					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P17					Documenttitel: **Beleid inzake gegevensbescherming en privacy**							
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/artikel	Opmerking
ISO/IEC 27001:2022	Clausules 5.1, 6.1.3, 8.1, 10	Relevante algemene en technische beheersmaatregelen, inclusief maatregelen gericht op continue verbetering en gegevensbescherming
ISO/IEC 27002:2022	Beheersmaatregelen 5.34, 8.10, 8.11, 8.12	Beheersmaatregelen voor de verwerking van PII, bewaring, verwijdering, anonimisering en rechten van betrokkenen
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Vereisten voor governance, risico's, toegangsbeheer, logging, respons op inbreuken en het privacyprogramma
AVG (EU GDPR)	Artikelen 5, 6, 12–23, 25, 28, 30, 32–34; overweging 78	Alle kernvereisten inzake privacy, verantwoordingsplicht, rechten van betrokkenen, verzoeken van betrokkenen, inbreuken en gegevensbescherming door ontwerp en standaardinstellingen
EU NIS2	Artikel 21(2)(e), (f)	Risicogebaseerde beveiligingsmaatregelen voor essentiële en belangrijke entiteiten
EU DORA	Artikelen 6(2)(d), 11(1)(c), 15(1), 17	Governance, risico's van derde partijen en termijnen voor veilige verwerking
COBIT 2019	APO12, DSS01, DSS05, MEA	Risicobeheer, veilige bedrijfsvoering en toezicht op naleving

1. Doel

1.1 Dit beleid stelt verplichte organisatorische uitgangspunten en technische vereisten vast voor de bescherming van persoonsgegevens en de borging van privacy by design in alle omgevingen.

1.2 Het formaliseert de verantwoordelijkheden van de organisatie onder internationale normen en regelgevende kaders, zodat persoonsgegevens rechtmatig, veilig en transparant worden verzameld, verwerkt, bewaard, gedeeld en verwijderd.

1.3 Dit beleid versterkt tevens de naleving van toepasselijke privacywetgeving en normenkaders, waaronder de Algemene Verordening Gegevensbescherming (AVG), de EU-richtlijn NIS2, de EU Digital Operational Resilience Act (DORA), ISO/IEC 27001:2022 en COBIT 2019.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle organisatie-eenheden, alle medewerkers en alle systemen die betrokken zijn bij de verwerking van persoonsgegevens, waaronder:

2.1.1 Werknemers, contractanten, consultants en externe dienstverleners.

2.1.2 Gegevens die uit interne en externe bronnen worden verzameld binnen alle bedrijfsfuncties.

2.1.3 Fysieke en digitale media, waaronder clouddiensten, SaaS-platforms, mobiele apparaten en papieren registraties.

2.1.4 Alle omgevingen, waaronder productie-, ontwikkel-, test- en back-upsystemen waarin persoonsgegevens kunnen voorkomen.

2.2 Het beleid omvat alle verwerkingsactiviteiten die onder toepasselijke privacywetgeving en normen vallen, met inbegrip van, maar niet beperkt tot:

2.2.1 Het verzamelen, opslaan, gebruiken, verzenden en verwijderen van persoonsgegevens.

2.2.2 De uitoefening van rechten van betrokkenen, documentatie van de rechtsgrond en beheer van toestemming.

2.2.3 Grensoverschrijdende doorgiften, melding van inbreuken en het delen van gegevens met derden.

2.2.4 Veilige inrichting en handhaving van gegevensbescherming door standaardinstellingen in systemen en processen.

3. Doelstellingen

3.1 Waarborgen van een rechtmatige, transparante en aantoonbaar verantwoorde verwerking van persoonsgegevens in overeenstemming met ISO/IEC 27001:2022 en gerelateerde wettelijke verplichtingen.

3.2 Verankeren van de beginselen van privacy by design en privacy by default in alle informatiesystemen, diensten en bedrijfsprocessen.

3.3 Afdwingen van technische en organisatorische maatregelen (TOM's) die de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens gedurende de gehele levenscyclus waarborgen.

3.4 Vastleggen van governancerollen en verantwoordingsstructuren voor gegevensbescherming, waaronder de verantwoordelijkheden van de Functionaris voor Gegevensbescherming (FG), Informatiebeveiliging, Juridische Zaken en informatie-eigenaren.

3.5 Mogelijk maken van volledige naleving van de artikelen 5, 6, 25, 30 en 32 van de AVG, evenals van de vereisten inzake risicobeheersing en weerbaarheid onder NIS2 en DORA.

3.6 Waarborgen van de rechten van betrokkenen, waaronder inzage, rectificatie, wissing, beperking, overdraagbaarheid, bezwaar en bescherming tegen geautomatiseerde besluitvorming.

3.7 Beperken van regelgevende, reputatie-, juridische en operationele risico's die voortvloeien uit ongeautoriseerde toegang tot, misbruik van of verlies van persoonsgegevens.

4. Rollen en verantwoordelijkheden

4.1 Topmanagement

4.1.1 Biedt strategisch toezicht en wijst voldoende middelen toe ter ondersteuning van het privacyprogramma.

4.1.2 Keurt dit beleid goed en ziet toe op de handhaving ervan binnen de organisatie.

4.2 Functionaris voor Gegevensbescherming (FG)

4.2.1 Handelt onafhankelijk om toezicht te houden op de naleving van regelgeving inzake gegevensbescherming.

4.2.2 Beheert het register van verwerkingsactiviteiten (RoPA) overeenkomstig artikel 30 van de AVG.

4.2.3 Onderhoudt het contact met toezichthouders, voert gegevensbeschermingseffectbeoordelingen (DPIA's) uit en beheert processen voor meldingen van inbreuken.

4.2.4 Beoordeelt privacy-uitzonderingen en beheert het register van privacy-uitzonderingen.

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

9. Eisen voor herziening en actualisering

9.1 Dit beleid moet ten minste jaarlijks worden herzien of eerder onder de volgende omstandigheden:

9.1.1 Significante wettelijke of regelgevende actualisaties, zoals wijzigingen in de AVG of DORA-termijnen

9.1.2 Nieuwe systemen of verwerkingsactiviteiten waarbij persoonsgegevens betrokken zijn

9.1.3 Interne auditbevindingen die wijzen op hiaten in het beleid

9.1.4 Materiële inbreukincidenten of feedback van toezichthoudende autoriteiten

9.2 Verantwoordelijkheden voor herziening

9.2.1 De FG initieert de beleidsherziening en stemt af met Juridische Zaken, Risico, Informatiebeveiliging en het topmanagement.

9.2.2 Alle actualisaties moeten worden geregistreerd in het ISMS-register voor documentbeheer en worden verspreid onder de betrokken stakeholders.

9.3 Wijzigingsbeheer

9.3.1 Elke herziening van dit beleid moet formeel worden goedgekeurd door het topmanagement.

9.3.2 Verouderde versies moeten veilig worden gearchiveerd en de bijgewerkte versie moet een gedocumenteerde wijzigingshistorie bevatten.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 P1 – Informatiebeveiligingsbeleid. Stelt de overkoepelende uitgangspunten van informatiebeveiligingsgovernance vast die aan dit privacybeleid ten grondslag liggen. P1 ondersteunt de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens in alle systemen en diensten.

10.2 P6 – Beleid inzake risicobeheer. Definieert de methodologie van de organisatie voor risicobehandeling, die essentieel is voor de beoordeling van privacyrisico's, DPIA-processen en beoordelingen van restrisico die vereist zijn onder de AVG en ISO/IEC 27001 clausule 6.1.3.

10.3 P13 – Beleid inzake gegevensclassificatie en etikettering. Geeft richting aan de categorisering van persoonsgegevens en gevoelige gegevens en vormt de basis voor de toepassing van passende privacymaatregelen, waaronder handhaving van bewaartermijnen, beperking van toegang en veilige verwijdering.

10.4 P14 – Gegevensbewarings- en verwijderingsbeleid. Ondersteunt rechtstreeks de privacyvereisten uit de artikelen 5(1)(e) en 17 van de AVG door te waarborgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk en veilig worden verwijderd in overeenstemming met wettelijke verplichtingen.

10.5 P16 – Beleid inzake datamasking en pseudonimisering. Stelt beheersmaatregelen vast om de identificeerbaarheid van persoonsgegevens te verminderen door middel van technische maatregelen zoals tokenisatie, dynamische masking en pseudonimisering, en geeft daarmee uitvoering aan artikel 32 van de AVG en beheersmaatregel 5.34 van ISO/IEC 27002.

10.6 P30 – Incidentresponsbeleid (P30). Beschrijft de verplichte protocollen voor respons op inbreuken die aansluiten op de afhandeling van privacy-inbreuken en de meldtermijnen die zijn vereist onder de artikelen 33 en 34 van de AVG.

10.7 P33 – Beleid inzake audit- en nalevingsmonitoring. Borgt geplande beoordelingen van de doeltreffendheid van het privacyprogramma, handhaving van beleid en opvolging van corrigerende maatregelen binnen organisatie-eenheden en bij verwerkers van derde partijen.

11. Referentienormen en -kaders

11.1 ISO/IEC 27001

11.1.1 Clausule 5.1 – Leiderschap en betrokkenheid: Legt verantwoordelijkheid op directieniveau vast voor de bescherming van persoonsgegevens en de handhaving van privacybeginselen.

11.1.2 Clausule 6.1.3 – Behandeling van informatiebeveiligingsrisico's: Ondersteunt de identificatie, beoordeling en behandeling van privacyrisico's via DPIA's en uitzonderingen.

11.1.3 Clausule 8.1 – Operationele planning en beheersing: Vereist technische en procedurele maatregelen om te waarborgen dat persoonsgegevens veilig worden verwerkt.

11.1.4 Clausule 10.1 – Continue verbetering: Verplicht periodieke evaluatie en aanpassing van het privacyprogramma.

11.2 ISO/IEC 27002:2022 Beheersmaatregelen 5.34, 8.10, 8.11, 8.12: Biedt richtlijnen voor de verwerking van PII, handhaving van bewaring, verwijdering, anonimisering en transparantie ten aanzien van rechten van betrokkenen.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: Definiëren governance, rollen, verantwoordingsplicht en verantwoordelijkheden voor privacytraining.

11.3.2 PL-2, PL-8: Vereisen integratie van privacymaatregelen in de systeemlevenscyclus en de enterprise-architectuur.

11.3.3 AC-2, AC-6: Dwingen het need-to-know-principe, het principe van minimale bevoegdheden en accountbeheer af ter bescherming van persoonsgegevens.

11.3.4 AU-2, AU-6, AU-9: Verplichten logging, traceerbaarheid en auditintegriteit voor toegang tot persoonsgegevens.

11.3.5 IR-4, IR-5, IR-6: Definiëren gestructureerde processen voor detectie, analyse en melding van privacy-inbreuken.

11.3.6 PM-1, PM-21, PM-23: Stellen een alomvattend privacyprogramma vast, afgestemd op strategische doelstellingen voor risico- en datagovernance.

11.4 AVG (EU 2016/679)

11.4.1 Artikelen 5, 6, 12–23, 25, 28, 30, 32–34: Regelen rechtmatige verwerking, doelbinding, rechten van betrokkenen, verantwoordingsplicht, gegevensbescherming door ontwerp en standaardinstellingen, verplichtingen van derden en beheer van inbreuken.

11.4.2 Overweging 78: Versterkt de beginselen van privacy by design.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(e) en (f): Vereist implementatie van risicogebaseerde beveiligingsmaatregelen en bescherming van persoonsgegevens binnen de reikwijdte van essentiële en belangrijke entiteiten.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 6(2)(d): Verplicht interne governance voor ICT-risico's met betrekking tot gegevensverwerking.

11.6.2 Artikel 11(1)(c): Verplicht toezicht op risico's van derde partijen voor gegevensgerelateerde diensten.

11.6.3 Artikelen 15(1) en 17: Vereisen veilige gegevensverwerking door dienstverleners en tijdige meldingen aan toezichthouders na ICT-gerelateerde incidenten.

11.7 COBIT 2019

11.7.1 APO12 – Risicobeheer: Verankert privacyrisico's in het bredere ondernemingsbrede risicotoezicht.

11.7.2 DSS01 – Beheerde operaties en DSS05 – Beveiligingsdiensten: Borgen veilige bedrijfsvoering, waaronder toegangsbeheersing, bewaring en systeemintegriteit.

11.7.3 MEA03 – Nalevingsmonitoring: Vereist doorlopende beoordeling van de nalevingsstatus ten opzichte van regelgevende en beleidsmatige privacyverplichtingen.