					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P37					Dokumenttitel: **Politik for juridisk og regulatorisk efterlevelse**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

1. Formål

1.1 Denne politik fastlægger den obligatoriske ramme for identifikation, styring og efterlevelse af alle juridiske, regulatoriske og kontraktuelle forpligtelser, der er relevante for organisationens informationssikkerhed, databeskyttelse og driftsfunktioner.

1.2 Formålet er at forebygge manglende efterlevelse, der kan medføre bøder, juridisk ansvar, driftsforstyrrelser, omdømmeskade eller regulatoriske sanktioner.

1.3 Denne politik understøtter integrationen af efterlevelseskrav i styring, risikostyring, operationelle arbejdsgange, projektlivscyklusser og systemdesign.

1.4 Den sikrer, at alle relevante forpligtelser – på tværs af jurisdiktioner, brancher og regulatoriske anvendelsesområder – dokumenteres, vurderes, overvåges og håndhæves tydeligt i organisationen.

2. Omfang

2.1 Denne politik gælder for alle afdelinger, funktioner, forretningsenheder og personer, der handler på vegne af organisationen, herunder:

2.1.1 Fastansatte og midlertidigt ansatte

2.1.2 Kontraktansatte, konsulenter og praktikanter

2.1.3 Tredjepartsleverandører, databehandlere eller partnere, der håndterer organisationens data, systemer eller regulatoriske forpligtelser

2.1.4 Enhver forretningsproces, ethvert projekt eller initiativ, der er underlagt juridiske eller regulatoriske krav

2.2 Efterlevelsesområder, der er omfattet af denne politik, omfatter blandt andet:

2.2.1 Krav vedrørende informationssikkerhed og cybersikkerhed (f.eks. ISO/IEC 27001, NIS2, DORA)

2.2.2 Lovgivning om databeskyttelse og privatliv (f.eks. GDPR, sektorspecifik databeskyttelseslovgivning)

2.2.3 Sektorspecifik regulering (f.eks. finans, sundhed, automotive, forsvar)

2.2.4 Kontraktuelle forpligtelser, der følger af fortrolighedsaftaler, service level agreements (SLA'er) eller databehandleraftaler

2.2.5 Juridiske krav vedrørende hændelsesrapportering, samarbejde med retshåndhævende myndigheder og internationale dataoverførsler

3. Mål

3.1 At sikre, at alle relevante love, regler, standarder og kontraktuelle forpligtelser identificeres, dokumenteres, fortolkes og håndhæves i hele organisationen.

3.2 At integrere juridiske og regulatoriske krav i organisationens ledelsessystem for informationssikkerhed (ISMS), risikostyringsprocesser, leverandøraftaler samt design af produkter og tjenester.

3.3 At etablere en mekanisme til proaktiv overvågning af regulatoriske ændringer og tilhørende opdatering af kontroller og dokumentation.

3.4 At fastlægge tydeligt ansvar for tilsyn med efterlevelse, eskalering af overtrædelser, håndtering af undtagelser og ekstern rapportering.

3.5 At sikre revisionssporbarhed og juridisk robusthed i organisationens efterlevelse af juridiske og regulatoriske krav under inspektioner, undersøgelser eller certificeringsgennemgange.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Har det overordnede strategiske ansvar for juridisk og regulatorisk efterlevelse på tværs af hele organisationen.

4.1.2 Gennemgår og godkender efterlevelsesbeslutninger med høj risiko, herunder risikoaccept og juridiske tvister.

4.2 Compliance-ansvarlig/juridisk chef/juridisk rådgiver

4.2.1 Vedligeholder registret over efterlevelsesforpligtelser, som omfatter alle relevante love, standarder, certificeringer og kontraktklausuler.

4.2.2 Gennemfører juridiske konsekvensvurderinger for nye tjenester, markeder eller dataflows.

4.2.3 Leverer autoritativ fortolkning af love og standarder.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Årlig gennemgang af politikken

9.1.1 Denne politik skal gennemgås mindst én gang pr. kalenderår for at:

9.1.1.1 Sikre fortsat overensstemmelse med opdaterede love, branchestandarder og regulatoriske rammer

9.1.1.2 Validere operationel effektivitet på baggrund af revisionskonstateringer og hændelseshistorik

9.1.1.3 Afspejle organisatoriske ændringer (f.eks. nye jurisdiktioner, systemer eller forretningsområder)

9.2 Udløsende forhold for gennemgang

9.2.1 Ekstraordinære gennemgange skal iværksættes, når:

9.2.2 Et nyt juridisk eller regulatorisk krav vedtages eller opdateres

9.2.3 En efterlevelseshændelse eller revision afdækker mangler i politikken

9.2.4 Organisationen går ind på et nyt marked eller en ny tjenestelinje, der er underlagt særskilte efterlevelsesrammer

9.2.5 Håndhævelsestendenser eller vejledning fra tilsynsmyndigheder indikerer ændringer i organisationens risikobillede

9.3 Ejerskab og godkendelse

9.3.1 Jura og compliance-ansvarlig er i fællesskab ansvarlige for koordinering af gennemgangsprocessen.

9.3.2 Endelige revisioner af politikken skal godkendes af direktionen og registreres i registret over politikændringer med tilhørende referencer til ændringsstyring og kommunikationsplaner.

9.4 Versionsstyring og kommunikation

9.4.1 Enhver opdateret version af denne politik skal:

9.4.1.1 Indeholde en sammenfatning af væsentlige ændringer

9.4.1.2 Redistribueres via officielle kanaler (f.eks. politikportal, læringsstyringssystem, interne nyhedsbreve)

9.4.1.3 Kræve bekræftelse fra berørt personale, særligt personer i juridiske, driftsmæssige, sikkerhedsmæssige og leverandørstyringsrelaterede roller

10. Relaterede politikker og sammenhænge

10.1 Denne politik anvendes sammen med og understøtter følgende politikker i organisationens ledelsessystem for informationssikkerhed (ISMS):

10.1.1 P1 – Informationssikkerhedspolitik: Fastlægger de grundlæggende styringsprincipper, der sikrer, at alle informationssikkerhedspolitikker – herunder efterlevelse – er tilpasset strategiske forretningsmæssige og regulatoriske krav.

10.1.2 P2 – Politik for styringsroller og ansvarsområder: Definerer beslutningskompetencer, herunder juridiske roller og compliance-roller med ansvar for regulatorisk tilsyn og ansvarlighed.

10.1.3 P6 – Politik for risikostyring: Understøtter vurdering, ejerskab og begrænsning af juridiske og regulatoriske efterlevelsesrisici på tværs af organisationen.

10.1.4 P8 – Politik for bevidsthed om informationssikkerhed og uddannelse: Sikrer, at alt personale er informeret om deres efterlevelsesansvar og modtager rollebaseret træning.

10.1.5 P12 – Politik for styring af aktiver: Understøtter juridiske forpligtelser ved styring og beskyttelse af regulerede eller kontraktuelle aktiver, herunder aktiver, der omfatter personoplysninger og kritisk infrastruktur.

10.1.6 P30 – Politik for hændelseshåndtering: Regulerer obligatoriske juridiske underretninger (f.eks. GDPR artikel 33) og eskalationsprocedurer i tilfælde af et efterlevelsesbrud eller en regulatorisk hændelse.

10.1.7 P33 – Politik for overvågning af revision og efterlevelse: Fastlægger strukturerede sikkerheds- og kontrolaktiviteter – herunder kontroltest og indsamling af bevismateriale – som kræves for intern og ekstern verifikation af efterlevelse.

11. Referencestandarder og rammeværk

11.1 ISO/IEC 27001

11.1.1 Klausul 4.2 – Forståelse af interesserede parters behov og forventninger: Kræver identifikation og integration af juridiske og regulatoriske krav i ISMS.

11.1.2 Klausul 5.1 – Lederskab og engagement: Pålægger den øverste ledelse ansvar for at etablere og opretholde juridisk efterlevelse i hele organisationen.

11.1.3 Klausul 5.3 – Organisatoriske roller, ansvar og beføjelser: Sikrer klarhed om roller for juridisk tilsyn og regulatorisk efterlevelse.

11.1.4 Bilag A, kontrol 5.36 – Efterlevelse af juridiske, lovgivningsmæssige, regulatoriske og kontraktuelle krav: Fastlægger kravet om at identificere og opfylde forpligtelser, der følger af love, regler og kontrakter.

11.2 ISO/IEC 27002

11.2.1 Kontrol 5.36: Beskriver vejledning til implementering af et register over efterlevelsesforpligtelser, validering af regulatoriske krav og sikring af struktureret opbevaring af bevismateriale.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PL-1 – Politik og procedurer for sikkerhedsplanlægning: Kræver, at efterlevelseskrav indarbejdes i styringsstrukturer og dokumentation.

11.3.2 PM-1 – Plan for informationssikkerhedsprogrammet: Pålægger regulatoriske kontroller som en del af det overordnede sikkerhedsprogram.

11.3.3 CA-7 – Løbende overvågning: Understøtter tilsyn med kontroludførelse i forhold til opfyldelse af juridiske krav og politikkrav.

11.3.4 AU-9 – Beskyttelse af revisionsoplysninger: Sikrer, at revisionslogfiler og registreringer vedrørende efterlevelse er beskyttede og tilgængelige for inspektion.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 5 – Principper for behandling: Kræver lovlighed, gennemsigtighed og ansvarlighed.

11.4.2 Artikel 6 – Lovlig behandling: Kræver et passende behandlingsgrundlag for alle databehandlingsaktiviteter.

11.4.3 Artikel 24 – Den dataansvarliges ansvar: Fastlægger et direkte ansvar for at sikre regulatorisk efterlevelse.

11.4.4 Artikel 32 – Behandlingssikkerhed: Kræver implementering af passende tekniske og organisatoriske kontroller.

11.4.5 Artikel 33 – Underretning om brud på persondatasikkerheden: Kræver, at brud på persondatasikkerheden anmeldes til relevante myndigheder inden for 72 timer.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 20–21: Kræver, at væsentlige og vigtige enheder implementerer dokumenteret styring, strategier for juridisk efterlevelse og løbende gennemgang af juridiske risici.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(2) – Styringsramme for IKT-risiko: Kræver integration af juridisk efterlevelse i bredere risikostyrings- og tilsynsfunktioner.

11.6.2 Artikel 19 – IKT-risici ved tredjepart: Pålægger specifikke juridiske krav til styring af kontraktuelle og regulatoriske forpligtelser vedrørende eksterne leverandører og platforme.

11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: Indarbejder juridisk og regulatorisk efterlevelse som kritiske elementer i virksomhedens risikostyring.

11.7.2 MEA03 – Monitor Compliance with External Requirements: Definerer løbende overvågning, håndtering af undtagelser og revisionsberedskab for alle former for regulatoriske forpligtelser.