					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P17S					Dokumenttitel: **Databeskyttelses- og privatlivspolitik**						
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**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Kontrol 5.34, 8.10–8	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
GDPR	Artikel 5, 6, 12-23, 30, 32-34	
NIS2-direktivet	Artikel 21(2)(e), 21(2)(f)	
DORA	Artikel 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Formål

1.1. Denne politik fastlægger, hvordan organisationen beskytter personoplysninger i overensstemmelse med lovkrav, regulatoriske rammer og internationale sikkerhedsstandarder.

1.2. Den sikrer, at personoplysninger — uanset om de vedrører kunder, medarbejdere eller partnere — indsamles, anvendes, opbevares og slettes lovligt, rimeligt og sikkert.

1.3. Denne politik understøtter også overholdelse af ISO/IEC 27001:2022 og styrker revisionsberedskabet ved at håndhæve en ensartet, risikobaseret tilgang til beskyttelse af privatliv.

1.4. Gennem denne politik udviser organisationen ansvarlighed og opbygger kundetillid ved at prioritere gennemsigtighed, dataminimering og stærk styring af databeskyttelse.

2. Omfang

2.1. Denne politik gælder for:

2.1.1. Alle medarbejdere, kontrahenter og tjenesteudbydere, der tilgår, behandler eller administrerer personoplysninger

2.1.2. Ethvert system, enhver applikation og enhver lokation, hvor personoplysninger opbevares eller overføres

2.1.3. Alle personoplysninger, uanset om de opbevares elektronisk, på papir, i cloudmiljøer eller på mobile enheder

2.2. Denne politik gælder for oplysninger om kunder, medarbejdere, leverandører og andre identificerbare personer.

2.3. Politikken gælder, uanset om oplysninger behandles internt eller af tredjepartsleverandører.

3. Mål

3.1. Sikre, at personoplysninger håndteres i overensstemmelse med databeskyttelseslovgivning og sikkerhedsstandarder, herunder GDPR, NIS2 og ISO/IEC 27001.

3.2. Beskytte personoplysninger mod uautoriseret adgang, misbrug, ændring eller tab gennem klare tekniske og organisatoriske kontroller.

3.3. Respektere de registreredes rettigheder, herunder retten til indsigt i, berigtigelse af og sletning af egne oplysninger.

3.4. Etablere klare roller og ansvar for databeskyttelse i organisationen.

3.5. Håndhæve dataminimering, sikker opbevaring og rettidig sletning på tværs af alle systemer og processer.

3.6. Reducere risikoen for manglende overholdelse, juridiske sanktioner, omdømmeskade og tab af kundetillid.

4. Roller og ansvar

4.1. Direktør (GM)

4.1.1. Godkender denne politik og sikrer, at den håndhæves

4.1.2. Stiller de nødvendige ressourcer til rådighed for at styre privatlivsrisici og reagere på hændelser

4.1.3. Har det overordnede ansvar for overholdelse af databeskyttelseslovgivning og standarder

4.2. Databeskyttelseskoordinator (intern eller outsourcet)

4.2.1. Vedligeholder fortegnelser over behandlingsaktiviteter

4.2.2. Håndterer anmodninger fra registrerede og henvendelser fra tilsynsmyndigheder

4.2.3. Understøtter risikovurderinger, træning og implementering af politikken

4.2.4. Dokumenterer brud på persondatasikkerheden og underretter myndigheder, når det er påkrævet

[... 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. Planlagte gennemgange

9.1.1. Denne politik skal gennemgås mindst én gang hver 12. måned af Databeskyttelseskoordinatoren og godkendes af direktøren

9.1.2. Gennemgangen skal vurdere politikkens relevans, regulatoriske tilpasning og operationelle effektivitet

9.2. Udløsende forhold for løbende gennemgang

9.2.1. Opdateringer af politikken skal også iværksættes som følge af:

9.2.1.1. Nye eller reviderede databeskyttelseslove (f.eks. GDPR, DORA)

9.2.1.2. Sikkerhedshændelser eller brud på persondatasikkerheden, der omfatter personoplysninger

9.2.1.3. Idriftsættelse af nye systemer, værktøjer eller tjenester, der behandler personoplysninger

9.2.1.4. Væsentlige revisionskonstateringer eller anbefalinger fra tilsynsmyndigheder

9.3. Styring af ændringer og kommunikation

9.3.1. Alle ændringer af politikken skal dokumenteres formelt i en ændringslog

9.3.2. Reviderede versioner skal distribueres til alle medarbejdere og relevante kontrahenter

9.3.3. Arkiverede versioner skal opbevares som revisionsspor for efterlevelse

10. Relaterede politikker og sammenhænge

10.1. Denne politik fungerer sammen med andre SME-politikker for at etablere en samlet og håndhævelig ramme for databeskyttelse:

10.1.1. P13S – Politik for dataklassificering og mærkning: Sikrer, at personoplysninger klassificeres korrekt, så beskyttelsesforanstaltninger kan anvendes ud fra risiko.

10.1.2. P14S – Politik for dataopbevaring og bortskaffelse: Fastlægger klare regler for, hvor længe personoplysninger skal opbevares, og hvilke sikre metoder der skal anvendes ved bortskaffelse, når opbevaringsperioden er udløbet.

10.1.3. P16S – Politik for datamaskering og pseudonymisering: Angiver, hvordan personhenførbare identifikatorer skal transformeres, før oplysninger anvendes i et ikke-produktionsmiljø eller deles eksternt.

10.1.4. P30S – Politik for hændelseshåndtering: Omfatter de trin, der kræves for at håndtere brud på persondatasikkerheden, herunder underretning af tilsynsmyndigheder og berørte registrerede inden for gældende frister.

10.1.5. P2S – Politik for styringsroller og ansvarsområder: Præciserer ansvarlighedsstrukturen og de beslutningsroller, der gælder for håndhævelse og tilsyn med databeskyttelse.

10.2. Disse relaterede politikker skal gennemgås og anvendes samlet for at sikre fuldstændig dækning af databeskyttelse på tværs af systemer, medarbejdere og leverandører.

11. Referencestandarder og rammeværker

11.1. ISO/IEC 27001

11.1.1. Klausul 5.1 – Kræver, at den øverste ledelse udviser lederskab og forpligtelse i beskyttelsen af personoplysninger.

11.1.2. Klausul 6.1.3 – Kræver behandling af risici relateret til behandling af personoplysninger.

11.1.3. Klausul 8.1 – Kræver implementering af operationelle kontroller for at beskytte oplysninger gennem hele deres livscyklus.

11.2. ISO/IEC 27002

11.2.1. Kontrol 5.34 – Giver implementeringsvejledning om beskyttelse af privatliv og sikker håndtering af personhenførbare oplysninger (PII).

11.2.2. Kontrol 8.10 – Omhandler sikker bortskaffelse af personoplysninger for at forhindre utilsigtet videregivelse af restdata.

11.2.3. Kontrol 8.11 – Understøtter anvendelse af maskering og pseudonymisering til dataminimering.

11.2.4. Kontrol 8.12 – Forebygger uautoriseret datalækage gennem kontroller for adgang til og brug af data.

11.3. NIST SP 800-53 Rev.

11.3.1. AR-2 – Tildeler roller og ansvar for styring af privatlivsrisici.

11.3.2. PL-5 – Kræver dokumentation af en databeskyttelsesplan, der dækker brug og beskyttelse af data.

11.3.3. AC-6 – Kræver mindst privilegie-princippet og adgangsstyring for personoplysninger.

11.3.4. IR-4 – Kræver hændelseshåndteringsprocedurer for brud, der omfatter personoplysninger.

11.4. GDPR

11.4.1. Artikel 5 – Fastlægger de grundlæggende principper for lovlig, rimelig og gennemsigtig behandling af oplysninger.

11.4.2. Artikel 6 – Kræver et gyldigt behandlingsgrundlag for hver behandlingsaktivitet vedrørende personoplysninger.

11.4.3. Artikel 12–23 – Beskriver de registreredes rettigheder, herunder indsigt, berigtigelse, sletning og indsigelse.

11.4.4. Artikel 30 – Kræver fortegnelser over behandlingsaktiviteter.

11.4.5. Artikel 32 – Kræver passende tekniske og organisatoriske kontroller.

11.4.6. Artikel 33–34 – Fastlægger pligter til underretning om brud på persondatasikkerheden til myndigheder og registrerede.

11.5. NIS2-direktivet

11.5.1. Artikel 21(2)(e) – Kræver foranstaltninger, der sikrer databeskyttelse i overensstemmelse med cybersikkerhedspolitikker.

11.5.2. Artikel 21(2)(f) – Kræver mekanismer til at styre sikkerheden for personoplysninger og fortrolige oplysninger i IKT-systemer.

11.6. DORA

11.6.1. Artikel 6 – Kræver interne styringsrammer, der håndterer datarisici og databeskyttelse.

11.6.2. Artikel 15 – Pålægger finansielle enheder at sikre, at tredjepartsleverandører beskytter personoplysninger og understøtter regulatorisk efterlevelse.

11.6.3. Artikel 17 – Kræver, at virksomheder sikrer, at IKT-systemer, der behandler personoplysninger, er sikre, robuste og overvågede.

11.7. COBIT 2019

11.7.1. APO12 – Styring af risiko: Kræver identifikation og behandling af privatlivs- og databeskyttelsesrisici.

11.7.2. DSS05 – Styring af sikkerhedstjenester: Kræver sikkerhedsforanstaltninger, der forhindrer uautoriseret adgang til personoplysninger.

11.7.3. MEA03 – Overvågning af overholdelse: Kræver, at organisationer sikrer løbende overholdelse af lovgivning om databeskyttelse og privatliv.