					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P37S					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**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausules 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Beheersmaatregel 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
EU AVG	Artikelen 5, 6, 32, 33	
EU NIS2	Artikelen 21(2)(a), 21(2)(f), 23	
EU DORA	Artikelen 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Doel

1.1 Dit beleid beschrijft de aanpak van de organisatie voor het identificeren van, voldoen aan en aantoonbaar naleven van wettelijke, regelgevende en contractuele verplichtingen.

1.2 Het stelt duidelijke verantwoordelijkheden en praktische stappen vast om de organisatie te ondersteunen bij het nakomen van haar nalevingsverplichtingen, waaronder wetgeving inzake gegevensbescherming, cyberbeveiligingskaders, klantovereenkomsten en certificeringsnormen.

1.3 Het waarborgt dat de organisatie, ook zonder een eigen nalevingsteam, juridisch verantwoorde activiteiten kan uitvoeren, adequaat op incidenten kan reageren en auditgereed blijft.

1.4 Dit beleid is essentieel voor het faciliteren van certificering volgens ISO/IEC 27001:2022 en voor het voldoen aan externe verwachtingen van klanten, toezichthouders en partners.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle medewerkers, contractanten, freelancers en externe leveranciers;

2.1.2 alle diensten, activiteiten, systemen en gegevensverwerkingen waarvoor de organisatie aan wettelijke of contractuele vereisten moet voldoen;

2.1.3 alle locaties en apparaten die worden gebruikt voor de verwerking van bedrijfsinformatie, ongeacht of deze zich op kantoor bevinden, op afstand worden gebruikt of in de cloud worden gehost.

2.2 Dit beleid omvat:

2.2.1 wetgeving inzake gegevensbescherming, zoals de AVG;

2.2.2 cyberbeveiligingsregelgeving, zoals NIS2;

2.2.3 sectorspecifieke verplichtingen, indien van toepassing;

2.2.4 klantcontracten, geheimhoudingsovereenkomsten en auditclausules;

2.2.5 vrijwillige certificeringen (bijvoorbeeld ISO 27001) en interne beleidslijnen die voor naleving moeten worden gehandhaafd.

3. Doelstellingen

3.1 Verantwoordingsplicht borgen: duidelijke verantwoordelijkheid toewijzen voor het monitoren, actualiseren en handhaven van wettelijke, regelgevende en contractuele verplichtingen.

3.2 De organisatie beschermen: het risico op wetsovertredingen, boetes, datalekken en reputatieschade minimaliseren.

3.3 Auditgereed blijven: verifieerbare registraties bijhouden waaruit blijkt hoe de organisatie haar nalevingsverplichtingen nakomt.

3.4 Integratie in beleid ondersteunen: waarborgen dat wettelijke en regelgevende verplichtingen consequent worden geborgd in alle beleidslijnen en processen.

3.5 Uitzonderingen transparant beheren: waarborgen dat eventuele nalevingsuitzonderingen worden gedocumenteerd, onderbouwd en goedgekeurd om aansprakelijkheid te beperken.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Draagt de eindverantwoordelijkheid voor de juridische en regelgevende naleving binnen de organisatie.

4.1.2 Beheert het nalevingsregister en borgt dat dit actueel blijft.

4.1.3 Beoordeelt klantcontracten en borgt dat specifieke verplichtingen worden nageleefd en gehandhaafd.

4.1.4 Keurt uitzonderingen op nalevingsverplichtingen uitsluitend goed indien deze juridisch verdedigbaar zijn en compenserende beheersmaatregelen aanwezig zijn.

4.2 Externe adviseurs (bijvoorbeeld juridische, IT- of nalevingsadviseurs)

4.2.1 Ondersteunen de GM bij het identificeren van toepasselijke wetgeving, certificeringen en verplichtingen (bijvoorbeeld AVG, NIS2, ISO 27001).

4.2.2 Adviseren over de interpretatie van nieuwe regelgeving of wijzigingen in bestaande wetgeving.

4.2.3 Kunnen ondersteuning bieden bij beleidsactualisaties, audits of respons op inbreuken wanneer sprake is van juridische blootstelling.

[... 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 actualisering

9.1 Geplande jaarlijkse beoordeling

9.1.1 Dit beleid moet elke 12 maanden door de GM worden beoordeeld.

9.1.2 De beoordeling moet bevestigen:

9.1.2.1 dat het beleid relevant is voor de actuele juridische en contractuele context;

9.1.2.2 dat klantovereenkomsten en dienstverplichtingen correct zijn verwerkt;

9.1.2.3 dat het beleid in lijn is met het nalevingsregister en andere beleidslijnen.

9.2 Gebeurtenisgestuurde actualisaties

9.2.1 Onmiddellijke beoordeling is vereist indien:

9.2.1.1 nieuwe wet- of regelgeving van toepassing wordt (bijvoorbeeld nieuwe regels inzake gegevensbescherming);

9.2.1.2 een klant complexe nalevingsvoorwaarden aan een overeenkomst toevoegt;

9.2.1.3 een inbreuk of incident van niet-naleving plaatsvindt;

9.2.1.4 de organisatie uitbreidt naar een gereguleerde markt of sector.

9.3 Goedkeuring van actualisaties en versiebeheer

9.3.1 Alle actualisaties moeten worden gedocumenteerd, onder versiebeheer worden geplaatst en door de GM worden goedgekeurd.

9.3.2 Historische versies moeten worden bewaard voor audit- en juridische doeleinden.

9.4 Communicatie van wijzigingen

9.4.1 Medewerkers en contractanten moeten binnen 5 werkdagen na goedkeuring over beleidswijzigingen worden geïnformeerd.

9.4.2 Leveranciers die hierdoor worden geraakt, moeten eveneens kennisnemen van de bijgewerkte voorwaarden voordat de dienstverlening wordt voortgezet.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid wordt ondersteund en gehandhaafd via de volgende mkb-beleidslijnen:

10.1.1 P3S – Beleid inzake aanvaardbaar gebruik: voorkomt gedrag dat wettelijke of contractuele voorwaarden kan schenden (bijvoorbeeld niet-geautoriseerd delen van bestanden).

10.1.2 P8S – Beleid inzake informatiebeveiligingsbewustzijn en opleiding: maakt medewerkers vertrouwd met nalevingsverplichtingen en met het voorkomen van overtredingen.

10.1.3 P14S – Gegevensbewarings- en vernietigingsbeleid: waarborgt rechtmatige praktijken voor gegevensverwerking gedurende de volledige levenscyclus van gegevens.

10.1.4 P17S – Beleid inzake gegevensbescherming en privacy: ondersteunt naleving van de AVG en van klantvereisten voor gegevensverwerking.

10.1.5 P30S – Incidentresponsbeleid: beschrijft hoe moet worden gereageerd op datalekken of tekortkomingen in de naleving, inclusief meldtermijnen.

10.1.6 P36S – Beleid inzake sociale media en externe communicatie: waarborgt dat openbare communicatie geen wettelijke of regelgevende verplichtingen schendt.

10.2 Elke gekoppelde beleidslijn borgt een deel van het juridisch nalevingskader en moet in onderlinge samenhang worden toegepast.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 6.1 – Maatregelen om risico's en kansen aan te pakken: omvat nalevingsrisico's.

11.1.2 Clausule 8.1 – Operationele planning en beheersing: vereist uitvoering van processen die voldoen aan wettelijke en contractuele vereisten.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 5.36 – Geeft richting aan het bijhouden van registraties van verplichtingen en het waarborgen van passende reacties op juridische en regelgevende vereisten.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Beleid en procedures: schrijft formele nalevingsbeleidslijnen voor.

11.3.2 PM-1 – Informatiebeveiligingsprogrammaplan: vereist integratie van juridische naleving in de beveiligingsplanning.

11.3.3 CA-1 – Beoordeling, autorisatie en monitoring.

11.3.4 AU-1 – Auditbeleid: vereist het bijhouden van nalevingsbewijsmateriaal.

11.4 EU AVG

11.4.1 Artikel 5 – Beginselen voor gegevensverwerking, waaronder verantwoordingsplicht.

11.4.2 Artikel 6 – Rechtsgrondslag voor verwerking.

11.4.3 Artikel 32 – Beveiliging van de verwerking.

11.4.4 Artikel 33 – Melding van inbreuken binnen 72 uur.

11.5 EU NIS2-richtlijn

11.5.1 Artikel 21(2)(a) en (f) – Interne beleidslijnen voor risico- en nalevingsbeheersing.

11.5.2 Artikel 23 – Handhaving en sancties bij tekortkomingen in de naleving.

11.6 EU DORA-verordening

11.6.1 Artikel 5(2) – Toezicht op ICT-risicobeheer.

11.6.2 Artikel 9(1) – Interne governance van naleving.

11.6.3 Artikel 17 – Contractuele afspraken met ICT-dienstverleners.

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: waarborgt dat nalevingsrisico's worden gemonitord en aangepakt.

11.7.2 APO13 – Managed Security: omvat risicogebaseerde handhaving van naleving van regelgeving en contractuele verplichtingen.

11.7.3 DSS01 – Managed Operations: schrijft operationele gereedheid voor om aan wettelijke verplichtingen te voldoen.