					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P14S					Documenttitel: **Beleid voor gegevensbewaring en -afvoer**							
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 6.1.3, 8	Dekt risicobehandeling, operationele beheersmaatregelen en bewaareisen
ISO/IEC 27002:2022	Beheersmaatregel 5	Richtlijnen voor bewaartermijnen en methoden voor veilige vernietiging
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Bewaring van auditlogboeken, mediasanering, bewaarlimieten voor gegevens en handhaving
EU NIS2	Artikel 21(2)(a)	Vereist beleid voor risicogebaseerd levenscyclusbeheer
EU DORA	Artikel 5(1)	ICT-risicobeheer: beschikbaarheid en verwijdering van gegevens
COBIT 2019	BAI03.04, DSS01	Beheersmaatregelen voor de informatielevenscyclus, veilige afvoer
AVG	Artikel 5(1)(e), 17	Gegevens niet langer bewaren dan noodzakelijk; recht op gegevenswissing

1. Doel

1.1 Het doel van dit beleid is het vaststellen van afdwingbare regels voor de bewaring en veilige afvoer van informatie binnen een mkb-omgeving. Het waarborgt dat registraties uitsluitend worden bewaard gedurende de termijn die wettelijk, contractueel of vanuit bedrijfsmatige noodzaak vereist is, en daarna veilig worden vernietigd.

1.2 Dit beleid heeft tot doel informatierisico's te beperken, juridische blootstelling te beheersen en de opslag van redundante of verouderde gegevens te minimaliseren. Het ondersteunt naleving van ISO/IEC 27001 en privacykaders zoals de AVG door ongeautoriseerde bewaring van persoonsgegevens of gevoelige informatie tot een minimum te beperken.

1.3 Een goed ingericht kader voor bewaring en afvoer verlaagt operationele kosten, verbetert systeemprestaties en zorgt ervoor dat de organisatie auditgereed is. Voor het mkb met beperkte IT-capaciteit biedt dit een praktische manier om digitale en fysieke informatieactiva verantwoord te beheren.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle registraties, bestanden, logboeken, communicatie en datasets die door de organisatie worden aangemaakt, verzameld, verwerkt of opgeslagen

2.1.2 alle medewerkers, contractanten en externe dienstverleners die gegevens van de organisatie verwerken

2.1.3 alle gegevensformaten (bijvoorbeeld papier, elektronisch, beeld, audio of logbestand) en alle opslagmedia (bijvoorbeeld lokale schijven, clouddiensten, e-mailservers, back-ups)

2.2 De reikwijdte omvat:

2.2.1 bedrijfsdocumenten (bijvoorbeeld facturen, contracten, projectrapportages)

2.2.2 operationele registraties (bijvoorbeeld logboeken, toegangsgegevens, back-upsnapshots)

2.2.3 persoonsgegevens (bijvoorbeeld HR-dossiers, klantcommunicatie, supportregistraties)

2.2.4 gegevens die intern, extern of in hybride systemen worden gehost

2.2.5 gearchiveerde gegevens en back-upgegevens, ongeacht of deze actief of inactief zijn

2.3 Alle fasen van de gegevenslevenscyclus vallen binnen de reikwijdte, van aanmaak tot geautoriseerde afvoer.

3. Doelstellingen

3.1 Consistente bewaartermijnen vaststellen op basis van wettelijke, operationele en regelgevende criteria.

3.2 Voorkomen dat kritieke registraties voortijdig worden verwijderd en onnodige ophoping van gegevens elimineren.

3.3 Zorgen voor veilige en onomkeerbare afvoer van gegevens wanneer bewaring niet langer vereist is.

3.4 Eigenaarschap toewijzen voor het handhaven van bewaar- en verwijderingsbeslissingen binnen de personele beperkingen van het mkb.

3.5 Auditgereed beschikbare documentatie waarborgen om passende zorgvuldigheid onder ISO 27001, AVG, NIS2 en andere kaders aan te tonen.

3.6 Veilige verwerking van gegevens over de gehele levenscyclus bevorderen zonder onnodige technische belasting op te leggen aan niet-gespecialiseerd personeel.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 keurt dit beleid goed en is eigenaar van dit beleid.

4.1.2 ziet erop toe dat procedures voor bewaring en afvoer worden geïmplementeerd op een wijze die in overeenstemming is met juridisch risico en bedrijfsrisico.

4.1.3 autoriseert uitzonderingen, legal hold en opschorting van verwijdering wanneer nodig.

4.1.4 initieert beleidsbeoordelingen en keurt actualisaties goed op basis van wijzigingen in de bedrijfsvoering of regelgeving.

4.2 Aangewezen gegevenseigenaar

4.2.1 wordt toegewezen per gegevenscategorie (bijvoorbeeld financieel, HR, klantregistraties).

4.2.2 classificeert registraties en bepaalt de passende bewaartermijn op basis van beleid en juridisch advies.

4.2.3 autoriseert verwijdering wanneer aan de bewaareisen is voldaan.

4.2.4 ondersteunt interne audits door context te geven bij de bewaartermijnen en afvoeractiviteiten.

[... 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 Dit beleid moet ten minste eenmaal per jaar worden beoordeeld, of bij:

9.1.1 wijzigingen in toepasselijke wetgeving (bijvoorbeeld gegevensbescherming, financiële verslaglegging)

9.1.2 ingebruikname van nieuwe systemen of processen die van invloed zijn op de gegevenslevenscyclus

9.1.3 auditbevindingen of incidenten die hiaten in bewaarpraktijken aan het licht brengen

9.2 Bij beoordelingen moet worden gewaarborgd dat het bewaartermijnenregister volledig blijft en alle belangrijke categorieën registraties omvat.

9.3 Actualisaties van het beleid moeten door de GM worden goedgekeurd en aan de betrokken medewerkers worden gecommuniceerd. De meest recente versie moet toegankelijk zijn en onder versiebeheer staan.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 P2S – Beleid inzake governance-rollen en -verantwoordelijkheden: definieert beleidseigenaarschap en bevoegdheid voor uitzonderingen.

10.2 P13S – Beleid inzake gegevensclassificatie en etikettering: bepaalt hoe bewaartermijnen aansluiten op gegevensclassificatie.

10.3 P12S – Assetmanagementbeleid: regelt opslagmedia die gegevens bevatten waarop bewaring en afvoer van toepassing zijn.

10.4 P17S – Beleid inzake gegevensbescherming en privacy: waarborgt gegevensminimalisatie en ondersteunt rechtmatige verwerking onder de AVG.

10.5 P30S – Incidentresponsbeleid: wordt geactiveerd wanneer tekortkomingen in afvoer of bewaring leiden tot mogelijke blootstelling van gegevens.

11. Referentienormen en -kaders

11.1 ISO/IEC 27001

11.1.1 Clausule 6.1.3: vereist behandeling van informatiegerelateerde risico's, waaronder risico's rond bewaring.

11.1.2 Clausule 8.1: definieert operationele beheersmaatregelen voor de levenscyclus.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 5.33: richtlijnen voor het vaststellen van bewaartermijnen en methoden voor veilige vernietiging.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: vereist bewaring van auditlogboeken.

11.3.2 MP-6: definieert procedures voor mediasanering.

11.3.3 SI-12: behandelt bewaarlimieten voor gegevens en de handhaving daarvan.

11.4 AVG

11.4.1 Artikel 5(1)(e): gegevens mogen niet langer worden bewaard dan noodzakelijk.

11.4.2 Artikel 17: het recht op gegevenswissing is van toepassing wanneer gegevens niet langer rechtmatig worden bewaard.

11.5 EU NIS2

11.5.1 Artikel 21(2)(a): vereist op het risico afgestemde organisatorische beleidslijnen, waaronder levenscyclusbeheer.

11.6 EU DORA

11.6.1 Artikel 5(1): ICT-risicobeheer omvat beschikbaarheid en verwijdering van gegevens.

11.7 COBIT 2019

11.7.1 BAI03.04: beheersmaatregelen voor de informatielevenscyclus zijn vereist.

11.7.2 DSS01.06: procedures voor veilige afvoer als onderdeel van de bescherming van informatieactiva.