Göteborgs Spårvägar AB, GS Buss AB och GS Trafikantservice AB

- Granskningsrapport av utbildningsinsatser och kunskapsnivå inom dataskyddslagstiftningen

2020-03-30

Mars 2020

Göteborgs Spårvägar AB, GS Buss AB och GS Trafikantservice AB – granskning av utbildningsinsatser och kunskapsnivå inom dataskyddslagstiftningen

Dataskyddsombud Johanna Brunzell Begby

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2020-03-13	0.9	Remiss till dataskyddskontakt	Johanna Brunzell Begby
2020-03-30	1.0	Slutversion	Johanna Brunzell Begby

Innehåll

1 Inledning

1.1 Bakgrund

Dataskyddsförordningen ställer höga krav på organisationers behandling av enskildas personuppgifter. Enligt artikel 5.2 dataskyddsförordningen är det den personuppgiftsansvarige som ansvarar för att organisationen följer dataskyddsförordningen. Utöver att insamlingen av personuppgifterna ska vara tillåten, måste den personuppgiftsansvarige dessutom hantera dessa uppgifter på ett korrekt sätt, med respekt för den enskildes integritet och med beaktande av lämpliga säkerhetsåtgärder.

Varje enskild nämnd eller bolagsstyrelse är personuppgiftsansvarig och ansvarar därigenom för att dess personuppgiftsbehandlingar utförs i enlighet med dataskyddsförordningens bestämmelser.

Att anställda har en grundläggande kännedom om dataskyddslagstiftning är en förutsättning för att organisationen ska kunna leva upp till kraven i förordningen. En grundläggande förståelse för dataskyddsregleringen är också en förutsättning för att de anställda exempelvis ska kunna identifiera en personuppgiftsincident och på så sätt kunna minimera skada dels för de registrerade, dels för organisationen i stort.

Dataskyddsombudets skyldighet, som regleras i artikel 39 dataskyddsförordningen, är bland annat att övervaka den personuppgiftsansvariges efterlevnad av förordningen, vilket innefattar granskning av anställdas utbildning som deltar i behandlingar av personuppgifter.

1.1.1 Granskningsområdet

Granskningsområdet som valts ut är arbetet med utbildning inom dataskyddslagstiftningen i er organisation.

1.1.1.1 Syfte

Syftet med granskningen av organisationens kunskaper om dataskyddslagstiftningen och frågor kring utbildning är att undersöka vilken nivå av kunskap organisationen har och identifiera eventuellt behov av ytterligare utbildningsinsatser.

1.2 Tillvägagångssätt

Granskningen delades upp i två delar där den ena delen var riktad till dataskyddskontakterna och den andra delen var en enkät riktad till medarbetare och chefer. Dataskyddskontakterna fick generella frågor om hur utbildning av dataskyddslagstiftningen har genomförts och vilka framtida utbildningsinsatser som planeras inom organisationen. Enkäten bestod dels av ett antal kortare frågor om dataskyddslagstiftningen, dels av frågor kring vilka utbildningsinsatser som den anställde har erhållit i organisationen. Enkäten har genomförts anonymt då syftet var att få en organisatorisk överblick.

Enkätsvaren kommer delas upp i kategorierna chef och medarbetare. Med ”chef” menas personer som företräder arbetsgivaren i det dagliga arbetet och ”medarbetare” är personer som inte är chefer. När båda kategorierna redovisas i ett gemensamt resultat eller ska benämnas gemensamt används begreppet ”anställda” nedan.

I enkäten skulle medarbetarna och cheferna ange huruvida de arbetar på Göteborgs Spårvägar AB, GS Buss AB eller GS Trafikantservice och dataskyddskontakterna har skickat in tre separata svarsdokument. Denna rapport kommer dock att avhandla bolagen gemensamt. Detta för att det dataskyddsarbete som sker på bolagen, sker gemensamt och svaren från dataskyddskontakterna är identiska. Dataskyddsombudet bedömer också att det inte går att dra några särskilda slutsatser av enkätsvaren baserat på bolagstillhörighet. Göteborgs Stads Kollektivtrafik AB ingår inte i denna granskning då det inte fanns några anställda på bolaget när granskningen påbörjades.

Nedan kommer Göteborgs Spårvägar AB, GS Buss AB eller GS Trafikantservice AB att benämnas som ”Bolagen”.

1.3 Bilagor

Bilaga 1	Frågor och svar – Dataskyddskontakter Göteborgs Spårvägar AB
Bilaga 2	Frågor och svar – Dataskyddskontakter GS Trafikantservice AB
Bilaga 3	Frågor och svar – Dataskyddskontakter GS Buss AB
Bilaga 4	Frågor och facit – enkät
Bilaga 5	Resultat av enkät

2 Granskning

2.1 Organisatoriska strategier för utbildning inom dataskydd

Dataskyddskontakterna har fått frågor om hur verksamheten lagt upp sin organisation kring utbildning inom dataskydd. Frågorna och svaren återfinns i bilaga 1–3.

Sammanfattning av organisationens utbildningsstrategier

En extern konsult informerade cheferna på en ledarträff under september/oktober 2019. Utöver detta har ingen utbildning skett på Bolagen. Det finns heller inget sätt att säkerställa hur nyanställda ska få den utbildning som krävs.

När det gäller framtida utbildningsbehov anger Bolagen att det finns stora behov och en grov plan finns. Planen består i följande:

- Information/utbildning till ledningsgruppen
- Information/utbildning till nivån under ledningsgruppen samt ytterligare ner i organisationen där behov finns. Annars allmän information på intranätet.
- Implementera dataskyddsförordningen i utbildning vid nyanställningar.
- Medverka vid arbetsplatsträffar vid behov

På frågan om hur Bolagen ska se till att kunskapen underhålls hos medarbetarna anger Bolagen att planen är baserad på den framtida linjeorganisationen, som inte finns förhandlad och klar när svar angavs den 4 februari 2020. Planen innebär att regelbundna uppföljningar genom närvaro vid olika möten i linjeorganisationen, skicka ut enkäter för att säkerställa kunskapen underhålls samt säkerställa om det finns eventuella glapp i kunskapen kring dataskyddsförordningen. Bolagen ska hålla informationen i utbildningarna uppdaterade genom att vara aktiv i olika forum gällande dataskyddsförordningen och uppdatera därefter.

2.2 Utbildningsinsatser och kunskapsnivå hos organisationen

Enkätundersökningen skickades ut av Bolagens dataskyddsombud via e-post och gick ut till 142 personer. Fyra av dessa e-postadresser fungerade dock inte trots upprepade försök och extra kontroll av e-postadresserna med Bolagens dataskyddskontakt. Det totala antalet personer som faktiskt fick enkäten var således 138.

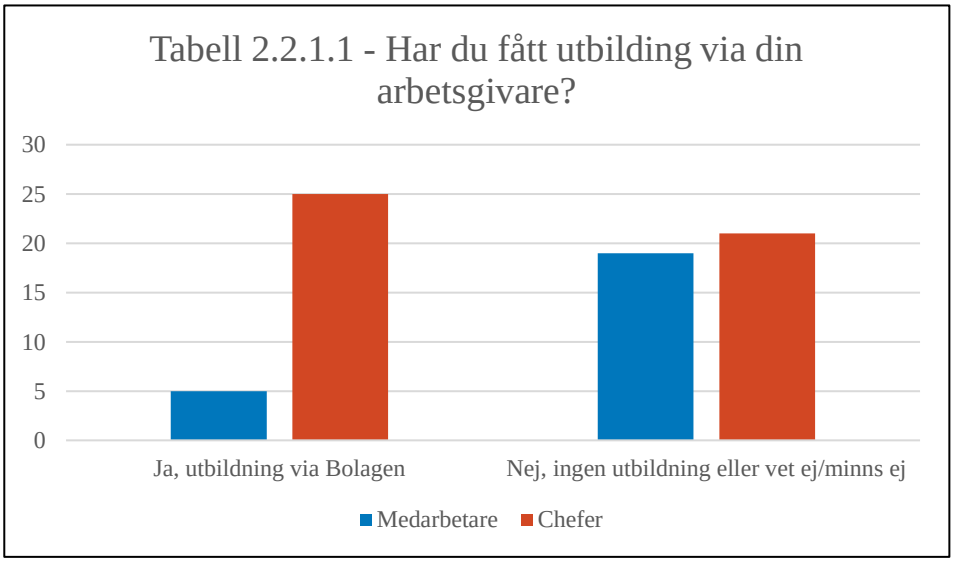
De som har fått enkäten är samtliga chefer på Bolagen och medarbetare på HR, IT, ekonomi samt medarbetare på Resurspoolen. Anledningen till att enkäten skickas till dessa grupper är för att deras arbetsuppgifter innebär behandling av personuppgifter i mer eller mindre stor omfattning.

Totalt har 71 personer svarat på enkäten, dock har en person angett att hen arbetar på GS Trafikantservice AB och att hen är chef men inte fortsatt besvara de efterföljande frågorna. Det är alltså 70 personer som svarat på enkäten, vilket motsvarar cirka 51 % av de tillfrågade. Av de svarande är fem chefer på GS Buss AB, tre medarbetare och åtta chefer på GS Trafikantservice AB samt 21 medarbetare och 33 chefer på Göteborgs Spårvägar AB. Alla tillfrågade har dock inte svarat på samtliga frågor varför antal svar kan varier på de olika frågor men antal svarande kommer att redovisas i aktuella fall.

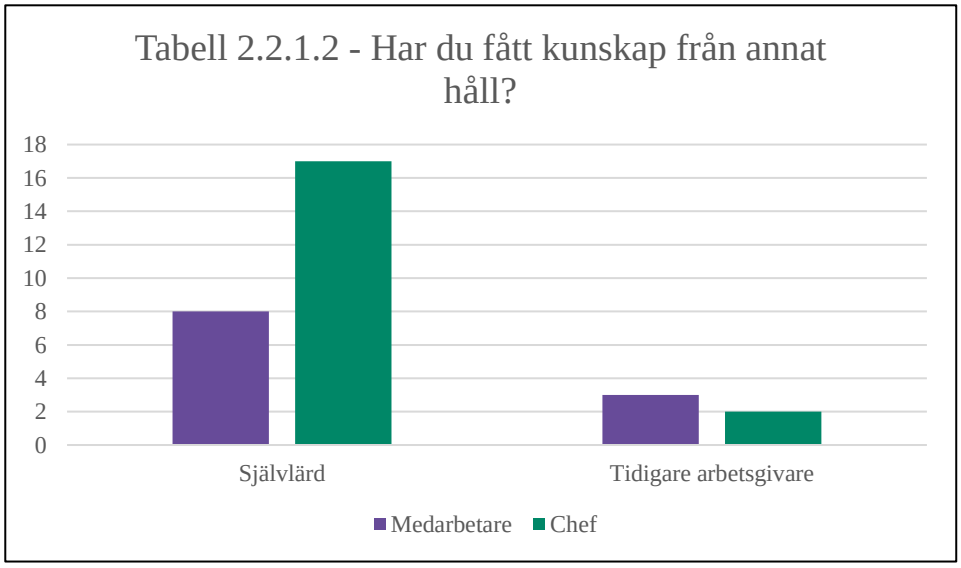
2.2.1 Svaren angående utbildningsinsatser

Utbildningsinsatser

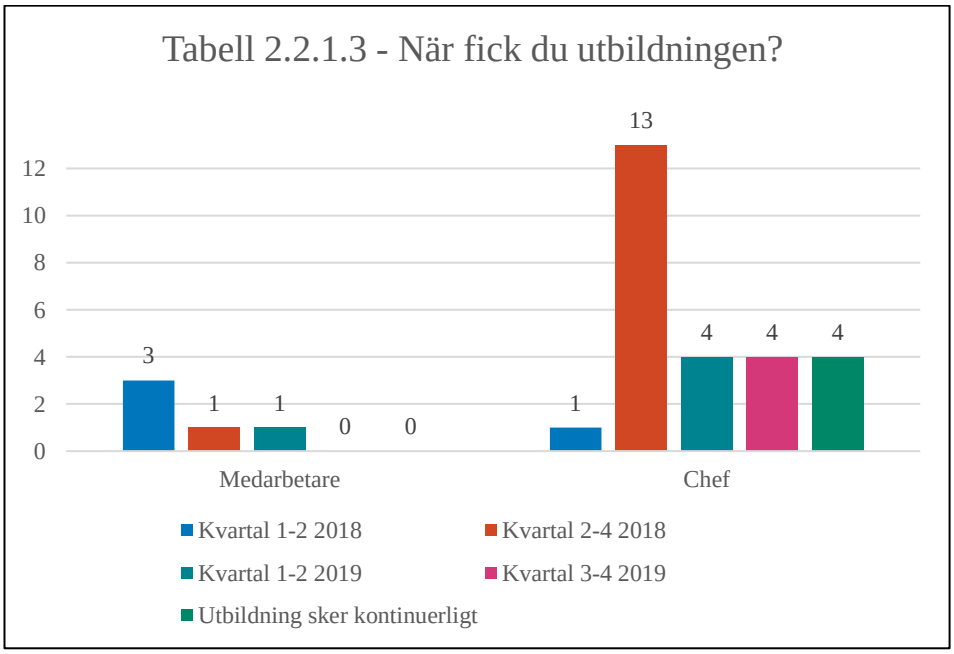
Den första frågan i enkäten handlade om utbildningsinsatser från arbetsgivaren, alltså från Bolagen. Det var möjligt att ge mer än ett svar på frågan och samtliga har svarat. 21 % av medarbetarna och 54% av cheferna anger att de fått någon form av utbildning av Bolagen.



79 % av medarbetarna och 46 % av cheferna har svarat att de inte fått någon utbildning eller att de inte minns eller vet huruvida de fått någon utbildning. Dessa personer fick även frågan om de fått kunskap kring dataskyddslagstiftning på annat håll och flertalet angav att de är självlärda eller att de fått utbildning av tidigare arbetsgivare.



De anställda som angett att de fått någon utbildning av Bolagen ombads svara på när denna utbildningen genomförts. Medarbetarna angav främst att de fått utbildning under början av 2018 och de flesta av cheferna har fått utbildning under andra halvan av 2018. Värt att notera är att fyra chefer anger att de får utbildning kontinuerligt (se tabell 2.2.1.3).



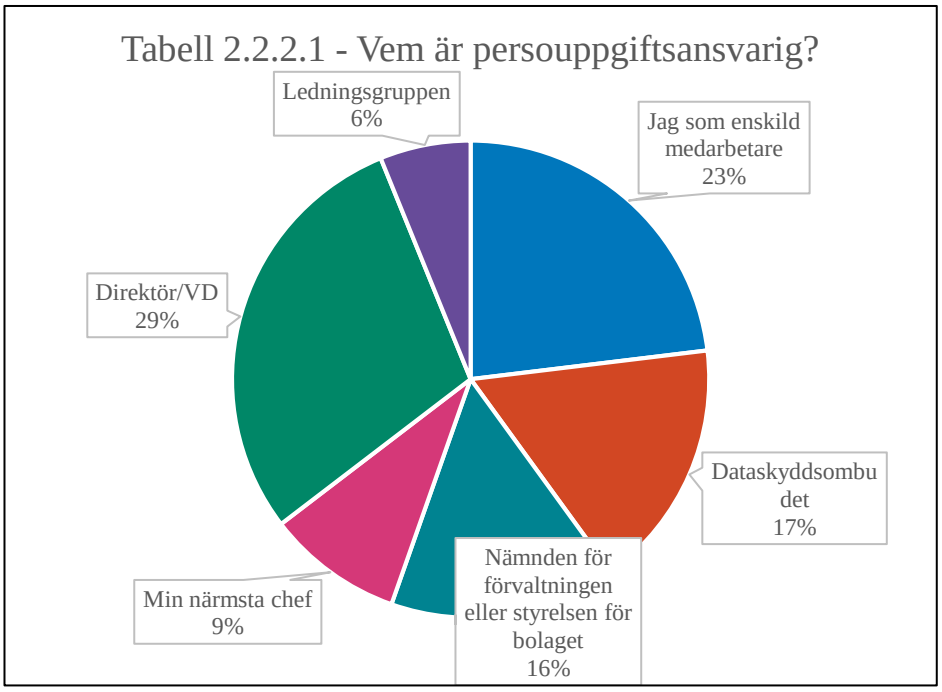
2.2.2 Svaren avseende kunskapsfrågorna

Andra delen av enkätundersökningen bestod av sex kunskapsfrågor inom dataskydd. Frågor och facit återfinns i bilaga 4.

Personuppgiftsansvaret

På frågan om vem som är ansvarig för organisationens personuppgiftsbehandlingar svarade 42 chefer och 23 medarbetare.

Det korrekta svaret på frågan är ”Nämnden för förvaltningen eller styrelsen för bolaget”. Av de chefer som svarade på frågan var det endast nio chefer som angav det korrekta svaret och av medarbetarna var det bara en person som svarade rätt. Utav de som svarat på frågan är det alltså endast 16 % som vet vem det är som är personuppgiftsansvarig.



Identifiering av personuppgifter

I enkäten fanns två frågor om personuppgifter. Den ena frågan var vilka av de åtta angivna alternativen som är en personuppgift, där fem av alternativen var rätt (namn, personnummer, e-postadress, fingeravtryck och telefonnummer) och tre var felaktiga (portkod, ett aktiebolags namn och växelnumret till arbetsplatsen). 42 chefer och 24 medarbetare svarade på frågan.

Av cheferna var det 33 % som angett samtliga korrekta alternativ och för medarbetarna var den siffran 46 %. Resterande har antingen missat ett eller flera av de korrekta alternativen eller angett ett eller flera av de felaktiga alternativen.

Värt att notera är att 26 % av chefer inte angett att namn är en personuppgift. För medarbetarna var denna siffra 13 %.

Den andra frågan om personuppgifter var vilka av de sex angivna alternativen i frågan som klassificeras som känsliga personuppgifter, där fyra av alternativen var rätt (medlemskap i fackförening, hälsa, filosofisk övertygelse, politiska åsikter) och två felaktiga (lösenord till dator och mobilnummer).

Totalt var det 38 chefer och 23 medarbetare som svarade på frågan och av dessa var det åtta chefer och två medarbetare som angav de fyra korrekta alternativen. Resterande har antingen missat ett eller flera av de korrekta alternativen eller angett ett eller flera av de felaktiga alternativen.

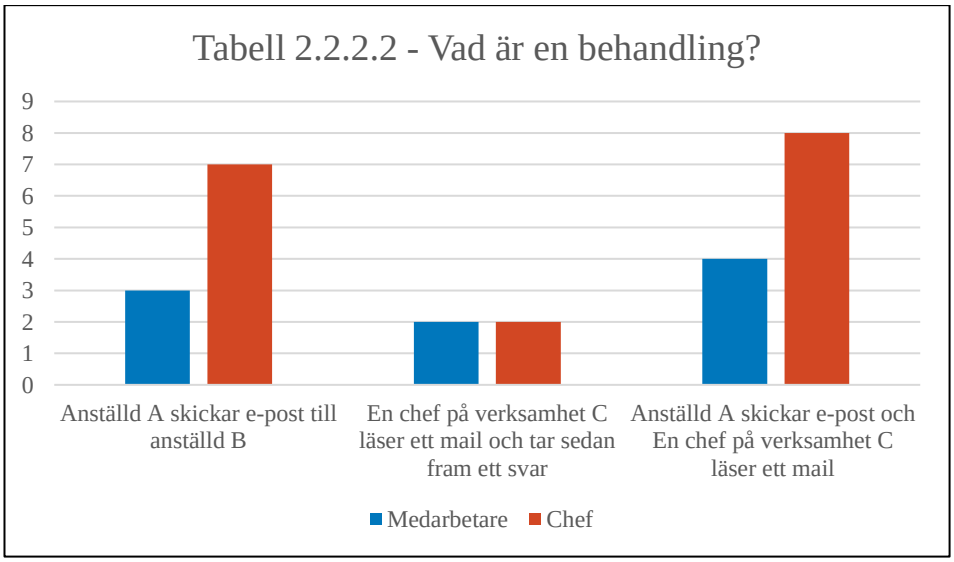
Värt att notera är att 22 chefer och 14 medarbetare trodde att ”Lösenord till dator” var en känslig personuppgift.

Identifiering av personuppgiftsbehandlingar

Enkäten innehöll en fråga med nio olika påståenden/senarior där man ska ange vilka av dessa som räknas som en personuppgiftsbehandling i dataskyddsförordningens mening. Av dessa nio alternativen är sex rätt och tre felaktiga. Se bilaga 4 för frågorna och facit.

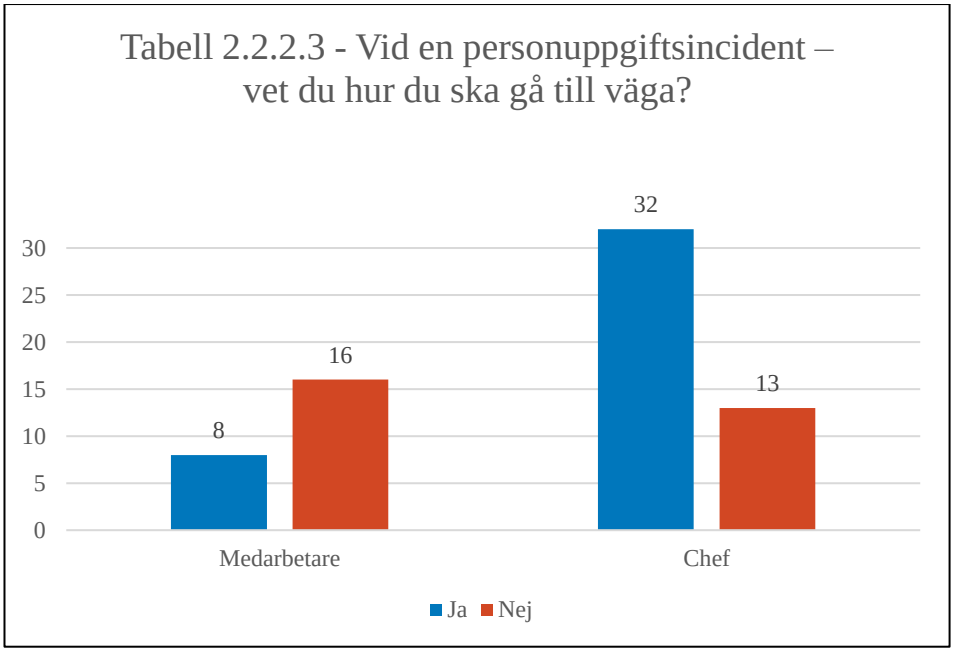
40 chefer och 21 medarbetare har svarat på frågan. En medarbetare har angett de sex korrekta alternativ. Fyra chefer och en medarbetare har angett samtliga korrekta alternativ men har även angett ett eller flera av de felaktiga alternativen.

Värt att notera här är att ett fåtal av de tillfrågade har identifierat att det är en behandling att skicka och/eller läsa e-post. Av tabell 2.2.2.2 framgår att endast 12 anställda identifierat att skicka och läsa e-post är en behandling (staplar till höger). De andra staplarna redogör för de anställda som angett ett av de korrekta svaren.



Personuppgiftsincidenter

På frågan om man vet hur man ska gå tillväga vid en personuppgiftsincident svarade 45 chefer och 24 medarbetare. 71 % av cheferna vet hur de ska gå tillväga vid en personuppgiftsincident, motsvarande siffra för medarbetarna är 33 %.



Enkätundersökningen innehöll även en fråga med fyra olika påståenden/scenarier där man ska ange vilka av dessa som räknas som en personuppgiftsincident i dataskyddsförordningens mening. Av dessa fyra alternativen är tre rätt och ett felaktigt. Se bilaga 4 för frågorna och facit.

Totalt svarade 38 chefer och 22 medarbetare på frågan och två chefer angav samtliga korrekta alternativ. Av de inkomna svaren var det 13 chefer och nio medarbetare som har angett två av de tre korrekta svaren. Dock var det endast fyra chefer och tre medarbetare som svarade att ett virusangrepp på datorn var en personuppgiftsincident (vilket var ett av de tre rätta svaren).

Värt att notera är att det bara var en chef och två medarbetare som angav det felaktiga alternativet.

2.3 Analys och sammanfattning

Det första som kan konstateras är att endast hälften av de tillfrågade har besvarat enkäten. Ett visst manfall får man räkna med då det kan finnas anställda som är sjukskrivna, föräldralediga eller som har haft en längre semester men sannolikt är det inte 68 personer som faller in under någon av dessa kategorier. Dessutom har det framkommit att vissa personer har trott att e-postmeddelandet från Dataskyddsombudet innehöll virus och därför inte svarade på enkäten. Det är bra att Bolagens anställda är uppmärksamma men cheferna borde ha uppmuntrat sina medarbetare att besvara enkäten.

Utbildningsinsatser

Sammanfattningsvis kan det konstateras att Bolagen inte har utbildat sina medarbetare i någon större utsträckning och att utbildningen till stor del skett innan eller i samband med att dataskyddsförordningen trädde i kraft den 25 maj 2018. Endast en medarbetare har angett att hen fått utbildning av Bolagen under första halvan av 2019.

När det gäller utbildning av cheferna har 54 % angett att de fått någon form av utbildning inom dataskyddslagstiftningen av Bolagen. Utbildningen har främst skett under andra halvan av 2018. Fyra chefer angav att de får utbildning kontinuerligt av Bolagen vilket är anmärkningsvärt med tanke de svar som Bolagens dataskyddskontakter angivit där det framgår att Bolagen inte har några utbildningar och att den enda utbildning som skett hölls av extern konsult under hösten 2019.

Varför svaren skiljer sig är svårt att säga. Kanske har man olika bild av vad ”utbildning” är. Oavsett vilken bild som är mest korrekt så har Bolagen inte utbildat sina anställda tillräckligt kring dataskyddslagstiftningen. Det är inte tillräckligt att hålla en utbildning för medarbetarna i samband med dataskyddsförordningens ikraftträdande eller att cheferna utbildats vid ett tillfälle antingen hösten 2018 eller av konsult hösten 2019. Kunskap är en färskvara som måste underhållas och det är framför allt viktigt när det gäller dataskyddslagstiftningen där det hela tiden kommer vägledningar och avgöranden som kan förändra tidigare gällande tolkningar.

Bolagen har en grov plan för framtida utbildningsinsatser och det är positivt att det finns en plan även om det inte framgår hur planen ska genomföras. Det finns en viss förståelse för att det inte finns en fastställd och detaljerad plan på grund av den organisationsförändring som Bolagen genomgått (och genomgår) men det vore önskvärt att Bolagen tar tillfället i akt och gör dataskyddsarbetet till en naturlig del av organisationen nu vid omorganiseringen.

Den grova plan som beskrivits av Bolagens dataskyddskontakter innebär att utbildning och information ska ges till ledningsgruppen och relevanta grupper under ledningsgruppen. Det är viktigt att ledningsgruppen hålls uppdaterad så att de kan vidta de åtgärder som krävs för att Bolagen ska följa gällande dataskyddslagstiftning. Anpassade utbildningsinsatser till relevanta grupper är också att föredra så att de anställda ges goda förutsättningar för att hantera personuppgifter på ett lagligt och säkert sätt. Dataskyddskontakterna anger även att Bolagen ska lägga

upp allmän information på intranätet vilket är en klok åtgärd för att öka medvetandet bland de anställda. Det är dock viktigt att informationen är ”levande” och uppdateras när det behövs.

På frågan om hur Bolagen ska se till att kunskapen underhålls hos medarbetarna anger man att det ska baseras på framtida linjeorganisationen. Eftersom denna inte är klar ännu är det svårt för dataskyddsombudet att uttala sig om denna del. Vidare anger man att uppföljningar ska ske genom att närvara på olika möten, det framgår inte hur detta ska bidra till kunskapsunderhåll. Till sist anger Bolagen att enkäter ska skickas ut för att säkerställa att kunskapen underhålls och kontrollera huruvida det finns eventuella glapp. Enkäter är ett bra sätt att få en överblick över hur kunskapsnivån på Bolagen ser ut och kan bidra till identifieringen av eventuella kunskapsglapp. Det är dock viktigt att Bolagen uppmuntrar sina anställda att svara på enkäterna.

I den enkät som dataskyddsombudet skickade ut till de anställda fick de som angett att de inte fått någon utbildning eller om de inte minns/vet om det fått någon utbildning en fråga om de fått kunskap om dataskyddslagstiftningen på annat håll. Det var ett antal anställda som angav att de är självlärda, vilket både är bra och mindre bra. Varför det är bra är för att Bolagen har engagerade anställda som vill lära sig mer om gällande lagstiftning och att de vill behandla personuppgifter på ett korrekt sätt. Dock kan det vara mindre bra om informationen inte kommer från en säker källa, exempelvis kanske man har läst om en specifik fråga hos en branschorganisation som har gjort en tolkning till sin fördel. Kanske läser man information om personuppgiftsbehandling i privat sektor och missar de specialdelar som gäller för offentliga verksamheter. Det blir därför svårt för Bolagen att veta vilka kunskaper de anställda har och om den är adekvata. Bolagen saknar idag ett sätt att säkerställa att de anställda har tillräcklig och uppdaterad kunskap inom dataskyddslagstiftningen.

Personuppgiftsansvaret

Det är 16 % av de svarande som visste att det är bolagets styrelse som är ansvarig för bolagets personuppgiftsbehandlingar. Som framgår av tabell 2.2.2.1 tror 29 % att det är Vd:n som är personuppgiftsansvarig och 23 % tror att det är de själva som enskilda medarbetare. Du har som anställd ett ansvar att utföra dina arbetsuppgifter enligt gällande lag samt instruktioner och rutiner från arbetsgivaren, så att de anställda tror att det är de själva som är ansvariga tyder på att man förstår allvaret. Det är dock viktigt att personuppgiftsansvaret är tydligt och att man känner till att du inte är personligt ansvarig enligt dataskyddsförordningen. Det är styrelsen för respektive bolag som är ansvariga för att Bolagen följer dataskyddslagstiftningen och det är viktigt att styrelsen, tillsammans med ledningsgruppen, ger medarbetarna de förutsättningar och den tid som behövs för att kunna bedriva ett lagenligt och effektivt dataskyddsarbete.

En risk med att de anställda tror att de personuppgiftsansvariga är om de också tror de behöver betala eventuella sanktionsavgifter eller kanske tror de att det kan ge negativa konsekvenser om de råkat orsaka en personuppgiftsincident. Det är viktigt att Bolagen dels informerar om det egentliga personuppgiftsansvaret, dels

uppmuntrar sina anställda till att följa lagstiftningen och att följa personuppgiftsincidentrutinen.

Identifiering av personuppgifter

Resultatet av de två frågorna som rörde identifieringen av personuppgifter tyder på att de anställda behöver få bättre kunskap i vad som faktiskt är en personuppgift och vad som är känsliga personuppgifter. 33 % av cheferna och 45 % av medarbetarna identifierade samtliga korrekta personuppgifter, men hela 26 % av cheferna och 13 % av medarbetarna har inte identifierat ”namn” som en personuppgift.

När det kommer till de känsliga personuppgifterna var det 21 % av cheferna och 8 % av medarbetarna som identifierat samtliga korrekta alternativ. De flesta hade identifierat att ”hälsa” är en känslig personuppgift men knappt hälften av de svarande känner till att filosofisk övertygelse är en känslig personuppgift.

Sett till Bolagens kärnuppdrag är det osannolikt att filosofisk övertygelse behandlas i någon större omfattning. Den bristande kunskapen kring att filosofisk övertygelse är en känslig personuppgift medför sannolikt inte en överhängande risk för varken verksamheten eller de registrerades fri- och rättigheter.

Något som är en mer överhängande risk är att 43 % av de svarande inte känner till att medlemskap i fackförening är en känslig personuppgift. Till skillnad från filosofisk övertygelse så behandlar Bolagen uppgifter om facklig tillhörighet om samtliga anställda.

Något annat som utmärker sig i svaren till frågan om känsliga personuppgifter är att 59 % av cheferna och 61 % av medarbetarna har identifierat ”lösenord till dator” som en känslig personuppgift. Att det är så många som har identifierat lösenord men inte facklig tillhörighet beror troligtvis på att man inte känner till vad känsliga personuppgifter är enligt dataskyddsförordningen. Ur ett informationssäkerhetsperspektiv är det positivt att de anställda anser lösenord vara en känslig personuppgift, även om det var fel i denna fråga.

Identifiering av personuppgiftsbehandlingar

Denna kunskapsfråga får anses vara en av de svårare i enkätundersökningen. Syftet med frågan var att se hur många som förstått att i princip allt vi gör med personuppgifter, bortsett från ett fåtal undantag, innebär en personuppgiftsbehandling enligt dataskyddsförordningen.

Såsom ovan redovisats var det en medarbetare som angav samtliga sex korrekta alternativ. Dessutom angav fyra chefer och ytterligare en medarbetare samtliga korrekta alternativ men som också angav ett eller flera av de felaktiga alternativen. De flesta har identifierat att utlämnade av personuppgifter är en behandling.

Det fanns två scenarier som handlade om e-post, ena scenariot rörde skickandet av e-post och det andra rörde läsandet av e-post. Både dessa scenarier är behandlingar men endast åtta chefer och fyra medarbetare identifierade båda scenarierna

som en behandling. Ytterligare nio chefer och fem medarbetare identifierade ett av scenarierna som en behandling men missade alltså den andra.

Att skicka/ta emot/skriva/läsa e-post är kanske en av våra vanligaste personuppgiftsbehandlingar och det är en behandling oavsett om det sker internt mellan två kollegor eller om det sker externt till exempelvis en kund eller leverantör. De flesta e-postmeddelande innehåller personuppgifter då våra e-postadresser ofta innehåller för- och/eller efternamn. E-postmeddelande kan också innehålla integritetskänsliga uppgifter (t.ex. uppgifter om lön) eller känsliga personuppgifter (t.ex. uppgifter om sjukdom eller facklig tillhörighet). Felskickade mail är också en av de vanligaste personuppgiftsincidenterna och det är viktigt att de anställda känner till att skicka/ta emot/skriva/läsa epost är en behandling.

Personuppgiftsincidenter

71% av cheferna känner till hur de ska få tillväga vid en personuppgiftsincident, det får anses som ett godkänt resultat även om denna siffra bör vara ännu högre. Dessvärre är det enbart 33 % av medarbetarna som känner till Bolagens rutin för personuppgiftsincidenter, vilket givetvis inte är bra. Medarbetarna är ofta de som kommer att upptäcka personuppgiftsincidenter först och om de inte vet hur de ska agera när de upptäcks kan Bolagen inte heller åtgärda dem. Det är viktigt att komma ihåg att en personuppgiftsincident alltid utgör en säkerhetsincident. Bolagen bör se identifieringen av personuppgiftsincidenterna som ett sätt att hitta eventuella säkerhetsluckor och det kan även bidra till att identifiera områden som kan effektiviseras.

Utöver frågan om de anställda känner till hur de ska gå tillväga vid en personuppgiftsincident skulle de även identifiera huruvida ett antal scenarier utgjorde personuppgiftsincidenter eller inte. Som angetts ovan är det två chefer som identifierat de korrekta alternativen. 13 chefer och nio medarbetare har angett två av de tre korrekta svaren och endast tre anställda har angett det felaktiga alternativet. Överlag får detta ändå anses vara ett godkänt resultat. Dock var det endast ett fåtal anställda som identifierade att virusangrepp är en personuppgiftsincident och vad detta beror på är såklart svårt att veta. Kanske kan det bero på att de anställda enbart ser detta som en säkerhetsincident eller kanske beror det på att de anställda inte fått tillräcklig utbildning inom dataskyddslagstiftning.

2.4 Reflektion och rekommendationer

Enligt rapporten ”Data Gets Personal: 2019 Global Data Risk Report”[1] har varje anställd i snitt tillgång till 17 miljoner filer och av de europeiska tillsynsmyndigheternas rapporter om personuppgiftsincidenter framgår det att den mänskliga faktorn står för majoriteten av de inrapporterade personuppgiftsincidenterna.

I Datainspektionens rapport ”Anmälda personuppgiftincidenter januari – september 2019”[2] kan vi läsa att 35 % av alla anmälda personuppgiftsincidenter avser felskickade brev eller e-post. En annan vanlig personuppgiftincident är att verksamheter upptäcker att personuppgifter funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning. Vad beror då personuppgiftsincidenterna på? Enligt de anmälningarna som Datainspektionen fick in under januari – september 2019 beror 51 % på den mänskliga faktorn. Att anställda begått ett misstag vid hantering av personuppgifter eller att anställda, medvetet eller omedvetet, inte följer verksamhetens rutiner för personuppgiftshantering.

Som konstaterats ovan var det få anställda på Bolagen som identifierat att det är en personuppgiftsbehandling att skicka/läsa e-post. Resultatet är oroväckande då just felskickade e-post är en av de vanligaste personuppgiftsincidenterna.

Bolagen bör ta fram en mer konkret plan för utbildningsinsatser, identifiera vilka yrkesgrupper där utbildning bör prioriteras och kartlägga om de behöver olika kunskap. Bolagen behöver skapa en rutin för att informera/utbilda nyanställa och man bör synliggöra de rutiner som finns idag för samtliga anställda. Därtill bör Bolagen utbilda och öva på personuppgiftsincidenter. Särskilt bör man fokusera på att ge sina anställda tillräcklig 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 Bolagen ska uppfylla sin ansvarsskyldighet enligt förordningen och minimera riskerna för eventuella beslut om sanktionsavgifter.

[1] https://www.varonis.com/2019-data-risk-report/
[2] https://www.datainspektionen.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter---jan-sept-2019.pdf

Göteborgs Stad
Dataskyddsombud Johanna Brunzell Begby
E-post: dso@intraservice.goteborg.se