					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P14					Documenttitel: **Gegevensbewarings- en vernietigingsbeleid**							
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, 8.1	
ISO/IEC 27002:2022	Beheersmaatregelen 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
AVG	Artikelen 5(1)(e), 17, 32	
NIS2-richtlijn	Artikel 21(2)(a-e)	
DORA	Artikelen 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Doel

1.1 Het doel van dit beleid is het vaststellen van de organisatorische vereisten voor gegevensbewaring en veilige vernietiging gedurende alle fasen van de informatielevenscyclus. Dit beleid waarborgt naleving van toepasselijke wettelijke, reglementaire en contractuele verplichtingen en voorkomt onnodige of risicovolle accumulatie van gegevens.

1.2 Dit beleid ondersteunt de implementatie van ISO/IEC 27001:2022 door beheersmaatregelen af te dwingen voor gegevensbewaring en onomkeerbare vernietigingspraktijken. Het maakt traceerbare documentatie van registraties mogelijk, dwingt bewaring af in lijn met de gevoeligheid en classificatie van informatie en zorgt ervoor dat de organisatie voorbereid is op audits, inspecties door toezichthouders en juridische bewijsvoering.

1.3 Het beleid heeft voorts tot doel de vertrouwelijkheid, integriteit en beschikbaarheid (CIA) van gegevens te waarborgen, terwijl bedrijfsrisico's, operationele inefficiënties en blootstelling aan privacyschendingen als gevolg van onjuiste bewaring of vernietiging van gegevens tot een minimum worden beperkt.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle fysieke bedrijfsmiddelen en digitale informatieactiva die eigendom zijn van de organisatie, door de organisatie worden verwerkt of door de organisatie worden bewaard, met inbegrip van gegevens onder beheer van derden, dochterondernemingen of uitbestedingspartners.

2.2 De reikwijdte omvat, maar is niet beperkt tot:

2.2.1 Documenten, bestanden en registraties (digitaal en op papier)

2.2.2 Databases en archieven

2.2.3 E-mails en logboeken van instant messaging

2.2.4 Back-ups, systeemlogboeken en audittrails

2.2.5 Broncode, applicatiegegevens en in de cloud gehoste activa

2.2.6 Verwisselbare media en verouderde hardware die gegevens bevat

2.3 Het beleid is van toepassing op zowel operationele registraties als gereguleerde datasets (bijvoorbeeld financiële, juridische, HR-, klantgerelateerde en auditrelevante inhoud), ongeacht de opslaglocatie of het systeem.

2.4 Het is van toepassing op alle afdelingen van de organisatie en op alle medewerkers, contractanten en externe leveranciers die betrokken zijn bij het creëren, opslaan, beheren of vernietigen van gegevens.

3. Doelstellingen

3.1 Waarborgen dat gegevens uitsluitend worden bewaard zolang dit wettelijk, contractueel of operationeel noodzakelijk is en veilig worden vernietigd wanneer zij niet langer nodig zijn.

3.2 Voorkomen dat registraties die nodig zijn voor lopende operaties, naleving, gerechtelijke procedures of auditdoeleinden voortijdig, ongeautoriseerd of per ongeluk worden verwijderd.

3.3 Vaststellen en afdwingen van consistente bewaarschema's op basis van informatieclassificatie, type bedrijfsmiddel, toepasselijke wet- en regelgeving en risicoblootstelling.

3.4 Beschermen van de privacy en vertrouwelijkheid van gegevens gedurende de bewaartermijn en op het moment van vernietiging, met inbegrip van de uitoefening van rechten van betrokkenen (zoals wissing op grond van artikel 17 AVG).

3.5 Waarborgen dat alle methoden voor gegevensvernietiging onomkeerbaar zijn, passend worden gedocumenteerd en voldoen aan erkende normen zoals NIST SP 800-88.

3.6 Minimaliseren van operationele inefficiënties, extra kosten en juridische blootstelling als gevolg van te lange bewaring of het niet verwijderen van verouderde gegevens.

3.7 Ondersteunen van doelstellingen voor bedrijfscontinuïteit en herstel na verstoringen door geïntegreerde governance voor back-upbewaring en verdedigbare archiveringspraktijken.

4. Rollen en verantwoordelijkheden

4.1 Directie

4.1.1 Keurt dit beleid goed en zorgt voor passende financiering, capaciteit en integratie in organisatiebrede programma's voor risicobeheer en naleving.

4.1.2 Draagt de eindverantwoordelijkheid voor juridische en reglementaire naleving met betrekking tot gegevensbewaring en veilige vernietiging.

4.2 Chief Information Security Officer (CISO)

4.2.1 Is eigenaar van dit beleid en verantwoordelijk voor het definiëren en beoordelen van de governance voor bewaring en vernietiging in overeenstemming met het ISMS.

4.2.2 Zorgt ervoor dat op classificatie gebaseerde vereisten voor bewaring en vernietiging worden geïmplementeerd binnen bedrijfseenheden en technische systemen.

4.2.3 Bewaakt de naleving van het beleid en ziet zo nodig toe op corrigerende maatregelen.

[... 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 jaarlijks worden beoordeeld of wanneer aan een van de volgende voorwaarden is voldaan:

9.1.1 Wijzigingen in toepasselijke wet- of regelgeving die van invloed zijn op gegevensbewaring (bijvoorbeeld actualisaties van de AVG, belastingwetgeving of DORA)

9.1.2 Wijzigingen in het classificatiekader of bedrijfsprocessen die invloed hebben op fasen van de gegevenslevenscyclus

9.1.3 Invoering van nieuwe IT-systemen, archiveringsplatforms of technologieën voor mediavernietiging

9.1.4 Bevindingen van interne audits of aanbevelingen van toezichthouders die hiaten in bewaar- of vernietigingspraktijken aantonen

9.2 De beoordeling wordt geleid door de CISO en de Functionaris voor gegevensbescherming (FG), met input van Juridische Zaken en Compliance, IT en bedrijfseenheden.

9.3 Het centraal bewaarschema voor gegevens (MDRS) en het vernietigingsregister moeten parallel worden beoordeeld om te waarborgen dat:

9.3.1 Schema's accuraat blijven en operationele, juridische en reglementaire behoeften weerspiegelen

9.3.2 Vernietigingsdocumentatie volledig en auditeerbaar is

9.3.3 Registraties van legal hold worden gevalideerd en opgeheven wanneer dat passend is

9.4 Eventuele actualisaties van het beleid moeten:

9.4.1 Formeel onder versiebeheer worden geplaatst en worden bewaard in de documentrepository van het ISMS

9.4.2 Een versiehistorie en onderbouwing van de wijziging bevatten

9.4.3 Worden goedgekeurd door de directie

9.4.4 Worden gecommuniceerd aan relevant personeel met geactualiseerd trainings- of richtlijnmateriaal

9.5 Wanneer significante beleidswijzigingen plaatsvinden, moeten betrokken medewerkers binnen 30 dagen na publicatie gerichte training voltooien om voortdurende naleving te waarborgen.

9.6 Gerelateerde beleidslijnen en samenhang

10. Gerelateerde beleidslijnen en samenhang

10.1.1 P4 - Beleid inzake toegangscontrole: Waarborgt dat uitsluitend geautoriseerde personen tijdens de bewaartermijn toegang hebben tot gegevens en dat verlopen gegevens worden afgeschermd in afwachting van vernietiging.

10.1.2 P12 - Beleid inzake beheer van bedrijfsmiddelen: Identificeert welke bedrijfsmiddelen gegevens bevatten waarvoor geplande vernietiging vereist is en volgt hun levenscyclus van verwerving tot vernietiging.

10.1.3 P13 - Beleid inzake gegevensclassificatie en etikettering: Stuurt classificatiebeslissingen die rechtstreeks bepalen hoe lang gegevens worden bewaard en welke vernietigingsmethode vereist is.

10.1.4 P15 - Beleid inzake back-up en herstel: Definieert bewaartermijnen en vernietigingsprocedures voor back-upmedia en gerepliceerde gegevensactiva.

10.1.5 P18 - Beleid inzake cryptografische beheersmaatregelen: Ondersteunt cryptografische wissing voor vernietiging en dwingt encryptie af tijdens gegevensopslag tot aan vernietiging.

10.1.6 P30 - Incidentresponsbeleid (P30): Wordt geactiveerd in gevallen waarin onjuiste vernietiging leidt tot mogelijk gegevensverlies, een datalek of een reglementaire overtreding.

10.2 Elk gekoppeld beleid speelt een rol bij het afdwingen van een samenhangend governancemodel voor gegevens ten aanzien van classificatie, levenscyclusbeheersing, toegang en auditgereedheid.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op wereldwijd erkende normen en reglementaire raamwerken die veilige, conforme en efficiënte praktijken voor de gegevenslevenscyclus definiëren.

11.2 ISO/IEC 27001:

11.2.1 Clausule 6.1.3 - risicobehandelingsplan: Ondersteunt de beperking van risico's die samenhangen met te lange bewaring, datalekken of falende vernietiging.

11.2.2 Clausule 8.1 - operationele planning en beheersing: Legt levenscyclusbeheersmaatregelen vast voor opslag, archivering en vernietiging.

11.3 ISO/IEC 27002:2022 - Beheersmaatregelen 5.10, 5.12, 5.30, 5: Bieden praktische richtlijnen voor aanvaardbaar gebruik van gegevens, rechtvaardiging van bewaring, gecontroleerde verwijdering en verdedigbare registratiepraktijken in overeenstemming met de risicotolerantie van de organisatie.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - bewaring van auditregistraties: Waarborgt voldoende opslag van auditlogs en nalevingsbewijsmateriaal.

11.4.2 MP-6 - sanitization van media: Vereist veilige, gedocumenteerde vernietigingsmethoden voor fysieke en elektronische media.

11.4.3 SI-12 - informatieverwerking: Dwingt passende omgang met gegevens af in lijn met beheersmaatregelen voor bewaring en vernietiging.

11.4.4 PL-2 - systeembeveiligings- en privacyplan: Vereist systeemspecifieke documentatie van de omgang met de gegevenslevenscyclus en bepalingen voor veilige vernietiging.

11.5 AVG (2016/679):

11.5.1 Artikel 5(1)(e) - gegevensminimalisatie en opslagbeperking: Vereist dat gegevens niet langer worden bewaard dan noodzakelijk.

11.5.2 Artikel 17 - recht op wissing ("recht om vergeten te worden"): Vereist snelle en permanente verwijdering van persoonsgegevens op grond van een geldig verzoek.

11.5.3 Artikel 32 - beveiliging van verwerking: Versterkt gegevensbescherming tijdens bewaring en verplicht tot veilige vernietiging van verlopen registraties.

11.6 NIS2-richtlijn (2022/2555):

11.6.1 Artikel 21(2)(a-e): Vereist dat entiteiten beleidslijnen en technische maatregelen vaststellen voor veilige gegevensverwerking, waaronder opslagbeperkingen en vernietigingsmethoden.

11.7 DORA (2022/2554):

11.7.1 Artikel 5 - governance en beheersing: Verplicht tot gestructureerd ICT-risicobeheer, waaronder veilige omgang met de informatielevenscyclus.

11.7.2 Artikel 9 - kader voor ICT-risicobeheer: Vereist beleidslijnen voor gegevensbewaring, vernietiging en juridische/reglementaire naleving van digitale operaties.

11.8 COBIT 2019:

11.8.1 DSS01 - beheerde operaties: Ondersteunt het volgen van bewaartermijnen en consistentie binnen gegevenssystemen.

11.8.2 DSS05 - beheerde beveiligingsdiensten: Waarborgt bescherming van opgeslagen en gearchiveerde gegevens tot aan veilige vernietiging.

11.8.3 MEA03 - monitoren, evalueren en beoordelen van naleving: Maakt auditing mogelijk van handhaving van bewaartermijnen, verwijderingsprocedures en naleving van regelgeving.