2024-04-08

Granskningsrapport Tranås kommun

Innehåll

Inledning

För att granska efterlevnaden av dataskyddsförordningens krav har en granskning genomförts, dels genom en kontroll av dokumenterade personuppgiftsbehandlingar i registerförteckningen, dels kontroll av beslutade styrdokument. Dataskyddsombudet kommer även i denna granskning påpeka andra delar av dataskyddsförordningens principer som uppmärksammats under arbetet.

Enligt dataskyddsförordningen och dess kompletterande lagar är nämnderna i kommunen personuppgiftsansvariga. Det är ett ansvar som inte går att delegera till exempelvis andra medarbetare eller chefer. Det praktiska arbetet utförs dock på tjänstemannanivå. Nedan i denna granskningsrapport hänvisas ofta till personuppgiftsansvarig, även om det således är tjänstemän som utfört personuppgiftsbehandlingen.

Av artikel 39.1 b) Dataskyddsförordningen (DSF) framgår att dataskyddsombudet ska ”… *övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och 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.”*

Syfte

Granskningen syftar till att granska den personuppgiftsansvariges övergripande rutiner för efterlevnad av dataskyddsförordningen. Följande avser granskningsrapporten besvara:

- Har nämnden (personuppgiftsansvariga), säkerställt att det finns registerförteckningar över personuppgiftsbehandlingar i enlighet med artikel 30.1, dataskyddsförordningen?
- Anlitas personuppgiftsbiträden och har personuppgiftsansvarig tecknade personuppgiftsbiträdesavtal?
- Vilken information om personuppgiftsbehandlingar har de registrerade fått i e-tjänster?
- Vilka förbättringsområden och utmaningar finns inom dataskyddsarbetet?
- Har styrdokument för dataskydd implementerats?

Metod

Dataskyddsombudet har genomgått relevanta styrdokument samt övergripande granskning och analys av registerförteckningar avseende personuppgiftsbehandlingar som har genomförts.

EU-rättslig lagstiftning

Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande lagstiftning för behandling av personuppgifter. I och med ikraftträdandet av dataskyddsförordningen, (GDPR), upphävdes personuppgiftslagstiftningen, (PuL 1998:204). Den nya lagstiftningen syftar bland annat 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 organisationen som helhet samt personuppgiftsansvariga nämnder och

styrelser. Vid behandling av personuppgifter måste verksamheterna stödja sig på en så kallad ”rättslig grund”. Utan en rättslig grund är personuppgiftsbehandling ej laglig. Personuppgiftsbehandlingar ska ske utifrån dataskyddsförordningens grundläggande principer enligt följande:

• Laglighet

• Korrekthet

• Öppenhet

• Ändamålsbegränsning

• Uppgiftsminimering

• Riktighet

• Lagringsminimering

• Integritet och konfidentialitet

• Ansvarsskyldighet

Registerförteckning

Enligt artikel 30.1 DSF ska varje personuppgiftsansvarig och, i tillämpliga fall, dennes företrädare föra ett register över behandling som utförts under dess ansvar. En kontroll av registerförteckningen har genomförts.

Delar av registerförteckningen anses leva upp till kraven på ansvarsskyldigheten. Dataskyddsombudet anser dock att personuppgiftsansvarig ska granska hela registerförteckningen för att säkerställa att dokumentationen fortfarande är aktuell. Dataskyddsombudet har påpekat länge att en tjänst/system bör användas för att föra register över kommunens processer inom dataskydd. I dagsläget används ett Exceldokument för respektive personuppgiftsansvarig nämnd vilket kan vara sårbart samt är oöverskådligt.

Dataskyddsombudet har granskat den registerförteckning som finns för respektive personuppgiftsansvarig nämnd och har kommit fram till att delar av registerförteckningen lever upp till kraven. De största bristerna kan härledas till att personuppgiftsansvarig registrerat system i stället för processer/personuppgiftsbehandlingar. Som exempel kan nämnas registreringen ”Lönesystem” vilket är en registrering som innehåller många olika processer/personuppgiftsbehandlingar.

I samband med att dataskyddsombudet granskade de personuppgiftsansvarigas registerförteckningar har respektive utsedd ansvarig för sin förvaltning fått dataskyddsombudets rekommendation och kommentarer för sin registerförteckning. Dataskyddsombudets sammanfattande rekommendation gällande registerförteckning listas nedan.

- I samband med att Tranås kommun tar fram nya informationshanteringsplaner bör dessa harmonisera med registerförteckningen. Samma processer som anges i respektive förvaltnings informationshanteringsplan bör ingå i förvaltningens registerförteckning.

- En tjänst eller ett system bör användas för att det ska vara möjligt att föra en registerförteckning på korrekt sätt och underlätta för medarbetare.

Personuppgiftsbiträden

Det framgår av registerförteckningen att Tranås kommun har personuppgiftsbiträden och att det finns tecknade personuppgiftsbiträdesavtal.

Informationsplikt i e-tjänster

Dataskyddsombudet har granskat de e-tjänster som Tranås kommun använder. Det fanns initialt brister i hur kommunen informerade de registrerade om hur deras personuppgifter behandlas. Vissa e-tjänster hade ingen information till de registrerade, en del e-tjänster hade information som var bristfällig. Det fann även e-tjänster som dataskyddsombudet anser lever upp till kravet som informationsplikten ställer upp.

Förbättringsområden och utmaningar

Dataskyddsombudet har under tiden som dataskyddsombud för Tranås kommun identifierat tre förbättringsområden.

Principen om ansvarsskyldighet enligt artikel 5.2, 30 (registerförteckning)

Detta förbättringsområde har redovisats ovan med förslag till åtgärder.

Informationssäkerhetsarbete

I många fall där det finns brister i dataskyddsarbetet går dessa brister att härleda till att det finns brister i det proaktiva informationssäkerhets- och IT-säkerhetsarbetet. Vid lågt ställda krav på leverantörer gällande ett systems skydd av konfidentialitet, riktighet och tillgänglighet finns stora risker att det påverkar dataskyddet. Vid informationsklassning säkerställs att informationen som är tänkt att behandlas får rätt skydd.

Utbildningsinsatser

Den största källan till personuppgiftsincidenter beror på den mänskliga faktorn. Vi kan aldrig eliminera risken för personuppgiftsincidenter men med utbildning av anställda och förtroendevalda kan risken reduceras.

Styrdokument för dataskydd

Tranås kommun har relevanta styrdokument för dataskydd. Dataskyddsombudet har granskat beslutade styrdokument och finner inga brister. Tranås kommun har varit delaktiga till en ny dataskyddspolicy som är ute för antagande i de sex kommuner som delar dataskyddsombud.

Personuppgiftsincidenter under år 2023

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter.

Tranås kommun har under 2023 anmält två personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY). Personuppgiftsincidenterna har inträffat inom socialtjänsten. Följande personuppgiftsincidenter har inträffat:

- Leverantör av trygghetslarm (Careium) hade i mars månad en cyberattack som medförde att personuppgifter kan ha blivit röjda för obehöriga.
- Kvarglömda genomförandeplaner har legat på en bänk på allmän plats vilket medförde att personuppgifter kan ha blivit röjda för obehöriga.

Sammanfattning av dataskyddsombudets rekommendationer

Av granskningen framgår att personuppgiftsansvarig inte uppfyller alla grundläggande krav som dataskyddsförordningen ställer. Nedanstående områden anser dataskyddsombudet att Tranås kommun bör prioritera.

- Principen om ansvarsskyldighet
- Informationssäkerhetsarbete
- Utbildning av anställda

Erik Selander

Dataskyddsombud