



Dataskyddspolicy

Sibbo kommun

7.10.2022

Innehåll

1 Centrala begrepp i dataskyddspolicyn	2
2 Vikten av dataskyddspolicyn	3
3 Dataskyddets roller och ansvar.....	3
4 Centrala dokument	5
5 Planering och rapportering.....	6
6 Behandling av personuppgifter	6
6.1 Principerna för behandling av personuppgifter	6
6.2 Riskbaserat förhållningssätt och riskhantering	7
6.3 Inbyggt dataskydd och dataskydd som standard	7
6.4 Registrerades rättigheter	7
6.5 Personuppgiftsincidenter.....	8
6.6 Tredje part och överföring av personuppgifter	8
7 Utbildning och ökad medvetenhet.....	8
8 Dokumentinformation och versionshistorik.....	9

1 Centrala begrepp i dataskyddspolicyn

Dataskydd	Dataskydd innebär en grundläggande rättighet som tryggar var och ens rättigheter och friheter vid behandling av personuppgifter. Dataskyddet fastställer principerna för när, under vilka förutsättningar och hur personuppgifter kan behandlas.
Datasäkerhet	Datasäkerheten säkerställer datas konfidentialitet, integritet, tillgänglighet och användbarhet. Datasäkerheten är nära förknippad med genomförandet av dataskyddsprinciperna.
Personuppgifter	Personuppgifter är alla sådana uppgifter som kan användas för att identifiera en person. En person kan identifieras om en uppgift kan kopplas till personen, antingen direkt eller indirekt, till exempel genom att kombinera uppgiften med en annan uppgift.
Behandling av personuppgifter	Med behandling av personuppgifter avses alla åtgärder som riktar sig till personuppgifter, såsom insamling, lagring, bevaring, redigering, ändring, hämtning, utlämnande och radering.
Personuppgiftsansvarig	Med personuppgiftsansvarig avses den person eller organisation som bestämmer ändamålen och medlen för behandlingen av personuppgifter eller som enligt lag har anförtrots behandlingen av personuppgifter. Den personuppgiftsansvarige ansvarar för den behandling av personuppgifter som utförs av denne.
Den registrerade	Den registrerade är den person vars personuppgifter behandlas av den personuppgiftsansvarige. EU:s dataskyddsförordning ger olika rättigheter till registrerade personer beroende på grunderna för behandlingen av personuppgifter.
Personuppgiftsbiträde	Personuppgiftsbiträdet är en person eller organisation som behandlar personuppgifter för den personuppgiftsansvariges räkning. Till exempel en tjänsteleverantör som används av den personuppgiftsansvarige. Med personuppgiftsbiträde avses inte organisationens egna anställda.
Konsekvensbedömning avseende dataskydd	Dataskyddsriskerna måste alltid bedömas när personuppgifter behandlas. En konsekvensbedömning av dataskyddet ska göras innan behandlingen av personuppgifter inleds för att mer exakt bedöma innehållet i den planerade behandlingen, proportionaliteten i förhållande till den registrerade och riskerna som personuppgifterna utsätts för. En konsekvensbedömning ska göras om behandlingen sannolikt innebär en hög risk för en fysisk persons rättigheter och friheter.

2 Vikten av dataskyddspolicyn

Dataskyddspolicyn är det övergripande dokument som definierar genomförandet och hanteringen av dataskyddet. Syftet med dataskyddspolicyn är att definiera hur Sibbo kommun strävar efter att säkerställa efterlevnaden av dataskyddsförordningen och annan lagstiftning som är tillämplig på behandlingen av personuppgifter. Dataskyddspolicyn fastställer de principer, verksamhetssätt, ansvarsområden och tillsyn som Sibbo kommun följer i genomförandet och utvecklingen av dataskyddet i kommunen. Principerna som följer av dataskyddspolicyn samt deras tillämpning kan specificeras med riktlinjer och krav, rutiner, instruktioner och annan dokumentation om dataskydd och datasäkerhet. Genom sin dataskyddspolicy förbinder sig Sibbo kommun att behandla personuppgifter på ett ansvarsfullt och rättvist sätt och att respektera de registrerades rättigheter.

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

Kommunstyrelsen har godkänt dataskyddspolicyn. Dataskyddspolicyn ses över årligen och vid behov oftare om det sker betydande förändringar i dataskyddsrutinerna, lagstiftningen eller myndigheternas anvisningar. Syftet med översynen är att säkerställa att policyn är aktuell och effektiv. Sibbo kommuns dataskyddsombud ansvarar för översynen av dataskyddspolicyn.

3 Dataskyddets roller och ansvar

Dataskyddets roller och ansvar i Sibbo kommun är fördelade enligt tabellen nedan:

Kommunstyrelsen	Ansvarar för ledningen, resurstilldelningen och övervakningen av dataskyddsarbetet.
Kommundirektören	Innehar uppgiften som ägare av dataskyddet i kommunen och skapar förutsättningar för ett korrekt genomförande av dataskyddet.
Arbetsgruppen för dataskydd och datasäkerhet	Sibbo kommun har en arbetsgrupp för dataskydd och datasäkerhet, som inrättades genom tjänsteinnehavarbeslut av kommundirektören den 8 november 2021. Arbetsgruppens uppgift är att följa upp hur dataskyddet genomförs, ge utvecklingsförslag och stödja dataskyddsombudet och systemadministratörerna. Arbetsgruppens roll är att vara expert och främjare av utvecklingen av dataskyddet i organisationen och anpassa de gemensamma modellerna till den egna organisationens verksamhet. Dataskyddsombudet är arbetsgruppens ordförande.

Dataskyddsbudjet	<p>Dataskyddsbudjet som utsetts för Sibbo kommun i enlighet med dataskyddsförordningen har meddelats till tillsynsmyndigheten som ansvarar för dataskydd. Dataskyddsbudjets uppgifter omfattar de lagstadgade uppgifterna som föreskrivs i dataskyddsförordningen.</p> <p>Dataskyddsbudjet ger råd om lagenlig behandling av personuppgifter, övervakar efterlevnaden av dataskyddslagstiftningen och god dataskyddspraxis och fungerar som kontaktpunkt för tillsynsmyndigheten.</p> <p>Dataskyddsbudjet rapporterar till kommunens högsta ledning om hur dataskyddet genomförs.</p>
Sektorledningen	<p>Ansvarar för att dataskyddet genomförs i den verksamhet som leds av den.</p>
Cheferna	<p>Ansvarar för att dataskyddet genomförs i den verksamhet som är underordnad dem. Cheferna rapporterar om dessa ärenden både till sektorledningen och till dataskyddsbudjet.</p>
Tjänsteinnehavarna, arbetstagarna, de förtroendevalda och andra personer i en position som kan jämföras med ett anställningsförhållande	<p>Ansvarar för egen del för genomförandet av dataskyddet i sina egna arbetsuppgifter. Det är på var och ens ansvar att utan dröjsmål meddela sin chef eller kommunens dataskyddsbudjet, alternativt den part som är ansvarig för en serviceproduktion eller verksamhet, om man upptäcker något hot, risk eller överträdelse gällande dataskydd.</p>
Ägaren av data, datasytem eller en tjänst	<p>Ansvarar med avseende på sitt ägande för definieringen och godkännandet av användare och deras användarrättigheter, implementeringen av riskhantering, säkerställande av dataintegritet och klassificeringen av data (definiering av offentlighet och sekretess samt arkivbildning).</p>

4 Centrala dokument

I enlighet med den ansvarsskyldighet som krävs enligt dataskyddsförordningen förbinder sig Sibbo kommun att påvisa att den följer dataskyddslagstiftningen i sin verksamhet.

De viktigaste dokument som upprätthålls av Sibbo kommun i syfte att uppfylla efterlevnad och ansvarsskyldighet är:

Dataskyddspolicy	Dataskyddspolicyn beskriver principerna för dataskydd, målen för dataskyddsförvaltningen, dataskyddets organisation och ansvar samt verksamhetssättet.
Datasäkerhetspolicy	Datasäkerhetspolicyn definierar verksamhetssättet för Sibbo kommuns datasäkerhet.
Register över behandling	Registret över behandling är en intern beskrivning av organisationens behandling av personuppgifter och ändamålen med behandlingen.
Informationsdokument för registrerade	Dataskyddsbeskrivningar och andra dokument avsedda att informera registrerade och med vilka registrerade informeras om behandlingen av personuppgifter på ett transparent sätt.
Dataskyddsbedömningar och riskbedömningar	Av kommunen genomförda förhandsbedömningar av dataskyddet, konsekvensbedömningar av dataskyddet och balanstester av berättigat intresse.
Årsplan för dataskydd	I årsplanen för dataskydd registreras de uppgifter som planeras för dataskyddsarbetet på månadsbasis. Den årliga dataskyddsplanen följer upp hur arbetet med dataskyddet framskrider.
Utbildningsprogram	Fastställer den dataskyddsutbildning som planeras för kommunens personal.
Avtalsmall för behandling av personuppgifter	Fastställer avtalsvillkoren som tillämpas för personuppgiftsbiträdena.
Dokument som rör den rättsliga grunden för behandlingen	Dokumentation och nödvändiga bedömningar som rör samtycke, såsom balanstester av berättigat intresse.
Dokument som rör behandling av registrerades begäranden	Anvisningar avseende genomförande av registrerade personers rättigheter, blanketter avseende begäranden och dokumentmallar avseende dokumentation.
Dokument som rör behandling av personuppgiftsincidenter	Anvisningar och dokumentation avseende hantering av personuppgiftsincidenter.

5 Planering och rapportering

Sibbo kommun planerar dataskyddsarbetet med hjälp av den årliga dataskyddsplnen. I planen har de uppgifter som ska utföras i dataskyddsarbetet fördelats över året. På grundval av årsplanen kan uppgifter delegeras till de ansvariga personerna.

I slutet av året sammanställs kommunens dataskyddsarbete i ett databokslut. Databokslutet bifogas till kommunens bokslut, som godkänns av kommunfullmäktige.

6 Behandling av personuppgifter

6.1 Principerna för behandling av personuppgifter

Sibbo kommun följer gällande lagstiftning vid behandling av personuppgifter som rör kunder, kommuninvånare, kommunens personal och andra intressentgrupper. Vid all behandling av personuppgifter följer Sibbo kommun följande principer i enlighet med dataskyddsförordningen.

Lagenlighet, korrekthet och transparens	Vid behandling av personuppgifter ska dataskyddsförordningen och övrig tillämplig lagstiftning om behandling av personuppgifter följas. Behandlingen av personuppgifter ska vara korrekt och rimlig i förhållande till syftet med behandlingen, med beaktande av informationskyldigheten och bundenheten till användningsändamålet. Information om behandlingen av personuppgifter ska ges på ett tydligt och begripligt sätt.
Bundenheten till användningsändamålet	Behandlingen av personuppgifter planeras i förväg och behandlingen grundar sig alltid på ett visst, uttryckligt och lagligt syfte. Personuppgifter behandlas inte senare på ett sätt som är oförenligt med det ursprungliga syftet. Om personuppgifter behandlas för nya syften ska den registrerade informeras om detta innan behandlingen påbörjas.
Korrekthet, minimering och lagringsbegränsning	<p>Man strävar efter att se till att personuppgifterna är korrekta. Felaktiga personuppgifter raderas eller korrigeras utan dröjsmål.</p> <p>Personuppgifter samlas in och behandlas endast i den utsträckning det är ändamålsenligt och nödvändigt för syftet. De uppgifter som behandlas måste vara ändamålsenliga, dvs. det måste finnas ett definierat syfte med uppgifterna. Uppgifterna ska vara relevanta och begränsade, dvs. nödvändiga för det användningsändamål de är avsedda för.</p> <p>Personuppgifter ska bevaras endast så länge som det är nödvändigt för det fastställda användningsändamålet. Lagringstiderna för personuppgifter definieras och dokumenteras.</p>

Uppgifternas konfidentialitet och säkerhet	<p>Personuppgifter behandlas konfidentiellt och säkert. Skyddsåtgärderna ska stå i proportion till de risker och omständigheter som är förknippade med behandlingen. Personuppgifter skyddas genom tekniska och organisatoriska skyddsåtgärder för att säkerställa nödvändig integritet, konfidentialitet och säkerhet, inklusive skydd mot obehörig eller olaglig behandling och mot oavsiktlig förlust, förstöring eller skada.</p> <p>Personalen och avtalspartner måste följa anvisningar och datasäkerhetspolicyer som rör behandling av personuppgifter.</p>
---	--

6.2 Riskbaserat förhållningssätt och riskhantering

Sibbo kommun följer ett riskbaserat förhållningssätt vid all behandling av personuppgifter och planerar åtgärder och skyddsmetoder i proportion till de dataskyddsrisiker som är förknippade med behandlingen. I syfte att genomföra principerna om inbyggt dataskydd och dataskydd som standard planeras och genomförs behandlingen av personuppgifter under hela livscykeln i enlighet med dataskyddsprinciperna och andra krav som gäller för behandlingen.

I sin verksamhet bedömer Sibbo kommun riskerna som är förknippade med behandlingen av personuppgifter, inklusive förvärv av nya system, samarbete med nya leverantörer och befintliga behandlingsrutiner. Risknivån bedöms och i de situationer som lagen förutsätter görs en bedömning av behandlingens inverkan på dataskyddet i enlighet med dataskyddsförordningen. Resultaten av konsekvensbedömningen används för att definiera metoder för att minimera riskerna med behandling av personuppgifter.

6.3 Inbyggt dataskydd och dataskydd som standard

Sibbo kommun följer principerna om inbyggt dataskydd och dataskydd som standard i sin verksamhet. Data-skyddsprinciperna beaktas i all verksamhet från ett så tidigt stadium som möjligt. Tekniska och organisatoriska åtgärder som är lämpliga i förhållande till risknivån vidtas.

6.4 Registrerades rättigheter

Sibbo kommun säkerställer genomförandet av de registrerades rättigheter enligt dataskyddsförordningen genom att upprätthålla och utveckla nödvändig praxis.

De registrerades rättigheter genomförs på det sätt som är tillämpligt i varje situation, med beaktande av den rättsliga grunden för behandlingen och den aktuella behandlingssituationen. De registrerade informeras om behandlingen av personuppgifter på ett transparent sätt. I enlighet med den rättsliga grunden för behandlingen har den registrerade rätt att få information om behandlingen av sina personuppgifter, rätt att få tillgång till sina egna uppgifter, rätt att korrigera sina uppgifter, rätt att radera uppgifterna, rätt att begränsa behandlingen av sina uppgifter, rätt att överföra uppgifterna från ett system till ett annat, rätt att invända mot behandlingen av sina uppgifter och rätt att inte bli föremål för automatiserat beslutsfattande.

De registrerades begäranden behandlas på det sätt och inom de tidsfrister som krävs enligt lag. Lämpliga operativa processer har definierats för behandling av begäranden från registrerade.

6.5 Personuppgiftsincidenter

Sibbo kommun strävar efter att minimera incidenter som riktar sig till registrerade genom att planera behandlingen av personuppgifter i enlighet med dataskyddsprinciperna och genomföra tekniska och organisatoriska skyddsåtgärder som står i proportion till den risk som de registrerade utsätts för i samband med behandlingen av personuppgifter.

Det finns lämpliga processer, anvisningar och dokumentationspraxis för att upptäcka, rapportera och behandla personuppgiftsincidenter. Personuppgiftsincidenter behandlas på det sätt och inom de tidsfrister som krävs enligt lag. Om en personuppgiftsincident redan har inträffat ska anvisningarna för sådana situationer följas.

Om en person som är anställd av eller arbetar för organisationen upptäcker en risk, avvikelse eller annan liknande situation som rör personuppgifter, är denne skyldig att rapportera om detta.

6.6 Tredje part och överföring av personuppgifter

Dataskyddet beaktas i kommunens avtal med olika parter. När kommunen ingår avtal säkerställer man att kraven i dataskyddsbestämmelserna uppfylls i avtalsvillkoren. Skriftliga avtal för behandling av personuppgifter enligt dataskyddslagstiftningen ingås med alla personuppgiftsbiträden som Sibbo kommun anlitar.

Dataskyddsriskerna som är förknippade med tredje part bedöms och hanteras genom att göra relevanta riskbedömningar och fastställa minimikrav för behandling av uppgifter innan samarbete med tredje part inleds.

Sibbo kommun överför inte i princip personuppgifter utanför EU eller det Europeiska ekonomiska samarbetsområdet. Eventuella överföringar omfattas av gällande lagar och förordningar, och överföringarna av uppgifter genomförs utifrån lämplig överföringsgrund.

7 Utbildning och ökad medvetenhet

Anvisningar om personuppgiftsbehandling görs för sådana arbetsuppgifter där personuppgifter behandlas. Riktlinjerna bör utarbetas med beaktande av principerna i dataskyddspolicyn. Kommunikationen om dataskyddsfrågor är transparent i organisationen.

Sibbo kommun anordnar grundläggande dataskyddsutbildning för sin personal i samband med introduktionen i arbetet. Att tillägna sig innehållet i dataskyddspolicyn är en del av nyanställdas introduktion i arbetet. Grundläggande dataskyddsutbildning tillhandahålls regelbundet och fördjupad utbildning anordnas enligt uppgiftsspecifika behov. För att säkerställa personalens kunnande förutsätts att hela personalstyrkan årligen genomgår en utbildning i datasäkerhet och dataskydd.

Dataskyddsutbildningar planeras och utbildningsplanen följs upp regelbundet.

8 Dokumentinformation och versionshistorik

Dokumentinformation	Förklaring
Dokumentnamn	Sibbo kommuns dataskyddspolicy
Ägare	Dataskyddsombudet
Godkännare	Kommunstyrelsen
Datum för godkännande	24.10.2022
Dokumentet har uppdaterats	14.6.2022

Version	Datum	Ändringar	Upprättat av
1.0	24.10.2022	Första godkända versionen	Privaon Oy