ÅRSRAPPORT 2019
MSN 2020/64

Nämnd och personuppgiftsansvarig
Miljö- och stadsbyggnadsnämnden

Dataskyddsombudets årsrapport 2019

Dataskyddsombud
Hanna Virtanen

Datum 2020-05-12

Innehåll

NACKA KOMMUN

Inledning

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, oavsett verksamhet, behandlar därmed personuppgifter i någon omfattning och måste därmed förhålla sig till dataskyddsförordningens regler.

Denna rapport sammanfattar miljö- och stadsbyggnadsnämndens arbete med dataskydd under år 2019 och ger en översiktlig granskning av hur långt miljö- och stadsbyggnadsnämnden har kommit i sin efterlevnad av dataskyddsförordningen. Förordningen ställer en rad krav; från säker hantering av information, till kontroll över vilka personuppgifter som hanteras, var, varför och hur samt kontinuerlig utvärdering av risker för enskildas fri- och rättigheter. Det är nämnden som är personuppgiftsansvarig för den personuppgiftsbehandling som sker inom dess verksamhet och därmed ansvarig för att förordningens krav följs.

Rapporten lämnas av nämndens Dataskyddsombud. Dataskyddsombud är en roll som varje nämnd är skyldig att utse enligt förordningen och har i uppdrag att granska och rapportera om nämndernas efterlevnad av förordningen. Därutöver har dataskyddsombudet även i uppgift att ge råd och stöd om skyldigheter som följer av lagen samt fungera som kontaktpunkt gentemot enskilda och tillsynsmyndigheten, Datainspektionen. Denna rapport lämnas till nämnden som en del av dataskyddsombudets uppdrag.

Sammanfattning av 2019 års arbete med dataskydd

Inför att dataskyddsförordningen den 25 maj 2018 skulle träda i kraft, fattade stadsledningskontoret beslut om 12 fokusområden för att anpassa verksamheten till förordningens krav. I årsrapporten 2018 konstaterades att samtliga enheter påbörjat anpassningen till dataskyddsförordningen inom majoriteten av de 12 beslutade fokusområdena. Under 2019 har dataskyddsarbetet fokuserat på att fortsätta anpassningen och inriktat sig främst på tre områden: hantering av personuppgiftsincidenter, uppdatering av registerförteckningen och konsekvensbedömningar (DPIA).

Ansvaret för att hantera och anmäla personuppgiftsincidenter flyttade under året från en central grupp till nämnderna. Samtidigt reviderades samtliga nämnders delegationsordningar för att delegera beslut om anmälan till tillsynsmyndighet till respektive enhetschef i samråd med Dataskyddsombud. Enligt den nya processen ligger ansvar för att rapportera, dokumentera och åtgärda en incident på respektive enhet men den centrala gruppen finns med som stöd. Detta arbetssätt ligger mer i linje med hur ansvaret är reglerat i dataskyddsförordningen där det är varje personuppgiftsansvariges uppgift att hantera och anmäla personuppgiftsincidenter.

Under året har även nämndernas förteckningar över sina personuppgiftsbehandlingar uppdaterades för att nu utgå från syftet med att personuppgifterna behandlas, istället för som tidigare efter IT-system. På detta sätt blir det tydligare för enskilda som önskar ta del av information om nämndens personuppgiftsbehandlingar och ger även en mer komplett bild över behandlingarna. Därutöver har ett arbete påbörjats för att säkerställa att nämnderna genomför konsekvensbedömningar, även kallat DPIA efter förkortningen av den engelska benämningen Data Protection Impact Assessment, där det krävs. Under 2019 uppdaterades underlag och en kartläggning påbörjades om vilka befintliga personuppgiftsbehandlingar kräver konsekvensbedömningar. Detta fortsätter även under år 2020

Nämndens efterlevnad av dataskyddsförordningen

I detta avsnitt sammanfattas nämndens efterlevnad av dataskyddsförordningens krav utifrån de 12 prioriterade fokusområden som tidigare beslutats av stadsledningskontoret. De 12 områdena beskrivs under respektive punkt nedan tillsammans med en sammanfattning av nämndens efterlevnad på området.

1. Registrera personuppgiftsbehandlingar

En grundläggande förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningens regler är att veta vilka personuppgifter som behandlas och varför (i vilket syfte). Varje personuppgiftsansvarig ska enligt artikel 30 ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, kategorier av registrerade, typer av personuppgifter och lagringstid framgår.

Miljö- och stadsbyggnadsnämnden har 10 personuppgiftsbehandlingar registrerade. Registerförteckningen bedöms vara komplett och innehåller i stort sett all nödvändig information, endast någon enstaka information fattas.

2. Rapportera personuppgiftsincidenter

Varje personuppgiftsansvarig ska ha processer för att upptäcka, utreda, åtgärda och anmäla vissa personuppgiftsincidenter till tillsynsmyndigheten Datainspektionen. Det innebär att medarbetare ska kunna identifiera när en personuppgiftsincident har hänt, veta hur den ska rapporteras och att det finns processer för att ta hand om en bekräftad incident.

I Nacka kommun finns en central process för personuppgiftsincidenter som följs av nämnden. Medarbetare har på enhetsmöten informerats om incidenthanteringsprocessen. Nämnden rapporterade under 2019 tre incidenter. Ingen av incidenten anmäldes till Datainspektionen utan hanterades internt.

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.

Nämnden har genomfört konsekvensbedömningar för vissa befintliga personuppgiftsbehandlingar och en kartläggning har delvis gjorts.

4. Personuppgiftsbiträdesavtal (PUB-avtal)

Personuppgiftsbiträdesavtal ska tecknas om en personuppgiftsansvarig anlitar en extern part som behandlar personuppgifter åt 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 även när det är någon annan än den personuppgiftsansvarige som behandlar personuppgifterna.

Nämndens biträden utgörs i huvudsak av leverantörer av nämndens system och personuppgiftsbiträdesavtal finns tecknade med dessa.

5. Lagringsminimering, arkivering och gallring

Lagringsminimering är en av dataskyddsprinciperna och handlar om att personuppgifter endast behandlas 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 är det styrdokument som ska visa vilka allmänna handlingar en verksamhet har och hur dessa ska hanteras.

Nämnden har nyligen antagna informationshanteringsplaner inom flera områden, men det bör säkerställas att samtliga planer som berör nämndens information är uppdaterade.

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. Kommuner hanterar generellt personuppgifter i stor omfattning vilket kräver att det finns utarbetade processer på plats om hur ett registerutdrag ska hanteras.

I Nacka kommun finns en central process för registerutdrag som följs av nämnden. Denna process följer dataskyddsförordningens krav och under 2019 har 11 registerutdrag hanterats inom nämnden.

7. E-post

I dataskyddsförordningen finns inte som tidigare i personuppgiftslagen ett undantag för personuppgifter i ostrukturerat material, vilket betyder att även personuppgifter i ett e-

postmeddelande omfattas av dataskyddslagstiftning. Detta ställer höga krav på att även hanteringen av e-post följer dataskyddsprinciperna, exempelvis att personuppgifter endast behandlas för specifika syften och inte sparas längre än nödvändigt samt att känsliga personuppgifter skyddas med säkerhetsåtgärder.

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. Medarbetare inom nämnden har informerats om säker e-posthantering, men granskningen har inte omfattat en uppföljning av om personuppgiftshantering sker enligt guiden för säker e-posthantering.

8. Systemsäkerhet

En viktig dataskyddsprincip är integritet och konfidentialitet som handlar om att kunna säkerställa personuppgifternas konfidentialitet (att inga uppgifter röjs för obehöriga), tillgänglighet (att uppgifterna är tillgängliga när de behövs) och riktighet (att uppgifterna är korrekta). En metod för att ta fram krav på ett system som uppfyller dessa aspekter är informationsklassning som visar hur skyddsvärd informationen är utifrån de tre aspekterna. System kan därefter anpassas så att kraven motsvarar informationens skyddsvärde.

Nämndens system har informationsklassats, men klassningen bör följas upp regelbundet. På en kommunövergripande nivå pågår ett arbete med systematisk informationssäkerhet där klassning av information ingår.

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 (dvs. att personuppgifternas konfidentialitet skyddas) 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.

Nämnden har framtagna rutiner för tilldelning av behörigheter för majoriteten av system och lagringsytor, där rutiner fattas pågår ett arbete med att ta fram dessa. Det finns dock ett behov av att följa upp behörigheterna över tid, särskilt när anställda inom kommunen byter arbetsuppgifter, samt säkerställa att tilldelade behörigheter är ändamålsenliga, dvs. att tilldelade behörigheter motsvarar användarens behov av informationen. De rutiner och beslut som fattas av systemägare kring behörigheter bör därför även inkludera åtgärder för hur behörigheterna hålls uppdaterade och vilken behörighetsnivå motsvarar vilka arbetsuppgifter i systemet.

10. Samtycke

I dataskyddsförordningen skärptes kraven på hur och när samtycke kan användas som stöd för en personuppgiftsbehandling. För offentlig verksamhet betyder det att det numera finns

begränsade möjligheter att använda samtycke eftersom ett samtycke måste kunna ges helt frivilligt och en myndighet ofta står i maktpositionen gentemot en enskild.

Nämnden använder samtycke för bland annat kontrollansvariga som byggherrar anlitar. Nämnden har rutiner för hur samtycke inhämtas och informerar om att ett samtycke kan återkallas. Granskningen har dock inte omfattat en uppföljning av hur rutinerna för återkallandet av samtycket sker i praktiken.

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 in av 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.

En stickprovsgranskning av fall där nämnden inhämtar personuppgifter visar att nämnden i samtliga granskade fall lämnar information på ett lättillgängligt sätt, dock fattades viss obligatorisk information i några fall. Granskningen har inte omfattat om nämnden behandlar personuppgifter som är inhämtade från en annan källa utan att informera och utan att ett undantag är tillämpligt.

12. Efterlevnad

Efterlevnad handlar om att nämnden ska kunna visa att dataskyddsförordningens krav följs.

Inom alla fokusområden har nämnden genomfört ett arbete för att anpassa sig till dataskyddsförordningen krav. Nämnden ges följande rekommendationer för att kunna uppfylla kraven inom samtliga områden:

- Genomföra konsekvensbedömningar om dataskyddsförordningen kräver det.
- Fortsätta med ett systematiskt informationssäkerhetsarbete genom att genomföra informationsklassningar och övriga analyser som syftar till att nämndens information omfattas av den säkerhet informationen kräver. Detta inkluderar även ett arbete med behörigheter till nämndens information som uppfyller dataskyddsförordningens krav, dvs. att behörigheterna är aktuella och ges utifrån behov.
- Fortsätta arbeta med informationshanteringsplaner inom nämndens samtliga verksamheter och hålla dessa uppdaterade för att uppfylla kraven på lagringsminimering i dataskyddsförordningen.