					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P16S					Documenttitel: **Beleid inzake datamaskering 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**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 6.1.3, Clausule 8	Informatiebeveiligingsrisico's en noodzakelijke beheersmaatregelen, waaronder maskering en pseudonimisering
ISO/IEC 27002:2022	Beheersmaatregelen 8.11, 8.12	Richtlijnen voor maskering en het voorkomen van datalekken
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Gegevensobfuscatie, privacybevorderende technologieën
EU NIS2	Artikel 21(2)(c)	Proportionele technische maatregelen, waaronder pseudonimisering als beheersmaatregel
EU DORA	Artikel 10(1)	ICT-risicobeheersmaatregelen, waaronder waarborgen voor gegevenstransformatie
COBIT 2019	DSS05.01, DSS06	Gegevensbescherming, obfuscatie- en pseudonimiseringstechnieken
AVG	Artikelen 4(5), 5(1)(c), 32	Gegevensminimalisatie, pseudonimisering als technische beheersmaatregel

1. Doel

1.1. Dit beleid stelt bindende eisen vast voor het gebruik van datamaskering en pseudonimisering ter bescherming van gevoelige, persoonlijke en vertrouwelijke gegevens binnen kleine en middelgrote ondernemingen (mkb).

1.2. Deze technieken zijn verplicht wanneer gebruik van echte gegevens niet noodzakelijk is, zoals bij ontwikkeling, analyses of situaties waarin derde partijen worden ingezet, en dragen bij aan het beperken van risico's op blootstelling, misbruik of een datalek.

1.3. Dit beleid ondersteunt rechtstreeks de naleving ten behoeve van certificering volgens ISO/IEC 27001:2022, evenals Europese wettelijke verplichtingen zoals de AVG, de NIS2-richtlijn en de DORA-verordening.

1.4. Door gegevens te transformeren voordat deze buiten hun oorspronkelijke bedrijfscontext worden gebruikt, beperkt de organisatie aansprakelijkheid en vergroot zij haar vermogen om aan te tonen dat passende zorg is betracht ten aanzien van privacy en informatiebeveiliging.

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle gestructureerde en ongestructureerde gegevens die als persoonlijk, vertrouwelijk of gevoelig zijn geclassificeerd, ongeacht of deze worden opgeslagen of verwerkt:

2.1.1. In productie-, test- of ontwikkelomgevingen

2.1.2. Op lokale apparaten, servers of cloudplatforms

2.1.3. Door intern personeel, contractanten of externe dienstverleners

2.2. Dit beleid is tevens van toepassing op alle hulpmiddelen voor gegevenstransformatie (maskering, tokenisatie, pseudonimisering), ongeacht of deze open source, commercieel of intern ontwikkeld zijn.

2.3. Toepassingsgevallen onder dit beleid omvatten:

2.3.1. Het voorbereiden van test- of ontwikkeldatasets

2.3.2. Het exporteren van gegevens naar analysesystemen

2.3.3. Toegang van leveranciers of consultants tot operationele systemen

2.3.4. Gegevensminimalisatie ten behoeve van betrokkenen om het verwerkingsrisico te verlagen

3. Doelstellingen

3.1. Waarborgen dat echte persoonsgegevens of gevoelige gegevens nooit worden blootgesteld in omgevingen met een lager beveiligingsniveau waar deze niet noodzakelijk zijn.

3.2. Vereisen dat maskerings- of pseudonimiseringstechnieken worden toegepast wanneer echte identificatoren niet strikt noodzakelijk zijn voor de uitvoering van de taak.

3.3. Voorkomen van ongeautoriseerde toegang tot of misbruik van gegevens door beheersmaatregelen voor gegevenstransformatie af te dwingen voorafgaand aan gegevensoverdracht of -verwerking.

3.4. Waarborgen dat alle processen voor maskering en pseudonimisering traceerbaar en auditeerbaar zijn en via goedgekeurde tools worden afgedwongen.

3.5. Voldoen aan toepasselijke wettelijke en regelgevende normen die gegevensminimalisatie, vertrouwelijkheid en waarborgen voor gegevenstransformatie vereisen.

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur (GM)

4.1.1. Is eigenaar van dit beleid en keurt het goed

4.1.2. Zorgt ervoor dat alle afdelingen en dienstverleners voldoen aan de vereisten voor gegevenstransformatie

4.1.3. Beoordeelt uitzonderingen, risicobeoordelingen en transformatielogboeken

4.1.4. Coördineert juridische, operationele of leveranciersgerelateerde maatregelen in geval van overtredingen

4.2. IT-dienstverlener / interne IT

4.2.1. Selecteert en beheert tools voor maskering of pseudonimisering

4.2.2. Zorgt ervoor dat passende transformatiemethoden worden toegepast op basis van het gegevenstype

4.2.3. Houdt logboeken bij van getransformeerde datasets en procedures voor sleutelbeheer

4.2.4. Zorgt ervoor dat maskering plaatsvindt vóór gebruik voor testdoeleinden, door leveranciers of voor analyses

[... 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 actualisatie

9.1. Jaarlijkse herziening

9.1.1. Dit beleid moet ten minste jaarlijks door de Algemeen directeur worden beoordeeld om te waarborgen dat het aansluit op:

9.1.1.1. Actualisaties in toepasselijke regelgeving (bijvoorbeeld AVG, DORA)

9.1.1.2. Nieuwe bedrijfssystemen of gegevensuitwisselingen met derden

9.1.1.3. Feedback uit audits of incidenten met gebruik van niet-gemaskeerde gegevens

9.2. Tussentijdse beoordelingen

9.2.1. Beoordelingen moeten ook plaatsvinden wanneer:

9.2.1.1. Nieuwe toepassingen of platforms die gevoelige gegevens verwerken worden geïntroduceerd

9.2.1.2. Een ernstig incident tekortkomingen in de bestaande beheersmaatregelen voor gegevenstransformatie blootlegt

9.2.1.3. Wijzigingen in classificatieniveaus gevolgen hebben voor procedures voor gegevensverwerking

9.3. Versiebeheer en wijzigingsbeheer

9.3.1. Alle beleidswijzigingen moeten:

9.3.1.1. Door de GM worden goedgekeurd en in een wijzigingslogboek worden gedocumenteerd

9.3.1.2. Duidelijk worden gecommuniceerd aan betrokken werknemers en dienstverleners

9.3.1.3. Veilig worden gearchiveerd, met beperkte toegang tot verouderde versies

10. Gerelateerde beleidsdocumenten en samenhang

10.1. Dit beleid moet in samenhang met de volgende mkb-beleidsdocumenten worden toegepast om een consistente en afdwingbare bescherming van gevoelige gegevens te waarborgen:

10.1.1. P13S – Beleid inzake gegevensclassificatie en etikettering: Definieert de classificatieniveaus (bijvoorbeeld Vertrouwelijk – Persoonsgegevens) die bepalen wanneer maskering of pseudonimisering moet worden toegepast. Dit beleid dwingt transformatieregels af op basis van de gevoeligheidsniveaus van gegevens.

10.1.2. P14S – Gegevensbewarings- en afvoerbeleid: Waarborgt dat getransformeerde datasets, waaronder back-ups met gemaskeerde of gepseudonimiseerde gegevens, worden bewaard en afgevoerd volgens toepasselijke regels, inclusief verwijdering van koppelingssleutels wanneer deze niet langer nodig zijn.

10.1.3. P17S – Gegevensbeschermings- en privacybeleid: Brengt transformatiepraktijken in lijn met bredere privacyverplichtingen, waaronder AVG-vereisten voor gegevensminimalisatie en het gebruik van pseudonimisering als waarborg voor de verwerking van persoonsgegevens.

10.1.4. P30S – Incidentresponsbeleid: Bevat meldings- en escalatieprocedures in geval van ongeautoriseerde openbaarmaking van gegevens, waaronder onjuist gebruik of terugdraaien van gemaskeerde of gepseudonimiseerde gegevens.

10.1.5. P2S – Beleid inzake governancerollen en -verantwoordelijkheden: Wijst de algehele verantwoordelijkheid toe voor beleidsimplementatie, risicoacceptatie en goedkeuring van uitzonderingen, primair aan de Algemeen directeur.

10.2. Deze beleidsdocumenten vormen samen een geïntegreerd kader voor gegevensbescherming en waarborgen dat inspanningen op het gebied van maskering en pseudonimisering de ISO 27001-certificering en naleving van verschillende regelgevingskaders ondersteunen.

11. Referentienormen en -raamwerken

11.1. ISO/IEC 27001

11.1.1. Clausule 6.1.3: Vereist de behandeling van informatiebeveiligingsrisico's, waaronder het beperken van blootstelling via technieken voor gegevenstransformatie.

11.1.2. Clausule 8.1: Verplicht de implementatie van beheersmaatregelen die nodig zijn om beveiligingsdoelstellingen te behalen, waaronder pseudonimisering en maskering.

11.2. ISO/IEC 27002

11.2.1. Beheersmaatregel 8.11: Biedt richtlijnen voor het maskeren van gevoelige gegevens in test- en ontwikkelsystemen.

11.2.2. Beheersmaatregel 8.12: Biedt strategieën om datalekken te voorkomen via beheerde transformatie- en toegangspraktijken.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Waarborgt de vertrouwelijkheid van informatie via gegevensobfuscatie.

11.3.2. SC-28: Beschermt informatie in rust en tijdens gebruik.

11.3.3. PT-2/PT-3: Bevordert het gebruik van privacybevorderende technologieën, waaronder pseudonimisering, bij de verwerking van persoonsgegevens.

11.4. AVG

11.4.1. Artikel 4(5): Definieert pseudonimisering juridisch en verplicht beheersmaatregelen voor koppelingssleutels en identificatoren.

11.4.2. Artikel 5(1)(c): Ondersteunt de beginselen van gegevensminimalisatie door middel van maskering.

11.4.3. Artikel 32: Erkent pseudonimisering als technische beheersmaatregel die privacyrisico's vermindert.

11.5. NIS2-richtlijn

11.5.1. Artikel 21(2)(c): Vereist proportionele technische maatregelen om risico's voor gegevensbeveiliging te minimaliseren, waaronder pseudonimisering als onderdeel van risicobeheersing.

11.6. DORA-verordening

11.6.1. Artikel 10(1): Verplicht ICT-gerelateerde risicobeheersmaatregelen die waarborgen voor gegevenstransformatie omvatten voor continuïteit en vertrouwelijkheid tijdens uitbesteding en systeemontwikkeling.

11.7. COBIT 2019

11.7.1. DSS05.01: Vereist de bescherming van informatieactiva, waaronder transformatie waar mogelijk.

11.7.2. DSS06.06: Vereist passende obfuscatie- en pseudonimiseringstechnieken om blootstelling van gegevens te beperken in omgevingen met een lager vertrouwensniveau.