Granskning av rutiner för efterlevnad av dataskyddsförordningen

Revisionsrapport

Burlövs kommun

KPMG AB

2021-03-01

Antal sidor 17

Burlövs kommun
Granskning av rutiner för efterlevnad av dataskyddsförordningen

2021-03-01

Innehållsförteckning

1 Sammanfattning

Vi har av Burlövs 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, 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.

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.

Sammantaget kan konstateras att det finns brister vad avser efterlevnaden av dataskyddsförordningen. Av granskningen framkommer att det finns en medvetenhet kring befintliga brister.

Vi upplever organisationen villig att införa förändringar och insatser i syfte att åtgärda befintliga brister.

Vi bedömer att det krävs ett ordentligt omtag vad gäller tillämpningen av dataskydds-förordningen i syfte att kunna uppnå en tillfredställande nivå vad avser efterlevnad av gällande lagstiftning.

Mot bakgrund av vår granskning rekommenderar vi:

- att det är av vikt att organisationen stödjer dataskyddsombudet genom att tillhandahålla erforderliga förutsättningar. Dataskyddsförordningen och dess tillämpning är ett komplext samt omfattande område, där dataskyddsombudet kommer att behöva ha en uppstarstid samt stöd för att kunna sätta sig in i dataskyddsförordningen, dess praktiska tillämpning samt nämndernas arbete. Det är dock av vikt att nämndernas omtagsarbete inte avstannar under tiden.
- kommunstyrelsen bör utifrån sin uppsiktsplikt följa upp nämndernas arbete vad avser efterlevnad av dataskyddsförordningen.
- Utifrån att nämndernas arbete vad gäller att uppnå lagstiftningens krav är eftersatt, erfordras en central styrning från kommunstyrelsen sida.
- Styrdokumenten med sikte på dataskyddsförordningen tillämpning bör ses över.
- Styrdokument i form av rutinbeskrivningar kan med fördel slås samman. Detta i syfte att reducera antal rutinbeskrivningar samt underlätta för medarbetarna genom att relevant information återfinns i ett och samma styrdokument.
- Vissa styrdokument/rutinbeskrivningar bör makuleras, (se sid. 10).
- Vi bedömer att det krävs ett omtag vad avser dokumentation av personuppgifts-incidenter i syfte att uppnå en korrekt dokumentation i enlighet

med lagstiftningens krav. Vi anser att det finns ett tydligt behov av utbildningsinsatser avseende hantering och dokumentation av incidenter inom verksamheterna.

- Dokumentationsmallar avseende personuppgiftsincidenter bör slås samman i syfte att bl.a. att minimera riskerna avseende att viktiga delar uteblir. Ett förslag är att använda Integritetsskyddsmyndighetens anmälningsblankett för dokumentation av samtliga incidenter.
- Vi bedömer att det är alltför få incidenter som har upptäckts/rapporterats till förhållande till verksamheternas omfattning, där medarbetarna är i behov av en ökad kunskapsnivå.
- Vi bedömer att det krävs ett ordentligt utvecklingsarbete vad avser upprättande och hantering av registerförteckningar. Registerförteckningar har till syfte att säkerställa att de **grundläggande principerna** inom dataskyddslagstiftningen efterlevs. Vi anser att verksamheterna bör skyndsamt genomföra en inventering av befintliga personuppgifters behandlingar för att därefter upprätta registerförteckningar.
- Vad avser angivande av rättslig grund för behandling av personuppgifter är verksamheterna i behov av en ökad kunskapsnivå. Ytterligare utvecklingsområden återfinns på sid. 14.
- Kommunstyrelsen bör upprätta en rutinbeskrivning avseende hanteringen av inkomna begäran om registerutdrag, rättelse, radering och begränsning.

2 Inledning/bakgrund

Vi har av Burlövs 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 leda till **förtroendeskador** för kommunen som helhet samt personuppgiftsansvariga nämnder och styrelser.

Med anledning av ovanstående har kommunens revisorer dragit slutsatsen i sin riskanalys, 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 avser rapporten besvara:

1. Finns det ett centralt utsett dataskyddsombud?
2. Befinner sig dataskyddsombudet i en oberoendeposition?
3. Har samtliga nämnder beslutat om att utse ett dataskyddsombud?
4. Har aktuella nämnder 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.
- Övergripande granskning och analys av registerförteckningar avseende personuppgiftsbehandlingar. Likaså har stickprovskontroller avseende personuppgiftsincidenter genomförts.
- Intervjuer och avstämningar har genomförts med dataskyddsombud, kanslichef samt kommunstyrelsens ordförande.

Rapporten är faktakontrollerad av tjänstemannaorganisationen.

3 Resultat av granskningen

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 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 om deras 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 dataskyddsombudet 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 Dataskyddsorganisation och dataskyddsombudets oberoende

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 får exempelvis inte 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.

Av granskningen framkommer att under våren 2020 har de tidigare dataskydds-ombuden i Burlövs kommun genomfört en intern kontroll av nämndernas arbete med tillämningen av dataskyddsförordningen, där följande fastslås:

”*Det föreligger en stor risk att nämnderna inte uppfyller kraven i dataskydds-förordningen*.”

Härigenom uppdras åt kommunledningskontoret att:

- se över organisationen och arbetssätt för dataskyddsarbetet i kommunen i syfte att ge bättre stöd och vägledning till verksamheterna.
- se över rutiner för att säkerställa att relevant kunskap om dataskyddsförordningen finns i verksamheterna
- fortsätta arbetet med registrering av personuppgiftsbehandlingar, (registerförteckningar, se sid 14)

Av intervjuerna med tjänstepersoner samt politiken framgår att kommunledningen har insett att det krävs ett omtag inom nämnderna vad avser tillämpningen av

dataskyddsförordningen.

I och med denna omorganisation har Burlövs kommun frångått tidigare struktur med fyra utsedda dataskyddsombud med ansvar för olika verksamheter och har sedan hösten 2020 har anställt en HR-specialist som är tillika dataskyddsombud. Av intervjuerna framgår en tjänsteuppdelning där 80% ska ägnas HR-frågor och resterande 20% ska ägnas dataskyddsfrågor.

3.3.1 Bedömning

Av granskningen framgår att det råder enighet kring att arbetet avseende efterlevnad av dataskyddsförordningen är eftersatt. En utmaning som anges är förståelsen och kunskapsnivån inom nämnderna. Vi bedömer det som positivt att det råder en medvetenhet inom kommunstyrelsen avseende att tillämpningen av dataskyddsförordningen kräver ett omtag i syfte att kunna uppfylla samt efterleva gällande lagstiftning.

Av granskningen framkommer att dataskyddsombudet inte har tidigare erfarenheter inom området. Därav anser vi att det är av vikt att organisationen stödjer dataskydds-ombudet genom att tillhandahålla erforderliga förutsättningar. Dataskyddsförordningen och dess tillämpning är ett komplext samt omfattande område, där dataskyddsombudet kommer att behöva ha en uppstarstid samt stöd för att kunna sätta sig in i dataskyddsförordningen, dess praktiska tillämpning samt nämnderna arbete. Dock är det av vikt att nämndernas omtagsarbete inte avstannar under tiden. Här har kommun-styrelsen utifrån sin uppsiktsplikt ett ansvar att följa upp nämndernas arbete.

Det bör vidare noteras att respektive nämnd är i egenskap av personuppgiftsansvarig juridiskt sett ansvarig för att uppnå en tillfredställande nivå vad avser efterlevnad av dataskyddsförordningen. Kommunstyrelsen kan därmed inte inta rollen som personuppgiftsansvarig för någon annan nämnd eller styrelse.

Vad avser dataskyddsombudets oberoende, bedömer vi att vederbörande vid tid för granskningen befinner sig organisatoriskt sett i en oberoendeposition.

3.4 Utnämning av dataskyddsombud

Samtliga personuppgiftsansvariga ska utse ett dataskyddsombud. Beslutet ska dokumenteras och vara protokollfört. Granskningen visar att nämnderna formellt har utsett ett dataskyddsombud under hösten 2020. Besluten är dokumenterade och protokollförda.

3.4.1 Bedömning

Utnämning av dataskyddsombud är korrekt hanterat.

3.5 Hantering av personuppgiftsincidenter, risk- och konsekvensbedömning mm.

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 nämn/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).

I Burlövs kommun fanns vid tid för granskningen tre styrdokument som avser att behandla hanteringen av personuppgiftsincidenter.

Det första styrdokumentet ”*Rutin för hantering av personuppgiftsincidenter*”, (KS/2018:465-009), fastställer bl.a. rutiner för risk- och konsekvensanalys, rapportering till tillsynsmyndighet, dokumentation, information till de registrerade m.m.

Det andra styrdokumentet ”*Dokumentation/rapport av personuppgiftsincident*”, fastställer den praktiska hanteringen vid upptäckt och rapporteringen av personuppgiftsincidenter, där en incident ska anmälas via en specifik e-tjänst. Dokumentet saknar beslutsinstans samt fastställelsedatum.

Det tredje styrdokumentet ”*Hantering av personuppgiftsincidenter*”, avser dock inte en direkt hantering av personuppgiftsincidenter, utan återger information om vilka personuppgifter som behandlas inom Burlövs kommun, till vem uppgifterna lämnas ut, hur länge dessa bevaras samt vilka rättigheter den registrerade har. Dokumentet är osammanhängande vad avser innehållet och det är oklart vem dokumentet vänder sig till, då rubriken samt innehållet inte överensstämmer. Dokumentet saknar vidare beslutsinstans samt fastställelsedatum.

Av dokumentet framgår en del felaktigheter, bl.a. att samtliga nämnder i Burlövs kommun behandlar dina personuppgifter…, de uppgifter som behandlas är namnuppgifter, e-postadress, telefonnr och arbetsställe…, i den här behandlingen kommer dina personuppgifter att sparas hos oss för alltid.., x-företag är person-uppgiftsbiträde och får inte använda uppgifterna i strid med vad kommunstyrelsen har bestämt mm.

Som exempel kan nämnas att personuppgifter får **endast samlas in och behandlas** för särskilda uttryckligt angivna, konkreta och berättigade ändamål, där också tillgången ska **begränsas till behöriga personal** inom respektive nämnd och verksamhetsområde. Vidare ska endast nödvändiga samt för ändamålet relevanta personuppgifter behandlas.

Det finns vidare ett fjärde styrdokument med stort sett samma innehåll, dock är rubriken ”*Register över personuppgiftsbehandlingar*”.

3.5.1 Bedömning

Vi bedömer det som positivt att rutinbeskrivningen avseende hantering av person-uppgiftsincidenter fastslår att samtliga incidenter ska dokumenteras, oavsett om de måste anmälas till tillsynsmyndigheten eller inte.

Vi anser att styrdokumentet ”Rutin för hantering av personuppgiftsincidenter” samt ”Dokumentation/rapport av incident”, kan med fördel slås samman. Detta i syfte att reducera antal rutinbeskrivningar samt underlätta för medarbetarna genom att relevant information återfinns i ett och samma styrdokument. På så sätt uppdateras även innehållet i det äldre styrdokumentet från 2018 per automatik, vad avser dokumentation, där det idag inte framgår att det finns en aktuell e-tjänst för dokumentation och rapportering av inträffade incidenter.

Vad avser det tredje och fjärde styrdokumentet bör dessa makuleras, där det finns felaktigheter samt att dokumenten inte fyller sin funktion.

Av intervju med kanslichefen och dataskyddsombudet framgår en medvetenhet av att styrdokumenten behöver ses över. Av granskningen framkommer att dataskydds-ombudet har fått i uppdrag att se över styrdokumenten. Kommunledningskontoret kommer att avvakta med revidering av styrdokumenten, där revisionsrapporten kommer att inväntas, i syfte att nyttja underlaget som stöd i förbättringsarbetet.

3.6 Dokumentation och omfattning av personuppgiftsincidenter

Av styrdokumentet ”Dokumentation/rapport av personuppgiftsincident” framgår att en personuppgiftsincident ska rapporteras inom 24h av den som har upptäckt incidenten. Incidenten ska anmälas via en e-tjänst. Därefter ska utsedd delegat besluta om huruvida incidenten ska rapporteras till Datainspektionen (nuvarande Integritetsskydds-myndigheten) samt huruvida den registrerade ska informeras. Vidare ska incidenten följas upp i en särskild mall.

Under 2018 och 2019 har det funnit fyra delar som skulle ha hanteras vid en incident:

-- Del 1, dokumentation/beskrivning av incident

-- Del 2, risk- och konsekvensanalys

-- Del 3, uppföljning av personuppgiftsincident

-- Del 4, delegationsbeslut

Under 2020 har del 2 och 4 slagits ihop, där risk- ock konsekvensanalysen genomförs i underlaget för delegationsbeslut.

Samtliga delar ska fyllas i vid en personuppgiftsincident.

Nedan redogörs för antal personuppgiftsincidenter per nämnd. Enligt uppgift har 48 incidenter inträffat/upptäckts sedan dataskyddsförordningen ikraftträdande maj 2018. Det bör beaktas att statistiken inte är komplett, där det enligt dataskyddsombudet inte har varit möjligt att ta fram statistik via aktuell e-tjänst före vecka 27 avseende år 2020. Likaså har dataskyddsombudet inte erhållit något svar från den gemensamma IT-nämnden vad avser incidenter under 2018 och 2019. Enligt uppgift har överförmyndarnämnden inte haft/upptäckt några incidenter under 2018 – 2020.

Vi har begärt in dokumentation avseende samtliga personuppgiftsincidenter i enlighet med tabellen nedan. Dock har vi inte kunnat ta del av samtlig dokumentation, där en del saknas (kommunstyrelsen, socialnämnden och samarbetsnämnd löneservice).

Vad avser samarbetsnämnden IT-drift saknas information avseende eventuella incidenter under 2018 och 2019 och därmed också eventuell dokumentation.

Nämnd	Antal incidenter 2018	Varav anmälda till DI	Antal incidenter 2019	Varav anmälda till DI	Antal incidenter 2020	Varav anmälda till DI
Kommunstyrelsen	1	0	4	0	9	0
Miljö- och byggnämnden	0	0	1	1	1	0
Utbildnings- och kulturnämnden	3	0	6	0	11	0
Socialnämnden	1	0	3	0	5	0
Samarbetsnämnd Löneservice	0	0	2	0	0	0
Samarbetsnämnd IT-drift	0	0	0	0	1	1
Överförmyndaren	0	0	0	0	0	0

Figur 3:6: Antal redovisade personuppgiftsincidenter per nämnd och år.
Källa: Burlövs kommun

3.6.1 Bedömning

Vi har noterat att personuppgiftesincidenter har dokumenterats med varierande kvalitet, där det förekommer centrala brister som leder till att lagstiftningen krav avseende dokumentation av incidenter inte uppfylls.

Vi har genomfört stickprovskontroller av 25 personuppgiftsincidenter. Av dessa saknar 16 incidenter en genomförd risk- och konsekvensbedömning. Vidare saknas del 3 i dokumentationen, d.v.s. ”uppföljning av incident”, som är en central del. Avsaknad av dessa delar förekommer framförallt inom socialnämnden samt utbildnings- och kulturnämnden.

Viktiga delar i uppföljningsmallen är bl.a.:

- huruvida den registrerade ska informeras om incidenten,
- vilka åtgärder som har vidtagits för att minimera samt mildra konsekvenserna av en Incident,
- vilka steg har förvaltningen vidtagit för att förhindra upprepning av aktuell typ av incident.

Det förekommer vidare inkonsekventa risk- och konsekvensbedömningar samt att olika chefer har bedömt riskerna olika avseende samma incident. Likaså att beslut om huruvida incidenten ska anmälas till tillsynsmyndigheten saknas.

Vi bedömer att det krävs ett omtag vad avser dokumentation av personuppgifts-incidenter i syfte att uppnå en korrekt dokumentation i enlighet med lagstiftningens krav. Vi anser att det finns ett tydligt behov av utbildningsinsatser avseende hantering och dokumentation av incidenter inom verksamheterna.

Förutom otillräckliga kunskapsnivåer kan en anledning till bristande dokumentation vara att det finns alltför många mallar att hålla reda på som leder till att centrala delar uteblir.

Vi rekommenderar en sammanslagning av mallarna, där den som har upptäckt incidenten kan tillsammans med utsedd delegat fylla i underlaget. Detta i syfte att undvika att väsentliga delar uteblir, så som risk- och konsekvensanalys, information om huruvida den registrerade ska informeras, vilka åtgärder som har vidtagits för att minimera och mildare konsekvenserna mm.

Vidare rekommenderar vi att samråd sker med dataskyddsombudet i samband med risk- och konsekvensanalys samt bedömningar om huruvida incidenten ska anmäla till tillsynsmyndigheten samt huruvida den berörda ska informeras.

Ett förslag är att ersätta dagens mallar med Integritetsskyddsmyndighetens anmälningsblankett i sin helhet där samtliga nödvändiga delar finns upptagna. Detta effektiviserar samt underlättar det interna arbetet, minskar administrationen, underlättar spårbarheten då dokumentationen återfinns i ett enda dokument, skapar en mer enhetlig hantering samt leder till att riskerna avseende att viktiga delar uteblir minimeras.

Vi bedömer vidare att det är alltför få incidenter som har upptäckts/rapporterats i förhållande till verksamheternas omfattning. Detta bekräftas också av en intern kontroll genomförd av de tidigare dataskyddsombuden, där det fastslås att det är orimligt få personuppgiftsincidenter samt att det förekommer att inträffade incidenter inte har rapporterats.

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 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.

Burlövs kommun har inledningsvis använt sig av ett digitalt verktyg för att registrera personuppgiftsbehandlingar. Dock upplevdes verktyget som svåranvänt och få behandlingar registrerades. Under hösten 2019 övergick kommunen till ett nytt verktyg Draftit Privacy.

Dock har vid tid för granskningen endast ett fåtal behandlingar registrerats i Draftit och vi har inte kunnat ta del av dessa då arbetet med att upprätta registerförteckningar är i ett startskede. Vi har delgivits ett äldre underlag med en del registerförteckningar för kommunstyrelsen, socialnämnden och utbildnings- och kulturnämnden. Förteckningarna återfinns i en och samma excelfil för samtliga tre nämnder. Dessa förteckningar är dock inte aktuella i och med att nya förteckningar behöver upprättas.

Av intervjuerna framgår att det finns utmaningar vad gäller kunskap, kompetens och förståelse för hantering och upprättande av registerförteckningarna, där dessa delar inte är på en tillfredställande nivå idag.

Arbete med att utbilda verksamheterna har inletts under 2021.

3.7.1 Bedömning

Vi bedömer att det krävs ett ordentligt utvecklingsarbete vad avser upprättande och hantering av registerförteckningar. Det har snart gått tre år sedan dataskydds-förordningen trädde ikraft, där registerförteckningar som är en central del i hanteringen av personuppgifter borde vara färdigupprättade. Vi anser att verksamheterna bör skyndsamt genomföra en inventering av befintliga personuppgifters behandlingar för att därefter upprätta registerförteckningar.

I det äldre underlaget som vi har tagit del av finns exempelvis endast sex behandlingar inom ramen för kommunstyrelsen verksamheter. Som referens kan nämnas att kommunstyrelsen verksamhet brukar innefatta 70 - 150 behandlingar beroende på vilka verksamhetsområden som lyder under kommunstyrelsen. Härigenom är det av vikt med en noggrann inventering i syfte att få med samtliga behandlingar.

Utifrån de äldre registerförteckningarna kan vi konstatera att nämnderna är i behov av riktade utbildningsinsatser och stöd vad avser de frågor som behöver besvaras för respektive behandling där följande brister förekommer:

Avsaknad av eller felaktig angivelse av laglig/rättslig grund för registreringen.

- *Uppgifter av allmänt intresse* förekommer frekvent som rättslig grund utan hänvisning till lagstöd. För att uppgifter av allmänt intresse ska kunna nyttjas krävs stöd i lagstiftningen eller beslut som har meddelats med stöd av lagstiftning. Det är av vikt att personuppgiftsansvarig nämnd kan motivera valet av rättslig grund.
- Benämningen ”myndighetsutövning” förekommer som svar på efterfrågat lagstöd. All myndighetsutövning ska grundas på lagar inom EU-rätten eller nationell rätt. Därmed ska aktuell författning och lagrum anges i samband med angivande av myndighetsutövning som rättslig grund.
- Vad avser ”känsliga personuppgifter” är utgångspunkten att det är förbjudet att behandla dessa. Det finns dock undantag. Det bör framhållas att vad gäller behandling av känsliga personuppgifter finns specificerade krav enligt artikel 9 i dataskyddsförordningen. Följande grunder anges bl.a. som rättslig grund för behandling av känsliga personuppgifter: *allmänt intresse, skydd av grundläggande intressen, uppgifterna är redan kända* mm. Känsliga uppgifter kan endast behandlas med stöd av gällande lagstiftning.
- Avsaknad av tidsfrister för gallring. Denna punkt berör dataskyddsförordningens grundläggande princip om ”lagringsminimering”.
- Avsaknad av allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.
- Avsaknad av information om anlitat personuppgiftsbiträde.

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 kan under visa omständigheter kräva att personuppgifter behandlas endast för vissa avgränsade syften.

Av granskningen framkommer att det finns en specifik blankett framtagen för kommunmedborgarna där begäran avseende registerutdrag, rättelse, radering, begränsning samt invändningar kan göras.

Dock saknas en rutinbeskrivning som fastställer ansvarsfördelning samt den praktiska hantering när en begäran inkommer.

3.8.1 Bedömning

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

4 Slutsats och rekommendationer

Sammantaget kan konstateras att det finns brister vad avser efterlevnaden av dataskyddsförordningen. Av granskningen framkommer att det finns en medvenhet kring befintliga brister.

Vi bedömer att det krävs ett ordentligt omtag vad gäller tillämpningen av dataskyddsförordningen i syfte att kunna uppnå en tillfredställande nivå vad avser efterlevnad av gällande lagstiftning.

4.1 Rekommendationer

Mot bakgrund av vår granskning rekommenderar vi:

- att det är av vikt att organisationen stödjer dataskyddsombudet genom att tillhandahålla erforderliga förutsättningar. Dataskyddsförordningen och dess tillämpning är ett komplext samt omfattande område, där dataskyddsombudet kommer att behöva ha en uppstarstid samt stöd för att kunna sätta sig in i dataskyddsförordningen, dess praktiska tillämpning samt nämndernas arbete. Det är dock av vikt att nämndernas omtagsarbete inte avstannar under tiden.
- kommunstyrelsen bör utifrån sin uppsiktsplikt följa upp nämndernas arbete vad avser efterlevnad av dataskyddsförordningen.

- Utifrån att nämndernas arbete vad gäller att uppnå lagstiftningens krav är eftersatt, erfordras en central styrning från kommunstyrelsen sida.
- Styrdokumenten med sikte på dataskyddsförordningen tillämpning bör ses över.
- Styrdokument i form av rutinbeskrivningar kan med fördel slås samman. Detta i syfte att reducera antal rutinbeskrivningar samt underlätta för medarbetarna genom att relevant information återfinns i ett och samma styrdokument.
- Vissa styrdokument/rutinbeskrivningar bör makuleras, (se sid. 10).
- Vi bedömer att det krävs ett omtag vad avser dokumentation av personuppgifts-incidenter i syfte att uppnå en korrekt dokumentation i enlighet med lagstiftningens krav. Vi anser att det finns ett tydligt behov av utbildningsinsatser avseende hantering och dokumentation av incidenter inom verksamheterna.
- Dokumentationsmallar avseende personuppgiftsincidenter bör slås samman i syfte att bl.a. att minimera riskerna avseende att viktiga delar uteblir. Ett förslag är att använda Integritetsskyddsmyndighetens anmälningsblankett för dokumentation av samtliga incidenter.
- Vi bedömer att det är alltför få incidenter som har upptäckts/rapporterats till förhållande till verksamheternas omfattning, där medarbetarna är i behov av en ökad kunskapsnivå.
- Vi bedömer att det krävs ett ordentligt utvecklingsarbete vad avser upprättande och hantering av registerförteckningar. Registerförteckningar har till syfte att säkerställa att de **grundläggande principerna** inom dataskyddslagstiftningen efterlevs. Vi anser att verksamheterna bör skyndsamt genomföra en inventering av befintliga personuppgifters behandlingar för att därefter upprätta registerförteckningar.
- Vad avser angivande av rättslig grund för behandling av personuppgifter är verksamheterna i behov av en ökad kunskapsnivå. Ytterligare utvecklingsområden återfinns på sid. 14.
- Kommunstyrelsen bör upprätta en rutinbeskrivning avseende hanteringen av inkomna begäran om registerutdrag, rättelse, radering och begränsning.

Datum som ovan

KPMG AB

Burlövs kommun
Granskning av rutiner för efterlevnad av dataskyddsförordningen

2021-03-01

Viktoria Berstam

Specialist/Certifierad kommunal revisor

Göran Acketoft
Certifierad kommunal revisor, kundansvarig