# Årsrapport

## Grefab

2020-12-18

dso@intraservice.goteborg.se
031-365 00 00 (kontaktcenter)

### Versionshantering

| Datum | Version | Beskrivning | Ändrat av |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# Innehåll

# 1 Inledning

## 1.1 Bakgrund

Det är över två år sedan dataskyddsförordningen infördes och även om flera av kraven i förordningen har funnits sedan 1998 då Personuppgiftslagen (PuL) trädde i kraft, så ställs det nu högre krav på att personuppgifterna hanteras på ett korrekt, säkert och transparent sätt. Tillsynsmyndigheten har nu också, till skillnad från PuL-tiden, möjlighet att tilldela verksamheter som inte följer förordningen sanktionsavgifter. I Göteborgs Stad är varje enskild nämnd eller bolagsstyrelse personuppgiftsansvarig och ansvarar därigenom för att dess personuppgiftsbehandlingar utförs i enlighet med dataskyddsförordningens bestämmelser.

I samband med att förordningen trädde i kraft 2018 tilldelades varje verksamhet i Staden ett dataskyddsombud. Stadens dataskyddsombud har till uppgift att övervaka efterlevnaden av dataskyddsförordningen hos samtliga personuppgiftsansvariga förvaltningar och bolag.

Som en del i arbetet med att informera personuppgiftsansvariga sammanställer dataskyddsombudet årligen en rapport där dataskyddsarbetet sammanfattas. Årsrapporten syftar till att ge personuppgiftsansvariga en överblick över verksamhetens personuppgiftshantering.

## 1.2 Granskningsperiod

Årsrapporten avser tidsperioden från januari 2020 till december 2020.

## 1.3 Dataskyddsombudets roll

Dataskyddsombudets roll är att övervaka personuppgiftsansvariges efterlevnad av dataskyddsförordningen. Det innebär bland annat att dataskyddsombudet ska granska hur personuppgiftsansvarige behandlar personuppgifter, kontrollerar att bestämmelser och interna styrdokument följs, informerar och ger råd till organisationen. Utöver det ska dataskyddsombudet även ge råd om konsekvensbedömningar, vara kontaktperson för Datainspektionen, registrerade och dataskyddskontakterna samt samarbeta med Datainspektionen vid till exempelvis inspektioner. Dataskyddsombudet är oberoende gentemot personuppgiftsansvarige och får inte instrueras hur jobbet som dataskyddsombud ska utföras. Dataskyddsombudets roll och uppgifter är reglerade i artiklarna 37, 38 och 39 i Dataskyddsförordningen.

# 2 Efterlevnad

## 2.1 Information och rådgivning

Dataskyddsombudets ska ge råd till den personuppgiftsansvarige. Råd kan antingen ges efter att dataskyddskontakten eller andra inom verksamheten ställt en fråga, när dataskyddsombudet deltar vid konsekvensbedömning eller vid avstämningsmöten. Under året har dataskyddsombudet mottagit olika frågor ifrån verksamheten utifrån dess personuppgiftsbehandlingar. Frågorna har bland annat handlat om att lämna ut personuppgifter till en tredje part och personuppgiftsbiträdesrelationer. Dataskyddsombudet har fått i uppdrag att genomföra en utbildning inom dataskydd för anställda under januari 2021. Därtill har även nyhetsbrev skickats ut innehållande omvärldsbevakning och information gällande specifika frågor/ämnen.

## 2.2 Granskning och kontroll

Dataskyddsombudets ska övervaka personuppgiftsansvariges efterlevnad av dataskyddsförordningen. Övervakning kan ske på olika sätt, antingen genom mer formella granskningar där rapporter skrivs och skickas till verksamheten och presenteras för högsta förvaltningsledningen, eller genom att dataskyddsombudet kontrollerar olika handlingar eller rutiner och återkopplar direkt till dataskyddskontakten för eventuella åtgärder.

Kontroller har gjorts av den information som skickats till dataskyddsombudet ifrån dataskyddskontakten eller funnits tillgänglig för läsning någon annan stans. Även rutiner, mallar och andra tillhörande dokument har granskats.

### 2.2.1 Granskningsområden

De områden som har granskats under perioden är kvalitetskontroll av befintliga personuppgifter, kunskapsnivån hos medarbetarna samt rutiner för notifiering av personuppgiftsincidenter.

#### 2.2.1.1 Kvalitetskontroll av befintliga personuppgifter

Dataskyddsombudet har utfört en granskning av verksamhetens registrerade personuppgiftsbehandlingar i personuppgiftsregistret. Fokus har varit på de behandlingar som har samtycke som rättslig grund. Granskningen handlar om huruvida samtycke är rätt rättsliga grund för den aktuella behandlingen. Eftersom verksamheten inte har några behandlingar registrerade i personuppgiftsregistret kunde dataskyddsombudet inte göra några bedömningar av behandlingarna. Istället kommer dataskyddsombudet gå igenom registret tillsammans med verksamheten under det kommande året för att säkerställa att de används som det ska. Under 2021 kommer dataskyddsombudet också fortsätta att fokusera på samtycke som rättslig grund och diskutera detta med verksamheten.

#### 2.2.1.2 Rutiner för notifiering av personuppgiftsincidenter

Dataskyddsombudet har utfört en skrivbordstillsyn av verksamhetens hantering av personuppgiftsincidenter. Granskning har gjorts på rutiner och tillhörande dokument. En rapport har skrivits och tillsänts verksamhetens dataskyddskontakter. Dataskyddsombudet lämnade följande rekommendationer:

Rutinerna behöver kompletteras ytterligare med information om dataskyddsombudets roll vid en inträffad incident. Dataskyddsombudet har en rådgivande funktion och ska meddelas direkt när en personuppgiftsincident inträffat. Dataskyddsombudet kan vara behjälplig och ge råd angående riskbedömningar, men ansvar för beslut ligger hos den personuppgiftsansvarige.

För att bolaget ska kunna identifiera och hantera personuppgiftsincidenter på rätt sätt krävs att personalen har tillräcklig kompetens. Därför är utbildningsinsatser inom det angivna området direkt avgörande. Bolaget behöver även säkerställa att personuppgiftsincidentsrutinen kommuniceras till de anställda samt att rutinen är lättillgänglig.

Vidare behöver rutinerna förtydligas kring hur riskbedömningarna ska genomföras med hänsyn till personuppgiftsansvariges ansvarsskyldighet som även innefattar rapporteringsskyldigheten och informationsplikten. Det finns också behov av att se över dokumentationsskyldigheten så att den överensstämmer med vad dataskyddsförordningen kräver av en personuppgiftsansvarigs verksamhet.

Genom ett aktivt arbete med rutinen som kommuniceras ut till medarbetarna integreras det i det dagliga arbetet, vilket är det bästa sättet för att undvika missade och felaktigt hanterade incidenter.

#### 2.2.1.3 Kunskapsnivån hos medarbetarna

En granskning av kunskapsnivån hos medarbetarna har gjorts där syftet med granskningen av verksamhetens kunskaper om dataskyddslagstiftningen och frågor kring utbildning är att undersöka vilken nivå av kunskap verksamheten har och identifiera eventuellt behov av ytterligare utbildningsinsatser. Dataskyddsombudets sammanfattning av granskningen är:

Samtliga har angett att de får/har fått utbildning från bolaget. Det ska dock poängteras att den utbildning som enligt dataskyddskontakten har förmedlats är i samband med ikraftträdandet av dataskyddsförordningen 2018. Rättsområdet är mycket föränderligt och utvecklas hela tiden, nästan i takt med varje behandling varför kontinuerlig utbildning, så som cheferna anser sig få, är något som borde utsträckas till samtliga anställda. Resultatet på många av kunskapsfrågorna visar också att kunskapsnivån hos de anställda inom dataskydd bör förbättras. Därmed kan det konstateras att fler utbildningsinsatser behövs göras och att det är viktigt att bolaget även följer upp utbildningsinsatserna för att säkerställa kunskapsnivån hos sina anställda. I synnerhet är det viktigt att säkerställa att de anställda som behandlar personuppgifter som klassificeras som känsliga personuppgifter, och som därmed endast i undantagsfall får behandlas och i sådana fall med tillräcklig

säkerhet, vet vilka som är känsliga personuppgifter. Bolaget bör därför ta fram en konkret plan för utbildningsinsatser, identifiera vilka yrkesgrupper där utbildning bör prioriteras och kartlägga om de behöver olika kunskap. Bolaget behöver även skapa en rutin för att informera/utbilda nyanställa och synliggöra de rutiner som finns idag. Därtill bör organisationen utbilda och öva på personuppgiftsincident. Särskilt bör organisationen fokusera på att ge sina anställda tillräckligt med kunskap om rutinerna så att de vet hur man ska gå tillväga vid en personuppgiftsincident. Detta för att säkerställa att incidenterna identifieras snabbt så att de kan hanteras på ett effektivt sätt för att visa att organisationen efterlever sin ansvarsskyldighet enligt förordningen och minimera riskerna för eventuella beslut om sanktionsavgifter.

Dataskyddsombudet har vidare bokat in utbildningstillfälle med personalen under januari månad 2021.

## 2.3 Sammantagen bedömning

Verksamheten har fått information och råd av dataskyddsombudet löpande under året. Granskningsarbetet har skett utifrån ett antal punkter och utbildning har givits av dataskyddsombudet. Medvetenheten hos medarbetarna är god och bör fortsättningsvis hållas ständigt uppdaterad. Kommande granskningsperiod utgår ifrån en kontrollplan där kontroller och granskningar är återkommande.

# 3 Framåt

Dataskyddsombudet kommer fortlöpande bistå verksamheten med information och råd, även om det är verksamheten som är ytterst ansvarig för att hålla sig informerade inom dataskyddsfrågorna. Med hjälp av löpande avstämningsmöten med dataskyddsombudet kan viktiga dataskyddsfrågor lyftas och hanteras innan de blir ett problem.

Att fortsätta utbilda personalen är viktigt, då den mänskliga faktorn är den största orsaken till att en organisation behandlar personuppgifter på ett felaktigt sätt. Genom regelbunden utbildning och uppföljning av medarbetarnas kunskap minskar verksamheten riskerna för att personuppgifter behandlas felaktigt.

Under kommande år kommer dataskyddsarbetet utgå ifrån en kontrollplan, som kommer tillsändas verksamheten i början på 2021. Fördjupande granskningar kommer att utföras likväl som mindre kontrollpunkter som kommer ske löpande. Mer information kommer att lämnas till verksamheten när kontrollplanen är fastställd.