					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P17S					Dokumenttitel: **Policy för dataskydd och integritet**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausuler 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Kontroller 5.34, 8.10–8.12	
NIST SP 800-53 Rev. 5	AR-2, PL-5, AC-6, IR-4	
EU:s dataskyddsförordning (GDPR)	Artiklar 5, 6, 12–23, 30, 32–34	
EU:s NIS2-direktiv	Artikel 21.2 e, 21.2 f	
EU:s DORA-förordning	Artiklar 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Syfte

1.1. Denna policy fastställer hur organisationen skyddar personuppgifter i enlighet med rättsliga skyldigheter, regulatoriska ramverk och internationella säkerhetsstandarder.

1.2. Den säkerställer att personuppgifter – oavsett om de avser kunder, personal eller partner – samlas in, används, lagras och raderas på ett lagligt, korrekt och säkert sätt.

1.3. Denna policy säkerställer även efterlevnad av ISO/IEC 27001:2022 och stärker revisionsberedskapen genom att tillämpa ett konsekvent och riskbaserat arbetssätt för integritetsskydd.

1.4. Genom denna policy visar organisationen ansvarsskyldighet och stärker kundförtroendet genom att prioritera transparens, uppgiftsminimering och en stark styrning av integritetsskyddet.

2. Omfattning

2.1. Denna policy gäller för:

2.1.1. Samtliga anställda, uppdragstagare och tjänsteleverantörer som får åtkomst till, behandlar eller hanterar personuppgifter

2.1.2. Samtliga system, applikationer och platser där personuppgifter lagras eller överförs

2.1.3. Samtliga personuppgifter, oavsett om de lagras elektroniskt, i pappersform, i molnbaserade system eller på mobila enheter

2.2. Denna policy gäller för uppgifter som avser kunder, personal, leverantörer och andra identifierbara individer.

2.3. Policyn gäller oavsett om personuppgifter behandlas internt eller av tredjepartsleverantörer.

3. Mål

3.1. Säkerställa att personuppgifter hanteras i enlighet med dataskyddslagstiftning och säkerhetsstandarder, inklusive GDPR, NIS2 och ISO 27001.

3.2. Skydda personuppgifter mot obehörig åtkomst, missbruk, ändring eller förlust genom tydliga tekniska och organisatoriska säkerhetsåtgärder.

3.3. Respektera individers rättigheter avseende integritet, inklusive rätten till tillgång, rättelse och radering av personuppgifter.

3.4. Fastställa tydliga roller och ansvar för dataskydd inom organisationen.

3.5. Säkerställa uppgiftsminimering, säker bevarandehantering och radering i rätt tid i alla system och processer.

3.6. Minska risken för bristande efterlevnad, rättsliga sanktioner, anseendeskada och minskat kundförtroende.

4. Roller och ansvar

4.1. Verkställande chef (GM)

4.1.1. Godkänner denna policy och säkerställer att den tillämpas.

4.1.2. Tillhandahåller nödvändiga resurser för att hantera integritetsrisker och hantera incidenter.

4.1.3. Har det övergripande ansvaret för efterlevnad av dataskyddslagstiftning och tillämpliga standarder.

4.2. Integritetssamordnare (intern eller outsourcad)

4.2.1. Upprätthåller register över behandlingsaktiviteter avseende personuppgifter.

4.2.2. Hanterar registrerades begäranden och förfrågningar från tillsynsmyndigheter.

4.2.3. Stödjer riskbedömningar, utbildning och införandet av policyn.

4.2.4. Dokumenterar personuppgiftsincidenter och anmäler dem till myndigheter när så krävs.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav på granskning och uppdatering

9.1. Planerade granskningar

9.1.1. Denna policy ska granskas minst en gång var 12:e månad av integritetssamordnaren och godkännas av verkställande chef.

9.1.2. Granskningen ska bedöma policyns relevans, anpassning till regelverk och operativa effektivitet.

9.2. Utlösande faktorer för mellanliggande granskning

9.2.1. Policyuppdateringar ska även initieras som svar på:

9.2.1.1. Nya eller reviderade dataskyddslagar (t.ex. GDPR, DORA)

9.2.1.2. Säkerhetsincidenter eller integritetsincidenter som rör personuppgifter

9.2.1.3. Införande av nya system, verktyg eller tjänster som behandlar personuppgifter

9.2.1.4. Väsentliga revisionsiakttagelser eller rekommendationer från tillsynsmyndighet

9.3. Ändringsstyrning och kommunikation

9.3.1. Alla ändringar i policyn ska dokumenteras formellt i en ändringslogg.

9.3.2. Reviderade versioner ska distribueras till samtliga anställda och tillämpliga uppdragstagare.

9.3.3. Arkiverade versioner ska bevaras för efterlevnad och revisionsspår.

10. Relaterade policyer och kopplingar

10.1. Denna policy ska tillämpas tillsammans med andra SME-policyer för att skapa ett fullständigt och bindande ramverk för integritetsskydd:

10.1.1. P13S – Policy för informationsklassificering och märkning: Säkerställer att personuppgifter klassificeras på ett lämpligt sätt så att skyddsåtgärder för integritet kan tillämpas utifrån risk.

10.1.2. P14S – Policy för bevarande och bortskaffande av data: Anger tydliga regler för hur länge personuppgifter ska bevaras och vilka säkra metoder som ska användas när de inte längre ska bevaras.

10.1.3. P16S – Policy för datamaskering och pseudonymisering: Anger hur personidentifierande uppgifter ska omvandlas innan data används i icke-produktionsmiljö eller delas externt.

10.1.4. P30S – Policy för incidenthantering: Omfattar de steg som krävs för att hantera personuppgiftsincidenter, inklusive anmälan till tillsynsmyndigheter och berörda individer inom fastställda tidsfrister.

10.1.5. P2S – Policy för styrningsroller och ansvar: Tydliggör ansvarsskyldighetsstrukturen och de beslutsroller som gäller för tillämpning och tillsyn av dataskydd.

10.2. Dessa relaterade policyer ska granskas och tillämpas tillsammans för att säkerställa ett heltäckande integritetsskydd i system, för personal och hos leverantörer.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 5.1 – Kräver att högsta ledningen visar ledarskap och engagemang för att skydda personuppgifter.

11.1.2. Klausul 6.1.3 – Kräver behandling av risker relaterade till behandling av personuppgifter.

11.1.3. Klausul 8.1 – Kräver att operativa kontroller införs för att skydda data genom hela dess livscykel.

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.34 – Ger vägledning för skydd av integritet och säker hantering av PII.

11.2.2. Kontroll 8.10 – Omfattar säker bortskaffning av personuppgifter för att förhindra kvarstående röjande.

11.2.3. Kontroll 8.11 – Stödjer användning av maskering och pseudonymisering för uppgiftsminimering.

11.2.4. Kontroll 8.12 – Förhindrar obehörigt dataläckage genom kontroller för dataåtkomst och dataanvändning.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AR-2 – Tilldelar roller och ansvar för hantering av integritetsrisker.

11.3.2. PL-5 – Kräver dokumentation av en integritetsplan som omfattar dataanvändning och skydd.

11.3.3. AC-6 – Kräver principen om minsta privilegium och åtkomstkontroller för personuppgifter.

11.3.4. IR-4 – Kräver incidenthanteringsrutiner för incidenter som rör personuppgifter.

11.4. EU:s dataskyddsförordning (GDPR)

11.4.1. Artikel 5 – Fastställer de grundläggande principerna för laglig, korrekt och transparent behandling av personuppgifter.

11.4.2. Artikel 6 – Kräver giltig rättslig grund för varje behandling av personuppgifter.

11.4.3. Artiklarna 12–23 – Beskriver registrerades rättigheter, inklusive tillgång, rättelse, radering och invändning.

11.4.4. Artikel 30 – Kräver register över behandlingsaktiviteter.

11.4.5. Artikel 32 – Kräver lämpliga tekniska och organisatoriska säkerhetsåtgärder.

11.4.6. Artiklarna 33–34 – Fastställer skyldigheter att anmäla personuppgiftsincidenter till myndigheter och registrerade.

11.5. EU:s NIS2-direktiv

11.5.1. Artikel 21.2 e – Kräver åtgärder för att säkerställa dataskydd i linje med cybersäkerhetspolicyer.

11.5.2. Artikel 21.2 f – Kräver mekanismer för att hantera säkerheten för personuppgifter och konfidentiella uppgifter i IKT-system.

11.6. EU:s DORA-förordning

11.6.1. Artikel 6 – Kräver interna styrningsramverk som hanterar datarisker och dataskydd.

11.6.2. Artikel 15 – Ålägger finansiella entiteter att säkerställa att tredjepartsleverantörer skyddar personuppgifter och stödjer regulatorisk efterlevnad.

11.6.3. Artikel 17 – Kräver att organisationer säkerställer att IKT-system som behandlar personuppgifter är säkra, resilienta och övervakade.

11.7. COBIT 2019

11.7.1. APO12 – Hantera risk: Kräver identifiering och behandling av integritets- och dataskyddsrisker.

11.7.2. DSS05 – Hantera säkerhetstjänster: Kräver skyddsåtgärder för att förhindra obehörig åtkomst till personuppgifter.

11.7.3. MEA03 – Övervaka efterlevnad: Kräver att organisationer säkerställer löpande efterlevnad av dataskyddslagstiftning och regler om integritetsskydd.