ANVISNINGAR FÖR BEHANDLING AV PERSONUPPGIFTER

Sibbo kommun

SIPOO
SIBBO

Innehåll

1. Principer för behandling av personuppgifter

Den här anvisningen är en sammanfattning av principer som ska följas av kommunens egen personal och kommunens avtalsparter samt av alla andra som behandlar personuppgifter som Sibbo kommun innehar eller har samlat in. Anvisningen delges till ovan nämnda parter.

Sibbo kommun beaktar i sin verksamhet två delvis motsatta grundrättigheter, det vill säga offentligheten i kommunens verksamhet samt integritetsskyddet.

Kommunen genomför sin verksamhet i enlighet med lagstiftningen så att man sammanjämkar skyddet för fysiska personers privatliv med den öppenhet och offentlighet som krävs av administrativ verksamhet.

- Sibbo kommun behandlar personuppgifter enbart på lagstadgade grunder och när det är nödvändigt för att genomföra kommunens verksamhet,
- kommunen ska också informera om personuppgiftsbehandlingen på ett öppet sätt,
- insamlingen av personuppgifter ska ske enbart för särskilda, uttryckligt angivna och berättigade ändamål,
- personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för uppgifterna och därmed uppgifternas integritet och konfidentialitet,
- personuppgifter lagras enbart under den tid som kan anses vara behövlig med hänsyn till det angivna ändamålet.

I undantagsfall får uppgifter förvaras längre om de behandlas för arkivändamål av allmänt intresse eller används för historiska forskningsändamål eller statistiska ändamål.

De uppgifter som ska arkiveras samt deras lagringstider definieras i arkivbildningsplanen och informationsstyrningsplanen.

När uppgifter arkiveras ska man se till att behandlingen och lagringen genomförs på ett sätt som garanterar de registrerades integritetsskydd.

De mest centrala aktörerna och rollerna angående datasäkerheten och dataskyddet i kommunen, inklusive ansvarsområden, definieras i kommunens datasäkerhetspolicy och dataskyddspolicy.

1.1 Begrepp

Med **personuppgift** avses varje upplysning som avser en identifierad eller identifierbar fysisk person.

En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till

- en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer (t.ex. ip-adress) eller
- en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
- Personuppgifter kan bland annat vara adress, e-postadress, fotografi, ljud- eller videoinspelning, bilens registernummer, fastighetsbeteckning, fingeravtryck eller annat biologiskt prov.

Med **behandling av personuppgifter** avses

- insamling,
- registrering,
- organisering,
- strukturering,
- lagring,
- bearbetning eller ändring,
- framtagning och
- läsning av personuppgifter.

Med **utlämnande av uppgifter** avses

- utlämning genom överföring,
- spridning eller tillhandahållande på annat sätt,
- justering,
- sammanförande,
- begränsning,
- radering eller
- förstöring av personuppgifter.

Ett **personregister** är en strukturerad uppsättning av personuppgifter som är åtkomlig enligt särskilda kriterier. Ett personregister kan bestå av uppgifter i både elektronisk och pappersform.

Personuppgiftsbiträdet är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

1.2 Krav för behandling av personuppgifter

- **Laglighet, korrekthet och öppenhet:** Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.
- **Ändamålsbegränsning:** Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.
- **Uppgiftsminimering:** Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till det angivna ändamålet med behandlingen av personuppgifter.
- **Korrekthet:** Personuppgifterna ska vara korrekta och om nödvändigt uppdaterade. Den personuppgiftsansvarige ska med rimliga åtgärder säkerställa att personuppgifter som är inexakta och felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.
- **Lagringsminimering:** Personuppgifter ska förvaras i en form som möjliggör identifiering av den registrerade endast under den tid som är nödvändig för de ändamål för vilka personuppgifterna behandlas.
- **Integritet och konfidentialitet:** Personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet för dem. Uppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse.

Enligt dataskyddsförordningen ska den personuppgiftsansvarige ansvara för att dessa principer och krav efterlevs. Den personuppgiftsansvarige ska även kunna bevisa att dessa principer efterlevs.

2. Behandling av personuppgifter

När Sibbo kommun som personuppgiftsansvarige **lämnar ut** till serviceleverantörer (avtalsleverantörer) olika uppgifter som förutsätter behandling av personuppgifter, är dessa serviceleverantörer i princip aktörer som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Om serviceleverantören inte har självständig beslutanderätt i fråga om behandling och användning av personuppgifter fungerar serviceleverantören som personuppgiftsbiträde för den personuppgiftsansvariges räkning.

I dessa fall ska den personuppgiftsansvarige ingå ett skriftligt avtal med personuppgiftsbiträdet.

Den personuppgiftsansvarige och personuppgiftsbiträdet ska skriftligen avtala om vilka personuppgifter som behandlas och för vilket ändamål. I avtalet ska man också precisera vem som har tillgång till personuppgifterna.

I enlighet med dataskyddsförordningen ska man i avtalet fastställa bland annat **föremålet för behandlingen samt behandlingens varaktighet och ändamål. Därtill ska man avtala om vilken typ av personuppgifter som behandlas.**

2.1 Allmänna bestämmelser och personuppgiftsbiträdets skyldigheter

Behandlingen av personuppgifter är bland annat tillåtet om

- man har den registrerades samtycke,
- behandlingen är nödvändig för att utföra kommunens lagstadgade skyldigheter eller utöva offentlig makt;
- behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås eller
- behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen.

När man ber om den registrerades samtycke ska man använda klart och tydligt språk och ärendet ska framföras tydligt skilt från övriga ärenden.

Den registrerade har rätt att när som helst återkalla sitt samtycke. Att återkalla sitt samtycke ska ske lika enkelt som att ge det.

Om Sibbo kommun erbjuder elektroniska tjänster som baserar sig på distansförbindelser för barn under 16 år, ska barnets vårdnadshavare ge sitt samtycke till behandlingen av barnets personuppgifter.

Att få vårdnadshavarens samtycke är inte nödvändigt när barnens personuppgifter behandlas till exempel för att utföra kommunens lagstadgade skyldigheter eller utöva offentlig makt. EU:s medlemsländer får själv bestämma om de vill sänka den åldersgräns som föreskrivs i förordningen. I den finländska dataskyddslagen är denna åldersgräns 13 år.

2.2 Anvisningar för personuppgiftsbiträden

Se till att behandla personuppgifter enbart i enlighet med dessa anvisningar.

Följ anvisningarna även när du överför, lagrar eller arkiverar personuppgifter.

<u>En person som behandlar personuppgifter ska följa följande anvisningar:</u>
1. Följ instruktionerna för sekretess.
2. Följ instruktionerna för datasäkerhet.
3. Lägg inte ut arbetsuppgifter som innefattar behandling av personuppgifter utan ett skriftligt förhandssamtycke av den personuppgiftsansvariga.
4. Personuppgiftsbiträdet ska utan separat ersättning hjälpa den personuppgiftsansvarige (Sibbo kommun) i att genomföra den registrerades rättigheter.
5. Personuppgiftsbiträdet ska hjälpa den personuppgiftsansvarige i att genomföra datasäkerhet, upptäcka och rapportera personuppgiftsincidenter och minimera skadorna förknippade med dem samt i att utarbeta konsekvensbedömningar och samråda med tillsynsmyndigheten (förhandssamråd).
6. Personuppgiftsbiträdet antingen raderar eller överför personuppgifterna tillbaka till den personuppgiftsansvarige när behandlingsservicen upphör. Personuppgiftsbiträdet ska även radera eventuella kopior av personuppgifterna som det förfogar över.
7. Personuppgiftsbiträdet tillåter att den personuppgiftsansvarige genomför auditeringar och deltar i dem. Personuppgiftsbiträdet ska även utan separat ersättning överlåta samtliga sådana uppgifter med vilka man kan visa att skyldigheterna i förordningen har efterlevts.

2.3 Behandling av särskilda personuppgifter

Dataskyddsförordningen definierar särskilda kategorier av personuppgifter som får behandlas enbart om den grund som särskilt nämns i förordningen uppfylls.

Definitionen av särskild personuppgift i förordningen motsvarar i huvudsak definitionen av känsliga personuppgifter i den gamla personuppgiftslagen.

Särskilda personuppgifter omfattar uppgifter som avslöjar

- ras,
- etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- genetiska och biometriska uppgifter med vilka man entydigt kan identifiera en fysisk person,
- uppgifter om hälsa samt
- uppgifter om en fysisk persons sexualliv eller sexuella läggning.

I enlighet med dataskyddsförordningen är även uppgifter om minderåriga särskilda personuppgifter.

Om man ämnar behandla uppgifter som hör till särskilda kategorier av personuppgifter ska man noggrant utreda huruvida behandlingen av uppgifterna är tillåtet med stöd av artikel 9 i EU:s allmänna dataskyddsförordning.

Dataskyddsförordningen innehåller dessutom en egen artikel om behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser.

Uppgifter om brott eller lagöverträdelser får behandlas enbart om det är fråga om

- ett brott eller en lagöverträdelse mot kommunen eller
- ett brott eller en lagöverträdelse som en kommunanställd har begått och som är av betydelse för personens anställningsförhållande eller
- en situation i vilken behandlingen av personuppgifter kan motiveras av ett annat synnerligt skäl som härrör till kommunens eller en tredje persons rättigheter eller skyldigheter.

Principer för behandling av straffregisterutdrag fastställs i speciallagstiftningen, till exempel i lagen om kontroll av brottslig bakgrund hos personer som arbetar med barn och i lagen om offentlig upphandling och koncession.

3. Övriga bestämmelser om personuppgiftsbehandling

3.1 Datasäkerhet

Personuppgiftsbiträdet ska alltid säkerställa att obehöriga inte har åtkomst till personuppgifterna oberoende om uppgifterna behandlas i datasystem, i papper- eller bildformat, under ett telefonsamtal eller i ett möte ansikte mot ansikte.

När personuppgifter behandlas ska man se till att platsen lämpar sig väl för personuppgiftsbehandling. Utomstående får inte höra vad som sägs eller se uppgifterna när de används.

Behandling av personuppgifter i ett datasystem ska alltid vara motiverad enligt arbetsuppgifterna och åtkomsten till uppgifterna ska vara begränsad med ett personligt användarnamn. Det är förbjudet att använda en annan persons användarnamn och lösenord. Användarrättigheterna för nätverket och program är personliga. Var och en ansvarar för den personuppgiftsbehandling som sker med ens användarrättigheter. Det är förbjudet att överlåta sitt användarnamn eller lösenord till andra.

Personuppgifter i systemet får inte kopieras från systemet. Personuppgifter får överföras enbart till förvaringsställen i vilka uppgifterna lagras i enlighet med registerbeskrivningen.

Personuppgifter kan levereras mellan olika parter med hjälp av skyddad e-post. Personuppgifter får dock inte lagras i den skyddade e-posten, utan meddelanden som innehåller personuppgifter ska raderas när meddelandet har skickats.

Om det är nödvändigt att överföra personuppgifterna till exempel till en minnessticka eller katalog ska de sparas krypterade. Vid krypteringen kan man använda en minnessticka som är skyddad med ett lösenord eller ett krypteringsprogram, till exempel programmet BitLocker. Även i dessa fall ska behandlingen av personuppgifter ske i enlighet med uppgifternas dataskyddsbeskrivning.

Det är bäst att i mån av möjlighet undvika utskrifter i pappersformat. Om det är nödvändigt att skriva ut material som innehåller personuppgifter ska man förvara detta material så att obehöriga inte kan få tillgång till det.

Särskild uppmärksamhet ska fästas vid hur dokument skickas per post. När uppgifter flyttas i pappersformat från en lokal till en annan ska man också iaktta särskild noggrannhet. Samtliga dokument som innehåller personuppgifter ska förstöras som konfidentiellt papper.

3.2 Användarrättigheter

Samtliga datasystem som innehåller personuppgifter kräver inloggning med ett personligt användarnamn.

Användarnamn är personliga och de får inte överlåtas till andra.

I princip har varje arbetstagare (eller samarbetspartners representant) ett personligt användarnamn, och varje användarnamn motsvaras således av en person som använder det. Användaren ansvarar för alla de åtgärder som görs eller har gjorts med hans eller hennes användarnamn.

Hantering av användarrättigheter är en väsentlig del av datasäkerhet och dataskydd. En person beviljas användarrättigheter enbart för att sköta arbetsuppgifter och enbart i den utsträckning som är nödvändigt för att sköta det egna arbetet.

Om arbetsuppgifterna förändras eller om personens anställningsförhållande hos kommunen eller samarbetspartner upphör ska användarrättigheterna avlägsnas omedelbart, ifall det inte finns någon grund för att behålla dem.

Användarna ska i samband med att de tar emot användarrättigheterna förbinda sig till att använda sina användarrättigheter enbart då arbetsuppgifterna så kräver och att de inte tittar på uppgifter som inte är nödvändiga för att sköta det egna arbetet. När användarrättigheter beviljas till systemen som innehåller sekretessbelagda eller känsliga personuppgifter ska särskild noggrannhet iakttas.

3.3 Logguppgifter

Med logguppgifter anser man i det här sammanhanget uppgifter som samlas i datasystem när personuppgifter behandlas, till exempel när användaren lägger till, raderar, ändrar eller söker personuppgifter.

Genom att samla in logguppgifter kan den personuppgiftsansvariga och personuppgiftsbiträdet bevisa att personuppgiftsbehandlingen sker enbart av personer som på grund av sina arbetsuppgifter behöver ha tillgång till uppgifterna.

Insamling av logguppgifter förutsätter personspecifika användarrättigheter.

3.4 Anmälan av en personuppgiftsincident

Personuppgiftsbiträdet ska anmäla en säkerhetsincident som påverkat integriteten, sekretessen eller tillgängligheten till personuppgifter till adressen tietoturvatiimi.datasakerhetsteam@sipoo.fi.

Med säkerhetsincident avses en situation i vilken

- uppgifter förändras,
- uppgifter förstörs eller
- uppgifter läcker ut till utomstående.

De uppgifter som berörs kan vara pappersdokument eller uppgifter i till exempel elektronisk format. En personuppgiftsincident ska anmälas omedelbart efter det att överträdelsen har upptäckts.

Följande uppgifter ska inkluderas i anmälan (minimikrav):

- beskrivning av händelseförloppet,
- om möjligt, förteckning av de uppgifter som berörs av incidenten (vilka grupper av registrerade, antalet registrerade),
- uppskattning av personuppgiftsincidentens sannolika konsekvenser.

För att kunna leva upp till anmälningsskyldigheten ska personuppgiftsbiträdet ha sådant kunnande att det kan upptäcka avvikelser, utreda orsaken till och konsekvenser av avvikelserna samt bedöma hur avvikelserna påverkar integritetsskyddet.

3.5 Uppföljning av dataskyddslagstiftningen

Utöver dessa anvisningar för behandling av personuppgifter ska personuppgiftsbiträdet i sin verksamhet följa den gällande lagstiftningen om personuppgiftsbehandling. På de punkter som bestämmelserna i den här anvisningen strider med lagstiftningen följs bestämmelserna i lagen.

Anvisningarna uppdateras om lagstiftningen eller nationella anvisningar så kräver och även annars vid behov.

Datasäkerhetsteamet i Sibbo ser till att anvisningarna uppdateras.