Stockholms stad

Implementering av dataskyddsförordningen
Nr 5, 2019

Projektrapport från Stadsrevisionen

Dnr: 3.1.3-107/2019

Den kommunala revisionen är fullmäktiges kontrollinstrument för att granska den verksamhet som bedrivits i nämnder och bolag. Stadsrevisionen i Stockholm stad granskar nämnders och styrelsers ansvarstagande för att genomföra verksamheten enligt fullmäktiges uppdrag. Stadsrevisionen omfattar både de förtroendevalda revisorerna och revisionskontoret.

I årsrapporter för nämnder och granskningspromemorior för bolagsstyrelser sammanfattar stadsrevisionen det gångna årets granskningar och bedömningar av verksamheten. Granskningar som genomförs under året kan också publiceras som projektrapporter.

Publikationerna finns på stadsrevisionens hemsida, stad.stockholm/revision. De kan också beställas från revisionskontoret, revision.rvk@stockholm.se.

Implementering av dataskyddsförordningen
Nr 5, 2019

Dnr: 3.1.3-107/2019 stad.stockholm/revision

Till
Kommunstyrelsen

Implementering av dataskyddsförordningen

Revisorsgrupp 1 har den 3 december 2019 behandlat bifogad revisionsrapport (nr 5/2019).

Utifrån granskningens resultat, som visar på flera brister gällande nämndernas implementering av dataskyddsförordningen, vill vi betona vikten av att kommunstyrelsen utvecklar sin styrning och uppföljning av nämndernas arbete med att efterleva förordningen.

Vi hänvisar i övrigt till rapporten och överlämnar den till kommunstyrelsen för yttrande. Yttrandet ska ha inkommit till revisorsgrupp 1 senast den 31 mars 2020. Rapporten överlämnas också till stadens övriga nämnder för kännedom.

På revisorernas vägnar

Ulf Bourker Jacobsson
Ordförande

Stefan Rydberg
Sekreterare

Stadsrevisionen

Hantverkargatan 3 D, 1 tr
Postadress: 105 35 Stockholm
Telefon: 08-508 29 000
Fax: 08-508 29 399
stad.stockholm/revision

Sammanfattning

Revisionskontoret har genomfört en granskning av nämndernas följsamhet till dataskyddsförordningen. Syftet med granskningen har varit att bedöma hur implementeringen av förordningen har genomförts. Samtliga nämnder har granskats förutom valnämnden. Kommunstyrelsen omfattas både i rollen som nämnd och som styrelse med uppsiktsplikt över stadens verksamheter. Genomförd granskning har ägt rum under juni-september 2019.

I denna rapport har granskningsresultatet redovisats på en stadsövergripande och aggregerad nivå. Detta med anledning av att granskningen har omfattat 30 nämnder. Rapporten tillställs kommunstyrelsen. Granskningsresultaten för enskilda nämnders personuppgiftshanteringar redovisas inom respektive nämnds årsrapport. Årsrapporterna utarbetas av revisionskontoret i samband med årsbokslutet för 2019.

Granskningen visar att det kvarstår arbete innan nämndernas arbete med personuppgiftshanteringar uppnår kraven i dataskyddsförordningen. I granskningen framkommer att samtliga nämnder har utsett dataskyddsombud och anmält dessa till Datainspektionen. För övriga delar som granskats finns avvikelser inom samtliga områden. Främst har avvikelser noterats beträffande nämndernas arbete med informationsklassning.

Som situationen ser ut idag är det nämnderna själva i rollen som personuppgiftsansvariga som säkerställer att kraven i dataskyddsförordningen efterlevs. Detta medför att det ställer krav på att t.ex. kompetens, resurser och förståelse finns på förvaltningarna för att uppnå kraven i dataskyddsförordningen. Med anledning av resultatet av granskningen, anser revisionskontoret att kommunstyrelsen behöver inta en mer aktiv roll i att styra, stödja och följa upp nämndernas implementering av dataskyddsförordningen. Att regelbundet tillhandahålla olika utbildningsinsatser om dataskyddsförordningen är en viktig del i detta arbete. I dagsläget finns inga obligatoriska utbildningar som stadens anställda måste genomgå inom detta område. Eftersom granskningen visar att det förekommer avvikelser beträffande informationsklassning, anser revisionskontoret att det är viktigt att förvaltningarna utbildas gällande informationsklassning.

Merparten av de stadsövergripande dokumenten avseende dataskyddsförordningen är att betrakta som rekommendationer, vägledningar, mallar och checklistor, d.v.s. är inte obligatoriska att följa

för nämnderna. Revisionskontorets uppfattning är att stadsövergripande styrdokument behöver utvecklas med tydliga skallkrav om vad som ska uppnås i implementeringen av förordningen. Det skulle också medföra enhetligare och tydligare styrning av stadens arbete för att efterleva kraven i förordningen.

Utifrån redovisade iakttagelser och bedömningar lämnas följande rekommendationer till kommunstyrelsen:

- Utveckla stadens styrning och uppföljning av nämndernas arbete med att efterleva dataskyddsförordningen.
- Tillhandahålla regelbundna utbildningar om dataskyddsförordningen och informationsklassning till stadens förvaltningar.

Innehåll

1. Inledning

1.1 Bakgrund

Dataskyddsförordningen eller GDPR (General Data Protection Regulation), innehåller regler om hur personuppgifter får behandlas. Dataskyddsförordningen är en EU-förordning som började gälla den 25 maj 2018 och som ersatte den tidigare personuppgiftslagen (PuL). Med personuppgifter avses alla slags information som direkt eller indirekt kan hänföras till en fysisk levande person. Enklaste typen av personuppgifter är personnummer, namn och adress. Förordningen gäller alla organisationer, företag och myndigheter som sparar eller hanterar personuppgifter om EU-medborgare. Syftet med dataskyddsförordningen är att ha ett anpassat regelverk till ett digitaliserat samhälle och att stärka den enskilde individens rättigheter och till skydd av personuppgifter.

Enligt dataskyddsförordningen är personuppgiftsansvarig den nämnd vars verksamhet behandlar personuppgifter. Detta innebär att varje nämnd har huvudansvaret för behandlingen av personuppgifter som förekommer inom sin organisation. Personuppgiftsansvarig bestämmer ändamål och medel för behandling av personuppgifter. Personuppgiftsansvarig har det yttersta ansvaret för att se till att verksamheten efterlever de krav som ställs i dataskyddsförordningen.

Det finns många likheter, men även en del skillnader, mellan dataskyddsförordningen och den tidigare personuppgiftslagen. Införandet av förordningen har generellt sett inneburit hårdare krav på hantering av personuppgifter. Bland annat behöver alla verksamheter föra register över vilka personuppgifter som hanteras. Det gäller samtliga personuppgifter som hålls strukturerade på något sätt. Missbruksregeln har försvunnit, vilket innebär att även personuppgifter i löpande text som t.ex. e-post, webbsida och strukturerade pärmar måste hanteras enligt den nya förordningen. Eftersom personuppgifter förekommer frekvent inom i princip alla områden, ställs stora krav på att verksamheterna implementerar rutiner som uppfyller de krav som finns i förordningen om ändamålsenlig hantering av personuppgifter. Medarbetare behöver ha kunskap om hur personuppgifter ska hanteras. Det finns risk att omfattande behandling av personuppgifter medför att nämnder inte har hunnit med att etablerat rutiner fullt ut för en ändamålsenlig hantering av personuppgifter. Brister i rutiner kan leda till skada för enskilda individer men också för staden i form av såväl anseendeförlust som ekonomisk förlust.

1.2 Syfte och revisionsfrågor

Syftet med granskningen är att bedöma hur implementeringen av dataskyddsförordningen har genomförts.

Granskningen besvaras med följande revisionsfrågor:

- Hur har nämnderna organiserat sitt arbete gällande hantering av personuppgifter?
- Hur säkerställer nämnderna kraven i dataskyddsförordningen om hur personuppgifter ska hanteras?
- Hur följer nämnderna upp sin hantering av personuppgifter?

1.3 Omfattning och avgränsning

Samtliga nämnder har granskats förutom valnämnden. Anledningen till att valnämnden inte har ingått i granskningen är att deras hantering av personuppgifter är av begränsad omfattning. Kommunstyrelsen omfattas både i rollen som nämnd och som styrelse med uppsiktsplikt över stadens verksamheter.

I denna rapport redovisas granskningsresultatet på en stadsövergripande och aggregerad nivå. Detta med anledning av att granskningen har omfattat 30 nämnder. Rapporten tillställs kommunstyrelsen. Granskningsresultaten för enskilda nämnders personuppgiftshanteringar redovisas inom respektive nämnds årsrapport. Årsrapporterna utarbetas av revisionskontoret i samband med årsbokslutet för 2019.

1.4 Revisionskriterier

Revisionskriterier är de bedömningsgrunder som revisionen utgår ifrån vid analys och bedömning. Följande revisionskriterier har tillämpats i granskningen:

- Dataskyddsförordningen. Europaparlamentets och rådets dataskyddsförordning (EU) 2016/679
- Rättelse till Europaparlamentets och rådets dataskyddsförordning (EU) 2016/679

1.5 Metod

Genomförd granskning har ägt rum under juni-september 2019.

Av dataskyddsförordningen framkommer ett antal krav som stadens nämnder ska uppfylla. Utifrån stadens information om förordningen på intranätet, anger stadsledningskontoret (SLK) att det krävs att ett antal grundläggande åtgärder är genomförda för att efterleva förordningen. Verksamheterna ska kunna säkerställa ett korrekt skydd för de personuppgifter som de behandlar.

Följande punkter ska uppnås:

- Dataskyddsombud har utsetts och anmälts till Datainspektionen.
- Inventering har skett av personuppgiftsbehandlingar.
- Registerförteckning är upprättad.
- Informationsklassning är genomförd.
- Skyddsåtgärder är införda.
- Personuppgiftsbiträdesavtal är upprättade med samtliga personuppgiftsbiträden.
- Rutiner har anpassats eller utarbetats för att säkerställa att personuppgifter behandlas på ett korrekt sätt.

Då SLK särskilt har lyft fram att ovanstående punkter är grundläggande åtgärder för att uppnå dataskyddsförordningens krav, har revisionskontoret utgått från dessa i granskningen. I den sistnämnda punkten har revisionskontoret valt att granska nämndernas rutiner för konsekvensbedömningar och personuppgiftsincidenter, egenkontroller av att personuppgiftshanteringar följer dataskyddsförordningen samt utbildningsinsatser om förordningen.

Dokumentstudier har genomförts av nämndernas rutiner för behandling av personuppgifter. Intervjuer har skett med samtliga nämnders dataskyddsombud. Under intervjuerna med dataskyddsombuden har även andra yrkeskategorier medverkat som t.ex. administrativa chefer, informationssäkerhetssamordnare, registratorer m.fl. Verifiering har därefter skett av nämndernas rutiner för personuppgiftshantering. Detta främst via utdrag av registerförteckningar men också rutiner för konsekvensbedömningar, incidentrapportering samt förteckning på informationsklassningar av IT-system.

Granskningen har genomförts av Erik Skoog och Örjan Palmqvist på revisionskontoret. Rapporten har faktakontrollerats av SLK.

2. Granskningens iakttagelser

2.1 Stadens styrning och organisation

Stadens modell för styrning av följsamhet till dataskyddsförordningen bygger på principen att varje nämnd har en lokal organisation, resurser, kompetens, utbildningar och instruktioner för att efterleva kraven i dataskyddsförordningen. Detta eftersom det är respektive nämnd som är personuppgiftsansvarig. Det innebär t.ex. att kommunstyrelsen har utsett ett dataskyddsombud för den egna verksamheten. I staden finns det däremot ingen uttalad funktion på kommunstyrelsen som leder stadens arbete kring dataskyddsförordningen. Enligt SLK ansvarar kommunstyrelsen via SLK för att stötta, samordna och följa upp nämndernas arbete med förordningen. Exempelvis har SLK via en särskild gruppering, *Centrala GDPR-projektet,* utarbetat ett antal stadsövergripande rekommendationer, vägledningar, mallar och checklistor inom specifika områden beträffande förordningen. Dessa handlar bl.a. om konsekvensbedömning, incidentrapportering m.m. Ordförande i styrgruppen för Centrala GDPR-projektet har varit stadens IT-direktör. Centrala GDPR-projektet bildades inför att dataskyddsförordningen skulle träda ikraft i maj 2018 men upphörde enligt uppgift i april 2019 p.g.a. att projektet skulle övergå i det ordinarie arbetet. Utöver olika stadsövergripande dokument utarbetade Centrala GDPR-projektet även bl.a. olika typer av utbildningsinsatser (t.ex. stadens e-utbildning om dataskyddsförordningen) och enkätundersökningar om förvaltningarnas fortlöpande arbete med förordningen. SLK samordnar också t.ex. nätverksträffar om dataskyddsförordningen för alla dataskyddsombud som finns på förvaltningarna. Möten hålls cirka sex gånger per år. Enligt uppgift handlar mötena bl.a. om nuläget för nämndernas arbete med förordningen, hur arbetet kan utvecklas vidare och att uppnå samsyn/praxis gällande följsamhet till förordningen.

Gällande stadens styrdokument i arbetet med dataskyddsförordningen är endast *Riktlinje informationssäkerhet* obligatoriska riktlinjer för nämnderna att följa. Riktlinjerna antogs av stadsdirektören 2014. Vissa redaktionella förändringar i riktlinjerna har skett i juni 2018 med anledning av att dataskyddsförordningens införande. Detta styrdokument är under revidering och enligt uppgift kan detta vara ett beslutsärende i fullmäktige tidigast under hösten 2020. Nuvarande riktlinjer kan ses som ett övergripande dokument som allmänt beskriver att insatser ska göras för att efterleva dataskyddsförordningen, inte på vilket sätt insatserna ska utföras. Detta medför att det ställer krav på att t.ex. kompetens, resurser och förståelse finns

på förvaltningarna för att korrekt hantering av personuppgifter ska uppnås.

Övriga stadsövergripande dokument gällande dataskyddsförordningen är att betraktas som rekommendationer, vägledningar, mallar och checklistor inom specifika områden. Enligt SLK vill kommunstyrelsen inte detaljstyra hur verksamheten ska arbeta med hanteringen av personuppgifter. Detta eftersom det är varje nämnd som ansvarar för sin personuppgiftsbehandling.

På stadens hemsida finns det bl.a. information om dataskyddsförordningen, stadens hantering av personuppgifter och uppgifter om nämndernas dataskyddsombud. Staden har också samlat information om dataskyddsförordningen på stadens intranät. På intranätet framgår bl.a. vad dataskyddsförordningen innebär, vilka rutiner, rekommendationer, vägledningar, mallar och checklistor som finns samt frågor och svar.

2.2 Implementering av dataskyddsförordningens krav

2.2.1 Dataskyddsombud

I dataskyddsförordningen framgår bl.a. att ett dataskyddsombud ska utses för respektive nämnd. Dataskyddsombudet ska delta i alla frågor som rör skyddet av personuppgifter. Vidare ska dataskyddsombudet informera och ge råd till nämnden eller nämndens personuppgiftsbiträde om personuppgiftshantering. Dataskyddsombudet ska ha en reviderande och rådgivande roll och inte delta i det operativa arbetet med behandling av personuppgifter som t.ex. inventering och upprättande av registerförteckning.

Samtliga nämnder har utsett dataskyddsombud och anmält ombuden till Datainspektionen. Flera nämnder delar på ansvarigt dataskyddsombud och det finns fall där en person är dataskyddsombud åt fyra nämnder. Merparten av dataskyddsombuden har dock andra arbetsuppgifter än att arbeta med frågor om dataskyddsförordningen som t.ex. arkivarie, nämndsekreterare, ILS-samordnare eller samordnare mot våldsbejakande extremism. Många dataskyddsombud uppger att det är svårt att uppskatta nedlagd arbetstid som kan hänföras till dataskyddsförordningen. Enligt genomförda intervjuer framkommer också att en del dataskyddsombud anger att de arbetar operativt med implementeringen av förordningen istället för att inta en rådgivande och reviderande roll i arbetet.

2.2.2 Inventering

I dataskyddsförordningen och i stadens *Vägledning för inventering av personuppgifter* framgår att förvaltningarna ska föra ett register över behandling av personuppgifter som utförts under dess ansvar. Innan dess behöver förvaltningarna inventera samtliga personuppgiftsbehandlingar som företas i verksamheten. Detta för att det ska kunna vara möjligt att kunna upprätta en fullständig registerförteckning.

De flesta förvaltningarna anger att de har genomfört en omfattande inventering av samtliga personuppgiftsbehandlingar i deras verksamheter. Det finns dock fall där det inte skett några kontroller av att alla enheter har inlämnat sina personuppgiftshanteringar till berörd avdelning.

Ingen av förvaltningarna arbetar regelbundet och systematiskt med inventering av samtliga personuppgiftsbehandlingar som företas i verksamheten. En tänkbar anledning till detta kan vara att förvaltningarna ser att personuppgiftshanteringarna i verksamheterna är relativt likartade över tid och att återkommande inventeringar inte medför några större förändringar i registerförteckningen. En del förvaltningar uppger dock att det finns en plan för att etablera rutiner för att genomföra inventeringar löpande.

2.2.3 Registerförteckning

Enligt dataskyddsförordningen ska varje nämnd föra register över samtliga personuppgiftsbehandlingar som sker inom respektive nämnds organisation, s.k. registerförteckning. Registerförteckningen uppfyller flera funktioner. Genom att upprätta en registerförteckning skapas kontroll över personuppgifter. Vidare kan förteckningen skapa förutsättningar för identifiering av lämpliga säkerhetsåtgärder som behöver vidtas om behandlingen t.ex. rör känsliga uppgifter. Utöver att ge en god överblick syftar en registerförteckning även till att säkerställa att det finns en laglig grund för personuppgiftsbehandlingen.

Samtliga förvaltningar har upprättat registerförteckning över vilka personuppgifter som de hanterar. I dataskyddsförordningen ställs inga krav på att en nämnd ska ha en samlad registerförteckning. Merparten av förvaltningarna har en samlad registerförteckning för samtliga personuppgiftshanteringar som förekommer inom en förvaltning. Av granskningen framgår dock att det finns förvaltningar som inte har en samlad registerförteckning för sina hanteringar av personuppgifter. I sådana fall finns det upprättade registerförteckningar per avdelning eller enhet på en förvaltning. Av intervjuerna

framkommer att berörda förvaltningar anser att ansvaret för inventering av personuppgiftshantering och upprättande av registerförteckning lämpligast utförs på avdelnings-/enhetsnivå. Detta eftersom det är där personuppgiftshantering uppstår.

Revisionskontoret har genomfört en verifiering av förvaltningarnas registerförteckning över vilka personuppgifter som nämnderna hanterar. I en registerförteckning kan det förekomma en mängd olika beskrivningar av en personuppgiftshantering. Revisionskontoret har valt att granska valda delar ur registerförteckningarna och utgått från dataskyddsförordningens och stadens krav på obligatoriska rubriker i en registerförteckning. Enligt dataskyddsförordningen och stadens *Vägledning för inventering av personuppgifter* ska följande rubriker vara ifyllda beträffande registerförteckning över personuppgiftshanteringar:

- Ändamål/verksamhetsprocess
- Kategori på personuppgifter
- Kategori på registrerade
- Kategori på mottagare
- Överföring till tredjeland (ej EU/EES-land)

Utifrån genomförd verifiering noterar revisionskontoret att merparten av förvaltningarna har en registerförteckning utifrån de obligatoriska rubrikerna. Det framkommer dock att det finns förvaltningar som i sina registerförteckningar utelämnar uppgifter inom vissa rubriker.

2.2.4 Informationsklassning

Av stadens *Riktlinje informationssäkerhet* framgår bl.a. att informationsklassning innebär att alla stadens informationstillgångar[1] ska klassificeras för att få rätt skyddsnivå som motsvarar dess betydelse för verksamheten. Informationsklassning är en metod som hjälper verksamheten att välja rätt åtgärder för att skydda informationen. Vidare framkommer i riktlinjen att SLK:s handbok för informationsklassificering ska användas. *Handbok för informationsklassning* har antagits av Styrgruppen för GDPR-projektet. I arbetet med att ta fram handboken har enligt uppgift samtliga informationssäkerhetssamordnare på förvaltningarna varit delaktiga. I handboken anges bl.a. att genomföra informationsklassning är i linje med kommunfullmäktiges beslut att staden ska arbeta strukturerat med informationssäkerhet enligt standarden ISO/IEC 27001 (Ledningssystem för informationssäkerhet). Även dataskyddsförordningen ställer krav på

[1] Informationstillgångar innebär informationen i sig och de resurser som används för att hantera den.

att säkerställa lämplig skyddsnivå beträffande hantering av personuppgifter.

Enligt SLK:s *Handbok för informationsklassning* ska informationsklassificering ske i fyra konsekvensnivåer utifrån:
- *Konfidentialitet* (K) – att obehöriga inte kan få tillgång
- *Riktighet* (R) – att de är korrekta
- *Tillgänglighet* (T) – att de finns tillgängliga när de behövs

Nivåbestämningen för konfidentialitet, riktighet och tillgänglighet utgår från bedömd skada vid obehörig åtkomst, bristande riktighet och bristande tillgänglighet till informationstillgång. Konsekvensnivå 0 innebär ingen eller försumbar skada, konsekvensnivå 1 innebär måttlig *skada*, konsekvensnivå 2 omfattar *betydande skada* och konsekvensnivå 3 medför *allvarlig/katastrofal skada*.

I *Stadens förvaltningsmodell Fguide* (2018) framkommer bl.a. informationsägarens och systemägarens ansvar. Informationen som hanteras inom objektet ägs av informationsägaren medan systemägaren säkerställer att systemen har ett tillräckligt skydd utifrån informationsägarens krav. Information i ett system kan ha sin källa i flera olika förvaltningar varpå det i praktiken också kan finnas flera olika informationsägare. Informationsägaren ansvarar för att fastställa verksamhetens krav på säkerhet genom en informationsklassning som ska genomföras årligen. Om det vid den årliga översynen av informationsklassningen av informationstillgången visar att det inte har skett några förändringar (t.ex. i lagstiftning, omvärld eller verksamhetsförändringar som inverkar på den klassning som genomförts tidigare) så ska detta formellt bekräftas. Det innebär att klassningen i dessa fall inte behöver göras om utan enbart bekräftas som fortfarande gällande. Systemägaren har det yttersta ansvaret för ett IT-system som hanterar information. Inom staden är nämnden som äger IT-systemet systemägare. Systemägaren ska se till att systemet uppfyller kraven på säkerhet i relation till skyddsvärdet för den information som hanteras i systemet. Vad tillräckligt skydd innebär, avgörs av bl.a. informationsägarens(-/nas) krav. Således är det viktigt att det sker en dialog mellan informationsägare och systemägare gällande informationsklassning.

Av genomförd granskning framkommer att det är många förvaltningar som inte informationsklassar sina informationstillgångar i alla de IT-system som hanterar personuppgifter. Detta oavsett om IT-systemen betraktas som nämndspecifika/lokala eller centrala. Ingen av förvaltningarna informationsklassar sina informationstillgångar i centrala IT-system som de inte är systemägare av men som

innehåller uppgifter för vilka de är informationsägare av. Förvaltningarna gör inte någon egen värdering eller bedömning av vilken klassning informationstillgångar bör ha i centrala IT-system utifrån den personuppgiftshantering som de berörda förvaltningarna gör i egenskap av informationsägare. Utifrån genomförd granskning framkommer att det inte sker någon dialog mellan systemägare och informationsägare vid informationsklassning.

Det framgår också utifrån revisionskontorets verifiering av förvaltningarnas förteckningar på informationsklassade informationstillgångar i IT-system att det saknas en fullständig bild av vilka IT-system som är informationsklassade och när klassning har skett. Detta har iakttagits på SLK och en del andra förvaltningar. Revisionskontoret har också uppmärksammat att merparten av förvaltningarna inte årligen informationsklassar informationstillgångar i de IT-system som de är systemägare av.

Ovanstående iakttagelser som har framgått av granskningen har också tidigare uppmärksammats av stadens informationssäkerhetsansvarig på SLK. Centrala GDPR-projektet genomförde i början av 2019 en enkät som skickades ut till stadens dataskyddsombud. Dataskyddsombuden gjorde en självskattning av nuläget i nämndernas arbete med att efterleva dataskyddsförordningen och bl.a. framkom brister inom informationsklassningen. Enligt stadens informationssäkerhetsansvarig saknas metodstöd och utbildningsinsatser till förvaltningarna när det gäller informationsklassning.

Enligt uppgift har SLK påbörjat ett arbete med dialoger mellan systemägare och informationsägare för informationsklassning, där SLK är systemägare och övriga förvaltningar är informationsägare. Detta för att säkerställa att informationsklassning genomförs enligt dataskyddsförordningen och stadens styrdokument.

2.2.5 Skyddsåtgärder

Av intervjuerna framgår att förvaltningarna anger att de har infört skyddsåtgärder för IT-system som hanterar personuppgifter. Flera förvaltningar uppger att de främst vidtar skyddsåtgärder gällande behörighetsstyrning samt koder och lösenord för inloggningar. Av granskningen framkommer att det inte finns koppling fullt ut mellan informationsklassning och vidtagna skyddsåtgärder. Detta med anledning av de avvikelser som revisionskontoret har noterat gällande informationsklassningar tidigare i rapporten.

2.2.6 Personuppgiftsbiträdesavtal

Personuppgiftsbiträde är den som behandlar personuppgifter för personuppgiftsansvariges räkning. Ett personuppgiftsbiträde kan exempelvis vara en IT-leverantör eller redovisningskonsult. Det är den personuppgiftsansvarige som ska tillse och kontrollera att anlitade personuppgiftsbiträden uppfyller kraven. När ett personuppgiftsbiträde anlitas måste ett skriftligt personuppgiftsbiträdesavtal (PuB-avtal) upprättas. PuB-avtalet ska säkerställa att leverantören endast behandlar personuppgifter i enlighet med personuppgiftsansvariges instruktioner. Detta framgår i dataskyddsförordningen. SLK har upprättat en mall och en instruktion som förvaltningarna kan använda sig av vid upprättande av PuB-avtal.

Merparten av förvaltningarna har genomfört en kartläggning av behovet av PuB-avtal. En del förvaltningar uppger att kartläggning pågår gällande PuB-avtal. Det framkommer dock att några förvaltningar inte har påbörjat en kartläggning av behovet av PuB-avtal. Enligt berörda förvaltningar beror detta bl.a. på att det inte har funnits resurser att genomföra kartläggningen och att inventeringen av registerförteckningen över personuppgiftshanteringen inte har slutförts. Det framkommer också av intervjuerna att flera förvaltningar inte har upprättat PuB-avtal med samtliga personuppgiftsbiträden. Enligt intervjuade är det i flera fall svårt att avgöra om PuB-avtal ska tecknas. Det är inte alltid tydligt vem som är personuppgiftsansvarig eller personuppgiftsbiträde. Det finns också fall där berörda leverantörer inte vill skriva på PuB-avtal. Förvaltningarna efterfrågar stöd och utbildning från SLK beträffande PuB-avtal. Det framkommer också i intervjuer att SLK behöver samla stadens centrala PuB-avtal på ett för staden gemensamt ställe. I nuläget är det svårt att få en överblick på alla upprättade PuB-avtal som finns i staden.

2.2.7 Rutiner

Konsekvensbedömning
En konsekvensbedömning är ett tillvägagångssätt som hjälper förvaltningarna att identifiera och minimera integritetsriskerna för personuppgifter som behandlas. I dataskyddsförordningen och i SLK:s *förslag till rutin för processen konsekvensbedömning avseende dataskydd* framgår att konsekvensbedömning ska genomföras om en personuppgiftsbehandling sannolikt kan leda till en hög risk för fysiska personers rättigheter och friheter. I stadens *Rutin för konsekvensbedömning* framgår de olika stegen när en konsekvensbedömning ska genomföras och vad som ska göras i de olika stegen i processen.

Av intervjuerna och genomförda verifieringar framgår att flertalet förvaltningar har rutiner för att genomföra konsekvensbedömningar. En del förvaltningar har etablerat egna rutiner medan andra förvaltningar följer stadens rutin för genomförande av konsekvensbedömning. Det är dock flera förvaltningar som inte har några rutiner för konsekvensbedömningar. Som skäl för detta har förvaltningarna framfört att det inte finns den typen av personuppgiftsbehandlingar som medför särskilda integritetsrisker. Därför är det inte aktuellt att göra konsekvensbedömningar enligt de berörda förvaltningarna.

Under revisionskontorets granskning har enligt uppgift SLK påbörjat dialoger mellan systemägare och informationsägare beträffande konsekvensbedömningar av ett antal personuppgiftsbehandlingar i IT-system, där SLK är systemägare och övriga förvaltningar är informationsägare. Det är dock alltid de personuppgiftsansvariga nämnderna som konsekvensbedömer personuppgiftsbehandlingarna. Detta för att säkerställa att konsekvensbedömningar av IT-system genomförs i enlighet med dataskyddsförordningen och stadens rutiner.

Incidentrapportering
En personuppgiftsincident är en säkerhetshändelse som har påverkat sekretessen, integriteten eller tillgängligheten till personuppgifter. En personuppgiftsincident har inträffat om personuppgifter har förstörts, oavsiktligt eller olagligt, gått förlorade eller ändrats eller röjts till någon obehörig. Angående incidentrapportering finns det en skyldighet i dataskyddsförordningen att förvaltningarna ska dokumentera alla incidenters omständigheter, effekter, konsekvenser och korrigerande åtgärder i de fall dessa har vidtagits. Detta om incidenterna sannolikt leder till hög risk för fysiska personers rättigheter och friheter. Information om incidenterna ska i sådana fall inrapporteras till Datainspektionen, vilket framgår i stadens *Vägledning vid händelse av en personuppgiftsincident* och *Riktlinje för incidentrapportering*. Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att de fått vetskap om den, anmäla personuppgiftsincidenten till tillsynsmyndigheten, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Dessutom ska personuppgiftsincidenter inrapporteras i stadens *incidentrapporteringssystem IA*. Berörd förvaltning ansvarar sedan för vidarehandläggning av inrapporterad incident i IA.

Merparten av förvaltningarna har rutiner för incidentrapportering till Datainspektionen gällande personuppgiftsincidenter. Flertalet av

förvaltningarna följer stadens vägledning vid händelse av en personuppgiftsincident eller stadens rutiner för inrapportering av incidentavvikelser, IA beträffande personuppgiftsincidenter. Det förekommer också att förvaltningar har egna rutiner för incidentrapportering. Ett fåtal förvaltningar saknar rutiner för incidentrapportering. Som skäl för detta har berörda förvaltningar framfört att det sker en avvaktan på att nya rutiner från SLK skulle implementeras i staden under 2019. Revisionskontoret vill understryka vikten av att alla nämnder tar fram rutiner för incidentrapportering.

Större delen av förvaltningarna uppger att det har inträffat personuppgiftsincidenter. Samtliga incidenter har dock inte behövt inrapporteras till Datainspektionen. Enligt förvaltningarnas bedömningar beror detta på att personuppgiftsincidenterna inte har medfört en risk för att de registrerades rättigheter och friheter åsidosätts.

Enligt Datainspektionen pågår en tillsyn av utbildningsnämndens hantering av elevuppgifter. Upprinnelsen till tillsynen är utbildningsförvaltningens anmälan till Datainspektionen om inträffad personuppgiftsincident. Enligt Datainspektionen är det oklart när granskningen kan slutföras. Datainspektionen uppger att det inte har skett någon ytterligare tillsyn av staden sedan dataskyddsförordningen trädde ikraft i maj 2018.

Egenkontroller
Enligt dataskyddsförordningen framgår att dataskyddsombudet har en reviderande roll och ska kontrollera att förordningen följs genom att utföra kontroller. Det är alltid personuppgiftsansvarigas ansvar att se till att all personuppgiftsbehandling sker i enlighet med förordningen.

Det framkommer i intervjuerna att förvaltningarna genomför begränsade kontroller av att deras hantering av personuppgifter följer dataskyddsförordningen. Dock finns det några nämnder som uppger att det sker omfattande egenkontroller av personuppgiftshanteringar. Exempelvis kan det handla om att gå igenom behörigheter till dokumentationssystem eller kontrollera valda delar av registerförteckningen. Många förvaltningar uppger att det finns planer på att genomföra egenkontrollerna på ett mer systematiskt sätt än vad som sker idag. En del förvaltningar uppger att en granskningsplan har upprättats för 2019, där vissa kontroller kommer att genomföras under året.

Utbildning

Av genomförda intervjuer framgår att utbildning om dataskyddsförordningen har genomförts på samtliga förvaltningar. Vissa förvaltningar har information om förordningen som en del i nyanställdas introduktionsutbildningar. Flera förvaltningar uppmuntrar sina anställda att genomgå stadens e-utbildning om dataskyddsförordningen. E-utbildningen är dock inte obligatorisk. Ett flertal förvaltningar uppger i intervjuerna att utbildningsinsatserna om förordningen har varit av generell karaktär och inte anpassats för de olika roller/funktioner som finns i organisationen. Merparten av förvaltningarna har inte rutiner för att säkerställa att samtliga anställda har genomgått utbildning om dataskyddsförordningen.

3. Slutsatser

Granskningen visar att nämndernas arbete med att implementera dataskyddsförordningen behöver utvecklas. I granskningen framkommer att samtliga nämnder har utsett dataskyddsombud och anmält dessa till Datainspektionen. För övriga delar som granskats finns avvikelser inom samtliga områden. Främst har avvikelser noterats beträffande nämndernas arbete med informationsklassning. Det har inte framkommit något tydligt mönster avseende vilka nämnder som har kommit längre än andra i att implementera förordningen. Nämndens ansvarsområden, storlek eller sätt att organisera arbetet förefaller inte ha haft avgörande betydelse för resultatet av det arbete som har genomförts hittills.

SLK drev initialt ett projekt i syfte att underlätta nämndernas arbete med dataskyddsförordningen. Utöver olika stadsövergripande dokument utarbetade projektet även bl.a. olika typer av utbildningsinsatser och informationsmaterial till intranätet för att stödja förvaltningarna i deras arbete. Efter det att projektet avslutades har projektet övergått i det ordinarie arbetet. Ett nätverk för dataskyddsombud finns dock som leds av SLK. Som situationen ser ut idag är det nämnderna själva i rollen som personuppgiftsansvariga som säkerställer att kraven i dataskyddsförordningen efterlevs. Detta medför att det ställer krav på att t.ex. kompetens, resurser och förståelse finns på förvaltningarna för att efterleva kraven i dataskyddsförordningen.

Med anledning av resultatet av granskningen, anser revisionskontoret att kommunstyrelsen behöver inta en mer aktiv roll i att styra, stödja och följa upp nämndernas implementering av dataskyddsförordningen. Att regelbundet tillhandahålla olika utbildningsinsatser om dataskyddsförordningen är en viktig del i detta arbete. I dagsläget finns inga obligatoriska utbildningar som stadens anställda måste genomgå inom detta område. Eftersom granskningen visade att det förekom avvikelser beträffande informationsklassning, anser revisionskontoret att det är viktigt att förvaltningarna utbildas gällande informationsklassning.

Merparten av de stadsövergripande dokumenten avseende dataskyddsförordningen är att betrakta som rekommendationer, vägledningar, mallar och checklistor, d.v.s. är inte obligatoriska att följa för nämnderna. Revisionskontorets uppfattning är att stadsövergripande styrdokument behöver utvecklas med tydliga skallkrav om vad som ska uppnås i implementeringen av förordningen. Det skulle

också medföra enhetligare och tydligare styrning av stadens arbete för att efterleva kraven i förordningen.

4. Sammanvägd bedömning och rekommendationer

Granskningen visar att det kvarstår arbete innan nämndernas arbete med personuppgiftshanteringar uppnår kraven i dataskyddsförordningen. Bland annat behöver arbetet med informationsklassning utvecklas. I kommande årsrapporter, som revisionskontoret utarbetar för varje nämnd, kommer specifika rekommendationer lämnas som riktar sig till respektive nämnd.

För att ge nämnderna förutsättningar att efterleva kraven i dataskyddsförordningen, bedömer revisionskontoret att kommunstyrelsen behöver inta en mer aktiv roll i att styra, stödja och följa upp nämndernas arbete.

Utifrån redovisade iakttagelser och bedömningar lämnas följande rekommendationer till kommunstyrelsen:

- Utveckla stadens styrning och uppföljning av nämndernas arbete med att efterleva dataskyddsförordningen.
- Tillhandahålla regelbundna utbildningar om dataskyddsförordningen och informationsklassning till stadens förvaltningar.