Arbets- och företagsnämnden

2021-08-10
TJÄNSTESKRIVELSE
Dnr: AFN 2021/156

# Återrapportering efterlevnad dataskyddsförordningen

## Förslag till beslut
Arbets- och företagsnämnden noterar informationen till protokollet.

## Sammanfattning
Den 16 juni 2021 presenterade Nacka kommuns dataskyddsombud sin årsrapport 2020 för arbets- och företagsnämnden. I rapporten framgår rekommendationer för nämndens efterlevnad av dataskyddsförordningens samtliga krav. I nedanstående ärende presenteras rekommendationerna samt vilka åtgärder som arbets- och företagsnämnden vidtar för ska säkerställa att kraven inom dataskyddsförordningen efterlevs. Åtgärderna omfattar att fortsatt följa upp personuppgiftsbehandlingar i syfte att konsekvensbedöma dessa, säkerhetsklassa system där dataskyddsförordningen så kräver samt fortsatt uppdatera nämndens informationshanteringsplan för efterlevnad av arkiv- och gallringsregler. Vidare kommer nämnden fortsatt upprätthålla de redan fungerande rutinerna för hantering av personuppgiftsincidenter och begäran om registerutdrag samt fortsätta det systematiska förbättringsarbetet och utveckling inom informationssäkerhet och efterlevnad av dataskyddsförordningen.

## Ärendet
Dataskyddsförordningen (GDPR) är den lagstiftning som reglerar hur myndigheter, bolag och andra organisationer får hantera personuppgifter. Personuppgift är varje typ av information som kan kopplas till en fysisk person. Varje organisation som behandlar personuppgifter i någon omfattning måste följa dataskyddsförordningens regler.

I samband med att dataskyddsförordningen den 25 maj 2018 skulle träda i kraft valde Nacka kommun en införandemodell för GDPR med tolv fokusområden, som utgör utvärderingsmodell för varje nämnds införandegrad och effektivitet avseende efterlevnaden av GDPR.

I dataskyddsombudets årsrapport 2020 (AFN 2021/121), som nämnden tog del av den 16 juni 2021, granskas arbets- och företagsnämnden efterlevnad av förordningen utifrån de tolv fokusområdena. I rapporten ger dataskyddsombudet rekommendationer för nämndens efterlevnad av kravbilden i dataskyddsförordningen. Efter att ha tagit del av årsrapporten gav nämnden utbildnings- och arbetsmarknadsdirektören i uppdrag att

säkerställa att rekommendationerna i dataskyddsombudets årsrapport 2020 följs och återrapportera detta till nämndsammanträdet den 25 augusti 2021. I detta ärende presenteras denna återrapportering. Ärendet redovisar en planering för hur årsrapportens rekommendationer och de 12 prioriterade fokusområdena säkerställs samt vilka åtgärder som vidtas för att efterleva förordningens krav.

Dataskyddsombudet gav i sin årsrapport en särskild rekommendation till Nacka kommun att det dagliga arbetet utifrån GDPR fungerar bra men att det inom kommunen saknas tydliga avrapporteringsvägar till ledningsfunktioner och att styrdokument inte på ett effektivt sätt når medarbetarna. Vidare anser Dataskyddsombudet att det generellt behövs en systematisk egenkontroll för varje enhet för att underlätta både rapportering till ledning och för att medvetandegöra enhetsledning om eventuella förbättringsbehov.

Utbildnings- och arbetsmarknadsdirektörens bedömning går i linje med Dataskyddsombudets vad avser kommunens arbete kring styrdokument och involvering av medarbetare. Vad gäller den systematiska egenkontrollen och tydliga avrapporteringsvägar ingår hanteringen av personuppgiftsincidenter i arbets- och företagsnämndens avvikelsehantering. Därmed ingår de i systematisk återrapportering till enhetens ledning och medvetandegörs medarbetare och ledning för förbättringsåtgärder samt ingår i nämndens egenkontroll.

## 1. Registrera personuppgiftsbehandlingar

Varje personuppgiftsansvarig ska ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, kategorier av registrerade, typer av personuppgifter och lagringstid framgår. Arbets- och företagsnämnden har tio personuppgiftsbehandlingar registrerade i det publika registret på nacka.se och nio i den databas som är avsedd för registrering av dessa. Eftersom det finns en diskrepans mellan databasens registreringar och det publika registret, rekommenderas nämnden att genomföra en genomgång och städning av databasen.

Det finns fyra registreringar i databasen som inte uppdaterats sedan 2019, och nämnden uppmanas att säkerställa att de årligen uppdateras och aktualitetskontrolleras.

#### Hantering för efterlevnad

Samtliga registrerade personuppgiftsbehandlingar har under juni månad aktualitetskontrollerats och uppdaterats. En beställning av uppdatering av det publika registret samt databasen har gjorts för att säkerställa att de överensstämmer.

## 2. Rapportera personuppgiftsincidenter

Varje personuppgiftsansvarig ska ha processer för att upptäcka, utreda, åtgärda och anmäla vissa personuppgiftsincidenter till tillsynsmyndigheten Integritetsskydds-myndigheten. Det innebär att medarbetare ska kunna identifiera när en personuppgifts-

incident har hänt, veta hur den ska rapporteras och att det finns processer för att ta hand om en bekräftad incident. Av stor vikt är organisationens lärande från inträffade incidenter, och nämnden uppmanas analysera och säkerställa att varje enhet redovisar lärdomar och aktiviteter utgående från dessa. Nämnden uppmanas att säkerställa att dokumentationen slutförs och alla ärenden för personuppgiftsincidenter avslutas.

#### Hantering för efterlevnad

Samtliga ärenden är från och med maj 2021 avslutade. Rapporterade incidenter följer den centrala processen och inkluderas även i nämndens avvikelsehantering för att förhindra framtida incidenter, återrapportera till enhetsledningen samt dra lärdomar om vilka förbättringar som behöver genomföras och ingår i nämndens egenkontroll.

## 3. Konsekvensbedömning (DPIA)

Om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, ska den personuppgiftsansvarige göra en konsekvensbedömning.
Konsekvensbedömningens syfte är både att säkerställa att enskildas fri- och rättigheter respekteras och är även ett sätt för den personuppgiftsansvarige att visa att dataskyddslagstiftningen följs. Något centralt register över vilka konsekvensregistreringar som genomförts inom nämndens ansvarsområde finns inte, varför nämnden uppmanas dokumentera förekomst och den eventuella bristen.

#### Hantering för efterlevnad

Personuppgiftsbehandlingar som omfattas av dataskyddsförordningens kriterier för genomförande av DPIA är de där det är sannolikt att behandlingen leder till en hög risk för kränkning av fysiska personers rättigheter och friheter. Då nämndens behandlingar är kopplade till myndighetsutövning reglerade av socialtjänstlagen och skollagen och behandlas i syfte att leva upp till lagstiftning samt sekretesskrav är bedömningen att dessa kriterier i förordningen inte uppfylls.

För att undanröja några risker för att personuppgiftsbehandling uppfyller kriteriet planerades under 2021 riskanalyser, i enlighet med Nacka kommuns riktlinjer, som ett första steg för att bedöma om fortsatt konsekvensbedömning behöver göras. Detta arbete som involverar dataskyddssamordnare, informationsägare, systemägare, systemförvaltare och sakkunnig handläggare har inte hunnit påbörjas i utsatt tid. Verksamheten har även begärt att få ett förtydligande från DSO kring när DPIA bör genomföras och vilket stöd som finns för detta omfattande arbete.

## 4. Personuppgiftsbiträdesavtal (PUB-avtal)

Personuppgiftsbiträdesavtal ska tecknas om en personuppgiftsansvarig anlitar en extern part som behandlar personuppgifter på uppdrag av den personuppgiftsansvariga. Den externa parten är då biträde till den personuppgiftsansvariga och ska genom avtalet förbindas att endast behandla personuppgifter efter instruktioner från den ansvarige.

Syftet med avtalet är att säkerställa att enskildas personuppgifter skyddas. Något centralt register över vilka leverantörer som har personuppgiftsbiträdesförhållande till nämnden finns inte, varför nämnden rekommenderas att uppdra åt dataskyddssamordnarna att dokumentera status och identifiera eventuella brister.

**Hantering för efterlevnad**
Nämndens PUB-avtal är registrerade i kommunens diarieföringssystem. För att systematisera uppföljningen av dessa och säkerställa att alla uppgifter är aktuella tas en förteckning fram över samtliga PUB-avtal med tillhörande uppgift om underbiträden. Detta för att säkerställa att ingen lagring eller behandling av personuppgifter inom dessa system överförs till ett land utanför EU/EES i enlighet med dataskyddsförordningens krav vad gäller information om underbiträden.

## 5. Lagringsminimering, arkivering och gallring

Lagringsminimering är en av dataskyddsprinciperna och handlar om att personuppgifter endast får behandlas så länge de behövs för ändamålet. Inom offentlig verksamhet innebär lagringsminimering att det finns ordning och reda bland myndighetens information, att information rensas, arkiveras och gallras. Informationshanteringsplanen (IHP) är det styrdokument som ska visa vilka allmänna handlingar en verksamhet har och hur dessa ska hanteras.

DSO rekommenderar nämnden att säkerställa att DSS dokumenterar informationshanteringsplanen då en central och strukturerad lagring av informationshanteringsplaner inte finns.

**Hantering för efterlevnad**
DSO: s uppgift om dokumentation av informationshanteringsplan är inte överstämmande med det faktiska läget. Nacka kommun publicerar samtliga nämnders informationshanteringsplaner på nacka.se. Arbets- och företagsnämndens IHP uppdaterades senast den 16 juni 2021.

## 6. Registerutdrag (rätten till tillgång)

Registerutdrag eller rätten till tillgång är en rättighet i dataskyddsförordningen som varje enskild har i förhållande till sina personuppgifter. Rättigheten innebär att varje person har rätt att vända sig till en personuppgiftsansvarig för att få bekräftat om ens personuppgifter behandlas och i så fall få tillgång till dessa.

Enligt DSO är processen för att producera registerutdrag komplex och nämnden rekommenderas att se över dess effektivitet avseende ledtider och innehållets kvalitet.

**Hantering för efterlevnad**
Nämnden fortsätter att följa Nacka kommuns centrala process för hantering av begäran om registerutdrag vilken följer dataskyddsförordningens krav. Utbildnings- och

arbetsmarknadsdirektörens delar inte DSO: s bedömning att processen är komplex. Processen är allt igenom är digital och nämnden har en rutin för hanteringen samt flera funktioner som har behörighet att hantera utdragen då de inkommer. Ledtiderna från inkommen till att besvarat registerutdrag har aldrig överstigit den tid som anges för hanteringen och innehållet i de besvarade utdragen har aldrig varit föremål för överklagan eller komplettering.

## 7. E-post

I dataskyddsförordningen finns inte, som tidigare i personuppgiftslagen, något undantag för personuppgifter i ostrukturerat material. Det betyder att även personuppgifter i ett e-postmeddelande omfattas av dataskyddslagstiftning. Detta ställer höga krav på att även hanteringen av e-post följer dataskyddsprinciperna. I Nacka kommun finns en framtagen guide för säker e-posthantering som beskriver hur e-post hanteras på ett säkert och med dataskyddsförordningen förenligt sätt.

#### Hantering för efterlevnad

Rutinen diskuteras kontinuerligt med medarbetare och rutiner för att hantera känsliga och extra skyddsvärda personuppgifter på ett säkert sätt har implementerats och utvecklas. Nämnden fortsätter att använda tjänsten Säkra meddelanden och säkra digitala mötes forum då personuppgifter är känsliga, extra skyddsvärda eller omfattas av sekretess.

## 8. Systemsäkerhet

En viktig dataskyddsprincip är integritet och konfidentialitet som handlar om att kunna säkerställa personuppgifternas konfidentialitet. Informationsklassningen görs i systemet KLASSA, levererat och utvecklat av Sveriges kommuner och regioner, SKR.

Nämnden har åtta system registrerade för informationsklassificering, varav ett helt saknar handlingsplan och fyra inte har uppdaterats sedan mitten av 2018. För de system som saknar uppdateringar (eller helt handlingsplan) noteras att riskanalyser inte är genomförda enligt dokumentationen. Detta är särskilt allvarligt och bör omgående korrigeras.

#### Hantering för efterlevnad

En planering för hur detta arbete regelbundet ska genomföras behöver tas fram i samarbete med de kommunens digitaliseringsenhet då flera av system är kommungemensamma och inte nämndspecifika. Verksamheten har begärt att få ett förtydligande kring vilka system som inte är säkerhetsklassade eller uppdaterade av kommunens dataskyddsombud, DSO samt efterfrågat stöd i hur detta arbete ska genomföras på ett effektivt sätt och i enlighet med GDPR. Detta som ett steg i ledet att säkerställa att de system som är nämndspecifika omfattas av säkerhetsklassning samt upprätta en rutin för kontinuerlig säkerhetsklassning av de system som är specifika för nämnden.

## 9. Behörighet

Korrekt hantering av behörigheter till system och andra ytor som lagrar personuppgifter är en förutsättning för att inte personuppgifter ska bli tillgängliga för obehöriga och för att personuppgifter inte behandlas för olovliga syften. Korrekt hantering av behörigheter betyder att behörighet till personuppgifter ges utifrån användarens behov av att behandla uppgifterna och att dessa behörigheter regelbundet ses över.

Det finns behov av att de framtagna rutinerna som finns även säkerställs att omfatta alla anställda som byter tjänst inom kommunen också får ändrade behörigheter utifrån sina nya arbetsuppgifter. DSO rekommenderar nämnden att använda kontrollplanen för att säkerställa att behörigheter kontinuerligt ses över.

#### Hantering för efterlevnad

Behörighet i nämndens verksamhetssystem som hanterar känsliga och sekretessbelagda personuppgifter upphör genom beställning från ansvariga funktioner vid både avslutande och byte av tjänst. Process och rutiner för nyanställning och hantering av behörigheter i samband med byte av tjänst ska införlivas i nämndens digitala kvalitetsledningssystem. Digitaliseringsenheten i Nacka kommun har i uppdrag att se över möjligheten till att automatisera denna hantering och därmed komma ifrån att manuell hantering av behörigheter.

## 10. Samtycke

I dataskyddsförordningen skärptes kraven på hur och när samtycke kan användas som stöd för en personuppgiftsbehandling. Det har inte framkommit i granskningen att nämnden använder samtycke som rättslig grund för att behandla personuppgifter. Nämnden rekommenderas att använda kontrollplanen för att dokumentera detta.

#### Hantering för efterlevnad

Nämnden använder myndighetsutövning med stöd av Socialtjänstlagen och Skollagen som rättslig grund för att behandla personuppgifter därför är samtycke inte aktuellt.

## 11. Informationsplikt

Informationsplikten i dataskyddsförordningen betyder att inga personuppgifter får behandlas utan att en enskild vet om detta, detta krav gäller oavsett om uppgifterna samlas direkt via kontakt med en enskild eller från en annan källa. Det finns i förordningen dessutom krav på vilken typ av informationen som ska ges samt att detta ska ske på ett enkelt och lättillgängligt sätt. Ett sammanställt och dokumenterat sätt att överblicka de informationstexter som ska föregå varje personuppgiftsbehandling finns inte, varför nämnden rekommenderas att uppdra dataskyddssamordnarna att årligen säkerställa informationens aktualitet och korrekthet

**Hantering för efterlevnad**

En inventering av nämndens behandlingar av personuppgifter i syfte att säkerställa att informationsplikten uppfylls och att informationstexten är aktuell och uppdaterad har genomförts under årsskiftet 2020/2021 och under våren 2021. I samband med inventeringen gavs även en kunskapshöjning om informationsplikten till medarbetarna för att säkerställa att detta efterlevs vid förändrade eller nya personuppgiftsbehandlingar. Verksamheten har rekommenderat DSO att ta fram kommungemensamma mallar för informationstexter då det är önskvärt att hela Nacka kommun använder liknande innehåll och formuleringar till enskilda. DSO har även meddelat att en standardtext för blanketter ska tas fram för samtliga nämnder. Rekommendationen att årligen se över informationen aktualitet säkerställs genom att DSS får uppdraget att hålla i en årlig översyn av efterlevnad av GDPR som en del av egenkontrollen.

## Ekonomiska konsekvenser

Genom att säkerställa att samtliga regler inom dataskyddsförordningen följs minimeras risken för att nämnden beläggs med sanktionsavgifter från tillsynsmyndigheten.

## Konsekvenser för barn

I de fall personuppgifter för barn hanteras ska utöver sekretess- och dataskyddsförordningens krav även barnkonventionens artikel 12 följas genom att barnet ska, i administrativa förfaranden som rör barnet, särskilt beredas möjlighet att höras, antingen direkt eller genom en företrädare eller ett lämpligt organ och på ett sätt som är förenligt med nationella procedurregler.

Pia Stark
Enhetschef
Arbets- och etableringsenheten

Nina Bäckström
Kvalitetsutvecklare
Arbets- och etableringsenheten