Granskning av efterlevnad av dataskyddsförordningen

Rapport

Säters kommun

KPMG AB

2020-09-01

Antal sidor 19

Säters kommun
Granskning av efterlevnad av dataskyddsförordningen

2020-09-01

Innehållsförteckning

1 Sammanfattning

Vi har av Säters kommuns revisorer fått i uppdrag att granska kommunens rutiner för efterlevnad av dataskyddsförordningen/GDPR. De förtroendevalda revisorerna har utifrån risk- och väsentlighet valt att granska kommunens övergripande arbete med att efterleva GDPR. Uppdraget ingår i revisionsplanen för år 2020.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunen till stor del har ändamålsenliga styrdokument för personuppgiftshantering samt en organisation för att bedriva ett systematiskt arbete med GDPR. Kommunstyrelsen och nämnder behöver säkerställa att dataskyddsombud får utbildning i sakfrågorna för att motsvara de lagkrav som finns för uppdraget samt resurser för att utföra sitt uppdrag.

Vår bedömning är att det finns registerförteckningar upprättade över kommunens personuppgiftsbehandlingar för samtliga nämnder och styrelsen men att dessa inte fullt ut är kompletta. Det är en högst väsentlig del i kommunens efterlevnad av dataskyddsförordningen och det är därför positivt att kontroll av dessa ingår i samtliga nämnder och styrelsens interna kontroll för 2020.

Vi ser det som positivt att arbetet under 2019 skett på ett strukturerat sätt och dokumenterats i en årlig förvaltningsplan som beslutats av förvaltningschefsgruppen och delgetts nämnder och styrelsen. Vi har dock i granskningen inte fått ta del av en sådan plan för 2020. Vi anser att detta sätt att systematisera arbetet med GDPR borde prioriteras då det även ingår som en kontrollpunkt i nämndernas och styrelsens interna kontrollplan.

Det finns en organisation för incidenthantering som är dokumenterad i beslutade riktlinjer samt i förvaltningsplan för GDPR. Vi anser däremot att medvetenheten och kunskapen om personuppgiftsincidenter och GDPR i stort är för låg vilket visar sig i få rapporterade personuppgiftsincidenter.

Att säkerställa kommunens efterlevnad av GDPR är ett pågående arbete och delar av arbetet kvarstår för att efterleva lagen fullt ut.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen och nämnderna att:

- säkerställa en tillräcklig kompetensnivå och resurser för dataskyddsombud
- säkerställa att dataskyddsombud involveras och rådfrågas i högre grad i alla frågor som rör skyddet av personuppgifter
- dataskyddsombud fullföljer sitt uppdrag och genomför regelbunden tillsyn över personuppgiftsansvarigas efterlevnad av dataskyddsförordningen
- utifrån kontrollmål för efterlevnad av GDPR i internkontrollplan för 2020 bedöma risk och konsekvenser för brister i efterlevnad av GDPR och upprätta kontrollåtgärder för dessa
- säkerställa att utbildning genomförs för samtliga medarbetare för att medvetenheten om hantering av personuppgifter ska vara tillräcklig

2 Inledning

Vi har av Säters kommuns revisorer fått i uppdrag att granska kommunens rutiner för efterlevnad av GDPR, den allmänna dataskyddsförordningen.

Dataskyddsförordningen är den svenska benämningen på GDPR (The General Data Protection Regulation) som trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. I och med ikraftträdandet av GDPR upphävdes personuppgiftslagstiftningen, (PuL 1998:204). Den nya lagstiftningen syftar bland annat till ett starkare skydd för individers integritet och större makt för att kunna bestämma över sina personuppgifter. Härigenom ska kommunen anpassa hanteringen av personuppgifter till gällande regler inom ramen för GDPR. Bristande hantering samt överträdelser kan innebära sanktionsavgifter till skillnad från tidigare lagstiftning. En ytterligare påtaglig risk är att en bristande hantering leder till förtroendeskador för personuppgiftsansvariga i nämnder och styrelser samt för kommunen i sin helhet.

Hantering av personuppgifter ska ske utifrån GDPR: s grundläggande principer:

- Laglighet
- Korrekthet
- Öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

Vid behandling av personuppgifter måste verksamheterna stödja sig på rättslig grund[1]. Utan en sådan är personuppgiftsbehandling inte laglig. Vidare ska kommunstyrelse och nämnder utse ett dataskyddsombud, vilken bland annat har till uppgift att övervaka efterlevnaden av GDPR.

De förtroendevalda revisorerna har utifrån risk- och väsentlighet valt att granska kommunens övergripande arbete med att efterleva GDPR. Det bedöms föreligga risk för att verksamheterna inte färdigställt allt som behöver anpassas samt införas och bedömer det därför som väsentligt att detta område granskas.

[1] En kommun använder främst rättslig förpliktelse, uppgift av allmänt intresse eller myndighetsutövning och avtal. En kommun får inte använda sig av intresseavvägning. Samtycke är oftast en olämplig rättslig grund för en kommun eftersom den måste vara frivilligt och jämlikt utformad.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningen har syftat till att svara på om kommunstyrelsen och nämnderna har vidtagit tillräckliga åtgärder för att säkerställa att kommunen följer lagstiftningen enligt GDPR.

Granskningen har besvarat följande revisionsfrågor:

- Finns det ändamålsenliga policys, riktlinjer och instruktioner upprättade inom området?
- Finns registerförteckning upprättad för personuppgiftsbehandlingar inom styrelsens förvaltning/ar?
- Har styrelse och nämnder genom beslut utsett ett dataskyddsombud?
- Har styrelsen genom beslut fastställt en ändamålsenlig arbetsbeskrivning för dataskyddsombudet utifrån dataskyddsförordningen krav?
- Har kartläggningar och analyser av anpassningsbehov inom IT-system genomförts?
- Har åtgärder vidtagits för att säkerställa att det hos medarbetarna inom förvaltningen finns en tillräcklig kunskap om de krav som följer av dataskyddsförordningens ikraftträdande?
- Finns en ändamålsenlig organisation för incidenthantering utifrån data-skyddsförordningens krav?
- Har styrelser och nämnd säkerställt en tillräcklig rapportering om arbetet med att uppfylla kraven i dataskyddsförordningen?

Granskningen avser kommunstyrelsen och samtliga nämnder.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Kommunallagen 6 kap. § 6
- Dataskyddsförordningen/GDPR
- Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
- Internt styrande dokument.

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier av riktlinjer, rutiner, rapportering
- Analys av vidtagna åtgärder
- Intervjuer med dataskyddsombud, informationssäkerhetsansvarig, fem dataskyddshandläggare som representerar de olika förvaltningarna

Samtliga intervjupersoner har erbjudits att faktagranska rapporten.

Granskningen är genomförd av Jenny Thörn, kommunal revisor under ledning av Karin Helin Lindqvist, certifierad kommunal revisor och kundansvarig i Säters kommun.

3 Resultat av granskningen

3.1 Styrdokument

Riktlinjer för behandling av personuppgifter

Säters kommun har fastställt ”Riktlinjer för behandling av personuppgifter” i kommunstyrelsen 2018-09-01.

Det framgår i inledningen av riktlinjerna att dessa avser att säkerställa att Säters kommun efterlever de lagrum som styr behandling av personuppgifter. Det framgår vidare att det gäller GDPR men även den särlagstiftning som finns för vissa verksamhetsområden såsom t.ex. Patientdatalag (2008:355) och Lag (2001:454) om behandling av personuppgifter inom socialtjänsten.

Syfte och mål med riktlinjerna är att:

> *”De personuppgifter som hanteras i Säters kommun, både direkta och indirekta, ska vara korrekta, riktiga och relevanta för ändamålet med behandlingen. Behandlingen ska ske med stöd av lag. Personuppgifterna ska skyddas så att de inte sprids vidare på ett otillåtet sätt.”*

I dokumentet finns beskrivningar av hur det systematiska arbetet ska bedrivas, moment som ingår för att säkerställa detta samt hantering av personuppgifter i kommunen.

Övriga styrande dokument

I Säters kommun finns även andra styrdokument som reglerar kommunens arbete med informationssäkerhet och informationshantering. Därtill finns rutiner för exempelvis arkivering och gallring som stödjer arbetet med personuppgiftshanteringen och GDPR.

Exempel på dessa dokument är Informationssäkerhetspolicy, Riktlinje för ledningssystem för informationssäkerhet, informationshanteringsplan mm.

3.1.1 Bedömning

Vår bedömning är att det finns ändamålsenliga riktlinjer och rutiner för personuppgiftshantering beslutade i kommunen. Det finns även en beslutad informationshanteringsplan samt styrdokument inom informationssäkerhet som kompletterar riktlinjer och rutiner för personuppgifter.

3.2 Organisation och ansvarsfördelning för arbetet med GDPR

3.2.1 Organisation

Kommundirektören är övergripande ansvarig för kommunens säkerhetsarbete. Tidigare fanns en säkerhetssamordnare som även hade rollen dataskyddsombud men sedan en omorganisation så finns inte rollen säkerhetssamordnare kvar.

I intervjuer framkommer en saknad av någon som håller ihop helheten i säkerhetsarbetet då ingen har detta som huvuduppdrag längre utan samtliga tjänster inom säkerhet är sidouppdrag.

Dataskyddsfrågorna rapporteras till förvaltningschef kommunkansliet vilken är underställd kommundirektören.

I Säters kommun har samtliga nämnder och styrelsen utsett dataskyddsombud genom beslut, vilket vi har tagit del av i protokoll från nämndernas och styrelsens sammanträden.

Förvaltningarna har även utsett dataskyddshandläggare inom varje förvaltning som ska vara ett stöd i nämndernas personuppgiftsansvar. Dataskyddshandläggarna utses av förvaltningschef inom respektive förvaltning och de ansvarar för det praktiska arbetet med GDPR.

GDPR-gruppen

Hösten 2017 inrättades en GDPR-grupp inför inträdet av GDPR 2018. I gruppen ingår dataskyddsombud och dataskyddshandläggarna. Det sker regelbundna möten där erfarenhetsutbyte, information och nyheter inom dataskyddsområdet avhandlas.

I intervjuer framkommer att man upplever att det finns ett stort stöd i gruppen och alla hjälper varandra med frågor inom området.

Gruppen ansvarar för att ta fram en årlig förvaltningsplan för arbetet med personuppgifter och dataskydd.

Informationssäkerhetsgruppen

Det finns en informationssäkerhetsgrupp som leds av informationssäkerhetsansvarig där dataskyddsombud och representanter från IT ingår. I intervjuer framkommer att informationssäkerhetsarbetet och arbetet med GDPR är nära sammankopplat i kommunen.

3.2.2 Roller och ansvar i arbetet med GDPR

Personuppgiftsansvarig

I GDPR finns krav på hur personuppgifter ska hanteras. Personuppgiftsansvariga är i kommunens fall nämnder och styrelser. Utifrån detta har nämnderna och styrelserna

att tillse att behandling av personuppgifter inom ramen för deras respektive verksamhetsområden följer de grundläggande principerna för personuppgifts-behandling, bland annat laglighet, korrekthet och öppenhet.

Dataskyddsombud

Det finns lagkrav på att ha dataskyddsombud för myndigheter och dataskyddsombudets roll är lagreglerad. I artikel 37–39 framgår de nya reglerna avseende dataskyddsombud.

Uppdraget som dataskyddsombud kan delas in i tre delar:

- Samla in information om personuppgiftsbehandling
- Kontrollera efterlevnad av GDPR (och anknytande lagstiftning)
- Informera och ge råd om personuppgiftsbehandling

Dataskyddsombudets uppdrag är huvudsakligen granskande och rådgivande och har inget eget ansvar för att organisationen följer GDPR. Enligt reglerna i GDPR ska dataskyddsombud kunna fungera oberoende i organisationen och rapportera till personuppgiftsansvariges högsta förvaltningsnivå.

På Datainspektionens hemsida finns ett dokument för riktlinje för dataskyddsombud. I det beskrivs ett antal skyddsåtgärder för att dataskyddsombudet ska kunna fungera på ett oberoende sätt:

- Personuppgiftsansvariga eller personuppgiftsbiträden får inte ge instruktioner som gäller utförandet av dataskyddsombudets uppgifter.
- Han eller hon får inte avsättas eller bli föremål för sanktioner för att ha utfört sina uppgifter.
- Det får inte förekomma intressekonflikter i samband med eventuella andra uppgifter och uppdrag.

Enligt SKR beskrivs rollen enligt följande: *”Personen som utses till dataskyddsombud ska utses baserat på yrkesmässiga kvalifikationer, sakkunskap och förmåga att utföra uppgifterna och därmed ha kunskap om dataskydd. Ombudet ska kunna agera självständigt och oberoende i organisationen. De personuppgiftsansvariga nämnderna inom kommunen eller regionen ansvarar för att ombudet får det stöd, befogenheter och tillräckliga resurser som krävs för att kunna utföra sitt uppdrag på ett effektivt och oberoende sätt. Ombudet ska också ges möjlighet att delta i alla frågor som rör dataskydd och rapportera direkt till högsta förvaltningsnivå.”*

Att det finns kompetenskrav för de dataskyddsombud som utses är förstärkt i reglerna sedan personuppgiftslagen, PuL. Detta medför att det är viktigt att kommunerna inte per automatik utser den person som tidigare hade rollen som personuppgiftsombud (tidigare benämning inom PuL).

I artikel 37, 38, 39 i dataskyddsförordningen tydliggörs dataskyddsombudets uppgifter. Där framgår att ett dataskyddsombud ska utses på grundval av sina yrkesmässiga

kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd. Ett dataskyddsombud ska vara oberoende och får inte ta emot instruktioner som gäller utförandet av uppgifterna. Ett dataskyddsombud får vid sidan av sina dataskyddsuppgifter utföra även andra uppgifter och uppdrag men dessa får inte leda till en intressekonflikt.

Dataskyddsombudet i Säters kommun bedriver dataskyddsarbetet på deltid vid sidan om sitt uppdrag som konsumentvägledare. Dataskyddsombud uppger i intervju att han upplever att det till viss del finns en uppdragsbeskrivning för uppdraget som dataskyddsombud i de beslutade riktlinjerna för personuppgiftsbehandling. Denna beskrivning överensstämmer i stora delar med hur SKR och Datainspektionen beskriver uppdraget och rollen som dataskyddsombud, se inledning av detta avsnitt.

Det framkommer vidare i intervju att dataskyddsombud inte har några formella kunskaper om dataskydd och att hans främsta uppgift är att sprida kunskap om GDPR i verksamheten. Han har inte genomfört någon tillsyn eller revisioner för att säkerställa efterlevnaden hos de personuppgiftsansvariga.

Intervjusvar visar att det inte är så ofta dataskyddsombudet bjuds in som bollplank i frågor men att det händer, exempelvis i fråga gällande kameraövervakning på en skola.

Dataskyddshandläggare

Till stöd för arbetet med personuppgiftsbehandlingar utser respektive förvaltningschef sina dataskyddshandläggare. Antalet dataskyddshandläggare ska återspegla antalet, komplexiteten samt skyddsvärdet hos nämndens personuppgiftsbehandlingar.

De utsedda dataskyddshandläggarna har andra huvudsakliga roller i kommunen, som exempelvis nämndsekreterare, registratorer, assistenter mm. De som utsetts till dataskyddshandläggare har i sina andra uppdrag arbetsuppgifter som tangerar arbetet med GDPR och kompetens inom arkivlag, offentlighet och sekretess mm som utgör ett stöd även i utförandet som dataskyddshandläggare.

Dataskyddshandläggarnas arbetsuppgifter beskrivs i dokumentet Riktlinjer för personuppgiftsbehandling:

- Vara ett kunskapsstöd för den egna förvaltningen i personuppgiftsfrågor
- Samla in information om behandlingar, och i samråd med systemförvaltare och verksamhet göra en laglighetsbedömning
- Hålla förteckningen över personuppgiftsbehandlingen uppdaterad så att den visar korrekt information
- Utforma styrdokument, rutiner, information och mallar rörande personuppgiftsbehandling
- Ta fram och utveckla processer för efterlevnad av regelverket för personuppgiftshantering
- Delta i implementeringen av framtagna rutiner och processer gällande dataskyddslagstiftningen

Dataskyddshandläggarna upplever själva att rollen är tydlig, dels utifrån ovan beskrivning men att uppgifter och ansvar även tydliggörs i förvaltningsplanen som tas

fram. Vissa av dataskyddshandläggarna uttalar önskemål om att få lära sig mer om GDPR för att utgöra ett bättre stöd till personuppgiftsansvariga då det ser olika ut om någon utbildning erbjudits eller inte.

Det upplevs i vissa delar finnas en otydlighet i förvaltningarna över vilket uppdrag dataskyddshandläggarnas har och hur ansvaret ser ut. Detta hör till viss del ihop med hur möjligheterna till information och aktiviteter på personalmöten med mera har sett ut.

Informationssäkerhetsansvarig

I intervjuer hänvisas till att det finns en nära koppling mellan informationssäkerhetsarbetet och GDPR även om andra lagrum, exempelvis offentlighet och sekretess, också måste beaktas i informationssäkerhetsarbetet. En formellt beslutad och fungerande informationssäkerhet i kommunen är en grundläggande förutsättning för att lyckas efterleva de ökade kraven på hantering av personinformation. Ikraftträdandet av GDPR har därigenom gett ett ökat fokus även på arbetet med informationssäkerhet då kommunen hanterar stora mängder informationstillgångar innehållande personuppgifter som behöver skyddas.

Informationssäkerhetsansvarige i Säters kommun är arkivarie till största delen av sin tjänst men även systemförvaltare. Rollen som informationssäkerhetsansvarig finns inte dokumenterad i en arbetsbeskrivning. Arbetet är inte så formaliserat eller organiserat ännu och en ökad tydlighet har efterfrågats av informationssäkerhetsansvarig.

Ansvarig för informationssäkerhet ordnar med utbildningar och gör viss tillsyn av att säkerhetsarbetet sköts. I intervju anges att det inom arbetet med informationssäkerhet varit ett huvudsakligt fokus på IT-säkerhet. Det har upplevts som otydligt hur verksamheternas ansvar ser ut i informationssäkerhetsarbetet. Det finns en förhoppning om att detta tydliggörs i en ny informationssäkerhetspolicy som ska beslutas samt i samband med implementeringen av LIS.

3.2.3 Bedömning

Vår bedömning är att det finns en organisation för att bedriva GDPR-arbetet i förvaltningarna genom utsedda dataskyddshandläggare som stöd i nämndernas personuppgiftsansvar. Det möjliggör att förvaltningarna på ett självständigt sätt kan bedriva dataskyddsarbetet. Vi bedömer vidare att det finns former för kunskaps- och erfarenhetsutbyte där information om nyheter och praxis inom GDPR ges regelbundet. Det finns en struktur för att gemensamt diskutera och utveckla kommunens arbete med informationssäkerhet och GDPR.

Vår bedömning är att uppdraget som dataskyddshandläggare är dokumenterat i styrdokument och att utförandet i uppdragen kan utföras i enlighet med uppdragsbeskrivningen. Vår bedömning är att vissa av dataskyddshandläggarna med kunskapshöjande insatser inom GDPR skulle ges ytterligare förutsättningar att utgöra ett bra stöd till personuppgiftsansvariga. Vi rekommenderar därför att kommunstyrelse och nämnder ska ta tillvara det engagemang som finns hos dessa resurser och

säkerställa att de har de kunskaper de har behov av för att utgöra ett stöd till styrelse och nämnder.

Alla nämnder och styrelsen har genom beslut utsett dataskyddsombud och meddelat detta till Datainspektionen. Vår bedömning är att det finns ett dokumenterat uppdrag för dataskyddsombud.

Vår bedömning är vidare att nuvarande dataskyddsombud inte uppfyller de krav som finns i dataskyddsförordningen avseende yrkesmässiga kvalifikationer, sakkunskap och förmåga att utföra uppgifterna. Vi baserar vår bedömning på att dataskyddsombud inte har någon juridisk bakgrund eller erfarenhet och ska utföra sitt uppdrag vid sidan av andra tidskrävande arbetsuppgifter. Utan tillräckliga kunskaper och tid är vår bild att det blir svårt för dataskyddsombud att utöva sitt uppdrag enligt den arbetsbeskrivning som kommunen har angett i sina riktlinjer.

Dataskyddsombudet i sig har inget formellt ansvar för GDPR-efterlevnaden vilket betyder att ansvaret åligger nämnderna som personuppgiftsansvariga. För att dataskyddsombud ska kunna granska att förvaltningarna och personuppgiftsansvariga tagit sitt ansvar och säkerställt efterlevnaden av lagen krävs kompetens inom området för att göra dessa bedömningar i interna revisioner och i tillsynsarbete.

Dataskyddsombudet ska enligt förordningen kunna agera med ett oberoende och erbjudas möjlighet att delta i samtliga frågor rörande dataskydd och rapportera till högsta förvaltningsnivå. Vår bedömning är att detta inte sker i tillräckligt stor utsträckning och att det med nuvarande organisering inte kan uteslutas att dataskyddsombud hamnar i beroendeställning till funktioner som kan bli föremål för granskning i tillsynsarbetet. Rapportering sker till underställd chef till högsta förvaltningsnivå och denna funktion är även personalchef och ansvarig för de register som hanterar anställda. Dessa innehåller en stor mängd personuppgifter som är en personuppgiftsbehandling som skulle kunna vara föremål för granskning.

3.3 Kommunens arbete för att säkerställa efterlevnad av GDPR

3.3.1 Förvaltningsplan/Organisationsbeskrivning personuppgiftsbehandling Säters kommun

Vi har i granskningen tagit del av en förvaltningsplan för GDPR-arbetet som avsåg året 2019. Planen är framtagen av dataskyddshandläggarna och beslutad av förvaltningschefsgruppen. I planen framgår hur det systematiska arbetet ska bedrivas och ett antal kontrollpunkter finns angivna där tid för kontroll, ansvarig och instans för rapportering framgår.

Förvaltningsplanen ska revideras årligen, beslutas av förvaltningschefsgruppen och delges styrelse/nämnd. Vi har i granskningen inte tagit del av någon förvaltningsplan för 2020 och kan genom protokollsgenomgång inte se att någon sådan delgetts nämnder och styrelser för året 2020. I fastställd förvaltningsplan för 2019 framgår att revidering inför kommande förvaltningsperiod ska ske i november. Att förvaltningsplanen följs ska vara ett kontrollmoment i nämndernas interna kontrollplan.

3.3.2 Registerförteckning

Registerförteckningar enligt artikel 30 i dataskyddsförordningen innebär att den personuppgiftsansvarige, personuppgiftsbiträdet och deras företrädare ska föra ett skriftligt och elektroniskt register över all behandling av personuppgifter.

I Säters kommun sker det i systemstödet GDPR Hero. För att en registrering ska anses komplett ska uppgifter om personuppgiftsbehandlingen dokumenteras. Bland annat anges ändamål med personuppgiftsbehandlingen samt vilken laglig grund som finns för behandlingen. Det behöver även framgå i vilka IT-system som uppgifterna finns och vilken typ av personuppgifter som lagras. Det ska också dokumenteras vilka rutiner för att tillgodose registrerades rättigheter som gäller för behandlingen t.ex. rätten till registerutdrag, radering och rättning.

I intervjuer beskrivs detta som det mest tidskrävande momentet i införandet, att få kännedom om alla personuppgiftsbehandlingar så att de kunde registreras i systemet. Tidigare dataskyddsombud granskade registerförteckningar i slutet av 2018 och gjorde då bedömning att det finns personuppgiftsbehandlingar som inte var kompletta. Bristerna ledde fram till rekommendationer om åtgärder. I internkontrollplanen för 2020 finns kontrollmoment över om alla personuppgiftsbehandlingar är kompletta och uppdaterade.

Intervjupersoner beskriver att granskningen som genomfördes av dataskyddsombud var bra för då fick nämnden och förvaltningen konkreta förslag på förbättringar som behövs för efterlevnad av lagen. Det framkommer vidare att arbetet fortfarande pågår att få alla personuppgiftsbehandlingar kompletta. Det finns behandlingar som inte är registrerade alls, eller inte registrerade i GDPR Hero och så finns det ett antal där man misstänker att exempelvis laglig grund eller andra uppgifter är felaktiga och behöver revideras. Det nya systemstödet som efterfrågas är en del i att få en bättre vägledning i laghänvisningar och bedömningar av kommunens personuppgiftsbehandlingar.

En åtgärd som pågår vid tiden för granskningen är en genomgång av kommunens servrar för att se om det finns personuppgifter där som inte är registrerade. Arbetet inleddes med att samtliga mappar och kataloger på servrarna scannades för att identifiera personuppgifter. Resultatet delades sedan ut mellan berörda förvaltningar och en genomgång av samtliga uppgifter ska ske där en bedömning ska genomföras om informationen ska sparas och registreras i en behandling eller raderas.

Det har också beslutats om en dokumenthanteringsplan som benämns Informationshanteringsplan som är tänkt att komplettera hanteringen av kommunens personuppgiftsbehandlingar.

Konsekvensbedömning

Om behandlingen av personuppgifter sannolikt är förknippad med stora risker, ska den personuppgiftsansvarige göra en konsekvensbedömning av dataskyddet. Då bedöms riskerna i anslutning till behandlingen och också den personuppgiftsansvariges

metoder att möta dessa risker. En konsekvensbedömning ska göras särskilt om det används ny teknik eller om det gäller omfattande behandling av personuppgifter.

Om konsekvensbedömningen visar att risken i anslutning till behandlingen är hög, och den personuppgiftsansvarige inte har vidtagit åtgärder för att minska risken, ska den personuppgiftsansvarige samråda med tillsynsmyndigheten innan behandlingen påbörjas (förhandssamråd).

I riktlinje för personuppgifter anges att kommunen har en mall för konsekvensbedömningar som avser att ge stöd i frågan om en konsekvensbedömning ska genomföras eller inte. Om beslutet är att inte göra en konsekvensbedömning ska det motiveras och dataskyddshandläggaren ska dokumentera anledningarna till beslutet i förteckningsprogrammet över personuppgiftsbehandlingar.

I intervjuer framkommer att arbetet inom kommunen behöver utvecklas gällande konsekvensbedömningar. I nuläget finns inte ett tillräckligt samarbete och dialog mellan dataskyddshandläggare och de som är utsedda systemförvaltare då det är systemförvaltarna som känner till systemen och som är delaktiga vid inköp av nya system.

Personuppgiftsbiträdes-avtal, PUB-avtal

Om personuppgiftsbiträden, dvs en extern part, anlitas för att hantera personuppgifter för en personuppgiftsansvarigs räkning, ska det också finnas ett underskrivet Personuppgiftsbiträdesavtal, PUB-avtal, kopplat till registreringen. Det framkommer i intervjuer att PUB-avtal inte registreras i registerförteckningen utan sparas i diariet för respektive nämnd. Vid granskningen som genomfördes av dataskyddsombudet framkom att det fanns behandlingar som saknade PUB-avtal. Ett arbete har genomförts och pågår för att samtliga behandlingar som behöver ska ha ett undertecknat avtal. Vissa större leverantörer har inte gått med på att skriva på kommunens avtal och en dialog pågår för att lösa detta.

Det har även beslutats om en fullmakt från nämnderna till kommunstyrelsen för att hantera PUB-avtal som berör verksamhetssystem på kommunövergripande nivå. Det innebär att Kommunstyrelsen nu kan underteckna PUB-avtal som även omfattar nämndernas personuppgifter och ärendet behöver inte hanteras i samtliga nämnder innan det kan undertecknas.

3.3.3 Stöd för rutiner

Det finns Riktlinjer för ledningssystem för informationssäkerhet (LIS) beslutat av kommunstyrelsen 2017-03-21. Ett nytt ledningssystem för informationssäkerhet är under framtagande och ska beslutas av politiken under 2020. I intervjuer framhålls att GDPR är en viktig del i informationssäkerhetsarbetet och en förhoppning är att ledningssystemet även bidrar till att tydliggöra arbetet med GDPR.

Det nu gällande LIS är beslutat innan GDPR trädde i kraft och innehåller inga delar om personuppgiftshantering. Däremot beskrivs informationsklassning som är en viktig del i

informationssäkerhetsarbetet. Informationsklassning innebär att kommunens digitala informationstillgångar klassas, vilket är en form av riskanalys som ska leda till att kommunen ska vidta de tekniska åtgärder som behövs för att skydda informationstillgångarna och personuppgifter. Säters kommun använder metoden KLASSA som är framtagen av SKR för att klassa sin information. Det framkommer i intervjuer att en klassning har genomförts för 61 av kommunens system och att åtgärdsplaner upprättats utifrån klassning samt åtgärder påbörjade. Konsekvensbedömningar har genomförts för ett antal system och sker alltid inför köp av nya IT-system. Risk och sårbarhetsanalyser genomfördes inför införandet av GDPR.

Kommunen har ett IT-system, GDPR Hero, där man dokumenterar sina personuppgiftsbehandlingar. Vi har tagit del av exempel på dessa men har inte kunnat granska om samtliga personuppgiftsbehandlingar är korrekt och fullt ut följer de lagkrav som finns i enlighet med GDPR. Ansvar att granska att varje personuppgiftsbehandling är korrekt ligger på dataskyddsombudets ansvar.

I intervjuer framkommer att man inte är helt nöjd med systemstödet och att ett inledande arbete har gjorts för att upphandla ett nytt systemstöd. Nuvarande stöd upplevs mer som ett register än som ett systemstöd där även utbildning, juridiskt stöd och koppling till lagtexter finns. Man har upplevt ett behov av ett mer kvalificerat system med mer direkt stöd när man kommit längre i GDPR-arbetet.

3.3.4 Rutiner för de registrerades rättigheter

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt dataskyddsförordningen. Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade, eller att få ut eller flytta sina uppgifter. De registrerades rättigheter har utökats, förstärkts och specificerats i dataskyddsförordningen jämfört med personuppgiftslagen.

De registrerades rättigheter behöver personuppgiftsansvarig ta ställning till för de personuppgiftsbehandlingar de har i sin registerförteckning och arbetet behöver därför ske på förvaltningsnivå.

Rätten till registerutdrag innebär att varje nämnd genom sin förvaltningsorganisation på begäran ska tillhandahålla ett skriftligt utdrag med sammanställning av vilka personuppgifter som behandlas tillsammans med förklaring om hur de hanteras.

I kommunens Riktlinjer för personuppgifter framgår hur ansvaret ser ut och hur hanteringen av begäran eller förfrågningar ska gå till. Förfrågan skickas till personuppgiftsansvarig eller dataskyddsombud. Om förfrågan gäller enskild verksamhet hanteras den inom respektive förvaltning och dataskyddshandläggaren samordnar uppgifterna i samarbete med handläggare som ansvarar för information om den registrerade. Om förfrågan gäller all information som kan finnas om den registrerade samordnar dataskyddsombud sammanställningen och samarbetar med dataskyddshandläggarna för att samla information om den registrerade.

Det har hittills inte inkommit några förfrågningar från de registrerade i Säters kommun. Information om registrerades rättigheter och hur de kan gå tillväga för att få registerutdrag eller någon av övriga rättigheter, finns på kommunens hemsida tillsammans med kontaktuppgifter.

3.3.5 Personuppgiftsincidenter

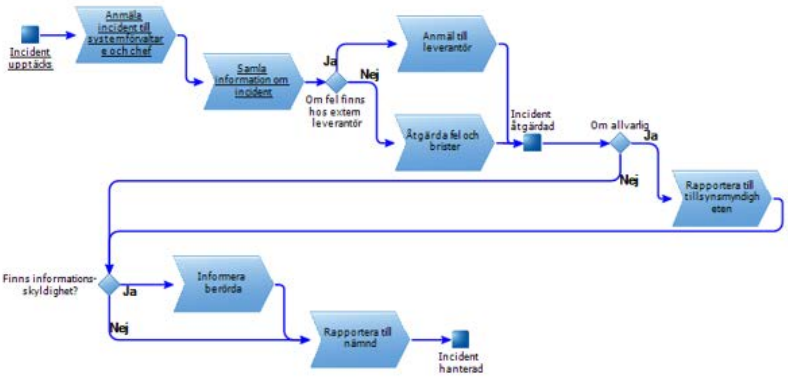
En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt.

Rutin för incidentrapportering finns i kommunens Riktlinjer för personuppgifter. Incidentrapporteringen i Säters kommun utförs i fyra moment, som kan ske parallellt med varandra för att hantera incidenten så snabbt som möjligt. Dataskyddsombud ska informeras och involveras inom 24 timmar i händelse av en incident.

De fyra momenten är:

1. Kartlägga och dokumentera
2. Åtgärda fel
3. Anmäla
4. Informera de registrerade om incidenten

Hantering av personuppgiftsincidenter beskrivs i riktlinjerna i form av en processbild:



Vidare framgår att det vid behov att rapportera till tillsynsmyndighet ska ske inom 72 timmar efter att incidenten har upptäckts. Berörd nämnd ansvarar för att incidentrapporteringen sker. Chef eller systemförvaltare rapporterar. Dataskyddsombudet ska få information om rapporteringen. Ärendet ska vidare diarieföras, med systemförvaltare eller chef som ärendehandläggare. Nämnden ska alltid delges incidenter som sker.

I intervjuer framkommer att det endast har skett ett fåtal personuppgiftsincidenter. Under 2019 anmäldes tio incidenter vilket intervjupersoner är eniga om att det är alldeles för få. Det behövs information- och utbildningsinsatser för att öka

medvetenheten och kunskapen om incidenter så att dessa kan upptäckas om de inträffar.

- I kommunstyrelseförvaltningen skedde under 2019 fem incidenter och fram till intervjutillfället i april 2020 var det tre incidenter som inträffat. Av dessa var ingen allvarlig så att den behövde rapporteras till tillsynsmyndighet.

- Inom Barn och utbildningsförvaltningen har det skett ett fåtal incidenter varav några allvarliga som rapporterats till Datainspektionen. Det handlade bland annat om en stulen dator vid ett inbrott och felutlämnad handling som innehöll känsliga personuppgifter.

- Inom kulturförvaltningen uppges att man inte har haft några personuppgiftsincidenter. Det framhålls i intervjuer att det finns både stor kunskap och medvetenhet inom förvaltningen i personuppgiftsfrågor då det redan innan GDPR bedrevs ett aktivt arbete utifrån PuL.

- Inom Socialförvaltningen har det skett ca fem incidenter varav en allvarlig som rapporterats till Datainspektionen.

- Inom samhällsbyggnadsförvaltningen har det inträffat ett fåtal incidenter.

3.3.6 Medvetenhet om hantering av personuppgifter

GDPR ställer krav på att de som ska hantera eller kommer i kontakt personuppgifter har kunskap om hur de ska hantera dem. De personuppgiftsansvariga ansvarar för att säkerställa att personal har adekvat utbildning utifrån de personuppgifter som de hanterar.

I Säters kommuns riktlinjer för personuppgiftsbehandling framgår att alla anställda som på något sätt hanterar personuppgifter i sitt arbete ska känna till dataskyddsförordningen och lagkraven ska uppfyllas. De anställda ska närvara vid utbildningar som tillhandahålls om personuppgiftshantering, samt följa instruktioner och rutiner som gäller för informationshantering och specifika system.

Det har inte genomförts någon utbildning för alla anställda i kommunen gällande GDPR men en utbildningsdag erbjöds vissa inför införandet av lagen. I intervjuer råder dock en osäkerhet över vilka som deltog denna utbildningsdag.

I samband med upphandling av nytt systemstöd har ett önskemål lagts fram om att det även ska genomföras en webbutbildning för samtliga medarbetare i dataskydd och personuppgiftshantering i enlighet med GDPR.

I intervjuer framhålls arbetsplatsträffar som det forum för dialog som används för att lyfta frågor kring GDPR men att det behövs fler insatser för att öka medvetenheten om allas ansvar och hur personuppgifter ska hanteras. Det behöver förankras på ett bättre sätt hos chefer och i förvaltningen så att en levande dialog finns om GDPR. Dataskyddsombud har tagit fram ett presentationsmaterial som kan användas som stöd i nämnder och förvaltningarna. Det upplevs finnas ett stort mörkertal vad gäller

personuppgiftsincidenter som beror på att medvetenheten och kunskapen om vad som är en incident är för låg i nuläget. I materialet som dataskyddsombud tagit fram finns därför information och exempel på personuppgiftsincidenter för att tydliggöra detta.

3.3.7 Bedömning

Vår bedömning är att det finns registerförteckningar upprättade över kommunens personuppgiftsbehandlingar för samtliga nämnder och styrelsen. Tidigare interna tillsyn av dataskyddsombud visade att dessa inte var kompletta vilket kvarstår även nu och har bekräftats i intervjuer. Det är en högst väsentlig del i kommunens efterlevnad av dataskyddsförordningen att samtliga personuppgiftsbehandlingar finns registrerade och är kompletta i enlighet med lagkrav. I samband med uppföljning av intern kontroll avseende personuppgiftsbehandlingar anser vi därför att en granskning av dessa bör genomföras av dataskyddsombud för att personuppgiftsansvariga ska få kännedom om nuläge och vad som krävs för att efterleva lagen fullt ut.

Arbetet med konsekvensbedömningar behöver utvecklas då vi i granskningen inte har fått någon dokumentation eller information om att sådana genomförs inför mer omfattande personuppgiftsbehandlingar eller införande av nya system.

Vi ser det som positivt att arbetet under 2019 skett på ett strukturerat sätt och dokumenterats i en årlig förvaltningsplan som beslutats av förvaltningschefsgruppen och delgetts nämnder och styrelsen. Vi har dock i granskningen inte fått ta del av en sådan plan för 2020. Vi anser att detta sätt att systematisera arbetet med GDPR borde prioriteras då det även ingår som en kontrollpunkt i nämndernas och styrelsens interna kontrollplan. Enligt de noteringar vi har tagit del av i tidigare förvaltningsplan skulle en ny plan tagits fram i november 2019 för året 2020.

Det finns en organisation för incidenthantering som är dokumenterad i beslutade riktlinjer samt i förvaltningsplan för GDPR. Vi anser däremot att medvetenheten och kunskapen om personuppgiftsincidenter är för låg vilket visar sig i få rapporterade personuppgiftsincidenter. I ett lärande förbättringsarbete är det bättre att många incidenter rapporteras som visar på att det finns kunskap och medvetenhet om när incidenter inträffar. Om dessa rapporteras kan åtgärder, utbildning och information riktas där det finns behov. I nuläget bedömer vi att det finns ett stort mörkertal gällande hur många personuppgiftsincidenter som faktiskt inträffar vilket inte felaktigt ska tolkas som att kommunen inte har några incidenter. Vi anser att kommunstyrelsen och nämnder behöver säkerställa att tillräcklig utbildning och information delges medarbetare och förtroendevalda för att var och en ska ha förutsättningar att fullgöra sitt ansvar för att skydda personuppgifter i kommunens verksamheter.

Vår bedömning är att det finns rutiner och en dokumenterad process för hantering utifrån de registrerades rättigheter och att denna är känd av dataskyddshandläggare som ansvarar för att sammanställa informationen till de registrerade. Då ingen förfråga har inkommit från någon registrerad ännu har vi i granskningen inte kunnat verifiera att rutinen och processen fungerar som den är avsedd att göra.

3.4 Uppföljning och rapportering

3.4.1 Intern granskning genomförd av dataskyddsombud

Tidigare utsedda dataskyddsombudet genomförde i slutet av 2018 en intern kartläggning och tillsyn av personuppgiftsansvarigas efterlevnad av dataskyddsförordningen. Denna tillsyn visade på ett flertal brister och mynnade ut i ett antal rekommendationer.

I rapporten för tillsynen framgår att syftet med tillsynen var: ”att samla in information om hur organisationen behandlar personuppgifter och kontrollera att organisationen följer bestämmelser och interna styrdokument samt informera och ge råd inom er organisation”. Det framgår vidare att ansvarig chef ansvarar för att åtgärder utifrån resultatet i tillsynen upprättas i en åtgärdsplan och att dessa ska vara genomförda och uppföljda senast 2019-06-15.

Förvaltningarna har besvarat tillsynen med yttranden som vi har tagit del av exempel på i granskningen. Yttranden visar att ett flertal åtgärder redan påbörjats vid tiden för yttrandet medan förvaltningen svarat att vissa åtgärder var mer kommunövergripande och behövde åtgärdas genom framtagande av styrdokument eller liknande. Av den förvaltningsplan för GDPR för 2019 som vi tagit del av så framkommer att nya rutiner, exempelvis för hantering av e-post tillkommit vilket var en av åtgärderna som efterfrågades.

3.4.2 Intern kontroll

Nämnderna har i sina internkontrollplaner beslutat om två kontrollmoment som berör kommunens arbete med GDPR.

Den ena är uppföljning av förvaltningsplanen för GDPR där syftet är att säkerställa förvaltningarnas arbete och planering med åtgärder. Det andra kontrollmomentet är att granska så att förvaltningen genomför kontroller av sina personuppgiftsbehandlingar och skickar förändringar av dessa till dataskyddshandläggaren för uppdatering av registret i GDPR Hero.

3.4.3 Rapportering

Rapportering av GDPR-arbetet från dataskyddsombud sker till förvaltningschef kommunkansliet som i sin tur vid behov lyfter frågeställningar till kommunens ledningsgrupp.

GDPR som enskilt ärende har behandlats vid några tillfällen på kommunstyrelsen och nämnderna. En gång per år redovisas alla personuppgiftsbehandlingar till kommunstyrelsen och nämnder.

Förvaltningsplanen delges nämnder och styrelser och det har skett informations- och utbildningsinsatser där dataskyddsombud och dataskyddshandläggare varit föredragande.

Enligt intervjuer så är övrig rapportering som sker till nämnder främst kopplad till incidenter som delges.

3.4.4 Bedömning

Vår bedömning är att kommunstyrelse och nämnder har säkerställt en tillräcklig rapportering av arbetet som sker för att uppfylla kraven i dataskyddsförordningen. De får årligen information om hur det systematiska arbetet ska bedrivas genom att förvaltningsplanen delges.

Samtliga nämnder och styrelsen har beslutat om kontrollmoment i intern kontroll som är väsentliga för kommunens efterlevnad av GDPR. Förutom detta så delges nämnder och styrelsen de inträffade personuppgiftsincidenter som sker.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunen till stor del har rutiner och en organisation för att säkerställa sitt arbete med GDPR. Kommunstyrelsen och nämnder behöver säkerställa att dataskyddsombud erhåller kompetenshöjande insatser för att motsvara de lagkrav som finns för uppdraget. Vår bedömning är att dataskyddsombud inte har den kompetens som erfordras eller resurser i tid för att fullgöra sitt uppdrag.

Vidare behöver medvetenheten och kunskapen utvecklas hos de i kommunen som har ansvar för personuppgifter för att säkerställa hanteringen och att incidenter kan upptäckas.

Att säkerställa kommunens efterlevnad av GDPR är ett pågående arbete och delar av arbetet kvarstår för att efterleva lagen fullt ut.

4.1 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen och nämnderna att:

- säkerställa en tillräcklig kompetensnivå och resurser för dataskyddsombud
- säkerställa att dataskyddsombud involveras och rådfrågas i högre grad i alla frågor som rör skyddet av personuppgifter
- dataskyddsombud fullföljer sitt uppdrag och genomför regelbunden tillsyn över personuppgiftsansvarigas efterlevnad av dataskyddsförordningen
- utifrån kontrollmål för efterlevnad av GDPR i internkontrollplan för 2020 bedöma risk och konsekvenser för brister i efterlevnad av GDPR och upprätta kontrollåtgärder för dessa
- säkerställa att utbildning genomförs för samtliga medarbetare för att medvetenheten om hantering av personuppgifter ska vara tillräcklig

Säters kommun
Granskning av efterlevnad av dataskyddsförordningen

2020-09-01

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

Karin Helin Lindqvist
Certifierad kommunal revisor