Granskning av kommunens styrdokument inom ramen för dataskyddsförordningen

Revisionsrapport

Täby kommun

KPMG AB

2021-03-10

Antal sidor: 18

Innehållsförteckning

1 Sammanfattning

Vi har av Täby kommuns revisorer fått i uppdrag att granska kommunens styrdokument inom ramen för dataskyddsförordningen.

Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. 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 samt leda till förtroendeskador för kommunen.

Sammanfattningsvis kan konstateras att kommunstyrelsen i huvudsak har tillfredställande styrdokument och rutiner vad avser tillämpningen av dataskyddsförordningen.

Det finns utvecklingsområden vad avser arbetet med och efterlevnaden av dataskyddsförordningen.

Mot bakgrund av vår granskning och våra iakttagelser rekommenderar vi följande:

- Mot bakgrund av den centraliserade dataskyddsorganisationen vill vi betona att det är av stor vikt att nämnder och styrelser är införstådda med ansvarsförhållandet, där respektive nämnd och styrelse är juridiskt sett ytterst ansvarig för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen samt ansvarar för att säkerställa att hantering av personuppgifter följer gällande föreskrifter. Kommunstyrelsen kan inte inta rollen som personuppgiftsansvarig för någon annan nämnd eller styrelse. Detta även att dataskyddsorganisationen lyder under kommunstyrelsen.
  Det är med andra ord inte dataskyddsombudet eller kommunstyrelsen som hålls ansvarig vid en eventuell bristande efterlevnad av dataskyddsförordningen inom övriga nämnder och styrelser.

- Kommunstyrelsen bör säkerställa att medarbetarna har en insikt för utredningsunderlagets funktion och syfte avseende **personuppgiftsincidente**r. Underlaget är avgörande för bedömning av incidenterna, där bl.a. risk- och konsekvensbedömning av inträffade incidenter är en central del som behöver genomföras och färdigställas.

- Den kommunövergripande utredningsmallen avseende personuppgiftsincidenter bör kompletteras med svars-/bedömningsrutor avseende information om huruvida incidenten kommer att anmälas till tillsynsmyndigheten samt huruvida de registrerade ska informeras om incidenten. Det är av vikt att denna information dokumenteras samt framgår på ett tydligt sätt i underlaget.

- Rutinbeskrivningen avseende hantering av personuppgiftsincidenter bör revideras vad avser formuleringen om ”information till den registrerade” i

samband med en incident, där dagens formulering riskerar leda till misstolkningar.

- Beskrivning av rutiner för utvärdering och avgörande av anmälningspliktiga incidenter i styrdokumentet samt den information som återges på intranätet bör vara densamma.

- Styrdokumentet avseende hantering av personuppgiftsincidenter kan med fördel förtydligas med att dokumentation av personuppgiftsincidenter ska ske **oaktat allvarlighetsgrad** samt oaktat om incidenten anmäls till tillsynsmyndigheten eller ej.

- Det finns ett behov av kunskapsökning bland personalen i verksamheterna, där utbildning i form av återgivning av konkreta exempel är av betydelse för en ökad förståelse samt upptäckt av eventuella personuppgiftsincidenter.

- Det finns ett behov av riktade utbildningsinsatser till verksamheterna vad avser registerförteckningar. Registerförteckningarna är en central del i hanteringen av personuppgifter, där kommunstyrelsen i egenskap av personuppgiftsansvarig bör se över styrelsens förteckningar och genomföra erforderliga kompletteringar och korrigeringar.

2 Bakgrund

Vi har av Täby kommuns revisorer fått i uppdrag att granska kommunens styrdokument inom ramen för dataskyddsförordningen.

2.1 Syfte och revisionsfråga

Rapporten syftar till att granska kommunövergripande styrdokument inom ramen för dataskyddsförordningen. Följande avser rapporten besvara:

1. Finns det ett centralt utsett dataskyddsombud?
2. Har samtliga nämnder beslutat om att utse ett dataskyddsombud?
3. Har nämnderna säkerställt att det finns registerförteckningar över personuppgiftsbehandlingar i enlighet med artikel 30.1, dataskyddsförordningen?
4. Finns kommunövergripande rutiner för hantering av personuppgiftsincidenter?
5. Förmedlar rutinerna en korrekt hantering av personuppgiftsincidenter i enlighet med lagens intentioner?
6. Har rutinerna för incidentrapportering efterlevts av nämnder och styrelser?
7. Sker en korrekt dokumentation av inträffade personuppgiftsincidenter i enlighet med dataskyddsförordningen?
8. Har det genomförts någon riskbedömning av incidenterna och hur många har kategoriserats som allvarliga?
9. Har incidenter som bedömts medföra allvarliga risker för den registrerades integritet anmälts till IMY?
10. Hur många personuppgiftsincidenter har inträffat sedan lagens ikraftträdande?
11. Är berörda nämnder/styrelser informerade om inträffade incidenter?
12. Finns dokumenterade rutiner för begäran om registerutdrag?
13. Finns dokumenterade rutiner för rättelse av uppgifter?
14. Finns dokumenterade rutiner för radering av uppgifter?

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

- Studium och genomgång av relevanta styrdokument och beslutsunderlag.
- Utifrån de förtroendevalda revisorernas önskemål har ett tillägg gjorts i granskningen i form av stickprovskontroller av registerförteckningar avseende personuppgifts-behandlingar.
- Intervjuer och avstämningar har genomförts med dataskyddsombud, trygghets- och säkerhetschef samt kommunstyrelsens ordförande. Dataskyddsombudet lyder organisatoriskt sett under trygghets- och säkerhetschefen.

Rapporten har faktakontrollerats av trygghets- och säkerhetschefen samt dataskydds-ombudet.

3. Övergripande 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.

4. Resultat av granskningen

4.1 Dataskyddsombudets uppdrag och oberoende

Dataskyddsförordningen, artikel 39 fastställer följande uppgifter för dataskydds-ombudet, (DSO):

- 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, inbegripet 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.

Dataskyddsombudets oberoende är en förutsättning för arbetsuppgifternas utförande.

Det är därmed av stor vikt att dataskyddsombudet befinner sig i en **oberoende-position**, där vederbörande ska kunna arbeta självständigt och fullgöra sina uppgifter på ett oberoende sätt.

Detta innebär att personuppgiftsansvariga eller personuppgifts- biträden inte får exempelvis instruera dataskyddsombudet om vilka resultat som bör uppnås, hur ett klagomål ska hanteras eller att inta en viss ståndpunkt i ärenden som rör dataskyddslagstiftningen.

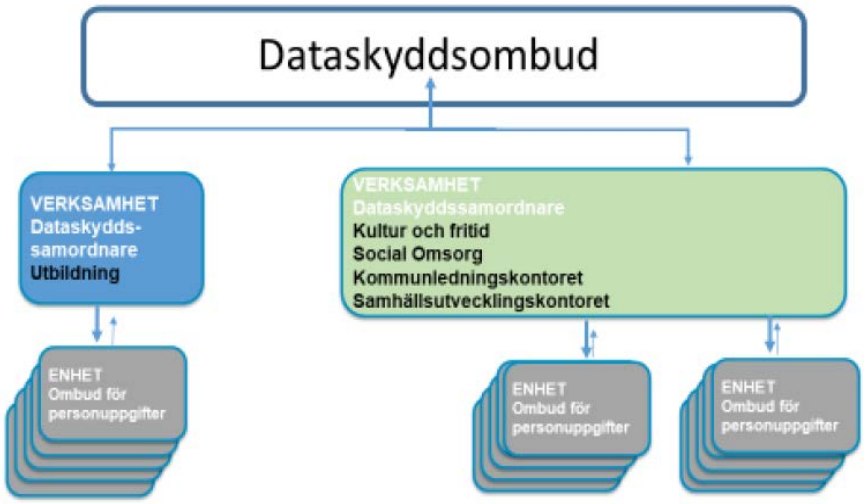
Som exempel kan nämnas att det inte är lämpligt att ett dataskyddsombud sitter i organisationens ledning eller är delaktig i att fatta strategiska beslut om kärn-verksamheten.

Iakttagelser

Täby kommun har inrättat en s.k. ”dataskyddsombudsorganisation” bestående av dataskyddsombud, dataskyddssamordnare samt ombud för personuppgifter, (se figur 4.1)

Sedan juni 2018 finns ett dataskyddsombud med en tjänsteomfattning på 100 %. Befattningen innebär därmed en heltidstjänst med fokus på dataskyddsfrågor. I organisationsbeskrivningen anges dataskyddsombudets huvudsakliga uppgift till att övervaka att Täby kommuns personuppgiftsansvariga efterlever dataskydds-förordningen.

Figur 4:1



Källa: Täby kommun

4.1.1 Kommentarer och bedömning

Dataskyddsförordningen är omfattande och komplext till sin karaktär, där verksamheterna är i ständigt behov av stöd och vägledning i syfte att kunna tillämpa gällande lagstiftning.

Utifrån dataskyddsförordningens omfattning samt komplexitet bedömer vi det som positivt att en centraliserad organisation har inrättats. Vi anser vidare att det är av vikt med en central styrning från kommunstyrelsen sida i syfte att uppnå en **enhetlig** hantering och skapa **samsyn** inom samtliga nämnder vad avser lagstiftningens tillämpning. I detta arbete ingår även att öka nämndernas förståelse och acceptans för dataskyddsförordningens intentioner samt för dataskyddsombudets roll och uppdrag.

Mot bakgrund av den centraliserade organisationen vill vi samtidigt betona att det är av stor vikt att nämnder och styrelser är införstådda med ansvarsförhållandet, där respektive nämnd och styrelse är juridiskt sett ytterst ansvarig för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen. Kommunstyrelsen kan inte inta rollen som personuppgiftsansvarig för någon annan nämnd eller styrelse. Detta även att dataskyddsorganisationen lyder under kommunstyrelsen.

Likaså behöver dataskyddsombudets roll som rådgivande samt bevakande beaktas, där det är personuppgiftsansvariga som ska agera verkställande.

Vad avser dataskyddsombudets oberoende, bedömer vi att vederbörande befinner sig i en oberoende position.

5. Utnämning av dataskyddsombud

Samtliga personuppgiftsansvariga ska utse ett dataskyddsombud. Beslutet ska dokumenteras och protokollföras.

Iakttagelser

Vi har tagit del av samtliga nämnders beslut avseende utnämning av dataskydds-ombud.

5.1 Kommentarer och bedömning

Av granskningen framgår att samtliga nämnder inklusive den gemensamma nämnden Södra Roslagens miljö- och hälsoskyddsnämnd, formellt har utsett ett dataskydds-ombud. Besluten är dokumenterade och protokollförda.

6. Personuppgiftsincidenter och risk- och konsekvens-bedömning

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 Integritetsskyddsmyndigheten. Därav är det av vikt att ansvarig nämnd genomför en konsekvensanalys vid eventuella incidenter i syfte att bedöma allvarlighetsgraden.

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

Iakttagelser

Vid tid för granskningen finns ett kommunövergripande styrdokument avseende personuppgiftsincidenter, utfärdat 2019-07-02, där rutinen för hantering av personuppgiftsincidenter anges. Dock framgår inte beslutsinstans. En rutinbeskrivning återfinns också på kommunens intranät ”Insidan”.

Av rutinbeskrivningen framgår att en misstänkt personuppgiftsincident ska omedelbart och skyndsamt anmälas direkt till dataskyddsombudet, där den som har upptäckt incidenten ska fylla i en särskild mall med benämningen ”*Utredning med anledning av personuppgiftsincident*”. Mallen följer till viss del Integritetsskyddsmyndighetens anmälningsblankett vid inrapportering av en incident.

I aktuell utredningsmall ska incidenten beskrivas, följt av bl.a. förtydligande av vilka personuppgifter som berörs, vilka kategorier av registrerade som berörs, konsekvens av incidenten, antal registrerade som berörs, åtgärder som har vidtagits vid upptäckt av incidenteten, huruvida incidenten berör ett personuppgiftsbiträde samt en bedömning av risker och allvarlighetsgraden för den enskilde individen.

Bedömning av allvarlighetsgraden följer Integritetsskyddsmyndighetens skala, enligt följande:

1. Obetydlig
2. Begränsad
3. Betydande
4. Mycket allvarligt

Styrdokumentet fastställer vidare att dataskyddsombudet utvärderar händelsen och avgör om det är en anmälningspliktig incident eller inte. Av rutinbeskrivningen på intranätet framgår dock att dataskyddsombudet **tillsammans** med den som har upptäckt incidenteten ska utvärdera och avgöra huruvida incidenten ska anmälas till Datainspektionen, (nuvarande IMY).

Av rutinbeskrivningen framgår att den personuppgiftsansvarige ska informera de registrerade som berörs av incidenten, om incidenten innebär en risk för de registrerades rättigheter och friheter. Dock behöver den registrerade inte informeras om skyddsåtgärder redan har vidtagits, till exempel att uppgifterna som omfattas av incidenten är krypterade.

Av intervjuerna framgår att **dataskyddsombudet avgör** huruvida den registrerade ska informeras om en personuppgiftsincident.

6.1 Kommentarer och bedömning

Dokumentation av personuppgiftsincidenter är av central betydelse i syfte att kunna efterleva gällande lagstiftning. Dokumentationen är obligatorisk, där den **personuppgiftsansvarige** ska dokumentera samtliga personuppgiftsincidenter inbegripet **omständigheterna kring incidenten**, **effekter** samt de **korrigerande åtgärder** som har vidtagits. Personuppgiftsincidenter som inte hanteras på ett korrekt sätt kan leda till sanktionsavgifter samt förtroendeskador för Täby kommun.

För att den personuppgiftsansvarige ska kunna avgöra huruvida en incident ska anmälas till tillsynsmyndigheten Integritetsskyddsmyndigheten samt huruvida den registrerade ska informeras, erfordras en risk- och konsekvensbedömning vid varje incident.

Vi har genomfört stickprovskontroller avseende dokumentationen i ett urval av inträffade personuppgiftsincidenter i Täby kommun. Det förekommer att utredningsmallen inte är komplett, där exempelvis beskrivning av incidenten saknas samt att risk- och konsekvensbedömningen inte är avklarad. Vi anser att kommunstyrelsen bör säkerställa att medarbetarna har en insikt för utredningsmallens funktion och syfte, där bl.a. risk- och konsekvensbedömningen är en central del i underlaget som behöver genomföras.

Vi bedömer att den kommunövergripande utredningsmallen bör kompletteras med svars-/bedömningsrutor avseende information om huruvida incidenten kommer att anmälas till tillsynsmyndigheten samt huruvida de registrerade ska informeras om incidenten. I dagsläget saknas denna information i mallen.

Vi bedömer vidare att följande information i rutinbeskrivningen bör tas bort, där dagens formulering riskerar leda till misstolkningar avseende när den registrerade ska informeras om en incident:

”*Dock behöver den registrerade inte informeras om skyddsåtgärder redan har vidtagits, till exempel att uppgifterna som omfattas av incidenten är krypterade*.”

Skyddsåtgärder som sätts in efter att en incident har upptäckts är inte alltid tillräckliga och kan komma i ett sent skede beroende på när i tid incidenten har upptäckts. Lagstiftningens främsta intention med information till enskilda utan onödigt dröjsmål är att mildra riskerna för skador, där de registrerade ska kunna vidta åtgärder för att skydda sig själva i samband med en personuppgiftsincident. Ett exempel är obehörig åtkomst till skyddade personuppgifter.

Beskrivning av rutiner för utvärdering och avgörande av anmälningspliktiga incidenter i styrdokumentet samt den information som återges på intranätet bör vara densamma.

Vidare anser vi att styrdokumentet med fördel kan förtydligas med att dokumentation av personuppgiftsincidenter ska ske **oaktat allvarlighetsgrad** samt oaktat om incidenten anmäls till tillsynsmyndigheten eller ej.

Det bör noteras att ett dataskyddsombud ska agera rådgivande samt bevakande. Dock är det personuppgiftsansvarig nämnd som ansvarar för **verkställighet** och **bedömningar**.

Av intervjuerna med tjänstepersonerna framgår en medvetenhet kring ovan beskrivna roller och ansvarsförhållanden samt lagstiftningens utformning. Dock uttrycks att utifrån dataskyddsförordningens komplexitet och stor efterfrågan på stöd och vägledning, genomförs bedömningarna avseende huruvida en incident ska anmälas till tillsynsmyndigheten samt huruvida den registrerade ska informeras, av dataskyddsombudet.
Vi har en förståelse för detta upplägg, dock är det av vikt att nämnder och styrelser är medvetna om att de i egenskap av personuppgiftsansvariga innehar det fulla ansvaret för att säkerställa att hantering av personuppgifter följer gällande föreskrifter. Det är med andra ord inte dataskyddsombudet eller kommunstyrelsen som hålls ansvarig vid en eventuell bristande efterlevnad av dataskyddsförordningen inom övriga nämnder och styrelser.

Vi anser att det är av vikt att samtliga personuppgiftsincidenter kommer till dataskyddsombudets kännedom. Därav bedömer vi uppmaningen i rutinbeskrivningen till att informera dataskyddsombudet om inträffade personuppgiftsincidenter som positiv.

Av aktuellt styrdokument bör beslutsinstans framgå.

7. Omfattningen av personuppgiftsincidenter

Iakttagelser

Nedan redogörs för antal personuppgiftsincidenter per nämnd.

Nämnd	Antal incidenter 2018	Varav anmälda till DI	Antal incidenter 2019	Varav anmälda till DI	Antal incidenter 2020	Varav anmälda till DI
Kommunstyrelse	0	0	9	1	0	0
Stadsbyggnadsnämnd	0	0	1	0	0	0
Barn- och grundskolenämnd	2	2	6*	1	1*	0
Socialnämnd	1	1	8	1	16	4
Lantmäterinämnd	0	0	0	0	0	0
Gymnasie- och näringslivsnämnd	0	0	1*	0	1*	0
Kultur- och fritidsnämnd	1	1	0	0	1	1
Överförmyndarnämnd	0	0	0	0	0	0
Södra Roslagns miljö- och hälsoskyddsnämnd	1	1	0	0	1	0
Valnämnd	0	0	0	0	0	0

Figur 7:1

** Avser samma incident.*

Av tabellen framgår ett fåtal incidenter i majoriteten av nämnderna. Det förekommer också att personuppgiftsincidenter inte har inträffat sedan lagens ikraftträdande.

Av granskningen framkommer att nämnderna får årligen kännedom om dokumenterade samt inrapporterade personuppgiftsincidenter via dataskyddsombudets årsrapport.

Nämnderna får vidare information om inträffade incidenter via redovisning av delegationsbeslut.

7.1 Kommentarer och bedömning

Vi bedömer sannolikheten att flertalet nämnder inte har haft någon form av personuppgiftsincident alternativt har endast ett eller två fall, som låg. Baserad på vår erfarenhet är en grundläggande orsak, avsaknad av tillräckliga kunskaper om vad en personuppgiftsincident är och vad som ska klassas som en incident. Bedömningen delas av de intervjuade där det råder enighet om att avsaknad av kunskap är den huvudsakliga orsaken och att det finns behov av utbildningsinsatser vad gäller förståelse och hantering av personuppgiftsincidenter.

Under 2019 fick Datainspektionen (nuvarande IMY), in ca 90 anmälningar per vecka. En ökning med ca 30 % i jämförelse med 2018. Ökningen härleds till en ökad medvetenhet och kunskap om anmälningsskyldigheten. Det bör också understrykas att det finns ett stort mörkertal avseende anmälningspliktiga incidenter som inte kommer till tillsynsmyndighetens kännedom.

Vi anser att det finns ett behov av kunskapsökning bland personalen i verksamheterna, där utbildning i form av återgivning av konkreta exempel är av betydelse för en ökad förståelse samt upptäckt av eventuella personuppgiftsincidenter.

8. Registerutdrag

Inom ramen för de registrerades rättigheter återfinns ”rätten till tillgång”, (dataskyddsförordningen artikel 15), som innebär att den registrerade har rätt till 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.

Iakttagelser

Vi har delgivits en kommunövergripande rutinbeskrivning vad avser hantering av begäran om registerutdrag, (utfärdad 2019-06-04).

8.1 Kommentarer och bedömning

Vi bedömer att kommunstyrelsen har en tillfredsställande rutin vad avser hantering av begäran av registerutdrag. Av rutinbeskrivningen framgår en tydlig praktisk hantering, följt av en roll- och ansvarsfördelning. Begäran om ett registerutdrag kan genomföras via en e-tjänst på kommunens hemsida samt även manuellt.

9. Rättelse, radering och begränsning

Rätten för de registrerade att begära rättelse, radering och begränsning av personuppgifter regleras i artikel 16-18, dataskyddsförordningen.

Den registrerade har 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.

Iakttagelser

Vi har tagit del av kommunövergripande rutinbeskrivningar avseende hantering av begäran om rättning, begränsning, radering och att lämna invändningar, (utfärdad 2019-06-04).

9.1 Kommentarer och bedömning

Vi bedömer att kommunstyrelsen har tillfredställande rutiner avseende begäran om rättelse, radering och begränsning av personuppgifter. Av granskningen framkommer att medborgarna kan inkomma med en begäran via kommunens e-tjänster samt även manuellt.

10. Registerförteckningar och övriga iakttagelser utanför ramen för revisionsfrågorna

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, att personuppgiftsansvariga ska 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

Täby kommun använder sig av verktyget Drafit Privacy vad avser upprättande av registerförteckningar över personuppgiftsbehandlingar. Verktyget innehåller ett frågebatteri som ska besvaras i samband med varje behandling. Frågebatteriet har reducerats vad avser antal frågor i syfte att underlätta för verksamheterna.

Enligt uppgift har samtliga nämnder upprättat registerförteckningar över personuppgiftsbehandlingar. Vi kan dock inte bedöma om samtliga behandlingar inom nämndernas verksamhetsområden har upptagits i en förteckning.

Vi har utifrån de förtroendevalda revisorernas önskemål gjort ett tillägg i granskningen som ligger utanför ramen för revisionsfrågorna, där vi har tittat närmare på kommunstyrelsens registerförteckningar samt genomfört stickprovskontroller.

Vid tid för granskningen finns 215 upprättade registerförteckningar inom ramen för kommunstyrelsen verksamhet, varav 20 st är färdigställda i enlighet med verktyget Drafit. Stödsystemet har en s.k. ”klarmarkeringsfunktion” för respektive förteckning. Enligt uppgift använde Täby kommun inte denna funktion, där kommunen har bett om att funktionen ska tas bort. Dock är detta inte möjligt enligt leverantören.

Frågor som behandlas i enlighet med dataskyddförordningens krav och intentioner i registerförteckningarna är bl.a.: uppgifter om personuppgiftsansvarig, 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, huruvida det finns upprättat personuppgiftsbiträdeavtal, utlämnande av uppgifter till tredjepart, överföring till tredjeland, säkerhetsåtgärder mm.

Av stickprovskontrollerna framgår bl.a. följande brister:

Vi har uppmärksammat att ”vet ej svar/avsaknad av svar” förekommer i ca 500 fall. Nedan återges några exempel:

- Vilken rättslig grund som används som stöd för behandlingen
- Huruvida känsliga personuppgifter behandlas
- Om uppgifter om barn behandlas
- Om det finns gallringsrutiner
- Vilka tidsfrister som gäller för gallring
- Om något personuppgiftsbiträde anlitas.

- Om det finns ett dokumenterat biträdesavtal med personuppgiftsbiträdet.
- Om informationskravet uppfyllts
- Om de registrerades rättigheter uppfylls
- Om det finns dokumentation som kan påvisa att samtycke har inhämtats
- Om personnummer behandlas
- Huruvida det finns en berättigad anledning till att informationskravet inte har uppfyllts
- Huruvida det finns en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder för den aktuella personuppgiftsbehandlingen
- Om några personuppgifter lämnas ut till tredjepart
- Huruvida personuppgifterna publiceras öppet
- Huruvida personuppgifterna lämnas till tredje land

Vidare behöver följande delar beaktas:

- **Uppgifter 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 beslut som har meddelats med stöd av lagstiftning. Det är av vikt att personuppgiftsansvarig nämnd kan motivera valet av rättslig grund.
- Speciallagstiftning förekommer som svar på vilken rättslig grund som finns som stöd. Vid angivande av s.k. speciallagstiftning ska författningen ifråga anges.
- Avsaknad av tidsfrister för gallring. Denna punkt berör dataskyddsförordningens grundläggande princip om ”lagringsminimering”. Vidare förekommer svar som: Oklart i dagsläget, hanteringsanvisningarna ej klara, utredning pågår, behöver kollas upp m.fl. förekommer.
- Vad avser ”känsliga personuppgifter” är utgångspunkten att det är förbjudet att behandla dessa. Det finns dock undantag. Det bör noteras att det finns specificerade krav enligt artikel 9 följt av i vissa fall **krav på konsekvens-bedömningar** i enlighet med artikel 35, vad gäller behandling av känsliga personuppgifter. Det ställs därmed krav på att behandling av känsliga personuppgifter ska vara väl motiverade och välgrundade med stöd lagstiftningen. Det förekommer att ”allmänt intresse” anges som stöd för behandling av känsliga personuppgifter utan hänvisning till aktuell lagstiftning och lagrum.
- Vi har uppmärksammat förekomst av behandling av känsliga personuppgifter i form av ”*Ras/etniskt ursprung, politiska åsikter, religiös/filosofisk övertygelse, hälsoinformation*”, men motivering saknas.
  Det är av vikt att det finns ett konkret och precist ändamål som kräver att känsliga personuppgifter behöver behandlas, där också lagstöd behöver redogöras.

- Vi har noterat att kommunstyrelsen anges som personuppgiftsansvarig avseende en förteckning tillhörande kommunrevisionen. Det bör noteras att det är kommunrevisionen som är personuppgiftsansvarig för eventuella behandlingar inom ramen för revisionens verksamhet.
- Det förekommer att styrelsen har anlitat ett personuppgiftsbiträde, dock saknas i vissa fall information om huruvida det finns ett personuppgiftsbiträdesavtal.

10.1 Kommentarer och bedömning

Vi bedömer att det finns ett behov av riktade utbildningsinsatser till verksamheterna vad avser registerförteckningar. Registerförteckningarna är en central del i hanteringen av personuppgifter, där kommunstyrelsen i egenskap av personuppgiftsansvarig bör se över styrelsens förteckningar och genomföra erforderliga kompletteringar och korrigeringar.

KPMG AB

Viktoria Berstam

Viktoria Berstam

Specialist/Certifierad kommunal revisor

Micaela Hedin

Micaela Hedin

Certifierad kommunal revisor/ Kundansvarig