

Författningssamling

Dokumenttyp Riktlinjer (bevaras)	Beslutsinstans Kommunstyrelsens arbetsutskott	Beslutsdatum 2025-04-01	§ 30
Dokumentansvarig Digitaliseringsstrateg			
Gäller för Nässjö kommun		Senast reviderad	

Generella riktlinjer inom dataskydd

Utbildning

Alla anställda ska få grundläggande dataskyddsutbildning, för att säkerställa förståelse för vikten av att hantera personuppgifter korrekt. Ansvarig för att utbildning sker är respektive nämnd.

Varje avdelning ansvarar för att berörda medarbetare får ta del av sådana instruktioner och rutiner som är relevanta för dem, och sådan information som behövs för att var och en ska kunna utföra sitt arbete i linje med dataskyddslagstiftningen. Detta inkluderar, men är inte begränsat till, utbildning av nyanställda.

Registerförteckning

Nässjö kommun har en registerförteckning över de personuppgiftsbehandlingar som sker inom kommunen. Förteckningen ska löpande hållas uppdaterad och fungera som ett heltäckande register över alla personuppgiftsbehandlingar, i enlighet med kraven i artikel 30 GDPR.

Registerförteckningen administreras av personuppgiftsadministratör. System- och informationsägare samt avdelningsansvariga kan komma att tilldelas ansvar för specifika delar av registerförteckningen i samarbete med personuppgiftsadministratör.

Förteckningen kan visas upp för tillsynsmyndigheten på begäran.

Rättslig grund

Varje behandling av personuppgifter ska ha en specificerad så kallad rättslig grund för att det ska vara lagligt att behandla personuppgifterna. Inga personuppgifter får behandlas hos Nässjö kommun utan att det finns en identifierad och lämplig rättslig grund. En godtagbar rättslig grund kan exempelvis vara ett avtal som ska uppfyllas, ett berättigat intresse, en rättslig förpliktelse (till exempel enligt bokföringslagen eller

arkivlagen) eller ett faktiskt samtycke från de registrerade. Alla de olika möjliga rättsliga grunderna finns listade i artikel 6 GDPR.

Det är inte tillåtet att behandla känsliga personuppgifter förutom i specifika undantagsfall, som i så fall ska finnas beskrivna i registerförteckningen samt i kompletterande rutiner eller instruktioner.

Ändamålsbegränsning och uppgiftsminimering

Personuppgifter får endast behandlas för specifika syften, i den utsträckning de behövs och i enlighet med dataskyddslagstiftningen.

Behörighetsbegränsning

De personuppgifter som förekommer i verksamheten ska endast vara tillgängliga för personer som specifikt behöver dem i sitt arbete. För känsliga personuppgifter ska en snävare behörighetstilldelning generellt sett gälla än för mer harmlösa personuppgifter.

Lagringsminimering

Personuppgifter som inte längre behövs (och som man inte heller är skyldig att spara) ska gallras löpande i enlighet med Nässjö kommuns informationshanteringsplan. Observera att det kan finnas lagkrav på att arkivera och spara uppgifter.

Information till registrerade

Alla vars personuppgifter hanteras av Nässjö kommun har rätt till information om hur deras personuppgifter hanteras. Informationen ska vara lättillgänglig samt tillräckligt utförlig för att motsvara kraven i dataskyddslagstiftningen. Informationen ska lämnas på ett klart och tydligt sätt innan, eller i samband med att personuppgifter behandlas av Nässjö kommun.

De registrerades rättigheter

Nässjö kommun ska ha rutiner och instruktioner på plats för hur organisationen ska fullgöra sina skyldigheter gentemot de registrerade. De registrerades rättigheter framgår av artikel 12–23 i dataskyddsförordningen och dessa rättigheter ska Nässjö kommun vara beredda att tillmötesgå i alla situationer där det krävs. Detta omfattar ovan nämnda informationsskyldighet, men också rätten till tillgång (begäran om registerutdrag), rättelse, radering, begränsning, dataportabilitet samt rätten att invända i tillämpliga fall.

Lagring och informationssäkerhet

Alla personuppgifter som finns hos Nässjö kommun ska skyddas genom säker IT-drift och andra lämpliga tekniska och organisatoriska säkerhetsåtgärder i enlighet med artikel 32 Dataskyddsförordningen. Vidare specifikationer gällande informationssäkerhet inom Nässjö kommun finns i separat Informationssäkerhetspolicy.

Personuppgiftsbiträdesavtal

Nässjö kommun anlitar endast personuppgiftsbiträden som garanterar lämpliga tekniska och organisatoriska säkerhetsåtgärder och på andra sätt kan ge garantier för att kraven i dataskyddsförordningen uppfylls. Det ska finnas skriftliga biträdesavtal med samtliga personuppgiftsbiträden. Personuppgiftsadministratör ansvarar för att kontrollera att

personuppgiftsbiträdesavtal finns och speglar kraven i artikel 28 dataskyddsförordningen. Personuppgiftssamordnare ska vid behov vara behjälplig med översyn av innehållet i personuppgiftsbiträdesavtalen.

Incidentrapportering

Var och en som upptäcker eller misstänker en incident som skulle kunna innebära en integritetsrisk, ska rapportera detta vidare till personuppgiftssamordnare och dataskyddsombud. En personuppgiftsincident kan vara allt ifrån att någon har tappat en mobiltelefon till en hackerattack. Rutiner kring hantering av personuppgiftsincidenter ska finnas för Nässjö kommun.

Tillsynsmyndighet

Integritetsskyddsmyndigheten (IMY) är tillsynsmyndighet gällande personuppgiftsrelaterade ärenden.

Enskilda personer som har klagomål gällande Nässjö kommuns hantering av personuppgifter har rätt att kontakta IMY.