de financiële sector" betekent een incident met betrekking tot persoonsgegevens dat gereguleerde financiële diensten, klanten in de financiële sector, financiële tegenpartijen, financiële transacties, financiële operaties of verwerking van persoonlijk identificeerbare informatie (PII) in de financiële sector raakt, kan raken of daarmee redelijkerwijs verband houdt.

1.7.4 "Ernstig incident in de financiële sector" betekent een incident met betrekking tot persoonsgegevens in de financiële sector of een gerelateerd ICT-incident dat voldoet aan gedocumenteerde materialiteits- of rapportagecriteria in REG10.

1.7.5 "Significante cyberdreiging" betekent een in REG10 geregistreerde cyberdreiging die financiële diensten, verwerking van persoonlijk identificeerbare informatie (PII), klanten, tegenpartijen of operaties binnen de reikwijdte wezenlijk kan raken.

1.7.6 "Datalekbeoordeling" betekent de gedocumenteerde evaluatie of een incident met betrekking tot persoonsgegevens een inbreuk in verband met persoonsgegevens is, welke persoonlijk identificeerbare informatie (PII) en welke betrokkenen zijn getroffen, welke risico's kunnen ontstaan, welke meldingen of communicaties vereist zijn en welke herstelmaatregelen nodig zijn.

1.7.7 "Bewustwording" betekent het moment waarop de organisatie een redelijke mate van zekerheid heeft dat zich een beveiligings- of privacy-incident heeft voorgedaan en dat persoonlijk identificeerbare informatie (PII) is of mogelijk is gecompromitteerd.

1.7.8 "Incident met hoge impact met betrekking tot persoonsgegevens in de financiële sector" betekent een incident met betrekking tot persoonsgegevens waarbij sprake is van verwerking met een hoog risico, bijzondere categorieën of zeer gevoelige persoonlijk identificeerbare informatie (PII), grootschalige persoonlijk identificeerbare informatie (PII), kwetsbare personen, gereguleerde klanten, wezenlijke verstoring van dienstverlening, financiële tegenpartijen, financiële transacties, impact in meerdere jurisdicties, compromittering van geprivilegieerde toegang, publieke blootstelling, ransomware, onbeschikbaarheid van dienstverlening of significante operationele, klant-, financiële of reputatie-impact.

1.7.9 "Wezenlijke wijziging van een incident" betekent nieuwe of gewijzigde informatie die de incidentreikwijdte, ernst, categorieën persoonlijk identificeerbare informatie (PII), impact op betrokkenen, dienstimpact, classificatie voor de financiële sector, meldingsbesluit, klantimpact, oorzaak, indamming, herstel, corrigerende maatregel of externe rapportageverplichtingen beïnvloedt.

2. Doel

2.1 Het doel van dit beleid is te waarborgen dat incidenten met betrekking tot persoonsgegevens en inbreuken in verband met persoonsgegevens in contexten van de financiële sector consistent, tijdig, rechtmatig, veilig en met auditgereed bewijsmateriaal worden afgehandeld.

2.2 Dit beleid ondersteunt verantwoordingsplicht door te vereisen dat incidenten met betrekking tot persoonsgegevens en inbreuken in verband met persoonsgegevens in de financiële sector worden geregistreerd in REG10 en worden gekoppeld aan getroffen verwerkingsregistraties, privacyrisico's, verwerkers- en subverwerkersrelaties, doorgifteregistraties, corrigerende maatregelen, trainingsregistraties, rapportagebesluiten voor de financiële sector en bewijsmateriaal van directiebeoordeling wanneer deze worden geactiveerd.

2.3 Dit beleid waarborgt dat verplichtingen van verwerkingsverantwoordelijken, gezamenlijke verwerkingsverantwoordelijken, verwerkers en subverwerkers via afzonderlijke toepasselijkheidsregels worden afgehandeld, met behoud van één geïntegreerd bewijsmodel voor incidenten en inbreuken in de financiële sector.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn:

3.1.1 waarborgen dat vermoedelijke incidenten met betrekking tot persoonsgegevens in de financiële sector tijdig worden gemeld en geregistreerd;

3.1.2 waarborgen dat incidenten met betrekking tot persoonsgegevens in de financiële sector worden getrieerd en geclassificeerd aan de hand van consistente privacy-, beveiligings-, operationele en sectorale criteria;

3.1.3 waarborgen dat datalekbeoordelingen rekening houden met getroffen persoonlijk identificeerbare informatie (PII), betrokkenen, systemen, diensten, verwerkingsactiviteiten, verwerkers, subverwerkers, doorgiften, risico's, klanten, tegenpartijen en herstelmaatregelen;

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

3.1.5 waarborgen dat meldingen van inbreuken door verwerkers en subverwerkers aan klanten of upstream partijen zonder onredelijke vertraging en overeenkomstig toepasselijke overeenkomsten worden gedaan;

3.1.6 waarborgen dat rapportagetriggers voor de financiële sector waar van toepassing worden beoordeeld, gedocumenteerd en gevolgd;

3.1.7 waarborgen dat bewijsmateriaal tijdens incidentafhandeling wordt bewaard en beschermd;

3.1.8 waarborgen dat indamming, uitroeiing, herstel en validatie via REG10 worden gevolgd;

3.1.9 waarborgen dat significante cyberdreigingen en ernstige incidenten in de financiële sector naar passende besluitvormings- en rapportageworkflows worden geleid;

3.1.10 waarborgen dat geleerde lessen uit incidenten leiden tot corrigerende maatregelen, training, verbetering van beheersmaatregelen en directiebeoordeling;

3.1.11 waarborgen dat incident- en inbreukregistraties beschikbaar zijn voor audit, directiebeoordeling, klantassurance en beoordeling door toezichthouders waar van toepassing;

3.1.12 waarborgen dat PII15-FS PII15 voor dezelfde reikwijdte in de financiële sector vervangt en geen dubbel bewijswerk voor PII15 veroorzaakt.

4. Beleidsverklaringen

4.1 Activering van variant, gereedheid en intake

4.1.1 [Conditional] The Privacy Lead / PIMS Manager MUST de activering van PII15-FS in REG01 en REG03 documenteren voordat dit beleid voor een PIMS-reikwijdte in de financiële sector wordt gebruikt.

4.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST in REG03 en REG12 documenteren dat PII15 niet gelijktijdig voor dezelfde PIMS-reikwijdte in de financiële sector is geïmplementeerd voordat PII15-FS wordt goedgekeurd.

4.1.3 [All] The Incident Response Coordinator MUST elk gemeld of gedetecteerd vermoedelijk incident met betrekking tot persoonsgegevens in de financiële sector in REG10 registreren binnen één werkdag na ontvangst, of eerder wanneer een toepasselijke meldings-, klant- of rapportagetermijn kan worden geactiveerd.

4.1.4 [Conditional] The Privacy Lead / PIMS Manager MUST criteria voor afhandeling van incidenten met betrekking tot persoonsgegevens en inbreuken in verband met persoonsgegevens in de financiële sector in REG10 onderhouden, ten minste jaarlijks en na elke wezenlijke wijziging van de PIMS-reikwijdte, juridische context, klantverplichtingen, contractuele verplichtingen, sectorale rapportagecontext of verwerking met hoog risico.

4.1.5 [Both] The Information Security Lead MUST vereisten voor bewaring van incidentbewijsmateriaal in REG10 bevestigen binnen 24 uur nadat een vermoedelijk incident een systeem, dienst of toepassing raakt die persoonlijk identificeerbare informatie (PII) verwerkt.

4.1.6 [Conditional] The Vendor / Procurement Owner MUST vereisten voor incidentcontacten en bewijsroutering van derde partijen in de financiële sector in REG08 onderhouden vóór onboarding en ten minste jaarlijks voor verwerkers, subverwerkers, leveranciers en uitbestede rapportageaanbieders binnen de reikwijdte.

4.2 Classificatie en datalekbeoordeling

4.2.1 [All] The Incident Response Coordinator MUST elke REG10-registratie binnen 24 uur na intake classificeren als niet-PII-gebeurtenis, vermoedelijk incident met betrekking tot persoonsgegevens, bevestigd incident met betrekking tot persoonsgegevens, bevestigde inbreuk in verband met persoonsgegevens, incident met betrekking tot persoonsgegevens in de financiële sector, ernstig incident in de financiële sector, significante cyberdreiging of registratie in afwachting van classificatie.

4.2.2 [Conditional] The Information Security Lead MUST getroffen diensten, cliënten, tegenpartijen, transacties, dienstuitval, geografische spreiding, gegevensverlies, dienstkritikaliteit en economische impact in REG10 beoordelen wanneer een incident met betrekking tot persoonsgegevens financiële diensten of operaties kan raken.

4.2.3 [Both] The Privacy Lead / PIMS Manager MUST de getroffen verwerkingsactiviteit, categorieën persoonlijk identificeerbare informatie (PII), categorieën betrokkenen, systemen, verwerkers, subverwerkers, doorgiftelocaties en privacyrisico's in REG02, REG04, REG08, REG09 en REG10 identificeren voordat het besluit over melding van de inbreuk wordt afgerond.

4.2.4 [Controller] The Data Protection Officer / Privacy Advisor MUST het risico voor getroffen betrokkenen beoordelen voor elke bevestigde of redelijkerwijs vermoede inbreuk in verband met persoonsgegevens en de meldingsaanbeveling, risicomotivering en het advies in REG10 vastleggen voordat het externe meldingsbesluit wordt genomen.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST de verdeling van incidentverantwoordelijkheid tussen gezamenlijke verwerkingsverantwoordelijken in REG08 en REG10 registreren binnen 24 uur na identificatie van gedeelde verantwoordelijkheid voor een vermoedelijke of bevestigde inbreuk in verband met persoonsgegevens.

4.2.6 [Processor] The Privacy Lead / PIMS Manager MUST klantinstructies, contractuele meldingsverplichtingen en samenwerkingsverplichtingen in REG08 en REG10 beoordelen binnen 24 uur nadat een vermoedelijke of bevestigde inbreuk in verband met persoonsgegevens verwerking raakt die als verwerker wordt uitgevoerd.

4.2.7 [Subprocessor] The Vendor / Procurement Owner MUST de upstream meldingsketen en vereiste bewijsroutering in REG08 en REG10 identificeren binnen 24 uur nadat een vermoedelijk of bevestigd incident met betrekking tot persoonsgegevens verwerking raakt die als subverwerker wordt uitgevoerd.

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

9.1.2 [Conditional] Top Management MUST elke uitzondering goedkeuren die wezenlijke gevolgen heeft voor timing van inbreukmelding, timing van rapportage in de financiële sector, publieke communicatie, klanttoezeggingen, 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 melding, elk besluit tot niet-melden, elke rapportage-uitzondering of elke uitzonderlijke communicatieaanpak vóór incidentafsluiting, waarbij advies in REG10 wordt bewaard.

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

9.1.5 [All] The Privacy Lead / PIMS Manager MUST openstaande uitzonderingen op dit beleid ten minste maandelijks beoordelen tot afsluiting, waarbij de beoordelingsstatus in REG12 wordt bewaard.

10. Handhaving

10.1.1 [All] The Process Owner / Business Owner MUST het niet melden van een vermoedelijk incident met betrekking tot persoonsgegevens in de financiële sector, het niet bewaren van bewijsmateriaal, het niet opvolgen van toegewezen acties of het niet meewerken aan

datalekbeoordeling escaleren naar de Privacy Lead / PIMS Manager binnen twee werkdagen na ontdekking, waarbij bewijsmateriaal in REG12 wordt bewaard.

10.1.2 [Both] The Incident Response Coordinator MUST late melding, gemiste classificatie, ontbrekend bewijsmateriaal, gemiste escalatie of achterstallige indammingsactie escaleren naar de Privacy Lead / PIMS Manager binnen één werkdag na identificatie van de kwestie, waarbij bewijsmateriaal in REG10 en REG12 wordt bewaard.

10.1.3 [Both] The Privacy Lead / PIMS Manager MUST een REG12-non-conformiteit registreren wanneer een schending van dit beleid incidentintake, triage, indamming, melding, rapportage, bewijsintegriteit, communicatie of corrigerende maatregelen raakt.

10.1.4 [Both] The Vendor / Procurement Owner MUST remediatie door leveranciers, verwerkers, subverwerkers of uitbestede aanbieders initiëren via REG08 en REG12 binnen vijf werkdagen wanneer een derde partij overeengekomen verplichtingen voor incidenten, inbreuken, bewijsmateriaal of rapportage niet nakomt.

10.1.5 [Conditional] Top Management MUST wezenlijke of terugkerende PII15-FS-non-conformiteiten beoordelen tijdens de eerstvolgende geplande directiebeoordeling, waarbij besluiten en vereiste acties in REG12 worden bewaard.

10.1.6 [All] The Privacy Lead / PIMS Manager MUST hersteltraining in REG11 activeren binnen 30 kalenderdagen wanneer een beleidsnon-conformiteit betrekking heeft op rolbewustzijn, late melding, escalatiefalen, falen bij bewijsbehandeling of communicatiefalen.

11. Beoordeling en onderhoud

11.1.1 [Conditional] 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 [Conditional] The Incident Response Coordinator MUST een post-incidentbeoordeling van dit beleid activeren binnen 30 kalenderdagen na afsluiting van elk incident met hoge impact met betrekking tot persoonsgegevens in de financiële sector, elke bevestigde inbreuk in verband met persoonsgegevens, elk ernstig incident in de financiële sector of elke significante cyberdreiging, waarbij beoordelingsbewijsmateriaal in REG10 en REG12 wordt bewaard.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUST dit beleid beoordelen binnen 30 kalenderdagen nadat kennis is genomen van een wezenlijke wijziging in juridische, sectorale, klant-, contractuele, verwerkers-, subverwerkers-, rapportagesjabloon-, rapportagetermijn- of doorgiftegerelateerde vereisten voor incidentrapportage, 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 [Conditional] Top Management MUST incidenttrends, significante inbreuken, rapportageprestaties, achterstallige corrigerende maatregelen en beleidseffectiviteit beoordelen tijdens geplande directiebeoordeling, waarbij outputs in REG12 worden bewaard.

11.1.6 [Conditional] The Privacy Lead / PIMS Manager MUST de vervangingsrelatie tussen PII15-FS en PII15 ten minste jaarlijks en na elke wijziging in PIMS-afbakening beoordelen om te verifiëren dat beide beleidslijnen niet voor dezelfde reikwijdte in de financiële sector zijn geïmplementeerd, waarbij beoordelingsbewijsmateriaal in REG03 en REG12 wordt bewaard.

12. Gerelateerde beleidslijnen

12.1 Dit beleid moet worden gelezen in samenhang met:

12.1.1 PII01 - Beleid voor privacy-informatiemanagementsysteem

12.1.2 PII02 - Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht

12.1.3 PII03 - Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag

12.1.4 PII04 - Beleid inzake privacyverklaring en transparantie

12.1.5 PII06 - Beleid inzake beheer van rechten van betrokkenen

12.1.6 PII07 - Beleid inzake privacyrisicobeoordeling en DPIA

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

12.1.8 PII10 - Beleid inzake bewaring, verwijdering en vernietiging van persoonlijk identificeerbare informatie (PII)

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

12.1.10 PII13 - Beleid inzake internationale doorgifte van persoonlijk identificeerbare informatie (PII)

12.1.11 PII14 - Beleid inzake beveiliging en toegangscontrole van persoonlijk identificeerbare informatie (PII)

12.1.12 PII16 - Beleid inzake privacytraining, bewustwording en competentie

12.1.13 PII17 - Beleid inzake PIMS-gedocumenteerde informatie en bewijsbeheer

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

12.1.15 PII23 - Beleid voor cloudverwerkers van persoonlijk identificeerbare informatie (PII), wanneer verplichtingen voor cloudverwerkers in de financiële sector binnen de reikwijdte vallen

12.2 PII15 - Beleid voor incident- en inbreukbeheer rond persoonlijk identificeerbare informatie (PII) is het basisbeleid voor incidenten en inbreuken. PII15-FS is een vervangende variant voor de financiële sector voor PII15. PII15 en PII15-FS mogen niet gelijktijdig worden geïmplementeerd voor dezelfde PIMS-reikwijdte, bedrijfseenheid, product, klantomgeving, gereguleerde dienst of bewijsgrens.

13. Referentienormen en -raamwerken

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 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; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 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 [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].