



Nämnd och personuppgiftsansvarig
Kommunstyrelsen

Dataskyddsombudets årsrapport 2019

Dataskyddsombud
Hanna Virtanen

Datum 2020-05-05

Innehåll

Inledning.....	2
Sammanfattning av 2019 års arbete med dataskydd	2
Nämndens efterlevnad av dataskyddsförordningen	3
1. Registrera personuppgiftsbehandlingar.....	3
2. Rapportera personuppgiftsincidenter	3
3. Konsekvensbedömning (DPIA)	4
4. Personuppgiftsbiträdesavtal (PUB-avtal).....	4
5. Lagringsminimering, arkivering och gallring.....	4
6. Registerutdrag (rätten till tillgång)	4
7. E-post.....	5
8. Systemsäkerhet.....	5
9. Behörighet	5
10. Samtycke	6
11. Informationsplikt.....	6
12. Efterlevnad.....	6

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 kommunstyrelsen arbete med dataskydd under år 2019 och ger en översiktlig granskning av hur långt kommunstyrelsen 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).

Ansvar 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.

Kommunstyrelsen har 30 registrerade personuppgiftsbehandlingar. Förskolor, skolor och gymnasium inom Välfärd skola registrerar sina personuppgiftsbehandlingar separat och är inte inräknade. De registreringar som gjorts är i stort sett kompletta, endast någon enstaka information saknas. Registerförteckningen är dock ännu inte helt komplett då vissa verksameters personuppgiftsbehandlingar saknas.

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. Nämnden har under 2019 rapporterat in 20 incidenter, varav hälften anmäldes till Datainspektionen. I de ärenden där Datainspektionen återkopplat till nämnden har ärendena avslutats utan åtgärd. I övriga ärenden har Datainspektionen ännu inte gett återkoppling.

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.

I delar av nämndens verksamhet har en kartläggning gjorts över vilka personuppgiftsbehandlingar som kräver konsekvensbedömning och arbetet med att genomföra konsekvensbedömningarna har påbörjats men inte slutförts. Inom Valfärd skola har konsekvensbedömningar gjorts på systemnivå.

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.

Nämnden har tecknat personuppgiftsbiträdesavtal med sina biträden förutom i några enstaka fall där ett arbete pågår. En stickprovsgranskning av avtalen utifrån de formella kraven på avtalen visar att det i ett fall inte fanns instruktioner bilagda till avtalet och i tre fall saknades lista över underbiträden. Detta kan åtgärdas i samband med att bitrådets personuppgiftshantering följs upp.

5. Lagringsminimering, arkivering och gallring

Lagringsminimering är en av dataskyddsprinciperna och handlar om att personuppgifter endast 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 antagna informationshanteringsplaner inom flera områden, men det bör säkerställas att planerna är uppdaterade och omfattar den information nämnden hanterar.

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 10 registerutdrag hanterats av 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 framtagna 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.

Majoriteten av system som används inom nämnden har informationsklassats, men det finns behov av att följa upp klassningarna regelbundet och säkerställa att samtliga system informationsklassats. 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.

Framtagna rutiner för behörighetstilldelning finns, men det finns 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.

Samtycke används som rättslig grund vid publicering av bilder och filmer. Det finns framtagna rutiner för hur samtycket inhämtas och dokumenteras.

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 ger tillräcklig information enligt dataskyddsförordningen. Granskningen har dock 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 dataskyddsförordningens krav, men ett visst arbete kvarstår fortfarande. Följande rekommendationer ges till nämnden för att kunna uppfylla kraven inom samtliga områden:

- Prioritera att samtliga personuppgiftsbehandlingar förtecknas då en grundläggande förutsättning för att efterleva övriga krav enligt dataskyddsförordningen är att veta vilka personuppgifter nämnden behandlar.
- Säkerställa att personuppgiftsbiträdesavtalen uppfyller dataskyddsförordningens krav, särskilt vad gäller instruktioner till biträdet och information om underbiträden. Detta arbete kan göras i samband med en avtalsuppföljning för att kontrollera att ett biträde även lever upp till kraven på personuppgiftshantering.
- Arbeta med informationshangeringsplaner och hålla dessa uppdaterade. En stor del av nämndens personuppgifter finns i allmänna handlingar varför en uppdaterad



informationshanteringsplan är en förutsättning för att kunna uppfylla kraven på lagringsminimering enligt dataskyddsförordningen.

- Fortsätta med ett systematiskt informations säkerhetsarbete 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.