



Dataskyddspolicy

Sibbo kommun

Innehåll

1 Centrala begrepp i dataskyddspolicyn.....	2
2 Dataskyddspolicyns betydelse	3
3 Dataskyddsroller och -ansvar	4
4 Centrala dokument.....	6
5 Planering och rapportering.....	6
6 Behandling av personuppgifter	7
6.1 Principer för behandling av personuppgifter	7
6.2 Riskbaserat förhållningssätt och riskhantering	8
6.3 Inbyggt dataskydd och dataskydd som standard	8
6.4 De registrerades rättigheter	8
6.5 Personuppgiftsincidenter.....	9
6.6 Tredje parter och överföring av personuppgifter	9
7 Utbildning och ökad medvetenhet.....	9
8 Dokumentets uppgifter och versionshistorik.....	10

1 Centrala begrepp i dataskyddspolicyn

Dataskydd	Dataskydd avser en grundläggande rättighet som tryggar var och ens rättigheter och friheter i behandling av personuppgifter. Dataskyddet fastställer principer för när, under vilka förutsättningar och hur personuppgifter kan behandlas.
Datasäkerhet	Datasäkerhet avser skyddet av data och informationsmaterial. Datasäkerhet innebär konkreta säkerhetsåtgärder som kommunen vidtar för att skydda data och datautrustning. Datasäkerhet är starkt förknippad med förverkligande av principerna för dataskyddet.
Informationssäkerhet	Informationssäkerhet är ett omfattande begrepp som avser allt skydd av data och den information som data representerar. Med hjälp av informationssäkerhet försäkras man uppgifternas integritet, tillgänglighet och användbarhet. Bland annat skyddet av uppgifter, informationsmaterial, utrustningar, programvaror, datakommunikation, lokaler och verksamhet ingår i informationssäkerheten.
Personuppgifter	Personuppgifter är alla sådana uppgifter utifrån vilka en person kan identifieras. En person kan identifieras om uppgiften kan förknippas med personen antingen direkt eller indirekt genom att till exempel kombinera en enskild uppgift med en annan uppgift.
Behandling av personuppgifter	Behandling av personuppgifter avser alla åtgärder som riktas mot personuppgifter, såsom insamling, upptagning, lagring, redigering, ändring, sökning, överlåtelse och förstöring.
Personuppgiftsansvarig	Den personuppgiftsansvarige avser en person eller en organisation som fastställer syftet och metoderna för behandlingen av personuppgifter eller vars uppgift behandlingen av personuppgifter är enligt lag. Den personuppgiftsansvarige svarar för den behandling av personuppgifter som denne utför.
Den registrerade	Den registrerade avser en person vars personuppgifter den personuppgiftsansvarige behandlar. EU:s dataskyddsförordning ger den registrerade olika rättigheter beroende på grunden för behandling av personuppgifter.
Personuppgiftsbiträde	Personuppgiftsbiträde avser en person eller en organisation som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Till exempel en serviceproducent som den personuppgiftsansvarige använder. Personuppgiftsbiträde avser inte organisationens egna anställda.
Konsekvensbedömning av dataskydd (DPIA)	Dataskyddsrisker ska alltid bedömas då man behandlar personuppgifter. Konsekvensbedömningen av dataskydd ska göras innan behandling av personuppgifter inleds. Konsekvensbedömningen är en närmare evaluering av innehållet i den planerade behandlingen, behandlingens proportionalitet i förhållande till den registrerade och de risker som eventuellt orsakas för de registrerades personuppgifter. Konsekvensbedömningen ska göras om det är sannolikt att behandlingen orsakar en hög risk för en fysisk persons rättigheter och friheter.

Personuppgiftsbiträdesavtal (PUB-avtal, DPA)	Med ett personuppgiftsbiträdesavtal kommer den personuppgiftsansvarige och personuppgiftsbiträdet överens om hur biträdet ska skydda de personuppgifter som den personuppgiftsansvarige överläter till biträdet. Avtalet ska innehålla bestämmelser om bland annat hur länge behandlingen av personuppgifter varar, det geografiska läget för behandlingen, behandlingens art och ändamål, typen av personuppgifter och kategorier av registrerade.
---	---

2 Dataskyddspolicyns betydelse

Dataskyddspolicyn är den handling som fastställer genomförandet och hanteringen av dataskyddet på den högsta nivån. Syftet med dataskyddspolicyn är att fastställa de åtgärder med vilka Sibbo kommun stävar efter att säkerställa att behandlingen av personuppgifter följer dataskyddsförordningen och annan lagstiftning om behandling av personuppgifter. Dataskyddspolicyn fastställer de principer, verksamhetssätt och ansvarsområden samt den övervakning som Sibbo kommun följer i genomförandet och utvecklingen av dataskyddet i kommunen. Principerna i dataskyddspolicyn och hur de tillämpas kan preciseras med riktlinjer och krav, praxis, anvisningar och andra dataskydds- och informationssäkerhetsdokument. Med dataskyddspolicyn förbinder Sibbo kommun sig till att behandla personuppgifter på ett ansvarsfullt och jämlikt sätt med respekt för de registrerades rättigheter.

Dataskyddspolicyn ålägger Sibbo kommuns personal, ledning, förtroendevalda, tjänsteinnehavare samt alla andra personer som behandlar uppgifter hos eller för kommunen, såsom konsulter, underleverantörer och intressentgrupper, oberoende av uppgifternas format. Även kommunens serviceleverantörer och intressentgrupper ska beakta dataskyddspolicyn i sin verksamhet. Dataskyddspolicyn gäller all verksamhet i Sibbo kommun.

Kommunstyrelsen har godkänt dataskyddspolicyn. Dataskyddspolicyn granskas årligen och vid behov oftare om betydande ändringar sker i dataskyddspraxis, lagstiftningen eller myndighetsanvisningarna. Granskningens avsikt är att säkerställa policyns aktualitet och effektivitet. Sibbo kommuns dataskyddsansvarig ansvarar för granskningen av dataskyddspolicyn.

3 Dataskyddsroller och -ansvar

Dataskyddsroller och -ansvar fördelas i Sibbo kommun enligt tabellen nedan:

Kommunstyrelsen	Kommunstyrelsen leder och övervakar dataskyddet och allokerar resurser för dataskyddsarbetet.
Kommundirektör	Dataskyddet i kommunen är i kommundirektörens besittning. Hen ska se till att dataskyddet kan genomföras på ett vederbörligt sätt. Kommundirektören tillsätter en dataskydds- och datasäkerhetsgrupp, som uppföljer genomförandet av dataskydd och informationssäkerhet, ger utvecklingsförslag och erbjuder stöd till sektorerna, systemadministratörerna, uppgifternas ägare och de personuppgiftsansvariga.
Dataskydds- och datasäkerhetsgruppen	Dataskydds- och datasäkerhetsgruppen har som uppgift att uppfölja dataskyddets förverkligande, ge utvecklingsförslag och erbjuda stöd till den dataskyddsansvariga, sektorerna, huvudanvändarna av system, uppgifternas ägare och de personuppgiftsansvariga. Dataskydds- och datasäkerhetsgruppen fungerar som expert i utveckling av dataskyddet och som främjare av dataskyddet i organisationen samt anpassar de gemensamma modellerna för den egna organisationens verksamhet. Dataskydds- och datasäkerhetsgruppen ansvarar för styrning av datasäkerhetsprocesserna och för deras integrering i det övergripande säkerhetsarbetet samt för kommunikation om informationssäkerhetsärenden inom ramen för de resurser och behörigheter som beviljats gruppen av kommunens ledning. Uppgiften inkluderar även anvisningar för och koordinering av hanteringen av datasäkerhetsrisker och informationssäkerhetsincidenter. Den dataskyddsansvarige fungerar som dataskydds- och datasäkerhetsgruppens ordförande.
Dataskyddsansvarig	Sibbo kommun har en utsedd dataskyddsansvarig i enlighet med dataskyddsförordningen och meddelat till tillsynsmyndigheten som ansvarar för dataskyddet om den dataskyddsansvarige. Den dataskyddsansvariges uppgifter inkluderar lagstadgade uppgifter enligt dataskyddsförordningen. Den dataskyddsansvarige ger råd i lagenlig behandling av personuppgifter, övervakar uppföljning av dataskyddslagstiftning och goda dataskyddspraxis och fungerar som kontakt med tillsynsmyndigheten. Den dataskyddsansvarige rapporterar till kommunens högsta ledning om hur dataskyddet genomförs.
Digital förvaltning	Enheten Digital förvaltning ansvarar för genomförandet av datasäkerhet och teknisk övervakning i informationssystemmiljön med hjälp av de metoder som står till deras förfogande enligt

	lagen och som de har befullmäktigats till i samband med samarbetsförfarandet. Enheten ansvarar för fastställande och ordnande av den tekniska datasäkerheten. Enheten ansvarar också för systemet för identitetshantering och kontroll av användarrättigheter i enlighet med den nationella lagstiftningen och de EU-förordningar som tillämpas.
Sektorns ledning	Sektorns ledning ansvarar för att dataskyddet genomförs inom sektorns verksamhet. Sektorns ledning ansvarar för de system, register, informationsmaterial och datalager som sektorn äger. Ledningen säkerställer att medlemmarna i dataskydds- och datasäkerhetsgruppen har tillräckliga resurser och nödvändigt kunnande att sköta sin uppgift.
Chefer	Cheferna ansvarar för att dataskyddet genomförs i de underlydande funktionerna. Cheferna rapporterar om dataskydds- och datasäkerhetsärenden till sektorns ledning och den dataskyddsansvarige.
Tjänsteinnehavare, anställda, de förtroendevalda och övriga personer som är jämförbara med ett anställningsförhållande	Var och en ansvarar för sin del att dataskyddet genomförs i de egna arbetsuppgifterna. Det är på var och ens ansvar att utan dröjsmål meddela sin chef eller kommunens dataskyddsansvarige, alternativt den part som är ansvarig för serviceproduktionen eller verksamheten, om man upptäcker något hot eller någon risk eller överträdelse gällande dataskydd.
Ägare av en uppgift, ett datasystem eller en tjänst	Ägaren ansvarar för att definiera och godkänna systemanvändare och deras användarrättigheter, att genomföra riskhanteringsmetoder, att garantera uppgifternas integritet och att klassificera uppgifterna (definiera vilka uppgifter är offentliga respektive sekretessbelagda samt utarbeta en arkivbildningsplan) samt att förstöra uppgifterna.

4 Centrala dokument

Sibbo kommun förbinder sig till att i enlighet med ansvarsskyldigheten uppvisa att kommunens verksamhet följer dataskyddslagstiftningen enligt dataskyddsförordningen.

Sibbo kommuns centrala dokument för att uppfylla kraven på överensstämmelse och ansvarsskyldighet är:

Dataskyddspolicy	Dataskyddspolicyn beskriver principer för dataskyddet, mål för hanteringen av dataskyddet, dataskyddets organisering och ansvar samt praxis för dataskyddet.
Informationssäkerhetspolicy	Informationssäkerhetspolicyn fastställer Sibbo kommuns praxis för informations- och datasäkerhet.
Register över behandling	Registret över behandling är en intern beskrivning av organisationens behandling av personuppgifter och behandlingens syften.
Informeringsdokument till de registrerade	Dataskyddsbeskrivningarna och andra dokument som är avsedda för informering av de registrerade beskriver på ett transparent sätt hur de registrerades personuppgifter behandlas.
Bedömningar av dataskyddet och riskbedömningar	Kommunens förhandsbedömningar av dataskyddet, konsekvensbedömningar av dataskyddet och jämviktstester för ett berättigat intresse.
Årsplan för dataskyddet	I årsplanen för dataskyddet antecknas uppgifterna inom dataskyddsarbetet för varje månad. Årsplanen för dataskyddet används för att uppfölja hur dataskyddsarbetet framskrider.
Utbildningsplan	I utbildningsplanen fastställs planerade dataskyddsutbildningar för kommunens personal.
Personuppgiftsbiträdesavtal	I personuppgiftsbiträdesavtalet fastställs avtalsvillkor för personuppgiftsbiträden.
Dokument gällande rättsliga grunder för behandlingen av personuppgifter	Dokument gällande samtycke och nödvändiga bedömningar, såsom jämviktstest för berättigat intresse.
Dokument gällande behandling av de registrerades begäranden	Anvisningar gällande förverkligande av de registrerades rättigheter, blanketter gällande begärandena och dokumentmallar för dokumentering.
Dokument för behandling av personuppgiftsincidenter	Anvisningar och dokument för hantering av personuppgiftsincidenter.

5 Planering och rapportering

Sibbo kommun planerar dataskyddsarbetet med hjälp av årsplanen för dataskyddet. I årsplanen fördelas uppgifterna inom dataskyddsarbetet för hela året. Enligt årsplanen kan arbetsuppgifterna delegeras till ansvariga personer.

Kommunens dataskyddsarbete sammanställs till ett databokslut i slutet av året. Databokslutet bifogas till kommunens bokslut och godkänns av kommunfullmäktige.

6 Behandling av personuppgifter

6.1 Principer för behandling av personuppgifter

Sibbo kommun följer den gällande lagstiftningen när den behandlar uppgifter om kunder, kommuninvånare, kommunens personal och andra intressentgrupper. Nedan beskrivs principer för behandling av personuppgifter enligt dataskyddsförordningen, som Sibbo kommun följer i all behandling av personuppgifter.

Lagenlighet, korrekthet och transparens	Behandlingen av personuppgifter följer dataskyddsförordningen och andra bestämmelser om behandling av personuppgifter. Personuppgifter behandlas korrekt och rimligt i förhållande till behandlingens syfte, med beaktande av informationsskyldigheten och bundenheten till användningsändamålet. Den registrerade informeras om behandlingen på ett tydligt och begripligt sätt.
Bundenhet till användningsändamålet	Behandlingen av personuppgifter planeras i förväg och behandlingen grundar sig alltid på ett tydligt definierat, uttryckligt och lagenligt syfte. Personuppgifterna behandlas inte senare på ett sätt som inte passar ihop med de ursprungliga syftena. Nya användningsändamål meddelas till den registrerade före behandlingen.
Exakthet, uppgiftsminimering och lagringsminimering	Strävan är att säkerställa personuppgifternas riktighet. Felaktiga personuppgifter raderas eller korrigeras utan dröjsmål. Personuppgifter samlas in och behandlas endast i den mån som är ändamålsenligt och nödvändigt med tanke på behandlingens syfte. Uppgifterna som behandlas ska vara korrekta, det vill säga det ska finnas ett fastställt användningsändamål för uppgifterna. Uppgifterna ska vara väsentliga och avgränsade, det vill säga nödvändiga för användningsändamålet. Uppgifterna lagras endast så länge som det är nödvändigt för att uppfylla det fastställda användningsändamålet. Lagringstiderna för personuppgifterna fastställs och dokumenteras.
Uppgifternas konfidentialitet och säkerhet	Personuppgifterna behandlas konfidentiellt och säkert. Skyddsåtgärdernas tillräcklighet ska ställas i proportion till behandlingens förhållanden och risker. Personuppgifterna skyddas med tekniska och organisatoriska skyddsåtgärder för att säkerställa den ändamålsenliga integriteten, konfidentialiteten och säkerheten, med beaktande av skydd mot olovlig och lagstridig behandling eller mot förlust, förstöring eller skada genom olyckshändelse.

	Personalen och avtalsparterna ska följa anvisningar om behandlingen av personuppgifter och datasäkerhetspraxis.
--	---

6.2 Riskbaserat förhållningssätt och riskhantering

Sibbo kommun följer ett riskbaserat förhållningssätt i all behandling av personuppgifter och planerar åtgärderna och skyddsåtgärderna i förhållande till de risker som är förknippade med behandlingen av personuppgifter. Behandlingen av personuppgifter planeras och genomförs under uppgifternas hela livscykel enligt dataskyddsprinciperna och andra lämpliga bestämmelser således att principerna om inbyggt dataskydd och dataskydd som standard uppfylls.

Sibbo kommun bedömer risker med anknytning till behandlingen av personuppgifter i sin verksamhet, inklusive upphandling av nya system, samarbete med nya leverantörer och befintliga behandlingsåtgärder. Risknivån bedöms och en konsekvensbedömning av dataskydd som avses i dataskyddsförordningen utförs för behandlingsåtgärder i sådana fall som lagen förutsätter. Resultaten av denna konsekvensbedömning används för att fastställa metoder för att hantera och minska risknivån i samband med behandlingen av personuppgifter.

6.3 Inbyggt dataskydd och dataskydd som standard

Sibbo kommun följer principerna för inbyggt dataskydd och dataskydd som standard. Behandlingen av personuppgifter följer de principer för behandling av personuppgifter som bestäms i dataskyddsförordningen och andra bestämmelser om behandling av personuppgifter.

Dessa tekniska och organisatoriska åtgärder garanterar att man som standard samlar in enbart sådana personuppgifter som är nödvändiga för behandlingsändamålet. Dataskyddsprinciperna beaktas i all verksamhet redan i det tidigaste möjliga skedet och nödvändiga tekniska och organisatoriska åtgärder vidtas i förhållande till risknivån.

6.4 De registrerades rättigheter

Sibbo kommun säkerställer att de registrerades rättigheter uppfylls enligt dataskyddsförordningen genom att upprätthålla och utveckla nödvändiga praxis.

De registrerades rättigheter verkställs på ett lämpligt sätt för varje situation med beaktande av den rättsliga grunden för behandlingen och i vilken situation personuppgifterna behandlas. De registrerade informeras transparent om behandlingen av personuppgifter. Enligt de rättsliga grunderna har en registrerad rätt att bl.a. få information om behandlingen av sina personuppgifter, få tillgång till sina uppgifter, rätta uppgifterna, förstöra uppgifterna, begränsa behandlingen av uppgifterna, överföra uppgifterna mellan system, göra en invändning mot behandling av sina personuppgifter och inte bli föremål för automatiskt beslutsfattande.

De registrerades begäran behandlas på det sätt och inom den tidsfrist som lagen förutsätter. Ändamålsenliga processer har fastställts för behandling av de registrerades begäranden.

6.5 Personuppgiftsincidenter

Sibbo kommun strävar efter att minimera personuppgiftsincidenter genom att planera behandlingen av personuppgifter enligt dataskyddsprinciperna och vidta tekniska och organisatoriska skyddsåtgärder som anpassas till de risker som behandlingen av personuppgifter medför för de registrerade.

Det finns lämpliga processer, anvisningar för och praxis för dokumentering av identifiering, anmälning och behandling av personuppgiftsincidenter. Personuppgiftsincidenterna behandlas på det sätt och inom den tidsfrist som lagen förutsätter. Om en personuppgiftsincident redan har skett, vidtas åtgärder enligt den utarbetade anvisningen.

Varje anställd i organisationen och varje person som arbetar för organisationens räkning är förpliktad att göra en anmälan om de upptäcker risker, avvikelser eller övriga dylika situationer som kan äventyra personuppgifterna.

6.6 Tredje parter och överföring av personuppgifter

Dataskyddet beaktas i kommunens avtal med andra parter. När kommunen ingår avtal säkerställer man att uppfyllandet av kraven på dataskyddsbestämmelserna beaktas i avtalsvillkoren. Kommunen ingår skriftliga avtal om behandling av personuppgifter i enlighet med dataskyddslagstiftningen med alla personuppgiftsbiträden som Sibbo kommun använder.

Dataskyddsrisker som hänför sig till tredje parter bedöms och hanteras genom att utföra nödvändiga riskbedömningar och ställa minimikrav på behandlingen av personuppgifter innan samarbetet med de tredje parterna inleds.

Sibbo kommun överför i princip inte personuppgifter utanför Europeiska unionen eller det Europeiska ekonomiska samarbetsområdet. Kommunen följer gällande lagar och förordningar vid eventuella överföringar av personuppgifter, och personuppgifterna överförs med en ändamålsenlig överföringsgrund.

7 Utbildning och ökad medvetenhet

Anvisningar om behandlingen av personuppgifter är nödvändiga i de arbetsuppgifter i vilka man behandlar personuppgifter. Anvisningarna ska upprättas med beaktande av dataskyddsprinciperna. Informering om dataskyddsärenden sker transparent inom organisationen.

Sibbo kommun ordnar en grundutbildning i dataskydd för personalen i samband med introduktionen. Att tillägna innehållet i dataskyddspolicyn är en del av introduktionen för nyanställda. Grundutbildning i dataskydd erbjuds regelbundet, och fördjupad utbildning ordnas enligt uppgiftsrelaterade behov. För att garantera personalens kunskande förutsätter kommunen därtill att samtliga anställda utför årligen en utbildning i datasäkerhet och dataskydd.

Utbildningar i dataskydd planeras och utbildningsplanen uppföljs regelbundet.

8 Dokumentets uppgifter och versionshistorik

Version	Datum	Ändringar	Gjord av
1.0	24.10.2022	Den första godkända versionen	Privaon Oy
2.0	24.2.2025	Den andra godkända och publicerade versionen	Den dataskyddsansvarige, Sibbo kommun

Dokumentets namn	Sibbo kommuns dataskyddspolicy
Ägare	Den dataskyddsansvarige
Godkänt av	Kommunstyrelsen
Datum för godkännandet	29.09.2025