					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P17S					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	
ISO/IEC 27002:2022	Beheersmaatregelen 5.34, 8.10–8	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
AVG	Artikelen 5, 6, 12-23, 30, 32-34	
EU NIS2	Artikel 21(2)(e), 21(2)(f)	
EU DORA	Artikelen 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Doel

1.1. Dit beleid bepaalt hoe de organisatie persoonsgegevens beschermt in overeenstemming met wettelijke verplichtingen, toepasselijke regelgeving en internationale beveiligingsnormen.

1.2. Het waarborgt dat persoonsgegevens van klanten, medewerkers en partners op rechtmatige, behoorlijke en veilige wijze worden verzameld, gebruikt, opgeslagen en verwijderd.

1.3. Dit beleid ondersteunt tevens de naleving van ISO/IEC 27001:2022 en de auditgereedheid door een consistente, risicogebaseerde benadering van privacybescherming af te dwingen.

1.4. Met dit beleid toont de organisatie bevoegdheid en verantwoordingsplicht en versterkt zij het vertrouwen van klanten door prioriteit te geven aan transparantie, gegevensminimalisatie en robuuste privacygovernance.

2. Reikwijdte

2.1. Dit beleid is van toepassing op:

2.1.1. alle medewerkers, contractanten en dienstverleners die persoonsgegevens raadplegen, verwerken of beheren;

2.1.2. alle systemen, toepassingen en locaties waar persoonsgegevens worden opgeslagen of verzonden;

2.1.3. alle persoonsgegevens, ongeacht of deze elektronisch, op papier, in cloudgehoste systemen of op mobiele apparaten zijn opgeslagen.

2.2. Dit beleid is van toepassing op gegevens van klanten, medewerkers, leveranciers en alle overige identificeerbare natuurlijke personen.

2.3. Dit beleid blijft van kracht ongeacht of gegevens intern worden verwerkt of door externe dienstverleners.

3. Doelstellingen

3.1. Waarborgen dat persoonsgegevens worden verwerkt in overeenstemming met privacywetgeving en beveiligingsnormen, waaronder de AVG, NIS2 en ISO 27001.

3.2. Persoonsgegevens beschermen tegen ongeautoriseerde toegang, misbruik, wijziging of verlies door middel van duidelijke technische en organisatorische beheersmaatregelen.

3.3. De privacyrechten van betrokkenen respecteren, waaronder het recht op inzage, correctie en verwijdering van hun gegevens.

3.4. Duidelijke rollen en verantwoordelijkheden vaststellen voor gegevensbescherming binnen de organisatie.

3.5. Gegevensminimalisatie, veilige bewaring en tijdige verwijdering afdwingen in alle systemen en processen.

3.6. Het risico op niet-naleving, juridische sancties, reputatieschade en verlies van klantvertrouwen beperken.

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur

4.1.1. keurt dit beleid goed en ziet toe op de naleving ervan;

4.1.2. stelt de benodigde middelen beschikbaar om privacyrisico's te beheersen en op incidenten te reageren;

4.1.3. draagt de eindverantwoordelijkheid voor naleving van privacywetgeving en toepasselijke normen.

4.2. Privacycoördinator (intern of uitbesteed)

4.2.1. onderhoudt het register van verwerkingsactiviteiten;

4.2.2. behandelt privacyverzoeken van betrokkenen en vragen van toezichthoudende autoriteiten;

4.2.3. ondersteunt risicobeoordelingen, training en beleidsimplementatie;

4.2.4. documenteert datalekken en meldt deze, waar vereist, aan de bevoegde autoriteiten.

[... 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 actualisering

9.1. Geplande herzieningen

9.1.1. Dit beleid wordt ten minste eenmaal per 12 maanden door de privacycoördinator herzien en door de algemeen directeur goedgekeurd.

9.1.2. De herziening beoordeelt de relevantie van het beleid, de afstemming op regelgeving en de operationele doeltreffendheid.

9.2. Aanleidingen voor tussentijdse herziening

9.2.1. Actualisering van het beleid wordt ook gestart naar aanleiding van:

9.2.1.1. nieuwe of herziene wetgeving inzake gegevensbescherming, zoals de AVG of DORA;

9.2.1.2. beveiligingsincidenten of privacyschendingen waarbij persoonsgegevens betrokken zijn;

9.2.1.3. ingebruikname van nieuwe systemen, tools of diensten die persoonsgegevens verwerken;

9.2.1.4. materiële auditbevindingen of aanbevelingen van toezichthouders.

9.3. Wijzigingsbeheer en communicatie

9.3.1. Alle wijzigingen in dit beleid worden formeel vastgelegd in een wijzigingslogboek.

9.3.2. Herziene versies worden verspreid onder alle medewerkers en relevante contractanten.

9.3.3. Gearchiveerde versies worden bewaard ten behoeve van audittraceerbaarheid van de naleving.

10. Gerelateerde beleidsdocumenten en samenhang

10.1. Dit beleid functioneert in samenhang met andere beleidsdocumenten van het mkb om een volledig en afdwingbaar privacykader te vormen:

10.1.1. P13S – Beleid inzake gegevensclassificatie en etikettering: waarborgt dat persoonsgegevens passend worden geclassificeerd, zodat privacybescherming op basis van risico kan worden toegepast.

10.1.2. P14S – Gegevensbewarings- en afvoerbeleid: biedt duidelijke regels voor hoe lang persoonsgegevens moeten worden bewaard en welke veilige methoden worden gebruikt voor afvoer na het verstrijken van de bewaartermijn.

10.1.3. P16S – Beleid inzake gegevensmaskering en pseudonimisering: specificeert hoe persoonsgegevens moeten worden getransformeerd voordat gegevens worden gebruikt in niet-productieomgevingen of extern worden gedeeld.

10.1.4. P30S – Incidentresponsbeleid: beschrijft de vereiste stappen voor de respons op datalekken, waaronder melding aan toezichthouders en betrokkenen binnen de vereiste termijnen.

10.1.5. P2S – Beleid inzake governancerollen en verantwoordelijkheden: verduidelijkt de verantwoordingsstructuur en beslissingsrollen die van toepassing zijn op de handhaving van privacy en het toezicht daarop.

10.2. Deze gerelateerde beleidsdocumenten worden gezamenlijk herzien en toegepast om end-to-enddekking voor privacy te waarborgen in systemen, bij medewerkers en bij leveranciers.

11. Referentienormen en -raamwerken

11.1. ISO/IEC 27001

11.1.1. Clausule 5.1 – Vereist dat het topmanagement leiderschap en betrokkenheid toont bij de bescherming van persoonsgegevens.

11.1.2. Clausule 6.1.3 – Verplicht tot behandeling van risico's die verband houden met de verwerking van persoonsgegevens.

11.1.3. Clausule 8.1 – Vereist de implementatie van operationele beheersmaatregelen om gegevens gedurende de gehele levenscyclus te beschermen.

11.2. ISO/IEC 27002

11.2.1. Beheersmaatregel 5.34 – Biedt implementatierichtlijnen voor de bescherming van privacy en de veilige verwerking van PII.

11.2.2. Beheersmaatregel 8.10 – Behandelt veilige afvoer van persoonsgegevens om resterende openbaarmaking te voorkomen.

11.2.3. Beheersmaatregel 8.11 – Ondersteunt het gebruik van maskering en pseudonimisering voor gegevensminimalisatie.

11.2.4. Beheersmaatregel 8.12 – Voorkomt ongeautoriseerde gegevenslekkage door beheersmaatregelen voor gegevenstoegang en -gebruik.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – Wijst rollen en verantwoordelijkheden toe voor het beheersen van privacyrisico's.

11.3.2. PL-5 – Vereist documentatie van een privacyplan dat gegevensgebruik en gegevensbescherming afdekt.

11.3.3. AC-6 – Verplicht het least-privilegebeginsel en toegangsbeheersmaatregelen voor persoonsgegevens.

11.3.4. IR-4 – Vereist incidentresponsprocedures voor inbreuken waarbij persoonsgegevens betrokken zijn.

11.4. AVG

11.4.1. Artikel 5 – Definieert de kernbeginselen van rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.

11.4.2. Artikel 6 – Vereist een geldige rechtsgrond voor iedere verwerking van persoonsgegevens.

11.4.3. Artikelen 12–23 – Beschrijven de rechten van betrokkenen, waaronder inzage, rectificatie, verwijdering en bezwaar.

11.4.4. Artikel 30 – Verplicht tot het bijhouden van een register van verwerkingsactiviteiten.

11.4.5. Artikel 32 – Vereist passende technische en organisatorische beveiligingsmaatregelen.

11.4.6. Artikelen 33–34 – Stellen meldingsverplichtingen vast voor inbreuken aan autoriteiten en betrokkenen.

11.5. EU NIS2

11.5.1. Artikel 21(2)(e) – Vereist maatregelen om gegevensbescherming te waarborgen in samenhang met het cybersecuritybeleid.

11.5.2. Artikel 21(2)(f) – Verplicht mechanismen voor het beheren van de beveiliging van persoonsgegevens en vertrouwelijke gegevens in ICT-systemen.

11.6. EU DORA

11.6.1. Artikel 6 – Vereist interne governanceraamwerken voor het beheren van gegevensrisico's en gegevensbescherming.

11.6.2. Artikel 15 – Verplicht financiële entiteiten te waarborgen dat externe dienstverleners persoonsgegevens beschermen en naleving van regelgeving ondersteunen.

11.6.3. Artikel 17 – Vereist dat organisaties waarborgen dat ICT-systemen die persoonsgegevens verwerken veilig en veerkrachtig zijn en worden bewaakt.

11.7. COBIT 2019

11.7.1. APO12 – Risico beheren: vereist identificatie en behandeling van privacy- en gegevensbeschermingsrisico's.

11.7.2. DSS05 – Beveiligingsdiensten beheren: vereist waarborgen om ongeautoriseerde toegang tot persoonsgegevens te voorkomen.

11.7.3. MEA03 – Naleving bewaken: vereist dat organisaties doorlopende naleving van privacy- en gegevensbeschermingswetgeving waarborgen.