					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P37					Documenttitel: **Beleid inzake juridische en regelnaleving**							
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**

1. Doel

1.1 Dit beleid stelt het verplichte kader vast voor het identificeren, beheren en naleven van alle juridische, reglementaire en contractuele verplichtingen die relevant zijn voor de informatiebeveiliging, gegevensbescherming en operationele functies van de organisatie.

1.2 Het doel is niet-naleving te voorkomen die kan leiden tot boetes, juridische aansprakelijkheid, verstoring van de bedrijfsvoering, reputatieschade of handhaving door toezichthouders.

1.3 Dit beleid ondersteunt de integratie van nalevingsverplichtingen in governance, risicobeheer, operationele processen, projectlevenscycli en systeemontwerp.

1.4 Het waarborgt dat alle relevante verplichtingen — over jurisdicties, sectoren en toezichtsdomeinen heen — binnen de organisatie duidelijk worden gedocumenteerd, beoordeeld, bewaakt en gehandhaafd.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle afdelingen, functies, bedrijfseenheden en personen die namens de organisatie handelen, waaronder:

2.1.1 vaste en tijdelijke werknemers

2.1.2 contractanten, consultants en stagiairs

2.1.3 externe leveranciers, verwerkers of partners die gegevens, systemen of reglementaire verantwoordelijkheden van de organisatie verwerken of beheren

2.1.4 elk bedrijfsproces, project of initiatief dat aan juridische of reglementaire eisen is onderworpen

2.2 De nalevingsdomeinen die onder dit beleid vallen, omvatten onder meer:

2.2.1 verplichtingen op het gebied van informatiebeveiliging en cyberbeveiliging (bijvoorbeeld ISO/IEC 27001, NIS2, DORA)

2.2.2 wetgeving inzake gegevensbescherming en privacy (bijvoorbeeld AVG, sectorspecifieke privacywetgeving)

2.2.3 sectorspecifieke regelgeving (bijvoorbeeld financieel, medisch, automotive, defensie)

2.2.4 contractuele verplichtingen die voortvloeien uit geheimhoudingsovereenkomsten, Service Level Agreements (SLA's) of verwerkersovereenkomsten met derde partijen

2.2.5 wettelijke vereisten met betrekking tot incidentmelding, interactie met opsporingsinstanties en internationale gegevensdoorgifte

3. Doelstellingen

3.1 Waarborgen dat alle toepasselijke wet- en regelgeving, normen en contractuele verplichtingen in de gehele organisatie worden geïdentificeerd, gedocumenteerd, geïnterpreteerd en nageleefd.

3.2 Juridische en reglementaire vereisten integreren in het managementsysteem voor informatiebeveiliging (ISMS), risicobeheerprocessen, leveranciersovereenkomsten en het ontwerp van producten en diensten van de organisatie.

3.3 Een mechanisme bieden voor het proactief monitoren van wijzigingen in wet- en regelgeving en het dienovereenkomstig actualiseren van beheersmaatregelen en documentatie.

3.4 Duidelijke verantwoordingsplicht vaststellen voor nalevingstoezicht, escalatie van overtredingen, afhandeling van uitzonderingen en externe rapportage.

3.5 Auditeerbaarheid en verdedigbaarheid van de juridische en reglementaire positie van de organisatie waarborgen tijdens inspecties, onderzoeken of certificeringsbeoordelingen.

4. Rollen en verantwoordelijkheden

4.1 Topmanagement

4.1.1 Draagt de strategische eindverantwoordelijkheid voor juridische en reglementaire afstemming binnen de gehele organisatie.

4.1.2 Beoordeelt en keurt nalevingsbesluiten met een hoog risico goed, waaronder risicoacceptaties en juridische geschillen.

4.2 Compliance Officer / juridisch adviseur

4.2.1 Beheert het nalevingsregister, waarin alle toepasselijke wet- en regelgeving, normen, certificeringen en contractuele clausules zijn opgenomen.

4.2.2 Voert juridische impactbeoordelingen uit voor nieuwe diensten, markten of gegevensstromen.

4.2.3 Geeft gezaghebbende interpretaties van wet- en regelgeving en normen.

[... 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 beleidsbeoordeling

9.1.1 Dit beleid moet ten minste eenmaal per kalenderjaar worden beoordeeld om:

9.1.1.1 voortdurende afstemming met geactualiseerde wet- en regelgeving, branchenormen en reglementaire kaders te waarborgen

9.1.1.2 de operationele doeltreffendheid te valideren op basis van auditbevindingen en incidenthistorie

9.1.1.3 organisatorische wijzigingen te verwerken (bijvoorbeeld nieuwe jurisdicties, systemen of bedrijfslijnen)

9.2 Triggergebaseerde beoordelingen

9.2.1 Tussentijdse beoordelingen moeten worden gestart wanneer:

9.2.2 een nieuwe juridische of reglementaire vereiste wordt vastgesteld of bijgewerkt

9.2.3 een nalevingsincident of audit tekortkomingen in het beleid aan het licht brengt

9.2.4 de organisatie een nieuwe markt of dienstverleningslijn betreedt die onder afzonderlijke nalevingskaders valt

9.2.5 handhavingstrends of richtsnoeren van toezichthouders wijzen op verschuivingen in de risicopositie

9.3 Eigenaarschap en goedkeuring

9.3.1 De juridische afdeling en de Compliance Officer zijn gezamenlijk verantwoordelijk voor de coördinatie van het beoordelingsproces.

9.3.2 Definitieve beleidswijzigingen moeten worden goedgekeurd door het topmanagement en worden geregistreerd in het beleidswijzigingsregister, met de bijbehorende verwijzingen naar wijzigingsbeheer en communicatieplannen.

9.4 Versiebeheer en communicatie

9.4.1 Elke bijgewerkte versie van dit beleid moet:

9.4.1.1 een samenvatting van de belangrijkste wijzigingen bevatten

9.4.1.2 opnieuw worden verspreid via officiële kanalen (bijvoorbeeld beleidsportaal, LMS, interne nieuwsbrieven)

9.4.1.3 kennisname vereisen van betrokken medewerkers, met name in juridische, operationele, beveiligings- en leveranciersmanagementrollen

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit beleid werkt samen met en versterkt de volgende beleidsdocumenten binnen het ISMS van de organisatie:

10.1.1 P1 – Informatiebeveiligingsbeleid: stelt de basisbeginselen voor governance vast die waarborgen dat alle beleidsdocumenten inzake informatiebeveiliging — waaronder naleving — zijn afgestemd op strategische bedrijfs- en reglementaire vereisten.

10.1.2 P2 – Beleid inzake governancerollen en -verantwoordelijkheden: definieert beslissingsbevoegdheden, waaronder juridische en compliancerollen die verantwoordelijk zijn voor reglementair toezicht en verantwoordingsplicht.

10.1.3 P6 – Beleid inzake risicobeheer: ondersteunt de beoordeling, het eigenaarschap en de mitigatie van juridische en reglementaire nalevingsrisico's binnen de gehele organisatie.

10.1.4 P8 – Informatiebeveiligingsbewustzijns- en opleidingsbeleid: waarborgt dat alle medewerkers op de hoogte zijn van nalevingsverantwoordelijkheden en passende training voor hun rol ontvangen.

10.1.5 P12 – Beleid inzake bedrijfsmiddelenbeheer: versterkt juridische verplichtingen voor het beheren en beschermen van gereguleerde of contractuele bedrijfsmiddelen, inclusief bedrijfsmiddelen die persoonsgegevens en kritieke infrastructuur omvatten.

10.1.6 P30 – Incidentresponsbeleid: regelt verplichte juridische meldingen (bijvoorbeeld AVG artikel 33) en escalatieprocedures in geval van een nalevingsinbreuk of reglementair incident.

10.1.7 P33 – Beleid inzake audit- en nalevingsmonitoring: biedt gestructureerde assurance-activiteiten — waaronder toetsing van beheersmaatregelen en verzameling van bewijsmateriaal — die vereist zijn voor interne en externe verificatie van naleving.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 4.2 – Inzicht in de behoeften en verwachtingen van belanghebbende partijen: vereist identificatie en integratie van juridische en reglementaire vereisten in het ISMS.

11.1.2 Clausule 5.1 – Leiderschap en betrokkenheid: verplicht tot verantwoordelijkheid op directieniveau voor het vaststellen en in stand houden van juridische naleving binnen de organisatie.

11.1.3 Clausule 5.3 – Organisatorische rollen, verantwoordelijkheden en bevoegdheden: waarborgt duidelijkheid over rollen voor juridisch toezicht en reglementaire naleving.

11.1.4 Bijlage A, beheersmaatregel 5.36 – Naleving van juridische en contractuele vereisten: stelt de vereiste vast om verplichtingen die voortvloeien uit wetgeving, regelgeving en contracten te identificeren en na te leven.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 5.36: bevat implementatierichtlijnen voor het bijhouden van een nalevingsregister, het valideren van reglementaire vereisten en het waarborgen van gestructureerde bewaring van bewijsmateriaal.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Beleid en procedures voor beveiligingsplanning: vereist dat nalevingsverplichtingen in governancestructuren en documentatie zijn verankerd.

11.3.2 PM-1 – Beveiligingsprogrammaplan: verplicht reglementaire beheersmaatregelen als onderdeel van het bredere beveiligingsprogramma.

11.3.3 CA-7 – Continue monitoring: ondersteunt toezicht op de doeltreffendheid van beheersmaatregelen bij het voldoen aan juridische en beleidsvereisten.

11.3.4 AU-9 – Bescherming van auditinformatie: waarborgt dat auditlogs en nalevingsregistraties worden beschermd en beschikbaar zijn voor inspectie.

11.4 AVG (EU 2016/679)

11.4.1 Artikel 5 – Beginselen inzake verwerking: vereist rechtmatige verwerking, transparantie en verantwoordingsplicht.

11.4.2 Artikel 6 – Rechtmatigheid van verwerking: verplicht passende rechtsgronden voor alle gegevensverwerkingsactiviteiten.

11.4.3 Artikel 24 – Verantwoordelijkheid van de verwerkingsverantwoordelijke: legt directe verantwoordingsplicht vast voor het waarborgen van reglementaire naleving.

11.4.4 Artikel 32 – Beveiliging van de verwerking: vereist implementatie van passende technische en organisatorische beheersmaatregelen.

11.4.5 Artikel 33 – Meldplicht bij inbreuken: vereist dat inbreuken in verband met persoonsgegevens binnen 72 uur worden gemeld aan de relevante autoriteiten.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikelen 20–21: vereisen dat essentiële en belangrijke entiteiten gedocumenteerde governance, strategieën voor juridische naleving en continue beoordeling van juridische risico's implementeren.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(2) – ICT-risicobeheerkader: vereist integratie van juridische naleving binnen bredere functies voor risicobeheer en toezicht.

11.6.2 Artikel 19 – ICT-risico van derde partijen: legt specifieke juridische vereisten op voor het beheren van contractuele en reglementaire verplichtingen met betrekking tot externe leveranciers en platforms.

11.7 COBIT 2019

11.7.1 APO12 – Risicobeheer: neemt juridische en reglementaire naleving op als kritieke componenten van ondernemingsbrede risicogovernance.

11.7.2 MEA03 – Naleving van externe vereisten bewaken: definieert doorlopende monitoring, uitzonderingsbeheer en auditgereedheid voor alle vormen van reglementaire verplichtingen.