					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P16					Documenttitel: **Beleid inzake gegevensmaskering en pseudonimisering**							
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**

Afstemming op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 6.1	Algemene vereisten voor risicobeheer en operationele beheersmaatregelen voor maskering en pseudonimisering
ISO/IEC 27002:2022	Beheersmaatregelen 8.11, 8	Richtlijnen voor beheersmaatregelen voor de implementatie van maskering en pseudonimisering
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Privacy- en vertrouwelijkheidsmaatregelen voor gegevensminimalisatie, transformatie en toegangsbeperking
AVG	Artikelen 4(5), 5(1)(c,f), 32	Rechtsgrondslag en vereisten voor pseudonimisering en gegevensbeschermingsmaatregelen
NIS2	Artikel 21(2)(c)	Verplichting tot technische en organisatorische maatregelen, waaronder privacyverhogende technologieën (PET's)
DORA	Artikelen 10(1), 10(2)(e)	ICT-risicobeheer en vertrouwelijkheidsmaatregelen voor gegevensmaskering en pseudonimisering
COBIT 2019	DSS05.01, DSS06.06, MEA	Governancebeheersmaatregelen voor gegevensbescherming door middel van maskering en nalevingsbeoordeling

1. Doel

1.1 Dit beleid definieert de aanpak van de organisatie voor de implementatie van gegevensmaskering en pseudonimisering als privacyverhogende technologieën (PET's) om de identificeerbaarheid en blootstelling van persoonsgegevens of gevoelige gegevens te beperken.

1.2 Dit beleid ondersteunt het veilige gebruik van informatie in test-, analyse- en productieomgevingen, waarborgt naleving van wettelijke en regelgevende vereisten, beperkt de impact van een datalek en handhaaft de beginselen van gegevensminimalisatie en vertrouwelijkheid.

1.3 Dit beleid is afgestemd op ISO/IEC 27001:2022, ondersteunt artikel 4(5) van de AVG inzake pseudonimisering en integreert een risicogebaseerde implementatie in lijn met NIST-, NIS2-, DORA- en COBIT 2019-normen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle medewerkers, contractanten, derden en leveranciers met toegang tot systemen die persoonsgegevens, vertrouwelijke informatie of gevoelige informatie verwerken.

2.1.2 alle gegevensomgevingen, waaronder productie-, ontwikkel-, test- en acceptatieomgevingen.

2.1.3 alle vormen van gegevensmaskering (bijvoorbeeld statisch, dynamisch, deterministisch, tokenisatie) en pseudonimiseringstechnieken die worden gebruikt om privacyrisico's te beperken.

2.1.4 alle gegevenstypen (gestructureerd of ongestructureerd), systemen (on-premises of in de cloud) en applicaties waarbij persoonsgegevens of gereguleerde gegevens betrokken zijn.

2.2 De reikwijdte omvat gebruik in:

2.2.1 applicatieontwikkel- en QA-/testomgevingen

2.2.2 analyse- of rapportageplatforms

2.2.3 gegevensuitwisseling met derden of dienstverleners

2.2.4 back-up-, archiverings- of herstelomgevingen

3. Doelstellingen

3.1 Zorgen voor een consistente en doeltreffende toepassing van maskering en pseudonimisering om risico's van gegevensblootstelling of misbruik te beperken.

3.2 Waarborgen dat echte gegevens nooit worden gebruikt in niet-productieomgevingen, tenzij deze via goedgekeurde PET-technieken zijn getransformeerd.

3.3 Waar nodig de referentiële integriteit, bruikbaarheid en formaatbehoudende transformaties handhaven ten behoeve van operationele consistentie.

3.4 Strikte toegangsbeheersing afdwingen voor brongegevens, gemaskeerde gegevens en sleutels voor heridentificatie.

3.5 Gemaskeerde of gepseudonimiseerde datasets behandelen als gevoelige gegevens en onderwerpen aan toegangslogging, bewaarbeheersmaatregelen en incidentresponsprocedures.

3.6 De doeltreffendheid van deze beheersmaatregelen valideren door middel van doorlopende tests, monitoring en audits.

4. Rollen en verantwoordelijkheden

4.1 Directie

4.1.1 Keurt dit beleid goed en ziet toe op de handhaving ervan als onderdeel van bredere IT-governance- en gegevensbeschermingsinitiatieven.

4.2 Chief Information Security Officer (CISO) / ISMS-manager

4.2.1 Houdt toezicht op de implementatie en de doorlopende naleving.

4.2.2 Borgt de afstemming op clausule 6.1.3 van ISO/IEC 27001 (risicobehandeling) en clausule 8.1 (operationele beheersing).

4.2.3 Beoordeelt auditlogs en valideert de doeltreffendheid van beheersmaatregelen.

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

9. Vereisten voor herziening en actualisatie

9.1 Dit beleid moet ten minste jaarlijks worden herzien, of eerder in geval van:

9.1.1 wijzigingen in wet- en regelgeving die maskering of pseudonimisering raken

9.1.2 invoering van nieuwe IT-systemen die gevoelige gegevens verwerken

9.1.3 materiële wijzigingen in het gegevensclassificatiemodel van de organisatie

9.1.4 auditbevindingen die tekortkomingen in de beheersmaatregelen aantonen

9.1.5 opkomst van nieuwe dreigingen of technologieën voor maskering

9.2 De ISMS-manager leidt de herziening in overleg met de FG, gegevenseigenaren, IT-beveiliging en Juridische Zaken. Actualisaties moeten onder versiebeheer worden uitgevoerd, door de directie worden goedgekeurd en aan alle relevante belanghebbenden worden gecommuniceerd.

10. Gerelateerde beleidslijnen en samenhang

10.1 P13 - Beleid inzake gegevensclassificatie en etikettering. Besluiten over maskering en pseudonimisering zijn rechtstreeks afhankelijk van de classificatie van gegevensvelden en gevoeligheidsniveaus zoals vastgelegd in P13.

10.2 P14 - Gegevensbewaringsbeleid. Getransformeerde datasets moeten worden bewaard en verwijderd overeenkomstig de levenscyclusregels in P14, waarbij wordt gewaarborgd dat gemaskeerde en gepseudonimiseerde gegevens als gevoelig worden behandeld.

10.3 P17 - Beleid inzake gegevensbescherming en privacy. Biedt privacybeginselen en wettelijke grondslagen voor de toepassing van pseudonimisering als nalevingsconforme verwerkingsactiviteit onder de AVG en vergelijkbare wetgeving.

10.4 P22 - Logging- en monitoringbeleid. Maakt gecentraliseerde auditing en waarschuwingen mogelijk van gebeurtenissen rond maskering en pseudonimisering in overeenstemming met gestructureerde protocollen voor beveiligingsmonitoring.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 6.1.3 - Risicobehandelingsplan: stelt maskering en pseudonimisering vast als mechanismen voor risicobehandeling om de identificeerbaarheid van gevoelige gegevens in niet-essentiële verwerkingsomgevingen te beperken.

11.1.2 Clausule 8.1 - Operationele planning en beheersing: vereist technische en procedurele beheersmaatregelen voor veilige gegevenstransformatie tijdens verwerking, opslag of overdracht.

11.2 ISO/IEC 27002:2022

11.2.1 Beheersmaatregelen 8.11, 8: richtlijnen voor gegevensmaskering en pseudonimisering om risico's op heridentificatie en datalekken te minimaliseren.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Bescherming van PII: implementatie van privacyverhogende technologieën zoals maskering en pseudonimisering.

11.3.2 PT-2, PT-3: minimalisatie en beveiliging van PII-verwerking - transformatie om identificeerbaarheid te beperken en toegangsbeheersing af te dwingen.

11.3.3 SC-12, SC-28, SC-30: vertrouwelijkheid en integriteit van gegevens - vertrouwelijkheids- en afschermingsmaatregelen voor opslag, transmissie en gebruik.

11.4 AVG (2016/679)

11.4.1 Artikel 4(5): formele definitie van pseudonimisering.

11.4.2 Artikel 32: beveiliging van de verwerking - organisatorische en technische maatregelen voor pseudonimisering.

11.4.3 Artikel 5(1)(c,f): gegevensminimalisatie en vertrouwelijkheid door het gebruik van pseudonimisering/maskering.

11.5 NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(c): vereist PET's zoals maskering en pseudonimisering als beveiligingsmaatregelen.

11.6 DORA (2022/2554)

11.6.1 Artikel 10(1): het ICT-risicobeheerkader omvat beheersmaatregelen voor maskering en pseudonimisering.

11.6.2 Artikel 10(2)(e): vereist het gebruik van transformatietechnologieën ter bescherming van persoonsgegevens en financiële gegevens.

11.7 COBIT 2019

11.7.1 DSS05.01: Bescherm informatieactiva - vereisten voor maskering en pseudonimisering.

11.7.2 DSS06.06: Veilig testen en analyseren - maskering in omgevingen buiten productie.
11.7.3 MEA03: nalevingsmonitoring van de doeltreffendheid van maskering en pseudonimisering.