Sammanställning Timrå Kommun

Uppföljning av persondataskydd- Checklista 2021

Medelpads Räddningstjänstförbund

Matts Boman Dataskyddsombud

2021-01-13

Innehållsförteckning

Inledning

Timrå kommun har ingått ett avtal med Medelpads Räddningstjänstförbund tillsammans med Sundsvall och Ånge kommun om ett gemensamt dataskyddsombud (DSO) för alla tre kommuner samt för de kommunala bolagen. Syftet med avtalet är att uppnå ett samordnat och systematiskt dataskyddsarbete, samt ökad kvalité och resurseffektivitet. Avtalet tecknades 2017 och ska enligt avtalet utvärderas årsvis.

Enligt GDPR eller Dataskyddsförordningen är varje nämnd och styrelserna var och en personuppgiftsansvarig (PuA) för sina verksamhetsområden. Respektive nämnd och styrelse ansvarar för att kraven som ställs i dataskyddsförordningen (DSF) efterlevs.[1]

I avtalet för samverkan gällande DSO mellan kommunerna står att respektive kommun ska utse en kontaktperson som tillsammans med DSO koordinerar och samordnar kommunens arbete. För Timrå kommun har Helen Peterzon haft denna roll sedan avtalet upprättades.

DSO:s roll är främst att övervaka att PuA följer DSF samt att ge information och råd till PuA i frågor som rör skyddet av personuppgifter. DSO ska inte driva eller utföra det operativa dataskyddsarbetet och inte heller fatta beslut avseende dataskydd. Dataskyddet ska ge råd och stöd samt rekommendationer.

Timrå kommun har i syfte att få en bild över nämndernas arbete kring DSF, skapat en e-tjänst, ”Uppföljning av persondataskydd – Checklista 2021”. Där ansvariga ska svara på frågor inom viktiga delar för att följa den omfattande förordningen.

Denna översiktliga sammanställning delges till samtliga nämnder som skickat in checklistan.

Nämnder och förvaltningar Timrå kommun

Timrå kommun består av fyra förvaltningar och ett kommunledningskontor:

- Kommunledningskontoret
- Barn- och utbildningsförvaltningen
- Kultur- och teknikförvaltningen
- Miljö- och byggförvaltningen
- Socialförvaltningen[2]

Alla ovan har fyllt i och skickat in checklistan. I e-tjänsten står angivet att frågorna kan besvaras för förvaltningen som helhet eller av en verksamhet

[1] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/

[2] https://www.timra.se/kommunpolitik/kommunensorganisation/kommunensbolagochkommunalforbund.4.714dad16d46439ef9441c.html

eller enhet om verksamhet bestämmer sig för det. Två verksamheter har skickat valt detta:

- Verksamhetsstöd och Informationshantering, VU-IT, Kommunledningskontoret
- Näringslivskontoret, Kommunledningskontoret

Checklistan

Genom att använda sig av en e-tjänst har DSO och Helen Peterzon bedömt att det är lättare och smidigare för nämnderna att besvara frågorna. Denna checklista ger kommunen och personuppgiftsansvariga en översiktbild om statusen kring dataskyddsarbetet. För varje område finns frågor samt möjlighet att utveckla sina svar.

Områden som tas upp i checklistan:

- Information och Utbildning
- Behandlingar av personuppgifter
- Organisation och roller (besvaras ej för 2021)
- De registrerades rättigheter
- Personuppgiftsincidenter
- Särskilda integritetsrisker (besvaras ej för 2021)
- Skydd för personuppgifter i IT-system
- Avtal med personuppgiftsbiträden (besvaras ej för 2021)

Att utlämna eller spara områden till senare uppföljning, syftar till att kunna arbeta ordentligt med de områden som bedöms vara prioriterade.

I denna sammanställning kommer svaren att redovisas för varje område och därefter har DSO gjort en bedömning för varje del. Efter följer ett avsnitt om åtgärder som ska starta omgående. Som avslutning, en kort sammanfattning från Dataskyddsombudet.

Frågor, redovisning av svar & bedömning från DSO

1. Information och utbildning

Under denna områdesrubrik ställs en fråga och beroende på svar, ställdes en följdfråga:

- ***Får nyanställda utbildning om behandling av personuppgifter, exempelvis i samband med introduktionen eller på annat sätt?***

Vid svar *Ja*:

- *Hur genomförs utbildningen?*

Första frågan kräver inte så uttömmande svar, dock är det svar som anges viktigt eftersom det är svårt att arbeta med dataskydd och korrekt hantering av personuppgifter om ingen utbildning eller stöd ges eller finns. ***Två verksamheter har angett det inte genomförs någon utbildning på sina respektive förvaltningar.***

Av de som svarat ja, skriver majoriteten av dem att använder sig av Nanoutbildning som erbjuds i utbildningen av nyanställda. En verksamhet svarar att de använder en rutin, en checklista, som används av närmaste chef vid nyanställning.

Två av verksamheter som svarat ja på första frågan, anger att utbildningen och informationen sker muntligt. En av dessa har skrivit att de siktar mot en skriftlig information till nyanställda samt att underteckna att de fått tagit del av den.

Dataskyddsombudets bedömning

Två verksamheter har angett att det inte ges någon information eller utbildning vid anställning. Det bedömer DSO är en stor brist i arbete kring dataskyddet och måste åtgärdas.

Dataskyddsombudet rekommenderar också att den muntliga information, som några nämnder skriver att de erbjuder, kompletteras med Nano-utbildningen. Att använda sig av en checklista som en verksamhet är ett sätt att säkerställa att detta, och andra viktiga delar för introduktion, genomförs.

2. Behandlingar av personuppgifter

Görs en löpande uppdatering av registerförteckningen i er förvaltning/verksamhet?

Denna del handlar om att uppfylla artikel 30 i DSF.[3] Verksamheter som hanterar personuppgifter ska ha ett register med obligatoriskt innehåll. Det är en grundläggande komponent i ett systematisk och strukturerat dataskyddsarbete.

På denna fråga har samtliga svarat ja och att detta görs vid förändringar av befintliga hanteringar av personuppgifter och vid nya som tillkommer. En verksamhet har angivit att de upplever att det sker ostrukturerat och efterlyser en dokumenterad rutin.

[3] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/fora-register-over-behandling/

Dataskyddsombudets bedömning

Personuppgiftsbehandlingar tillkommer och förändras ständigt. Det är därför viktigt att PuA har en systematik för att löpande lägga in nya personuppgiftsbehandlingar i registerförteckningen samt för att se över och uppdatera de personuppgiftsbehandlingar som lagts in i registerförteckningen.

Nämndernas antal registreringar är i sig inte jämförbara med varandra eftersom storlek och typ av verksamhet där mängden personuppgifter varierar har en stor påverkan. Att en nämnd har ett högt antal registreringar behöver inte betyda att registreringarna är fullständiga. Det behöver inte heller betyda att nämnden löpande ser över och uppdaterar befintliga registreringar.

En förvaltning efterlyser dokumenterad rutin, idag finns ingen skriftlig rutin utan mer ett arbetssätt som hittills varit att informationssäkerhetsansvarig varje halvår uppmanat verksamhet att uppdatera sina register.

Dataskyddsarbetet, och informationssäkerhetsarbetet, hamnar ofta på sidan av eller justeras, alternativt åtgärdas, i efterhand. Att detta arbete integreras i processer vid till exempel inköp och upphandlingar skulle enligt DSO lösa många situationer och frågetecken som uppstår idag, antingen i ett sent skede i införandet eller som upptäcks när en behandling har varit aktivt en längre period. DSO menar att det optimala vore om arbete med registerförteckningen var integrerat, inte en separat rutin.

DSO har inte gjort någon djupare analys av registerförteckningen och enskilda behandlingar. En sådan analys kommer att göras vid framtida revisioner.

3. De registrerades rättigheter

Är informationen i e-tjänster och blanketter om behandlingen av personuppgifter uppdaterad och riktig?

Dataskyddsförordningen anger ett antal rättigheter som de registrerade har och som verksamheterna måste ha rutiner för.[4] En stor del av detta är att informera om sin verksamhets personuppgiftshantering.

Alla verksamheter har svarat ja på denna fråga, några utvecklar sina svar och skriver att de gör detta på både i sina e-tjänster samt de blanketter som finns.

En verksamhet anger också att detta arbete kommer att vara i fokus under 2022.

Dataskyddsombudets bedömning

[4] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/de-registrerades-rattigheter/

I en del verksamheter kan personuppgiftshanteringar förändras förhållandevis mycket under ett år, medans andras är mer eller mindre samma eller att de har ett mindre antal. Det kan vara en utmaning att arbeta med att hinna med att uppdatera både digitalt och på skriftliga blanketter p.g.a. de ska anges på flera språk, på ett lättförståeligt sätt.

DSO:s bedömningar är att verksamheterna i Timrå kommun har en hög ambition och nivå i detta arbete.

4. Personsuppgiftsincidenter

Används rutinen för anmälan av personuppgiftsincidenter i er förvaltning/verksamhet?

Alla har svarat ja på denna fråga. Tre av nämnderna har angett de inte haft någon incident.

Möjligheten att utveckla sitt svar fanns för denna fråga:

- ***”Det finns arbetssätt men ingen formell rutin.”***
- ***”Information om hur man gör kommer att finnas med i informationen som delas ut vid nyanställning”***
- ***”Gås igenom vid månadsmöte”***
- ***”Vi kommer att informera om rutinen på en APT.”***

Dataskyddsombudets bedömning

Att en nämnd anmäler personuppgiftsincidenter behöver inte vara en indikation på bristande säkerhet. Tvärtom, kan det tyda på att verksamheten har strukturer och rutiner som ger en god förmåga att upptäcka och rapportera personuppgiftsincidenter. DSO:s bedömning är att det är viktigt att förmedla ut att anmälda personuppgiftsincidenter inte är något negativt utan snarare kan tyda på att verksamheten har en bra rutin för att upptäcka och rapportera personuppgiftsincidenter.

Men precis som i andra kommuner och verksamheter bedömer DSO, tillsammans med informationssäkerhetsansvarig och kontaktpersonerna i verksamheterna, att det sker fler incidenter i kommunen än vad som anmälts hittills.

De kommentarer eller svar som ett antal verksamheter anger, visar på att det behövs ett samlat grepp kring detta område. En verksamhet anger att det inte finns någon rutin, men ett arbetssätt. DSO:S bedömning är att det finns men att det behövs kommuniceras ut tydligare att den finns och var den finns.

DSO rekommenderar också att detta område tas upp oftare eller med ett komplement än t.ex. vid en enstaka arbetsplatsträff, APT.

5. Skydd för personuppgifter i IT-system

Är kartläggning av tredjelandsöverföringar av personuppgifter genomförda i er förvaltning/verksamhet?

Efter EU-domstolens beslut, sommaren 2020, att tredjelandsöverföringar baserade på avtalet mellan EU och USA, Privacy Shield, inte skyddar EU-medborgare från den amerikanska säkerhetskyddlagstiftningen[5], har verksamheterna fått uppmaningar från DSO att genomföra ett antal åtgärder.

Den första av dessa var att kartlägga vilka personuppgiftshanteringar som berörs av denna dom. Det är väldigt stor del av de personuppgiftshanteringar som har någon leverantör som stödjer hantering, exempelvis företag som Amazon, Google och Microsoft.

Här har alla svarat ja och några har angett att det är vid tecknande av s.k. PUB-avtal (personuppgiftsbiträdesavtal) som detta görs och följs upp.

En verksamhet har skrivit de har en del att göra på denna punkt.

Dataskyddsombudets bedömning

DSO har sedan domen arbetat tillsammans med många förvaltningar och mycket av arbetet har varit att försöka styra om befintliga eller nya hanteringar när PUB-avtal ska tecknas eller revideras och där leverantörer använder sig av ovannämnda företag.

Det har varit ett relativt framgångsrikt arbetssätt då majoriteten av leverantörerna har förstått problematiken och gjort ändringar. Arbetssättet har byggt på dialog men kommunerna överlag kan bli bättre på kravställa detta i upphandlingar.

Dock kvarstår problemet med de större verksamhetssystem som används av en kommun t.ex. Microsoft Office 365. Där ser det olika ut i landet men det största hindret är att alternativen förnärvarande är obefintliga.

Åtgärder

Dataskyddsombudet har diskuterat med tre verksamheter och kommit fram till följande åtgärder ska påbörjas omgående, observera att de uppräknade kan komma att justeras och att antalet åtgärder kan förändras:

Informations- och utbildningspaket. Det finns framtagna ”paket” som används en eller flera nämnder i kommunen för introduktion av nyanställda. Genom att använda ett gemensamt paket för hela kommunen, säkerställs att de personer som börjar arbeta i kommunen får en stabil grund. Nano-utbildningen ska också revideras.

[5] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/schrems-ii-domen-overforingar-till-tredje-land/

Information och utbildning gällande personuppgiftsincidenter. Ett gemensamt utskick ska göras för att påminna personalen om:

- Vad en personincident är
- Att dokumentera personuppgiftsincidenter, oavsett allvarlighetsgrad
- Kommunens rutin för personuppgiftsincidenter.

Det viktigaste budskapet i utskicket är det inte är något negativt. Det är oerhört viktigt att personuppgiftsincidenter, dokumenteras.

Sammanfattning

Timrå kommun arbetade precis som många andra organisationer, företag och kommuner, hårt inför införandet av Dataskyddsförordningen. DSO:s intryck av svaren från checklistan, i kombination med det löpande arbete med kommunens verksamheter, är att de anställda som funnits med från denna period och framåt har en god förståelse för arbetet med dataskydd. Detta intryck blir, ibland, tydligt när anställda som inte varit lika involverad eller varit från början, hanterar personuppgifter. Det visar på vikten av att utbildning och information vid nyanställning och kontinuerligt under anställningens gång.

DSO bedömer att den PuA kan bli bättre på att i god tid involvera DSO i alla frågor som rör skyddet av personuppgifter. Medvetenheten om att DSO i god tid ska involveras i alla frågor som rör skyddet av personuppgifter tycks variera i verksamheterna. Detta är ett generellt bekymmer som alla dataskyddsombud ser i alla verksamheter, i alla kommuner, organisationer och företag.