Göteborgs Stad

Utbildning

Granskningsrapport för Grefab

2020-03-30

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2020-03-20	1.0	För påsyn av dataskyddskontakt	Ulrika Fredborg
2020-03-20	2.0	Korrektur och färdigställande, inga synpunkter har inkommit från DSK	Ulrika Fredborg

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. Att ha 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 skyldigheter, som regleras i artikel 39 dataskyddsförordningen, består bland annat av att övervaka den personuppgiftsansvariges efterlevnad av förordningen, vilket innefattar utbildning av anställda som deltar i behandling av personuppgifter.

1.1.1 Granskningsområdet

Granskningsområdet för denna rapport är arbetet med utbildning inom dataskyddslagstiftningen i er verksamhet.

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 dataskyddskontakten och den andra delen var en enkät riktad till medarbetare och chefer. Dataskyddskontakten fick frågor om hur utbildning inom dataskyddslagstiftningen genomförs inom organisationen och eventuellt planeras

att genomföras och hur verksamheten säkerställer en grundläggande kännedom om lagstiftningen hos de anställda.

Enkäten bestod dels av frågor kring vilka utbildningsinsatser som den anställde har erhållit, dels av ett antal kortare frågor om dataskyddslagstiftningen. Enkäten har genomförts anonymt då syftet var att få en organisatorisk överblick.

1.3 Bilagor

Bilaga 1 Enkätfrågor och svar om organisationens strategier för utbildning

Bilaga 2 Enkätundersökningsfrågor med facit

Bilaga 3 Underlaget för rapporten

2 Granskning

2.1 Organisatoriska strategier för utbildning inom dataskydd

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

Sammanfattning av organisationens utbildningsstrategier

Utbildning har skett i samband med att dataskyddsförordningen infördes i maj 2018 och då i form av ett utbildningsmaterial som presenterades under APT. Ungefär en gång i månaden förmedlar DSO information i form av ett nyhetsbrev med senaste nytt, relevanta avgöranden och en djupdykning i ett visst område inom dataskydd som tillgängliggörs på bolagets samtliga anställda.

Det är obligatoriskt att delta på utbildningsdagar för personalen. Samtliga i personalen har fått samma utbildning då en medarbetare kan inneha flera olika roller. Bolaget har inte rekryterat någon personal på befattningar där de anser att någon utbildning inom dataskydd är aktuellt och har därför ingen rutin kring hur nyanställda ska erbjudas utbildning.

Bolaget anger att som liten organisation har de god kontroll över de behandlingar de har, både för anställda och kunder, och kan i dagsläget inte se att det krävs några utbildningsinsatser. Skulle det bli aktuellt med vidare utbildning kommer bolaget att kontakta DSO.

Frågor kring dataskydd tas upp på ledningsgruppsmöten och förs vid behov vidare ned i organisationen för att hålla samtliga medarbetare uppdaterade.

2.2 Iakttagelser

Sammanfattningsvis kan konstateras att Grefab har i maj 2018 genomfört en utbildningsinsats i samband med ikraftträdandet av förordningen. Ingen uppföljning eller uppdatering har skett efter det.

Det är positivt att nyhetsbrevet som förmedlas av DSO tillgängliggörs för samtliga anställda men nyhetsbrevet ska inte ses som ett substitut för utbildning och vidare finns ingen garanti att de anställda faktiskt tillgodogör sig informationen.

Grefab har varken en rutin för att befintliga medarbetare har adekvat utbildning eller någon rutin för nyanställda utbildning vilket är problematiskt. Att hänvisa till att bolaget är litet och därmed endast behandlar personuppgifter i liten utsträckning är inte skäl att inte ha en rutin för att se till att medarbetarna håller sig uppdatera inom dataskyddslagstiftningen. Mycket har hänt sedan maj 2018 dels i form av nya vägledningar och tolkningar dels i avgöranden från tillsynsmyndigheter runt om Europa.

Av de rapporter som kommit från bland annat Datainspektionen framgår tydligt att den mänskliga faktorn är den största orsaken till att en organisation behandlar personuppgifter på ett felaktigt sätt. De som behandlar personuppgifter i sitt dagliga arbete är således de som innebär den största risken i en organisation och det är därför av allra största vikt att var och en av medarbetarna hanterar personuppgifter korrekt.

Grefab har förutom sina egna anställda även kunder som utgörs av medborgare i och kring Göteborgs stad. Samtliga av dessa registrerade har rättigheter som ska kunna tillgodoses enligt förordningen varför det är av yttersta vikt att man vet dels hur personuppgifterna ska hanteras korrekt från första början dels hur man ska agera vid eventuell incident eller vid krav från enskild gällande någon rättighet.

2.3 Utbildningsinsatser och kunskapsnivå hos organisationen

Enkätundersökningen har skickats ut per e-post till utvalda medarbetare som ingår i grupper i organisationen som DSO tillsammans med dataskyddskontakt (DSK) har identifierat som de som framförallt bör ha en grundläggande kunskap om dataskyddslagstiftningen. Det har inneburit att enkätundersökningen skickades ut till 5 personer i organisationen.

Enkäten var uppdelad i två delar; *del 1: Allmänt om utbildning* med övergripande frågor om organisationens utbildning och rutiner och *del 2: Kunskapstest* med frågor om bland annat personuppgifter och behandlingar. Rapporten kommer att följa samma uppdelning.

Totalt har fyra svar erhållits då ett svar är helt ofullständigt eftersom man endast angett att man arbetar på bolaget men ej fortsatt svara på efterföljande frågor i enkätundersökningen. Svaren har vid vissa frågor delats upp i yrkeskategorierna

chef eller medarbetare. Med medarbetare menas alla anställda som inte är chefer. I undersökningen har två svarande angett att det är chefer och två att de är medarbetare.

Vissa har inte svarat på alla frågor i enkäten varför totala antalet svar på respektive fråga skiljer sig åt.

2.3.1 Svaren avseende utbildningsinsatser

Utbildningsinsatser

På frågan om man har fått någon utbildning om dataskyddslagstiftningen har fyra svarat på frågan och samtliga har svarat att de har fått intern utbildning.

Cheferna har angett att de får utbildning kontinuerligt och medarbetarna har angett att de fick utbildning under 2018.

Personuppgiftsincidenter

På frågan om man vet hur man ska gå tillväga vid en personuppgiftsincident svarade samtliga ja.

Personuppgiftsansvaret

På frågan om vem som är ansvarig för organisationens personuppgiftsbehandlingar svarade samtliga fyra.

Tre svarande angav det korrekta svaret ”Nämnden/styrelsen”. En av de svarande angav att de själva som enskild medarbetare är ansvarig för personuppgiftsbehandlingen.

2.3.2 Svaren avseende kunskapsfrågorna

Andra delen av enkätundersökningen bestod av sex kunskapsfrågor inom dataskydd. Frågor, svarsalternativ och rätt svar återfinns i bilaga 2.

Identifiering av personuppgifter

I undersökningen 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).

Tre personer svarade varav en angav samtliga korrekta alternativen. Resterande har antingen missat en eller flera av de korrekta alternativen. Ingen av de svarande hade angett något av de felaktiga svarsalternativen.

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).

Tre personer svarade på frågan och av dessa var det ingen som hade angett ett fullständigt korrekt svar. En svarande hade angett de korrekta alternativen men i kombination med ett av de felaktiga.

Värt att notera är att samtliga svaranden angett det felaktiga svarsalternativet ”Lösenord till dator” som en känslig personuppgift.

Identifiering av personuppgiftsbehandlingar

Enkätundersökningen har innehållit en fråga med nio olika påståenden/scenarier där man ska ange vilka av dessa som räknas som en personuppgiftsbehandling enligt dataskyddsförordningens mening. Av dessa nio angivna alternativen är sex rätt och tre felaktiga.

Tre personer svarade på frågan varav ingen hade angett samtliga korrekta alternativ. Två av tre har korrekt identifierat att de tre första alternativen som gäller medlemsregister, molntjänster och utlämnande av uppgifter är behandlingar.

Värt att notera är att ingen har angett att mail till en kollega (”Anställd A skickar ett mail till Anställd B”) är att betrakta som en behandling, vilket det alltså är. Endast en svarande har korrekt identifierat att läsa ett mail och ta fram ett svar är en behandling.

Personuppgiftsincidenter

På frågan om man vet hur man ska gå tillväga vid en personuppgiftsincident svarade samtliga ja.

Enkätundersökningen innehöll en fråga med fyra olika påståenden/scenarier där man ska ange vilka av dessa som räknas som en personuppgiftsincident enligt dataskyddsförordningen. Av dessa fyra angivna alternativ är tre rätt och ett felaktigt.

Samtliga svarade på frågan men ingen angav alla korrekta svarsalternativ. Ingen av de svarande angav korrekt att svarsalternativet om ett virusangrepp på datorn är en personuppgiftsincident.

Värt att notera är att det inte var någon som angav det felaktiga alternativet.

2.3.3 Iakttagelser

Svarsfrekvensen

Att det totala deltagarantalet i enkäten, det vill säga antalet som fick enkäten skickad till sig, framstår som litet beror enligt dataskyddskontakten dels på att Grefab är ett litet bolag, dels på att personer inom bolaget har flertalet roller varför det inte är så många som i sina dagliga arbetsuppgifter behandlar personuppgifter.

Varför det finns avvikelser i svarsfrekvensen kan givetvis ha sin grund i flertalet omständigheter. Möjligtvis har man känt sig osäker på vad man ska välja för svar och därför avstått från att svara på frågan eller så har man inte förstått vikten av att faktiskt genomföra enkäten efter bästa förmåga.

De svar som kommit in får bedömas mot bakgrund dels mot ovanstående dels i ljuset av Grefabs kärnuppdrag och verksamhet i stort. Grefab är visserligen ett mindre bolag där största riskområdet är anställdas personuppgifter, däribland känsliga personuppgifter, men Grefab har även ett stort antal kunder i form av medborgare i staden och kranskommuner som bör beaktas vid bedömningen av resultatet.

Utbildningsinsatser

Sammanfattningsvis kan konstateras att samtliga fyra svarande har angett att de fått utbildning från bolaget. Cheferna har därtill angett att denna utbildning sker kontinuerligt vilket är intressant sett utifrån de svar som inkommit från dataskyddskontakten som alltså inte nämner något om kontinuerlig utbildning.

Varför medarbetarna inte upplever att de får kontinuerlig utbildning eller inte får ta del av den eventuella utbildningen som ges till cheferna är omöjligt utifrån resultatet i denna rapport att svara på. Iakttagelsen här blir närmast att samma utbildning bör utsträckas till allra helst samtliga medarbetare på hela bolaget men givetvis framför allt de som behandlar personuppgifter inom ramen för sina arbetsuppgifter.

Personuppgiftsansvaret

75 procent av de som svarade som visste att det är styrelsen som är ansvarig för bolagets personuppgiftsbehandlingar vilket är positivt.

En svarande hade angett att det är de själva som enskilda medarbetare som är ansvarig för bolagets personuppgiftsbehandlingar. Visserligen är man som anställd förpliktad att utföra sina arbetsuppgifter enligt de instruktioner och rutiner som bolaget har, så att man tror att man själv är ansvarig tyder på att man ändå förstår allvaret med att följa dessa instruktioner och rutiner.

Att medarbetare själva känner sig ansvariga får dock inte innebära att de blir oroliga eller rädda för att göra fel (eller flagga för felaktigheter som kan uppstå vid exempelvis personuppgiftsincidenter). Det är upp till bolaget att skapa

förutsättningar för att den enskilde medarbetaren ska kunna göra rätt och känner sig trygg med de behandlingar som ska utföras.

Sammanfattningsvis är det alltså viktigt med ett korrekt utpekat ansvar då dataskyddsarbetet ska genomsyra hela organisationen. Många av de dagliga behandlingarna utförs visserligen av medarbetarna men det måste finnas en förståelse och respekt för dataskyddsfrågorna även hos styrelse och ledningsgrupp så att dataskyddsarbetet får den plats och den tid som krävs.

Identifiering av personuppgifter

Resultatet på dessa frågor visar att anställda behöver få bättre kunskap om vad som är personuppgifter och känsliga personuppgifter. På frågan var det endast en av tre som angett samtliga rätta alternativ vilket är en tämligen låg siffra sett till vilka personuppgifter som var angivna.

Det är visserligen positivt att ingen angett något utav de felaktiga svarsalternativen men det hade varit mer önskvärt att man angett samtliga korrekta svarsalternativ i kombination med något felaktigt snarare än att missa någon av de grundläggande personuppgifter som angavs i frågan.

Gällande de känsliga personuppgifter var det ingen som hade angett samtliga rätta alternativ vilket är en stor brist. Visserligen hade samtliga svarande angett att uppgift om hälsa är en känslig personuppgift men däremot missat medlemskap i fackförening och politiska åsikter. I vart fall uppgift om medlemskap i fackförening bör väl vara något som förekommer inom Grefabs verksamhet.

Sett till bolagets kärnuppdrag och de administrativa arbetsuppgifter som förekommer, kan man dra slutsatsen att bolaget i det dagliga arbetet i princip aldrig ska behandla uppgifter om filosofiska övertygelser. Den bristande kunskapen om att detta är en känslig personuppgift är därför inte att anse som något särskilt riskfyllt.

Att samtliga svarande angav lösenord till dator som en känslig personuppgift kan bero på att man inte vet vad känsliga personuppgifter är enligt förordningen. Det är såklart viktigt att vi skyddar lösenordet till datorn där vi har vår information. Att så många angav detta alternativet som en känslig personuppgift är alltså bra ur ett informationssäkerhetsperspektiv även om detta alternativ var fel på denna fråga.

Identifiering av personuppgiftsbehandlingar

Denna kunskapsfråga får anses som 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 förordningens mening.

Såsom ovan redovisats var det ingen som klarade att ange bara de sex korrekta alternativen på frågan om vad som är en personuppgiftsbehandling. Merparten

hade angett och får antas förstå att när vi lämnar ut personuppgifter, lagrar personuppgifter i molntjänster samt innehar register och listor med personuppgifter är det en personuppgiftsbehandling. Detta tyder på att man ändå har relativt goda kunskaper om vad som är en personuppgiftbehandling.

De svarsalternativ som var rätt men som få trodde var en behandling var de två alternativen som handlade om e-post. Att ta emot, läsa och skicka e-post är en behandling, både om det sker internt eller externt i verksamheten, eftersom e-post i princip alltid innehåller någon form av personuppgift. Exempelvis innehåller som huvudregel e-postadressen vårt för- och efternamn eller så återfinns dessa uppgifter i signaturen i slutet av mailen. Även innehållet i e-posten kan innebära att det sker en behandling av personuppgifter.

Innehållet i e-posten kan innebära olika risker/risknivåer, men som utgångspunkt är det viktigt att ha med sig att läsa och skicka mail är en personuppgiftsbehandling. Rätt var det är skickas känslig e-post till exempelvis fel mottagare eller utan lämpligt skydd (exempelvis kryptering) och har man då inte den grundläggande vetskapen om att det utgör en behandling finns risk för en allvarlig personuppgiftsincident som i värsta fall kan passera utan att lämpliga åtgärder vidtas.

Personuppgiftsincidenter

Att samtliga svarande har angett att de vet hur de ska gå till väga vid en personuppgiftsincident är positivt men för att över huvud taget komma till det stadiet krävs i ett tidigare led att man kan identifiera vad en personuppgiftsincident faktiskt är.

Ingen angav samtliga korrekta alternativ och det var endast en svarande som angav de två första korrekta svarsalternativen gällande att felaktiga behörigheter och glömda papper i skrivare innehållande personuppgifter är personuppgiftsincidenter. Det är oroväckande att inte fler åtminstone angett dessa två alternativ då virusangreppet på datorn får anses utgöra det svåraste svarsalternativet att ange korrekt.

Varför ingen angav att ett virusangrepp utgör en personuppgiftsincident på datorn är svårt att veta. Kanske tror man att detta endast är en säkerhetsincident och inte också en personuppgiftsincident.

Det faktum att så få korrekt kunde identifiera samtliga incidentsscenarier ger anledning för Grefab att tillsätta informations- eller utbildningsinsatser dels gällande vad som anses utgöra en personuppgiftsincident, dels rutinerna kring incidentrapportering.

Personuppgiftsincidenter kan leda till sanktionsavgifter från Datainspektionen och även skadeståndstalan från registrerad. Grefab bör även av denna anledning se över kunskapen hos de anställda gällande personuppgiftsincidenter för att minimera risker för sanktionsavgifter.

3 Analys och sammanfattning

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.