Granskning av rutiner för efterlevnad av dataskyddsförordningen

Revisionsrapport
Trelleborgs kommun

KPMG AB

2021-03-09

Antal sidor 17

Trelleborgs kommun
Granskning av rutiner för efterlevnad av dataskyddsförordningen

2021-03-09

Innehållsförteckning

1 Sammanfattning

Vi har av Trelleborgs kommuns revisorer fått i uppdrag att granska kommunens rutiner för efterlevnad av dataskyddsförordningen.

Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. Bristande hantering samt överträdelser kan innebära betydande sanktionsavgifter till skillnad från tidigare lagstiftning. Likaså riskerar en bristande hantering av personuppgifter leda till förtroendeskador för kommunen som helhet samt personuppgiftsansvariga nämnder och styrelser.

Vi anser att dataskyddsombudet är engagerad. Vederbörande har arbetat intensivt med att öka förståelsen och kunskaperna i verksamheterna vad avser lagens syfte, tillämpning och intentioner. Vi upplever intervjuade tjänstepersoner och politiker villiga att införa förändringar i syfte att uppå en tillfredsställande nivå vad avser efterlevnad av dataskyddsförordningen.

Sammantaget bedömer vi att det finns brister vad avser efterlevnaden av dataskydds-förordningen. Vi konstaterar att det finns ett behov av ett förbättrings- och utvecklings-arbete följt av utbildningsinsatser.

Mot bakgrund av vår granskning rekommenderar vi följande:

- För att möjliggöra dataskyddsombudets uppdrag, att systematiskt arbeta och övervaka efterlevnaden av dataskyddsförordningen samt agera rådgivande, är det av vikt att organisationen stödjer dataskyddsombudet genom att tillhandahålla erforderliga resurser och förutsättningar.

- Kommunstyrelsen bör utifrån sin uppsiktsplikt ett par gånger per år samt vid behov bjuda in dataskyddsombudet till sammanträden för att ta del av en lägesrapport avseende verksamheternas efterlevnad av dataskyddsförordningen.

- Styrdokumenten avseende hantering av personuppgiftsincidenter bör ses över. Styrdokumenten bör reduceras vad avser mängden information samt slås ihop till ett dokument. Detta i syfte att underlätta för medarbetarna genom att väsentlig information återfinns i ett enda dokument. Likaså minimeras riskerna för att central information inte kommer till medarbetarnas kännedom beroende på vilket dokument som läses. Alltför många styrdokument ,som behandlar samma område följt av omfattande mängd information, kan leda till en dokumentationströtthet, vilket i sin tur riskerar leda till att styrdokumenten tappar sin legitimitet och verkningsgrad ute i verksamheterna.

- Vi rekommenderar att en inventering görs av **samtliga** styrdokument inom ramen för tillämpning av dataskyddsförordningen samt dataskyddsfrågor, där det idag finns en alltför omfattande mängd dokument som riskerar att leda till att flertalet styrdokument blir ”hyllvärmare” och därmed tappar sin funktion, vilket i sin tur leder

till minskad efterlevnad i organisationen.

- Vad avser omfattningen av incidenter bedömer vi antalet incidenter som har upptäckts/rapporterats vara för lågt i förhållande till verksamheternas omfattning. Sannolikheten att det finns ett mörkertal är stor. Vi anser att riktade utbildningsinsatser erfordras vad avser identifiering och upptäckt av personuppgiftsincidenter.

- Vi bedömer att det krävs ett förbättringsarbete vad avser upprättande av registerförteckningar som är central stomme vad avser hantering av personuppgifter (se sid 14-–5). Nämnderna bör genomföra en inventering i syfte att sondera vilka personuppgiftsbehandlingar som inte har upptagits i en registerförteckning.

- Vi anser att styrdokumenten avseende begäran om registerutdrag bör slås samman till ett sammanhållet dokument i syfte att underlätta för medarbetarna samt reducera antalet styrdokument inom samma område.

- Kommunstyrelsen bör upprätta en rutinbeskrivning avseende hanteringen av enskildas begäran om rättelse, radering och begränsning.

- Vi rekommenderar en central styrning från kommunstyrelsen sida vad avser utbildningar inom dataskyddsförordningen i syfte att skapa en enhetlig kunskapsnivå inom nämnderna.

2 Inledning

Vi har av Trelleborgs kommuns revisorer fått i uppdrag att granska kommunens rutiner för efterlevnad av dataskyddsförordningen.

Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. I och med ikraftträdandet av dataskyddsförordningen, (GDPR), upphävdes personuppgiftslagstiftningen, (PuL 1998:204). Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter. Härigenom ska både offentliga och privata verksamheter anpassa hanteringen av personuppgifter till gällande regler inom ramen för Dataskyddsförordningen.

Bristande hantering samt överträdelser kan innebära betydande **sanktionsavgifter** till skillnad från tidigare lagstiftning. Likaså riskerar en bristande hantering av personuppgifter att leda till **förtroendeskador** för kommunen som helhet samt personuppgiftsansvariga nämnder och styrelser.

Med anledning av ovanstående har kommunens revisorer i sin riskanalys dragit slutsatsen att kommunens rutiner avseende efterlevnad av dataskyddsförordningen behöver granskas. Uppdraget ingår i revisionsplanen för år 2020.

2.1 Syfte, revisionsfråga och avgränsning

Rapporten syftar till att granska kommunens övergripande rutiner för efterlevnad av dataskyddsförordningen. Följande frågor avser rapporten besvara:

1. Finns det ett centralt utsett dataskyddsombud?
2. Befinner sig dataskyddsombudet i en oberoende position?
3. Har samtliga nämnder beslutat om att utse dataskyddsombud?
4. Finns registerförteckningar över personuppgiftsbehandlingar i enlighet med artikel 30.1, dataskyddsförordningen?
5. Har dataskyddsombudet genomfört kontroller av registerförteckningarna?
6. Är registerförteckningarna korrekt upprättade utifrån dataskydds-förordningens grundläggande principer? (Ändamålsbeskrivning, rättslig grund för behandling, personuppgiftsansvarig, kategorier av personuppgifter, förekomst av känsliga personuppgifter, mottagare intern och externt, dokumentation om förekomst av överföring av personuppgifter sker till tredje land, personuppgiftsbiträden, tidsfrister för radering, beskrivning av tekniska och organisatoriska säkerhetsåtgärder m.m.)
7. Finns rutiner för incidentrapporteringar?

8. Hur många incidentrapporter har inkommit sedan lagens ikraftträdande?

9. Har det genomförts någon riskbedömning av incidenterna och hur många har kategoriserats som allvarliga?

10. Har incidenter som bedömts medföra allvarliga risker för den registrerades integritet anmälts till Integritetsskyddsmyndigheten (f.d. Datainspektionen)?

11. Finns dokumenterade rutiner för begäran om registerutdrag?

12. Finns dokumenterade rutiner för rättelse av uppgifter?

13. Finns dokumenterade rutiner för radering av uppgifter?

Granskningen har omfattat kommunens övergripande rutiner för efterlevnad av dataskyddsförordningen.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
- Riktlinjer från European Data Protection Board, (Europeiska dataskyddsstyrelsen)
- Interna riktlinjer/policys.

2.3 Metod

Granskningen har genomförts genom:

- Studium och genomgång av relevanta styrdokument och beslutsunderlag.
- Granskning och analys av registerförteckningar avseende personuppgifts-behandlingar.
- Intervjuer och avstämningar med dataskyddsombud, biträdande kommundirektör tillika ekonomichef samt kommunstyrelsens ordförande.

Rapporten är faktakontrollerad av biträdande kommundirektör tillika ekonomichef samt dataskyddsombudet.

3 Resultat av granskningen

Nedan följer resultatet av granskningen. I syfte att tydliggöra de kriterier som vi har granskat mot, föregås avsnitten av sammanfattande beskrivningar av gällande föreskrifter.

3.1 EU-rättslig lagstiftning

Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. I och med ikraftträdandet av dataskyddsförordningen, (GDPR), upphävdes personuppgiftslagstiftningen, (PuL 1998:204). Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter. Härigenom ska både offentliga och privata verksamheter anpassa hanteringen av personuppgifter till gällande regler inom ramen för dataskyddsförordningen.

Bristande hantering samt överträdelser kan innebära betydande **sanktionsavgifter** till skillnad från tidigare lagstiftning. Likaså riskerar en bristande hantering av person-uppgifter leda till **förtroendeskador** för kommunen som helhet samt personuppgifts-ansvariga nämnder och styrelser.

Hantering av personuppgifter ska ske utifrån förordningens grundläggande principer enligt följande:

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

Vid behandling av personuppgifter måste verksamheterna stödja sig på en så kallad ”**rättslig grund**”. Utan en rättslig grund är personuppgiftsbehandling ej laglig.

Vidare ska styrelsen och nämnderna utse ett gemensamt dataskyddsombud, (DSO), som bl.a. har till uppgift att övervaka efterlevnaden av dataskyddsförordningen.

3.2 Dataskyddsombudets uppdrag

Enligt dataskyddsförordningen, artikel 39 ska dataskyddsombudet ha minst följande uppgifter:

- Att **informera och ge råd** till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar skyldigheter enligt dataskyddsförordningen.
- Att **övervaka och kontrollera** efterlevnaden av dataskyddsförordningen.
- Att övervaka och kontrollera efterlevnaden av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripen ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.
- Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den.
- Att samarbeta med tillsynsmyndigheten.
- Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling och vid behov samråda i alla andra frågor.

Det framhålls samtidigt att arbetet som dataskyddsombud ställer höga krav vad avser **integritet** och **hög yrkesetik**. Vad gäller erforderlig kompetens fastställer dataskydds-förordningen att ett dataskyddsombud ska utses på grundval av yrkesmässiga kvalifikationer och i synnerhet sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra ovan nämnda uppgifter.

3.3 Dataskyddsombudets uppdrag och oberoende, Trelleborgs kommun

Dataskyddsombudets främsta uppdrag är att **systematiskt arbeta och övervaka efterlevnaden** av dataskyddsförordningen samt agera **rådgivande.**

Det är av vikt att dataskyddsombudet befinner sig i en **oberoendeposition**, där vederbörande ska kunna arbeta självständigt och fullgöra sina uppgifter på ett oberoende sätt. Detta innebär att personuppgiftsansvariga eller personuppgiftsbiträden exempelvis inte får instruera dataskyddsombudet om vilka resultat som bör uppnås, hur ett klagomål ska hanteras eller att inta en viss ståndpunkt i ärenden som rör dataskyddslagstiftningen. Som exempel kan nämnas att det inte är lämpligt att ett dataskyddsombud sitter i organisationens ledning eller är delaktig i att fatta strategiska beslut om kärnverksamheten.

Iakttagelser

Av granskningen framkommer att nuvarande dataskyddsombud tillträdde sin tjänst i januari 2020 med en tjänsteomfattning på 100 %. Dataskyddsombudet är tillika informationssäkerhetssamordnare. Vellinge kommun samt Skurups kommun köper tjänsten som dataskyddsombud från Trelleborgs kommun, vilket innebär att data-skyddsombudet hanterar sammantaget tre kommuner. Vad avser omfattningen ägnas en halvtidstjänst åt Vellinge samt Skurups kommun. Anställningsmyndighet för dataskyddsombudet är Trelleborgs kommun.

Av intervjuerna framgår att det finns en del utmaningar vad avser efterlevnaden av dataskyddsförordningen och ett förbättringsarbete har påbörjats. Det framgår att stor del av arbetet ägnas till stöd och rådgivning till verksamheterna, där det finns ett stort behov av vägledningsinsatser. Härigenom ägnas mycket tid till att stödja enskilda i form av bl.a. ”hands-on-stöd”, i stället för riktade insatser för en större massa. Ytterligare delar som lyfts är vikten av ledningens stöd och resurser för att möjliggöra ett tillfredställande dataskyddsarbete i verksamheterna.

Dataskyddsombudet har under hösten 2020 påbörjat ett arbete med att se över styrdokumenten, granska huruvida registerförteckningar finns upprättade samt huruvida innehållet uppfyller gällande krav. Utifrån behovet av stöd till verksamheterna är tiden enligt uppgift inte tillräcklig till att agera förebyggande samt kontrollera efterlevnaden.

3.3.1 Kommentarer och bedömning

För att möjliggöra dataskyddsombudets uppdrag att systematiskt arbeta och övervaka efterlevnaden av dataskyddsförordningen samt agera rådgivande, är det av vikt att organisationen stödjer dataskyddsombudet genom att tillhandahålla erforderliga resurser och förutsättningar.

Det är vidare av vikt att kommunstyrelsen utifrån sin uppsiktsplikt ett par gånger per år samt vid behov bjuder in dataskyddsombudet till sammanträden för att ta del av en lägesrapport avseende verksamheternas efterlevnad av dataskyddsförordningen.

Utifrån dataskyddsförordningen breda omfattning samt komplexitet finns ett större behov av stöd till verksamheterna. Dock är det av vikt att dataskyddsombudets roll som rådgivande och bevakande funktion beaktas, där det är personuppgiftsansvariga nämnder och styrelser som ska agera **verkställande**. Det bör noteras att det är personuppgiftsansvariga nämnder och styrelser som juridiskt sett är ytterst ansvariga för att uppnå en tillfredsställande nivå vad avser efterlevnaden av dataskyddsförordningen.

Det kan också råda en missuppfattning om kommunstyrelsens roll vad gäller person-uppgiftsansvaret. Kommunstyrelsen kan inte inta rollen som personuppgiftsansvarig för någon annan nämnd eller styrelse.

Vi bedömer att dataskyddsombudet vid tid för granskningen befinner sig organisatoriskt sett i en oberoendeposition.

3.4 Utnämning av dataskyddsombud

Samtliga personuppgiftsansvariga[1] ska utse ett dataskyddsombud. Beslutet ska dokumenteras och vara protokollfört.

[1] Personuppgiftsansvarig är respektive nämnd och styrelse.

Iakttagelser

Vi har tagit del av samtliga nämnders beslut avseende utnämning av dataskyddsombud.

3.4.1 Kommentarer och bedömning

Granskningen visar att samtliga nämnder formellt har utsett dataskyddsombud.

3.5 Styrdokument personuppgiftsincidenter, risk- och konsekvensbedömning och dokumentation

En **personuppgiftsincident är** en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna innebär närmare att individer:

-- **förlorar kontrollen** över sina uppgifter eller
-- att **rättigheterna inskränks** genom exempelvis **obehörigt röjande** av eller
-- **obehörig åtkomst** till personuppgifter.

Dataskyddsförordningen, (artikel 33, punkt 1), fastställer att vid en personuppgifts-incident ska den personuppgiftsansvarige, utan onödigt dröjsmål och inte senare än **72 timmar** efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig. I Sverige är det Integritetsskyddsmyndigheten (f.d. Datainspektionen) som är behörig tillsynsmyndighet.

Den **registrerade ska informeras** om personuppgiftsincidenten **utan onödigt dröjsmål**, om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (artikel 34, punkt 1).

De personuppgiftsincidenter som inte bedöms medföra risker för individers rättigheter och friheter behöver ej anmälas till tillsynsmyndigheten. Därav är det av vikt att ansvarig nämnd/styrelse genomför en konsekvensanalys vid eventuella incidenter i syfte att bedöma allvarlighetsgraden.

Samtliga personuppgiftsincidenter ska **dokumenteras oaktat allvarlighetsgrad**.

EU-rätten fastställer vidare att i de fall där organisationen har anlitat ett personuppgiftsbiträde, (PuB), ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige, (nämnd/styrelse), utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident, (artikel 33, punkt 2).

Iakttagelser

Vi har tagit del av tre styrdokument som avser hanteringen av personuppgifts-incidenter enligt följande:

- *Personuppgiftsincident,* styrdokumentet återger lagstiftningens krav vad avser hantering av personuppgifter, där bl.a. kriterier för risk- och konsekvens-bedömning av incidenter beskrivs. Vidare upptas konkreta exempel på incidenter. Dokumentet fastställer också den praktiska hanteringen vid

inträffade och upptäckta personuppgiftsincidenter. Styrdokumentet saknar beslutsinsats och fastställelsedatum.

- *Process gällande hantering av personuppgiftsincidenter hos personuppgiftsansvariga*, framtagen av säkerhetsenheten 2020-10-12. Dokumentet beskriver den praktiska hanteringen i kortversion följt av en checklista som avser att säkerställa att ”verksamheten är förberedd på att hantera personuppgiftsincidenter.
- *Information gällande logghantering av personuppgiftsincidenter hos personuppgiftsansvariga*, framtagen av säkerhetsenheten, 2020-10-12. Dokumentet återger aktuella artiklar i dataskyddsförordningen vad avser personuppgiftsincidenter samt beskriver gällande krav kring dokumentationen av inträffade incidenter.

3.5.1 Kommentarer och bedömning

Vi bedömer att det finns relevant samt viktig information i styrdokumenten avseende hantering av personuppgiftsincidenter. Vi anser dock att styrdokumenten bör reduceras vad avser mängden information samt slås ihop till ett dokument. Detta i syfte att underlätta för medarbetarna genom att väsentlig information återfinns i ett enda dokument. Likaså minimeras riskerna för att central information inte kommer till medarbetarnas kännedom beroende på vilket dokument som läses.

Alltför många styrdokument som behandlar samma område följt av omfattande mängd information kan leda till en dokumentationströtthet, vilket i sin tur riskerar leda till att styrdokumenten tappar sin legitimitet och verkningsgrad ute i verksamheterna.

Viktig information som avser samma område, men som återfinns uppdelad i olika dokument kan också leda till viss förvirring bland medarbetarna som i sin tur riskerar leda till minskad efterlevnad eller felaktig hantering.

Vi rekommenderar att ett enda styrdokument arbetas fram innehållande en praktisk hantering av personuppgiftsincidenter (ansvarsfördelning och tillvägagångssätt, dvs. vem gör vad vid upptäckt av en incident, samråd med dataskyddsombud, information om risk- och konsekvensbedömning, dokumentation, kriterier för anmälan till tillsynsmyndighet och information om gällande krav och förutsättningar vad avser information till den registrerade). Vidare kan dokumentet med fördel innehålla konkreta exempel på personuppgiftsincidenter i syfte att vägleda samt öka kunskapsnivå bland medarbetarna. Ytterligare del av vikt som bör framgå av styrdokumentet är att samtliga incidenter bör komma till dataskyddsombudets kännedom.

Av styrdokumenten bör beslutsinstans samt fastställelsedatum framgå. Kommun-övergripande samt centrala styrdokument bör antas som lägst av kommundirektören.

Vi rekommenderar för övrigt att en inventering görs av **samtliga** styrdokument inom ramen för tillämpning av dataskyddsförordningen samt dataskyddsfrågor, där det idag finns en alltför omfattande mängd dokument som riskerar att leda till att flertalet styrdokument blir ”hyllvärmare” och därmed tappar sin funktion, vilket i sin tur leder till minskad efterlevnad i organisationen.

3.6 Omfattningen av personuppgiftsincidenter

Iakttagelser

Vi har begärt in statistik avseende antal upptäckta personuppgiftsincidenter under perioden 2018–2020. Nedan redogörs för antal personuppgiftsincidenter, där också de kommunala bolagen har inkluderats. Antal upptäckta incidenter sedan dataskyddsförordningens ikraftträdande i maj 2018 är:

- 2018: 29 st
- 2019: 38 st
- 2020: 34 st

Av granskningen framkommer att Trelleborgs kommun använder sig av Integritetsskyddsmyndighetens (dåvarande Datainspektion) dokumentations/ anmälningsblankett vad avser dokumentation av upptäckta personuppgiftsincidenter.

Figur 3.6.1

Personuppgiftsansvarig Nämnd/styrelse	Antal incidenter 2018	Varav anmälda till DI	Antal incidenter 2019	Varav anmälda till DI	Antal incidenter 2020	Varav anmälda till DI
Kommunstyrelse	12	3	8	1	13	0
Samhällsbyggnads - nämnd	0	0	0	0	0	0
Bildningsnämnd	2	0	4	0	2	0
Socialnämnd	5	2	12	4	13	4
Teknisk nämnd	1	0	3	1	1	1
Servicenämnd	2	0	0	0	0	0
Arbetsmarknadsnämnd	7	2	7	3	4	3
Kultur- och fritidsnämnd	0	0	1	0	0	0
Överförmyndaren	0	0	1	0	2	0
Trelleborgs Energiförsäljning	0	0	0	0	0	0
Trelleborgs fjärrvärme	0	0	0	0	0	0
AB Trelleborg Hem	0	0	2	0	0	0
AB Visit Trelleborg	0	0	0	0	0	0

3.6.1 Kommentarer och bedömning

Dokumentation av personuppgiftsincidenter är obligatorisk, där den **personuppgifts-ansvarige** ska dokumentera samtliga personuppgiftsincidenter inbegripet **omständigheterna kring incidenten**, **effekter** samt de **korrigerande åtgärder** som har vidtagits. Vi vill i sammanhanget betona vikten av en korrekt hantering av inträffade personuppgiftsincenter, där en hantering som strider mot dataskyddsförordningen kan leda till förtroendeskador för kommunen samt sanktionsavgifter.

Vi bedömer det som positivt att organisationen har valt att uteslutande använda sig av Integritetsmyndighetens dokumentations-/anmälningsblankett vad avser dokumentation av personuppgiftsincidenter. Detta oaktat om incidenten ska vidare till Integritets-skyddsmyndigheten eller inte. Tillsynsmyndighetens underlag omfattar **samtliga nödvändiga** delar i enlighet med lagstiftnings krav. Detta leder till en enhetlig hantering av upptäckta incidenter inom verksamheterna samt en effektivitet i form av att medarbetarna behöver endast hålla reda på ett enda dokument.

Det förekommer att vissa kommuner skapar egna mallar för dokumentation av person-uppgiftsincidenter, där det finns en risk att centrala delar uteblir samt att hanteringen blir en administrativ börda utifrån antalet underlag som ska fyllas i och hållas reda på.

Vad avser omfattningen av incidenter, bedömer vi att antalet incidenter som har upptäckts/rapporterats vara för lågt i förhållande till verksamheternas omfattning, där sannolikheten att det finns ett mörkertal är stor.

Denna bild bekräftas också av dataskyddsombudets interna kontroller, där det framgår att en kommun av Trelleborgs storlek med ca 4 500 anställda borde ha betydligt fler incidenter än de som har redovisats. Det konstateras vidare att omfattningen av redovisade incidenter innebär att det är mindre än en incident på hundra medarbetare, vilket tyder på att det finns ett högt mörkertal.

En grundläggande orsak till det låga antalet rapporterade incidenter torde vara avsaknad av tillräckliga kunskaper om vad en personuppgiftsincident är och vad som ska klassas som en incident. Bedömningen delas av de intervjuade.

Av granskningen framkommer att anställda har genomgått en så kallad e-learning inom GDPR. Vi anser dock att det krävs mer riktade utbildningsinsatser som tar sikte på enskilda områden, i detta fall upptäckt och hantering av personuppgiftsincidenter. Generella utbildningar är lämpliga i samband med att exempelvis nya lagstiftningar träder ikraft eller för nyanställd personal. Därefter krävs riktade områdesutbildningar i syfte att konkretisera tillämpningen.

Vi rekommenderar central styrning från kommunstyrelsen sida vad avser utbildningar inom dataskyddsförordningen i syfte att skapa en enhetlig kunskapsnivå inom nämnderna.

3.7 Registerförteckningar

All behandling av personuppgifter ska uppfylla de grundläggande principerna i enlighet med dataskyddsförordningen:

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

Dataskyddsförordningen fastställer att för att påvisa att förordningen följs ska personuppgiftsansvariga föra register över behandling som sker under deras ansvar, (s.k. registerförteckningar). Registerförteckningarna ska på begäran redovisas för tillsynsmyndigheten, dvs. Integritetsskyddsmyndigheten, där registren ska utgöra en grund för övervakning av behandling av personuppgifter.

Iakttagelser

Trelleborgs kommun använder sig av systemstödet Drafit Privacy för upprättande av registerförteckningar över personuppgiftsbehandlingar. Verktyget innehåller ett frågebatteri utifrån dataskyddsförordningen krav med bl.a. följande frågor: *Uppgifter om personuppgiftsansvarig, vilka kategorier av registrerade, ändamål med behandlingen, vilka personuppgifter som behandlas, huruvida känsliga personuppgifter behandlas, huruvida uppgifter om barn behandlas, vilken rättslig grund det finns för behandlingen, registrerades rättigheter, informationskrav, gallring och tidsfrister för lagring av uppgifter, anlitande av personuppgiftsbiträde*[2]*, huruvida det finns upprättat personuppgiftsbiträdeavtal, utlämnande av uppgifter till tredjepart, överföring till tredjeland, syftet med att uppgifterna lämnas ut, tekniska och organisatoriska säkerhetsåtgärder, vilka som har åtkomst till uppgifterna* m.m.

Av intervjuerna framgår att verksamheterna har upplevt frågebatteriet, som behöver besvaras i samband med varje behandling, som alltför omfattande och komplext. Antal frågor har reducerats från 80 till 40 i syfte att underlätta för verksamheterna. Det framgår vidare att målsättningen var att samtliga nämnder skulle vara färdiga med att upprätta registerförteckningar under 2020, och att dataskyddsombudet därefter skulle genomföra kontroller av dessa förteckningar. Dock är arbetet inte färdigställt, då det finns personuppgiftsbehandlingar som inte har registrerats samt att merparten av upprättade registerförteckningar är bristfälliga.

Vi har genomfört en övergripande kontroll av registerförteckningarna, där bl.a. följande brister förekommer:

- Fel angiven personuppgiftsansvarig, där det förekommer att förvaltningen eller benämningen ”kommunövergripande” anges i fältet som ansvarig. Ska anges nämnd som personuppgiftsansvarig.

[2] Personuppgiftsbiträde är ett biträde som kan anlitas av personuppgiftsansvarig för hantering av personuppgifter.

”Vet ej svar/avsaknad av svar” i följande fall:

- Huruvida känsliga personuppgifter behandlas
  Vad avser ”känsliga personuppgifter” är utgångspunkten att det är förbjudet att behandla dessa. Det finns dock undantag. Det ställs därmed krav på att behandling av känsliga personuppgifter ska vara väl motiverade och välgrundade med stöd i lagstiftningen.
- Huruvida personnummer behandlas
- Vilken rättslig grund som används som stöd för behandlingen
- Om uppgifter om barn behandlas
- Om informationskravet[1] uppfyllts
- Vilka av de registrerades rättigheter som uppfylls
- Vilka tidsfrister som gäller för gallring
- Om något personuppgiftsbiträde anlitas
- Från vilka källor inhämtas personuppgifterna
- Huruvida det finns en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder för den aktuella personuppgiftsbehandlingen
- Om några personuppgifter lämnas ut till tredje part
- Huruvida personuppgifterna lämnas till tredje land

Vidare har vi noterat att inom vissa behandlingar har antalet frågor reducerats till 8 frågor, där flertalet centrala frågor har tagits bort.

Ytterligare delar som vi har uppmärksammat är att ”**uppgift av allmänt intresse”** anges som rättslig grund utan hänvisning till lagstöd. För att uppgifter av allmänt intresse ska kunna nyttjas krävs stöd i lagstiftningen eller i beslut som har meddelats med stöd av lagstiftning. Det är av vikt att personuppgiftsansvarig nämnd kan motivera valet av rättslig grund för behandlingen.

Speciallagstiftning förekommer som svar på vilken rättslig grund som finns som stöd. Vid angivande av s.k. speciallagstiftning ska författningen ifråga anges. Likaså förekommer ”myndighetsutövning” som svar på efterfrågat lagstöd, dock utan hänvisning till någon författning. All myndighetsutövning ska grundas på lagar inom EU-rätten eller nationell rätt.

Vi har noterat att det förekommer att personuppgiftsbiträde har anlitats, dock saknas information om huruvida det finns ett personuppgiftsbiträdesavtal följt av information

[1] Dataskyddsförordningen fastslår att den registrerade har rätt att få information när dennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade begär det. Informationen ska vara en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk.

om personuppgiftbiträdet.

3.7.1 Kommentarer och bedömning

Vi bedömer att det krävs ett förbättringsarbete samt riktade utbildningar vad avser upprättande av registerförteckningar.

I likhet med dataskyddsombudets uppmaning till nämnderna anser vi att en inventering bör genomföras i syfte att sondera vilka personuppgiftsbehandlingar som inte har upptagits i en registerförteckning. Som exempel kan nämnas att bildningsnämnden har 35 upprättade registerförteckningar följt av socialnämnden som vid tid för granskningen har upprättat 46 registerförteckningar. Vi bedömer antalet registerförteckningar vara för lågt i förhållande till nämndernas verksamhetsomfattningar.

Vi anser vidare att följande frågor åter bör aktiveras i stödsystemet Drafit:

- Vid behandling av känsliga personuppgifter bör det framgå vilka typer av uppgifter som avses följt av en motivering
- Information om personuppgiftsbiträde i de fall där ett biträde anlitas
- Om samtycke används, hur har samtycket inhämtats?
- Huruvida det finns dokumentation som kan visa att samtycke har inhämtats
- Motivering i de fall där informationskravet ej uppfylls
- Syfte med utlämning av personuppgifter till tredjepart
- Vid överföring av personuppgifter till tredjeland, bör frågan om ”*På vilka grunder sker överföring till tredjeland?*” åter aktiveras.
- Vilken/vilka enheter/funktioner har tillgång till uppgifterna?

3.8 Registerutdrag, rättelse, radering och begränsning

I enlighet med dataskyddsförordningen har den registrerade rätt att begära ut ett så kallat registerutdrag från offentliga och privata organisationer. Ett registerutdrag ska redogöra för de personuppgifter som en myndighet eller ett företag behandlar om en person samt på vilket sätt uppgifterna behandlas.

Likaså har den registrerade rätt till att utan dröjsmål få felaktiga uppgifter rättade. På samma sätt finns rättigheten att utan onödigt dröjsmål få sina personuppgifter raderade om de exempelvis inte längre är nödvändiga för de ändamål för vilka de samlats in, eller att den registrerade återkallar sitt samtycke som behandlingen grundar sig på. Den registrerade kan också invända mot registreringen utifrån att det saknas en laglig grund för behandlingen.

Ytterligare rättigheter avser begränsning av behandling av personuppgifter, där den registrerade under visa omständigheter kan kräva att personuppgifter behandlas endast för vissa avgränsade syften.

Iakttagelser

Vi har tagit del av två styrdokument vad avser rutiner för begäran om registerutdrag. Dokumenten saknar beslutsinstans samt fastställedatum. Det finns vidare en framtagen blankett för kommunmedborgarna vad avser begäran om registerutdrag.

Vi saknar dock en rutinbeskrivning avseende begäran om rättelse, radering och begränsning.

3.8.1 Kommentarer och bedömning

Vi anser att styrdokumenten avseende begäran om registerutdrag bör slås samman till ett sammanhållet dokument i syfte att underlätta för medarbetarna samt reducera antalet styrdokument inom samma område.

Kommunstyrelsen bör upprätta en rutinbeskrivning avseende hanteringen av inkomna begäran om rättelse, radering och begränsning.

4 Slutsats och rekommendationer

Sammantaget bedömer vi att det finns brister vad avser efterlevnaden av dataskydds-förordningen. Vi konstaterar att det finns ett behov av ett förbättrings- och utvecklings-arbete följt av utbildningsinsatser.

Mot bakgrund av vår granskning rekommenderar vi följande:

- För att möjliggöra dataskyddsombudets uppdrag att systematiskt arbeta och övervaka efterlevnaden av dataskyddsförordningen samt agera rådgivande, är det av vikt att organisationen stödjer dataskyddsombudet genom att tillhandahålla erforderliga resurser och förutsättningar.

- Kommunstyrelsen bör utifrån sin uppsiktsplikt ett par gånger per år samt vid behov bjuda in dataskyddsombudet till sammanträden för att ta del av en lägesrapport avseende verksamheternas efterlevnad av dataskyddsförordningen.

- Styrdokumenten avseende hantering av personuppgiftsincidenter bör ses över. Styrdokumenten bör reduceras vad avser mängden information samt slås ihop till ett dokument. Detta i syfte att underlätta för medarbetarna genom att väsentlig information återfinns i ett enda dokument. Likaså minimeras riskerna för att central information inte kommer till medarbetarnas kännedom beroende på vilket dokument som läses. Alltför många styrdokument som behandlar samma område följt av omfattande mängd information kan leda till en dokumentationströtthet, vilket i sin tur riskerar leda till att styrdokumenten tappar sin legitimitet och verkningsgrad ute i verksamheterna.

- Vi rekommenderar att en inventering görs av **samtliga** styrdokument inom ramen för tillämpning av dataskyddsförordningen samt dataskyddsfrågor, där det idag finns en alltför omfattande mängd dokument som riskerar att leda till att flertalet styrdokument blir ”hyllvärmare” och därmed tappar sin funktion, vilket i sin tur leder till minskad efterlevnad i organisationen.

- Vad avser omfattningen av incidenter, bedömer vi antalet incidenter som har upptäckts/rapporterats vara för lågt i förhållande till verksamheternas omfattning, där sannolikheten att det finns ett mörkertal är stor. Vi anser att riktade utbildningsinsatser erfordras vad avser identifiering och upptäckt av personuppgiftsincidenter.

- Vi bedömer att det krävs ett förbättringsarbete vad avser upprättande av registerförteckningar som är central stomme vad avser hantering av personuppgifter (se sid 14-15). Nämnderna bör genomföra en inventering i syfte att sondera vilka personuppgiftsbehandlingar som inte har upptagits i en registerförteckning.

- Vi anser att styrdokumenten avseende begäran om registerutdrag bör slås samman till ett sammanhållet dokument i syfte att underlätta för medarbetarna samt reducera antalet styrdokument inom samma område.

- Kommunstyrelsen bör upprätta en rutinbeskrivning avseende hanteringen av inkomna begäran om rättelse, radering och begränsning.

- Vi rekommenderar en central styrning från kommunstyrelsen sida vad avser utbildningar inom dataskyddsförordningen i syfte att skapa en enhetlig kunskapsnivå inom nämnderna.

Datum som ovan

KPMG AB

Viktoria Berstam

Specialist/Certifierad kommunal revisor