NÄSSJÖ KOMMUN

Författningssamling

Dokumenttyp Policy	Beslutsinstans Kommunfullmäktige	Beslutsdatum 2020-04-23	§ 81
Dokumentansvarig Digitaliseringsstrateg			
Gäller för Nässjö kommun (Höglandsgemensam)		Senast reviderad 2024-06-13, § 82	

Dataskyddspolicy

1 Syftet med denna policy

Alla individer vars personuppgifter behandlas inom ramen för Nässjö kommuns verksamhet ska vara trygga med hur deras personuppgifter hanteras.
Denna policy ska säkerställa att Nässjö kommun:

- följer gällande dataskyddslagstiftning
- lagrar och hanterar personuppgifter på ett korrekt och enhetligt sätt
- kommunicerar tydligt och öppet gällande hur personuppgifter hanteras i verksamheten
- kan tillmötesgå anställdas, kommuninvånares och andra intressenters rättigheter
- skyddar den egna verksamheten mot hot och därmed minimerar integritetsrisker

2 Omfattning

Policyn har tagits fram av Höglandets dataskyddsnätverk och omfattar all behandling av personuppgifter som utförs inom organisationen.
Denna policy gäller samtliga verksamheter inom Nässjö kommun. Policyn ska kompletteras med riktlinjer och rutiner inom dataskydd samt andra specifika verksamhetsområden.
Riktlinjerna ska efterlevas av ledning, förtroendevalda, anställda och likaså av andra personer som arbetar på uppdrag av eller under översyn av Nässjö kommun.

3 Gällande dataskyddslagstiftning

Hanteringen av och skyddet för personuppgifter regleras övergripande av EU:s allmänna dataskyddsförordning (GDPR - Europaparlamentets och rådets förordning [EU] 2016/679) samt kompletterande svensk lagstiftning i form av den kompletterande dataskyddslagen och tillhörande förordning (SFS 2018:218 och SFS 2018:219).

Ytterligare relevant lagstiftning kan tillkomma i form av exempelvis registerförfattningar inom specifika branschområden. Integritetsskyddsmyndigheten (IMY) är tillsynsmyndighet gällande personuppgiftsrelaterade ärenden.

4 Viktiga begrepp och definitioner

Denna policy rör hantering av personuppgifter. Personuppgifter är all information som kan användas för att identifiera en enskild person, direkt eller indirekt. Begreppet personuppgifter inkluderar (men är inte begränsat till):

- Namn
- Personnummer
- E-postadress
- Telefonnummer
- IP-adress
- Kundnummer
- Bilder (på personer)

I uttrycket **behandling av personuppgifter** inkluderas allt som görs där personuppgifter förekommer, exempelvis administration av, kommunikation med och lagring av sådana uppgifter för olika ändamål och i olika sammanhang.
I den mån **känsliga personuppgifter** förekommer i Nässjö kommuns verksamhet gäller särskilda regler. Känsliga personuppgifter är:

- Uppgifter som avslöjar ras eller etniskt ursprung,
- Uppgifter som avslöjar politiska åsikter,
- Uppgifter som avslöjar religiös eller filosofisk övertygelse,
- Uppgifter om medlemskap i fackförening,
- Uppgifter om hälsa,
- Uppgifter om sexualliv eller sexuell läggning,
- Genetiska uppgifter, och
- Biometriska uppgifter för att entydigt identifiera en fysisk person.

Observera att även uppgifter som indirekt avslöjar känslig information av detta slag inkluderas.

Nämnderna i Nässjö kommun är **personuppgiftsansvariga** för de flesta av de personuppgiftsbehandlingar som förekommer i verksamheten. Kommunstyrelsen anses vara personuppgiftsansvarig för kommunövergripande personuppgiftsbehandlingar. Med detta menas att nämnden är den som är ytterst ansvarig för personuppgifterna, och som bestämmer över ändamål och medel. I specifika fall kan det vara så att någon annan än Nässjö kommun är personuppgiftsansvarig. Roller och ansvarsfördelning mellan organisationen och eventuella **personuppgiftsbiträden** ska framgå för varje behandling i registerförteckningen.

5 Ändamål med behandling av personuppgifter

Nässjö kommun behandlar en stor mängd personuppgifter för olika typer av ändamål. Nässjö kommun behandlar i många fall personuppgifter i ett allmänt intresse och myndighetsutövning för att leva upp till lagar och förordningar. I andra fall kan personuppgiftsbehandlingar bygga på avtalsförhållanden, exempelvis gällande anställdas personuppgifter. Nässjö kommun kan också behöva behandla personuppgifter genom rättsliga förpliktelser. Viss personuppgiftsbehandling kan ske genom att enskild har

samtyckt till att Nässjö kommun får behandla personuppgifter. Samtycke som rättslig grund för personuppgiftsbehandling ska ske restriktivt eftersom ett samtycke kan återkallas när som helst samt att registrerade ofta står i beroendeställning till myndigheter.

6 Dataskyddsförordningens grundläggande principer

Dataskyddsförordningen bygger på ett antal principer som styr efterlevnaden. Dessa principer beskriver de skyldigheter som organisationer måste följa när personuppgifter behandlas. Dataskyddsförordningens grundläggande principer är att personuppgiftsansvarig

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter. Personuppgifter måste behandlas på ett lagligt, korrekt och öppet sätt (*principen om laglighet*),
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål och får inte behandlas för något ändamål som är oförenligt med dessa ändamål (*principen om ändamålsbergränsning*),
- inte behandlar fler personuppgifter än vad som är nödvändigt för ändamålen (*principen om uppgiftsminimering*),
- ska se till att personuppgifterna är korrekta (*principen om riktighet*),
- ska radera personuppgifterna när de inte längre behövs (*principen om lagringsminimering*),
- ska skydda personuppgifterna på ett sätt som säkerställer lämpligt skydd, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs (*principen om integritet och konfidentialitet*),
- ska kunna visa att man lever upp till dataskyddsförordningen och på vilket sätt det görs (*principen om ansvarsskyldighet*).

7 Roller

7.1.1 Personuppgiftsansvarig

Inom kommunen är det den nämnd, styrelse eller bolagsstyrelse som är personuppgiftsansvarig, vilket innebär att de har ansvaret för att personuppgifter behandlas lagligt, säkert och i övrigt korrekt. Personuppgiftsansvarig kan överlåta det operativa arbetet kring personuppgifter men personuppgiftsansvaret kan aldrig överlåtas.

7.1.2 Dataskyddsombud

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen.

Det innebär bland annat att

- samla in information om hur personuppgiftsansvarig behandlar personuppgifter
- kontrollera att personuppgiftsansvarig följer bestämmelser och interna styrdokument
- informera och ge råd inom organisationen.

Dataskyddsombudet ska också

- ge råd om konsekvensbedömningar
- vara kontaktperson gentemot Integritetsskyddsmyndigheten
- vara kontaktperson för de registrerade och personalen inom verksamheten
- samarbeta med Integritetsskyddsmyndigheten, till exempel vid inspektioner.

Höglandkommunerna samverkar i denna fråga och har ett gemensamt dataskyddsombud som finns på Höglandsförbundet.

7.1.3 Personuppgiftssamordnare

Varje kommun och förbund ska utse representant för lokal samordning inom området dataskydd. Personuppgiftssamordnaren ska ges förutsättning för att kunna utföra uppdraget. Tid, kompetens och mandat bedöms utifrån vilka områden som ska prioriteras inom respektive kommun/förbund. Personuppgiftssamordnaren har regelbunden kontakt med dataskyddsombud och förmedlar information mellan Höglandsgemensamt dataskyddsnätverk och lokala dataskyddsnätverk.

7.1.4 Personuppgiftsadministratör

Varje förvaltning behöver utse en eller flera personuppgiftsadministratörer för att stödja förvaltningen (ledningsgrupp och medarbetare) i sitt dataskyddsarbete. Resursen ska delta i lokalt nätverk för dataskydd. Det är viktigt att personuppgiftsadministratör är en person som har god kännedom om förvaltningen och dess olika processer och verksamheter.
Varje personuppgiftsadministratör behöver få nödvändig kompetens inom dataskyddsområdet
genom höglandsgemensam internutbildning. Personuppgiftsadministratören ska ha förutsättning för att kunna utföra uppdraget. Tid, kompetens och mandat bedöms utifrån vilka områden som ska prioriteras inom respektive förvaltning.

7.1.5 Medarbetare

Medarbetare har ett ansvar att följa Nässjö kommuns styrdokument inom dataskydd. Man har som medarbetare också ansvar att vara uppmärksam på brister och fel gällande personuppgiftshantering. Medarbetare ska även genomföra de utbildningar inom dataskydd som Nässjö kommun tillhandahåller.

8 Personuppgiftsbehandlingar mellan myndighetsgränser

Dataskyddspolicyn reglerar även behandling av personuppgifter nämnder emellan. Det innebär att personuppgifter kan flöda över myndighetsgränser och hanteras av nämnd där annan nämnd är personuppgiftsansvarig. Detta kan ske under förutsättning att de grundläggande principerna i dataskyddsförordningen efterlevs och att samtliga behandlingar har rättslig grund. Det är varje personuppgiftsansvarigs skyldighet att ge instruktioner till mottagande nämnd avseende den behandling som mottagaren ska hantera för personuppgiftsansvarigs räkning. Detta kan exempelvis ske vid kommunövergripande processer som lönehantering, personalärenden eller support.

9 Kompletterande styrdokument

Vidare riktlinjer och instruktioner som rör Nässjö kommuns personuppgiftsbehandling finns i följande dokument:

- Informationssäkerhetspolicy
- IT-säkerhetspolicy
- Generella riktlinjer inom dataskydd