Gävle KOMMUN

2022-04-26 Kommunstyrelsen i Gävle kommun

Granskning av kommunstyrelsens dataskyddsarbete 2022

Sammanfattning

Dataskyddsombudet har vid den årliga dataskyddsgranskningen funnit brister i den personuppgiftsansvariges hantering av personuppgiftsbiträdesavtal och processen kopplat till detta arbete samt även funnit brister i användandet av rättslig grund för behandling av personuppgifter. Dataskyddsombudet har även följt upp föregående års granskningar och funnit vissa brister i dessa delar.

Allmänt om GDPR

Dataskyddsförordningen, GDPR, trädde i kraft den 25 maj 2018 inom EU och reglerar myndigheter och företags behandling av personuppgifter i syfte att tillvarata enskilda personers rättigheter och friheter vid behandling av deras personuppgifter. Dataskyddsförordningen ställer bland annat krav på rättslig grund för all sorts behandling av personuppgifter samt innehåller ett antal principer som behöver uppfyllas för att en behandling ska vara förenlig med dataskyddsförordningen (bl.a. principen om uppgiftsminimering, principen om lagringsminimering samt principen om ändamålsbegränsning). Kraven är sett 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, tidigare Datainspektionen) har för myndigheter möjlighet att utdöma administrativa sanktionsavgifter på 10 miljoner kronor samt för företag 20 miljoner euro.

Om årlig granskning

Enligt dataskyddsförordningen ska samtliga 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 enligt dataskyddsförordningen bland annat ge stöd och råd i verksamhetens arbete med dataskydd samt granska organisationens arbete med dataskyddsfrågor.

Inom ramen för dataskyddsombudets granskade 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 två olika områden: 1. personuppgiftsbiträdesavtal med tillhörande uppföljningsprocess samt 2. rättslig grund för behandling av personuppgifter. Dataskyddsombudet har även följt upp föregående två års granskningar.

Metod

Ett antal frågor har skickats ut till den personuppgiftsansvariges dataskyddssamordnare som besvarat skriftligt. Dataskyddsombudet har begärt in personuppgiftsbiträdesavtal och granskat ett urval av dessa samt haft ett muntligt möte med dataskyddssamordnaren där kompletterande frågor ställts.

Personuppgiftsbiträdesavtal

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 som behandlar den personuppgiftsansvariges personuppgifter. Ett personuppgiftsbiträde kan vara exempelvis en extern leverantör av IT-tjänster. Personuppgiftsbiträdesavtalen, som inte får vara muntligt, reglerar hur personuppgiftsbiträdet får behandla personuppgifterna och vilka extra skyddsåtgärder som behöver vidtas. Personuppgiftsbiträdesavtalet reglerar även om personuppgifter får överföras till tredjeland.

Personuppgiftsansvarig har efter upphandling av tjänst och tecknande av personuppgiftsbiträdesavtal fortfarande ansvar för att personuppgifter behandlas i enlighet med dataskyddsförordningen. Möjligheten för personuppgiftsansvarig att säkerställa revision av biträdet ska framgå i PUB-avtal utifrån artikel 28.3 h. Den kontroll som personuppgiftsansvarig äger rätt att genomföra kan ske genom att biträdet genomför egenkontroll eller att personuppgiftsansvarig genomför revision.

Dataskyddsombudet rekommenderar att använda de mallar som Sveriges kommuner och regioner, SKR, tillhandahåller vid upprättande av personuppgiftsbiträdesavtal.

Rättslig grund

All behandling av personuppgifter behöver ha stöd i en rättslig grund för att vara laglig, utan rättslig grund är en behandling otillåten. En av dessa rättsliga grunder är att behandlingen är av allmänt intresse. En annan rättslig grund är rättslig förpliktelse vilket innebär att den personuppgiftsansvarige enligt lag eller annan rättsakt är skyldig att vidta en åtgärd som kräver att personuppgifter behandlas.

Vilken grad av tydlighet och precision som krävs i fråga om den rättsliga grunden för att en viss behandling av personuppgifter ska anses vara nödvändig måste bedömas från fall till fall, utifrån behandlingens och verksamhetens karaktär. En personuppgiftsbehandling som inte utgör någon egentlig kränkning av den personliga integriteten, såsom när det gäller behandling av elevers namn i reguljär skolverksamhet, kan ske med stöd av en rättslig grund som är allmänt hållen. Ett mer kännbart intrång, t.ex. behandling av känsliga personuppgifter inom hälso- och sjukvården, kräver att den rättsliga grunden är mer preciserad och därmed gör intrånget förutsebart.

Granskning av personuppgiftsbiträdesavtal och tillhörande uppföljningsprocess

Dataskyddsombudet har vid granskningen av den personuppgiftsansvariges personuppgiftsbiträdesavtal funnit mindre brister. Bristerna bestod av bland annat användandet av personuppgiftsbiträden vars underbiträden kan innebära en risk ur ett

tredjelandsperspektiv samt att bilaga med instruktioner för personuppgiftsbiträdets behandling av personuppgifter delvis varit bristfällig.

Större brister har konstaterats i den personuppgiftsansvariges process avseende hur personuppgiftsbiträdesavtal ska hanteras då någon sådan process inte finns i dagsläget. Den personuppgiftsansvarige har även angivit att någon granskning av personuppgiftsbiträden inte utförts.

Dataskyddsombudet rekommenderar den personuppgiftsansvarige att ta fram ett dokument som reglerar hanteringen av personuppgiftsbiträdesavtal samt att den personuppgiftsansvarige överväger möjligheterna och behovet av att granska personuppgiftsbiträden.

Granskning av rättslig grund för behandling av personuppgifter

Dataskyddsombudet har vid granskning av den personuppgiftsansvariges rättslig grund för behandling av personuppgifter funnit brister i några av de behandlingar som dataskyddsombudet granskat. Bland annat har brist funnits i hanterandet av samtycke och för några av behandlingarnas rättsliga grund är det tveksamt om denna håller vid en eventuell prövning av en tillsynsmyndighet.

Dataskyddsombudet rekommenderar den personuppgiftsansvarige att säkerställa att den rättsliga grund som används vid behandling av personuppgifter är korrekt och att behandlingen ryms inom den rättsliga grunden. De eventuella behandlingar som saknar giltig rättslig grund är inte tillåtna och behöver avslutas.

Uppföljning av föregående års granskningar

Dataskyddsombudet har vid tidigare års granskningar funnit brister i bland annat hanteringen av personuppgiftsincidenter, brister i antalet genomförda konsekvensbedömningar samt brister i information till medarbetare.

Den personuppgiftsansvarige har efter tidigare års granskning arbetat med en ny rutin för hanterandet av personuppgifter samt diskuterar numera regelbundet (en gång i månaden) på dataskyddssamordnarmöten de personuppgiftsincidenter som uppstått. Den personuppgiftsansvarige deltar även i ett gemensamt arbete med Gävle kommuns övriga nämnder med att ta fram ett webbformulär för rapportering av personuppgiftsincidenter.

Den personuppgiftsansvarige har efter tidigare granskning utfört flertalet konsekvensbedömningar. I den personuppgiftsansvariges register över behandlingar av personuppgifter (artikel 30 register) så har det lagts till de kriterier över när en konsekvensbedömning behöver göras. Ett årshjul har även tagits fram där en del i årshjulet är att avgöra vilka behandlingar som det behöver genomföras konsekvensbedömning för.

Inget arbete har skett med information till medarbetare sedan tidigare granskning.

Dataskyddsombudet bedömer att den personuppgiftsansvarige utfört förbättringar på tidigare års granskade områden, vissa brister kvarstår dock fortfarande.

Slutsats

Arbetet med dataskydd är, precis som med övrigt kvalitetsarbete, en löpande process som ständigt pågår och som aldrig är något som blir färdig. Samhället fortsätter utvecklas, särskilt på IT-området, vilket ställer nya krav när det kommer till personuppgiftsbehandling. Trots att många förbättringar gjorts under de ca fyra åren som GDPR varit gällande har det i samband med årets granskning även framkommit brister som fortfarande kvarstår. Dataskyddsombudet rekommenderar därför den personuppgiftsansvarige att fortsätta arbeta med frågor kopplade till dataskydd för att hantera de brister som konstaterats och för att fortsätta arbeta för att skapa en god dataskyddskultur.

I tjänsten,

Gustav Öst
Dataskyddsombud
Gävle kommuns dataskyddsenhet