2023-12-14

Personuppgiftsansvarig

Socialnämnden

Granskningsrapport 2023

Dataskyddsombud

Boel Burman

Datum

2023-12-05

Innehåll

Sammanfattning

I dataskyddsombudets kontrollerande arbete ingår att göra årliga granskningar. I 2023 års granskning har dataskyddsombudet granskat de dokumenterade behandlingarna i registerförteckningen (artikel 30), den information som lämnats till de registrerade (artikel 13 och 14) samt processen för upprättande och uppföljning av personuppgiftsbiträdesavtal (artikel 28).

Dataskyddsombudet (DSO) har också följt upp åtgärder och handlingsplaner avseende de två närmast föregående årens granskningar.

Granskningen visar att registerförteckningen har vissa brister, det bedöms inte ske ett kontinuerligt arbete med att uppdatera förteckningen och de flesta personuppgiftsbehandlingar är mycket omfattande vilket påverkar bl.a. rättslig grund och ändamål. Det finns stora brister i informationen till de registrerade det saknas bland annat specifik information om det olika personuppgiftsbehandlingar nämnden utför. Det finns vidare vissa brister i hanteringen av personuppgiftsbiträdesavtal (PUB-avtal) där det är relativt få PUB-avtal tecknande för nämndens räkning och det görs inte någon uppföljning av ingångna PUB-avtal.

1. Inledning

1.1 Allmänt om dataskyddsförordningen, GDPR

Dataskyddsförordningen, GDPR, trädde i kraft inom EU den 25 maj 2018 och är det generella regelverk som reglerar behandlingen av personuppgifter i såväl privat som offentlig sektor. Dataskyddsförordningen är bindande och direkt tillämplig i samtliga EU:s medlemsländer, men tillåter och förutsätter att medlemsstaterna kompletterar förordningen med nationell lagstiftning.

Dataskyddförordningen ska skydda enskildas grundläggande fri- och rättigheter, särskilt rätten till skydd av personuppgifter. Förordningens syfte är också att anpassa regelverket till det digitala samhället samt att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras.

Kraven i förordningen är ur ett internationellt perspektiv högt ställda och de organisationer som inte lever upp till dessa riskerar sanktioner från respektive lands tillsynsmyndighet. Den svenska tillsynsmyndigheten IMY, Integritetsskyddsmyndigheten, har möjlighet att utdöma administrativa sanktionsavgifter för svenska myndigheter och företag.

1.2 Om årlig granskning

Enligt dataskyddsförordningen ska myndigheter samt företag som hanterar stora mängder personuppgifter ha ett utnämnt dataskyddsombud. Dataskyddsombudet, som har en fristående ställning i förhållande till myndigheten eller företaget, ska kontrollera att dataskyddsförordningen följs inom organisationen genom att bland annat genomföra kontroller och informationsinsatser.

Inom ramen för dataskyddsombudets kontrollerande arbete gör dataskyddsombudet en årlig granskning. Inriktningen på granskningen varierar år för år utifrån bland annat organisationens mognad och den risk som kan tänkas förekomma. I årets granskning har dataskyddsombudet granskat tre olika områden. Det som har kontrolleras är de dokumenterade behandlingarna i registerförteckningen och den information som lämnas till de registrerade. Även hanteringen av personuppgiftsbiträdesavtal har granskats.

Dataskyddsombudet har också följt upp handlingsplaner och åtgärder som personuppgiftsansvarig vidtagit enligt tidigare rekommendationer som getts i samband med granskningarna de senaste två åren:

- Personuppgiftsbiträdesavtal och uppföljning av leverantörer (2022)
- Motivering av rättsliga grunder (2022)
- Information till anställda (2021)
- Konsekvensbedömningar avseende dataskydd (2021)

1.3 Avgränsning

Dataskyddsombudet har inte bedömt och värderat dokumenterat innehåll i registerförteckningen, utan enbart huruvida dataskyddsförordningens uppställda innehållskrav finns med. Vidare har granskningen av de s.k. bör-krav som finns med i förteckningen avgränsats till ett antal bör-krav som dataskyddsenheten bedömer som mest centrala för att öka efterlevnaden (behandlingens namn och kategori/process, rättslig grund med motivering, information om personuppgiftsbiträden, information om konsekvensbedömningar, ev. begränsningar av de registrerades rättigheter, informations- och processägare på rollnivå samt senast uppdaterad).

Dataskyddsombudet har vidare begränsat granskningen av PUB-avtal till de nio frågor som ställdes i frågeformuläret till granskningen av resursskäl.

1.4 Metod

Ett antal frågor har skickats ut till den personuppgiftsansvariges dataskyddssamordnare som besvarats skriftligt. Dataskyddsombudet har begärt in registerförteckning, personuppgiftsbiträdesavtal och informationstexter.

1.5 Efterlevnad

Uppfyller dataskyddsförordningens krav

Uppfyller delvis dataskyddsförordningen krav, brister finns

Uppfyller till stora delar inte dataskyddsförordningens krav, stora brister finns

2. Granskning

2.1 Del 1: Registerförteckningen

2.1.1 Utgångspunkt

Enligt artikel 30.1 ska den personuppgiftsansvarige föra ett register över personuppgiftsbehandling som utförs under dess ansvar. Dessa ska kunna tillhandahållas till IMY vid en förfrågan eller tillsyn. Registerförteckningen är en upprättad handling och kan begäras ut såsom en allmän handling. Denna granskningsdel har som syfte att kontrollera dels att registerförteckningen innehåller de uppgifter som artikel 30.1 föreskriver, dels att det är rätt innehåll i registerförteckningen. Granskningen har även som syfte att säkerställa att registerförteckningen kan lämnas ut i ett lämpligt format såsom skulle bli aktuellt vid en tillsyn eller en begäran om allmän handling.

2.1.2 Efterlevnad

Uppfyller delvis dataskyddsförordningen krav, brister finns

Granskningen visade att:

Såsom dataskyddsombudet tolkar det utdrag av registerförteckningen i Excel, som skickats in som svar, så sker inget eller litet regelbundet arbete med socialnämndens registerförteckning. För merparten av behandlingarna verkar senaste uppdateringen vara gjorda 2021.En registerförteckning är ett levande dokument som, enligt artikel 35 i dataskyddsförordningen, ska uppdateras regelbundet (se rekommendationen nedan). Vidare är varje personuppgiftsbehandling, så som det bedöms, så pass omfattande att det i många fall egentligen rör sig om flera personuppgiftsbehandlingar vilket påverkar flera andra krav som ställs på en registerförteckning (se nedan).

Kommentarer till registerförteckningen avseende kraven i artikel 30.1:

- Det framgår av registerförteckningen vilken nämnd som är personuppgiftsansvarig, men kontaktuppgifter till PUA saknas, i vart fall i

utdraget till Excel vilket är det som troligen kommer att lämnas ut om en begäran sker. Den som står som ansvarig har, om dataskyddsombudet förstått det rätt, slutat. Det finns kontaktuppgifter till DSO men uppgifterna behöver uppdateras med nya dataskyddsombudet (artikel 30 1a).

- Ändamål finns angivet för de personuppgiftsbehandlingar som finns upptagna i förteckningen. Eftersom många av behandlingarna är omfattande i sitt innehåll som tex ”Förebyggande insatser för barn, unga och familj” eller ”Insatser för personer i behov av boende” blir också ändamålen omfattande. Detta påverkar också de rättsliga grunderna, se nedan (artikel 30 1b).
- Kategorier av registrerade och personuppgifter finns redovisat i förteckningen och dessutom finns viss information om känsliga och extra skyddsvärda personuppgifter. Någon granskning av om dessa stämmer har inte gjorts (artikel 30. 1c).
- Uppgifter om mottagare finns angivet för alla personuppgiftsbehandlingar i förteckningen, det finns även angivet syfte med utlämnandet och i vilken form det lämnas ut. Någon granskning av om informationen stämmer har inte gjorts (artikel 30 1d).
- Det finns information om överföring till tredjeland för nästan alla redovisade personuppgiftsbehandlingar. För merparten av behandlingarna sker överföringar till tredjeland (USA) då Microsoft Office 365 används för någon del av behandlingen. Som det förstås är beslutet om att använda Office 365 fattat före Schrems II då Privacy Shield ansågs ge tillräckligt gott skydd (artikel 30 1e).
- Det finns för samtliga i förteckningen redovisade behandlingar information om gallring/radering så till vida att man hänvisar till dokumenthanteringsplanen. Samtidigt svarar man ”vet ej” på frågan om det finns skriftliga gallringsrutiner vilket är lite motsägande då dokumenthanteringsplanen i vart fall är/bör vara styrdokumentet för skriftliga gallringsrutiner. I kommentarkolumnen till radering framgår att arkivansvarig ska under 2021 ska skapa en rutin för arkivering i ledningssystemet och det är gjort framgår inte (artikel 30 1f).
- Det finns (samma) information om framför allt organisatoriska skyddsåtgärder och i något fall om tekniska skyddsåtgärder. Vanligen anges samma organisatoriska skyddsåtgärder för alla personuppgiftsbehandlingar (artikel 30 1g).

Det finns ett antal bör-krav som är rekommenderade att ha med i registerförteckningen för att ha en högre efterlevnad. Dataskyddenheten har valt att fokusera på ett antal som nämns ovan. Som personuppgiftsansvarig kan man självklart välja att ha med fler bör-krav men fokus ligger på de som angivits ovan.

- Namn på de olika personuppgiftsbehandlingarna finns men de utgår inte ifrån processer eller är kopplade till processer vilket skulle underlätta förståelsen. Det är också omfattande innehåll i respektive behandling vilket påverkar såväl ändamål som rättslig grund (se nedan).
- Rättslig grund finns angivet för samtliga behandlingar men motivering saknas för nästan alla. För merparten av behandlingarna finns mer än en rättslig grund angiven vilket sannolikt beror på att varje behandling är omfattande (se även ovan).
- För nästan alla behandlingar finns det svar om det finns personuppgiftsbiträde eller ej, det saknas information i några fall om vem som är personuppgiftsbiträde och om det finns ett PUB-avtal (för något fler). Eftersom varje behandling vanligen är omfattande så finns det rimligen mer än ett personuppgiftsbiträde.
- Det är otydligt om och i så fall vilka konsekvensbedömningar och informationsklassningar som eventuellt gjorts. Det kan dels bero på att det är länge sedan registerförteckningen (i sin helhet) uppdaterades, på att varje behandling i förteckningen är omfattande eller att den informationen finns någon annanstans.
- Det saknas helt information om eventuella begränsningar i de registrerade rättigheter. Det finns möjlighet att lägga in den informationen i Draftit.
- Det finns information om kontaktperson på enhetsnivå men inte informations- och processägare. Den som står som ansvarig är troligen tidigare dataskyddssamordnare.
- Senaste uppdaterat finns det information om och för alla behandlingar utom ett fåtal så har ingen uppdatering gjort sedan 2021, dvs för två år sedan.

Dataskyddsombudet rekommenderar den personuppgiftsansvarige socialnämnden att:

- Registerförteckningen består i sin helhet av 28 personuppgiftsbehandlingar vilket framstår som (för) få för en så pass omfattande verksamhet. Ett skäl är att de behandlingar som finns i förteckningen är för omfattande. Detta behöver ses över och befintliga behandlingar delas upp. Därtill saknas det förmodligen också en del personuppgiftsbehandlingar som ingår i verksamheten. Det är en fördel att utgå ifrån verksamhetens processer i registerförteckningen.
- Att utifrån kommentarerna ovan justera och komplettera med information som att uppdatera med ny DSO, information om gallring, PUB-avtal, kategorier av personuppgifter m.m.
- Se över ändamål och också rättslig grund utifrån resonemanget ovan om att många av behandlingarna är (för) omfattande.
- Se över och bestämma om de bör-krav som dataskyddsombudet lyfter och som finns med i Draftit ska finnas med i registerförteckningen. Och om så är fallet komplettera med den informationen, tex. om konsekvensbedömningar och informations- och processägare.
- Att ta fram och besluta om en skriftlig rutin och/eller årshjul för att hålla registerförteckningen uppdaterade åtminstone årligen om inte en sådan redan finns samt tillsätta resurser för detta. Och att det av samma rutin framgår att förteckningen ska uppdateras så snart en ny behandling tillkommer eller en befintlig ändras.

2.2 Del 2: Information till de registrerade

2.2.1 Utgångspunkt

Den registrerade har rätt till insyn gällande personuppgiftsansvarigas behandling av dennes personuppgifter, vilket framgår av artikel 5.1 a dataskyddsförordningen, gällande principen om öppenhet. Artiklarna 13 och 14 i dataskyddsförordningen redogör vilken information som ska lämnas till den registrerade vid behandling. Ytterligare ett krav är att informationen ska lämnas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn, enligt artikel 12 dataskyddsförordningen. Vid bedömning av om informationen som lämnas till den registrerade lever upp till kraven i artikel 12 dataskyddsförordningen kan den europeiska dataskyddsstyrelsens ”Riktlinjer om öppenhet enligt förordning (EU) 2016/679” användas för tolkning. Syftet med granskningen är att kontrollera att artiklarna 13–14 efterlevs.

2.2.2 Efterlevnad

Uppfyller till stora delar inte dataskyddsförordningens krav, stora brister finns

Granskningen visade att socialnämnden har en generell information om nämndens personuppgiftsbehandling på Gävle kommuns hemsida. Till skillnad från arbetsmarknads- och funktionsrättsnämnden finns inte någon specifik information utifrån de olika personuppgiftsbehandlingar som görs av nämnden. Den generella informationen ger viss information men inte på den nivå som och utifrån de krav som ställs i dataskyddsförordningen. Eftersom informationen är generell blir det inte tillräckligt tydligt för den registrerade varifrån uppgifterna hämtas (om det inte är från den registrerade själv), vad som är ändamål, rättslig grund, hur länge de specifika personuppgifterna sparar, vem de lämnas ut till och inte minst vilka personuppgifter som behandlas. Enligt rekommendationer från artikel 29-gruppen så ska man undvika att använda ord som ”svävande” tex. kan, får, ofta och eventuellt, det skapar en osäkerhet om vad som gäller. De registrerades rättigheter framgår genom att länka till kommunens generella information om detta.

Några stickprovskontroller på de blanketter som används för ansökan av olika tjänster som socialnämnden ansvarar för visar att det finns en kort informationstext om dataskyddsförordningen och att det länkas vidare till informationen på hemsidan. Dock står det ”Gävle kommun” på flera blanketter och inte socialnämnden vilket gör det otydligt vem som är personuppgiftsansvarig. I andra fall står det en enhet inom socialnämnden vilket också gör det otydligt ur ett dataskyddsperspektiv Länken pekar också mot den generella informationen för hela kommunen. Om det ges någon information för respektive e-tjänst efter att man loggat in har inte kunnat granskas.

Informationen ska vidare vara lättillgänglig enligt dataskyddsförordningen, dvs den registrerade ska inte behöva leta efter den. Det finns inte någon information på hemsidan (eller länk till sidan om dataskydd) under fliken ”Omsorg och stöd” där socialnämndens olika verksamheter och därmed olika personuppgiftsbehandlingar beskrivs. Det blir, som dataskyddsombudet bedömer det, ett rätt stort glapp mellan den generella informationen och den något mer specifika som finns på blanketter och e-tjänster.

Dataskyddsombudet rekommenderar den personuppgiftsansvarige socialnämnden att:

- I likhet med arbetsmarknads- och funktionsrättsnämnden ta fram specifik information för de olika personuppgiftsbehandlingar nämnden utför. Där det framgår ändamål, rättslig grund, hur länge personuppgifterna sparas, vem som kommer ta del av uppgifterna, ev. tredjelandsöverföring och annat som är unikt för den specifika behandlingen. Uppgifter om registrerades rättigheter, kontaktuppgifter m.m. framgår av den generella informationen.
- Att förtydliga på ansökningsblanketter och likande vilken nämnd som är personuppgiftsansvarig.
- Att om möjligt ha information eller länka till sidan om dataskydd (med tillagd specificerad information om det olika personuppgiftsbehandlingarna) på den flik som heter Omsorg och stöd för att göra det enkelt för de registrerade att hitta informationen.

Ett exempel på hur man kan lägga upp informationen på kommunens hemsida är IMY:s egen information: Behandling av personuppgifter | IMY

2.3 Del 3: Personuppgiftsbiträdesavtal

2.3.1 Utgångspunkt

Ett så kallat personuppgiftsbiträdesavtal, ”PUB-avtal”, är ett avtal som den personuppgiftsansvarige, dvs respektive nämnd, kommunalt bolag och kommunalförbund, enligt GDPR artikel 28 måste upprätta med samtliga personuppgiftsbiträden. Avtalen, som inte får vara muntligt, reglerar hur biträdet får behandla personuppgifterna och vilka extra skyddsåtgärder som behöver vidtas. Avtalet reglerar även om personuppgifter får överföras till tredjeland. Syftet med granskningen är att kontrollera att artikel 28 efterlevs.

2.3.2 Efterlevnad

Uppfyller delvis dataskyddsförordningen krav, brister finns

I granskningsunderlaget ställdes nio frågor rörande tecknande av personuppgiftsbiträdesavtal och uppföljningen av dessa. Samt att en förteckning över samtliga PUB-avtal efterfrågades.

Granskningen visade att

- Sektor Välfärd och därmed socialnämnden har i augusti-september 2023 tagit fram en rutin för upprättande och uppsägning av PUB-avtal, den ska, som det förstås av svaret, publiceras i ledningssystemet när den är granskad och godkänd. Innehållet i rutinen har inte vid detta tillfälle granskats av dataskyddsombudet däremot har synpunkter lämnats tidigare.
- Av den inskickade förteckningen av PUB-avtal framgår att det finns fem PUB-avtal diarieförda för socialnämnden. Att det är så pass få PUB-avtal gör att dataskyddsombudet bedömer att det inte tecknats PUB-avtal för alla personuppgiftsbehandlingar som utförs av annan för nämndens räkning. Det skulle kunna bero på att avtalen förvaras på annat ställe och/eller att det saknas PUB-avtal för de leverantörer som behandlar personuppgifter för nämndens räkning.

- Det saknas rutiner för uppföljning av nämndens PUB-avtal. Att följa upp ingångna avtal är ett krav i dataskyddsförordningen, artikel 28.
- När det gäller frågan om samtliga personuppgifter som skickas till tredje land har en giltig överföringsmekanism som finns dokumenterat i PUB-avtal så lyfts frågan som gäller för hela Gävle kommun rörande bl.a. Microsoft 365 tjänster.

Dataskyddsombudet rekommenderar den personuppgiftsansvarige arbetsmarknads- och funktionsrättsnämnden att:

- Se över om det tecknats PUB-avtal med samtliga leverantörer som behandlar personuppgifter för nämndens räkning samt hålla dem ordnade enligt informationshanteringsplanen så att det uppfyller kraven vid ett utlämnande av allmän handling.
- Ta fram och implementera en rutin för granskning/uppföljning av ingångna PUB-avtal.
- Problematiken med tredjelandsöverföringar är gemensam för hela kommunen men varje nämnd behöver ta ställning till hur man bedömer nuvarande läge utifrån den nya överenskommelsen mellan EU/EES och USA.

2.4 Uppföljning av föregående års granskningar

Dataskyddsombudet har vid tidigare års granskningar funnit brister i funnit brister i vissa områden i dataskyddarbetet hos arbetsmarknads- och funktionsrättsnämnden.

2021 granskades Personuppgiftsansvarigas information om personuppgiftsbehandlingar till anställda samt konsekvensbedömningar.

När det gäller information till anställda så har tidigare DSO rekommenderat att hela sektor Välfärd ska komplettera information om personuppgiftsbehandling vid personaladministration till anställda; genomföra översyn över hur anställda informeras om personuppgiftsbehandlingen i passagesystem; fastställa rutin över hur anställda får använda sig av arbetsgivarens datorer och e-post samt informera anställda om rutin samt komplettera rutin för loggkontroll med att klargöra hur information lämnas till användare. Av svaret från dataskyddssamordnaren framgår att ingen överlämning gjorts från föregående DSS och det är därför oklart om rekommendationerna följts. Rekommendationen kvarstår därför.

Rekommendationen när det gäller konsekvensbedömningar var att dels att komplettera registerförteckningen med information om dessa genomförts dels att genomföra konsekvensbedömningar i de fall en personuppgiftsbehandling uppfyller kraven för det. Rekommendationen kvarstår framför allt när det gäller registerförteckningen. När det gäller genomförande av konsekvensbedömningar är dataskyddsombudets bild att de genomförts i rätt stor utsträckning men att det återstår arbete för flertalet behandlingar.

2022 granskades personuppgiftsansvariges uppföljning av personuppgiftsbiträden samt rättslig grund med motivering. När det gäller rutin för tecknande och uppsägning av PUB-avtal har ett förslag på rutin tagit fram och ska inom kort beslutas så den delen av föregående års rekommendation är färdig. I övrigt kvarstår föregående års rekommendationer (se även ovan om PUB-avtal).

3. Slutsats

Dataskyddsombudet har i sin årliga granskning funnit brister i kommunstyrelsens dataskyddsarbete. Arbetet med dataskydd, är precis som annat kvalitetsarbete, en pågående process med som aldrig blir helt färdigt. Samhällsutvecklingen som går i allt snabbare takt och de förändringar som sker i omvärlden i stort ställer både större och nya krav på dataskyddsarbetet. Dataskyddsombudet rekommenderar därför den personuppgiftsansvarige att fortsätta arbeta aktivt med frågor kopplade till dataskydd för att hantera de brister som konstaterats samt skapa en god dataskyddskultur.