Göteborgs Stad

Utbildning

Granskningsrapport för Renova AB

2020-03-23

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2020-03-13	1.0	Första utkast för påsyn av DSK	Ulrika Fredborg
2020-03-19	2.0	Två förtydliganden efter kommentar från DSK	Ulrika Fredborg
2020-03-23	3.0	Korrekturläsning	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 dataskyddslagstiftningen 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 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 (DSK) och den andra delen var en enkät riktad till medarbetare och chefer.

Dataskyddskontakterna fick frågor om hur utbildning inom dataskyddslagstiftningen har genomförts och eventuellt planeras att genomföras i verksamheten 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 av verksamheten, 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

Renova har tagit del av och genomfört en utbildning som Göteborgs stad har förmedlat i samband med dataskyddsförordningens ikraftträdande och dataskyddskontakterna har även utbildats genom extern utbildning. De medarbetare som ingår i ”incident” och ”begäran om uppgifter”-processerna har utbildats av en extern konsult. Chefer har fått information på ledarforum och styrelsen har informerats.

Bolaget har än så länge inte följt upp den utbildning som har genomförts, men ser att denna granskning kan bli ett första led i en sådan uppföljning. Bolaget planerar även att erbjuda utbildning till de grupper som efterfrågar det, exempelvis ”controllergruppen”.

Bolaget har identifierat vilka delar av organisationen som behöver ha fördjupade kunskaper inom dataskydd och har därefter utbildat dessa efter behov. Dataskyddskontakterna är de som har erhållit den mest fördjupade utbildningen.

Gällande nyanställda finns ett introduktionsschema och finns ett behov av utbildning inom dataskydd ska det ges utrymme i ett sådant schema. Det är närmsta chef som är ansvarig för att det genomförs. Bolaget har för avsikt att även lägga in uppföljningar.

Renova har inte kartlagt framtida utbildningsbehov utöver det som görs genom årliga utvecklingssamtal med samtliga i personalen. På sikt kommer bolaget att ta med denna kartläggning i uppföljningen av dataskyddsarbetet, det vill säga i den förvaltningsmodell som är under utarbetande.

2.1.1 Iakttagelser

Sammanfattningsvis kan konstateras att Renova har genomfört utbildningsinsatser och bolaget har identifierat de grupper som anses behöva utbildningen utifrån de anställdas arbetsuppgifter. Bolaget framstår generellt som att det har en god inställning och förståelse för vikten av att de anställda har adekvat kunskap kring dataskydd.

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 verksamheten.

Det framgår av dataskyddskontakternas svar att chefer har fått information. Dataskyddskontakterna har även förtydligat att samtlig personal som behandlar personuppgifter som ett led i sina arbetsuppgifter har fått utbildning av en extern konsult. Att chefer och styrelse hålls uppdaterade och informerade är vitalt för att dataskyddsarbetet ska tillmätas den betydelse som krävs för att bolaget ska efterleva förordningens krav.

Det är positivt att det i introduktionen till nyanställda finns utrymme för att addera dataskydd som en punkt. Här vilar ett ansvar på chefen att bedöma i vilken utsträckning den nyanställde behöver utbildning. En sådan bedömning görs vid behov i samråd med dataskyddskontakterna. Renova bör göra det obligatoriskt att genomföra en grundläggande utbildning för det fall den nyanställde tillhör en sådan grupp som är identifierad som i behov av kunskap om dataskydd. Det för att ytterligare förstärka dataskyddsarbetets ställning i verksamheten och motverka att bedömningen blir personbunden till en viss chef.

Det framgår av dataskyddskontakternas svar att närmast föreliggande åtgärd är ett införande av uppföljning av dels dataskyddsarbetet i stort, dels hur väl utbildningsinsatser har fallit ut. Resultatet av denna granskning ska förhoppningsvis bidra till att bolaget får en vidare översyn av sin organisations kunskapsnivå.

Sammantaget kan man säga att det således är positivt att bolaget vidtog grundläggande utbildningsåtgärder vid ikraftträdandet av förordningen men då rättsområdet ständigt utvecklas i form av nya avgöranden, vägledningar och tolkningar hade det varit önskvärt att dataskydd var en naturlig del av exempelvis fortbildning inom bolaget och vid introduktion av nyanställda.

2.2 Utbildningsinsatser och kunskapsnivå hos organisationen

Enkätundersökningen har skickats ut per e-post till utvalda anställda som ingår i grupper i verksamheten som DSO tillsammans med dataskyddskontakterna har identifierat som de som framförallt bör ha en grundläggande kunskap om dataskyddslagstiftningen då dessa anställda behandlar personuppgifter i sitt dagliga arbete. Det har inneburit att enkätundersökningen skickades ut till 71 personer i bolaget.

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.

Svarsfrekvensen skiljer sig för respektive fråga då det sannolikt är så att vissa antingen har valt att inte svara på samtliga frågor, dels att en del frågor medgav att man kunde ange flera svarsalternativ som svar. Avvikelser som bedöms inverka på resultatet kommer att kommenteras vid de frågor som berörs.

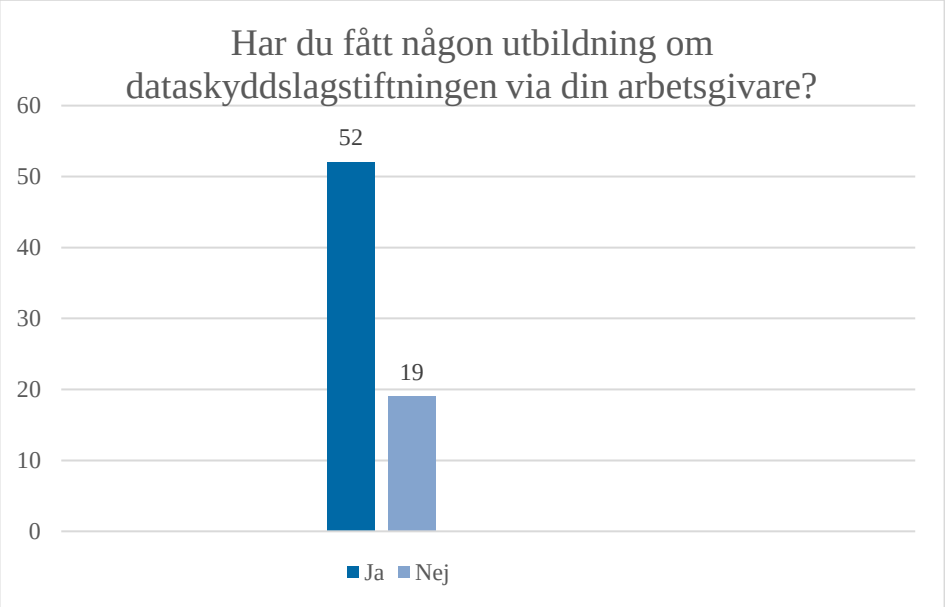
För totala sammanställningen från enkäten hänvisas till bilaga 3.

2.2.1 Svaren avseende utbildningsinsatser

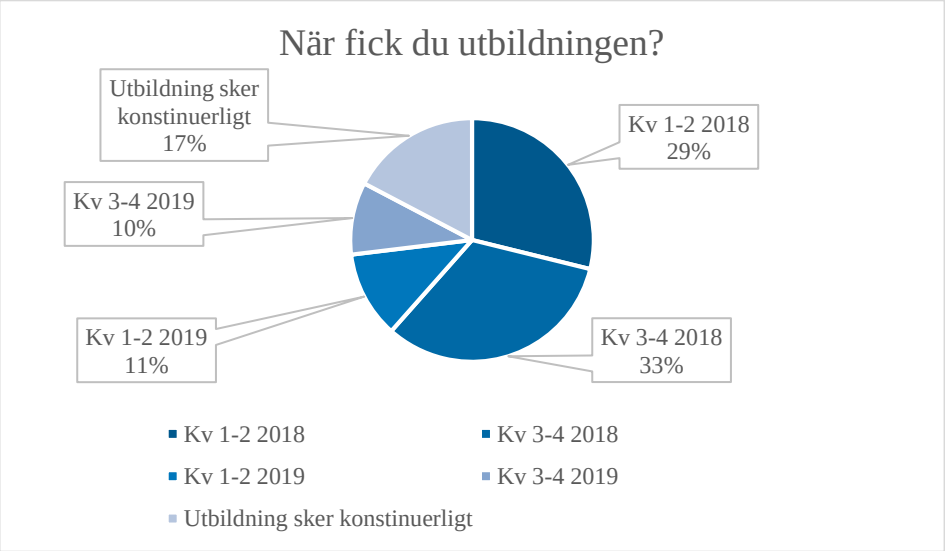
Utbildningsinsatser

På frågan om man har fått någon utbildning om dataskyddslagstiftningen har samtliga 71 tillfrågade svarat på frågan.

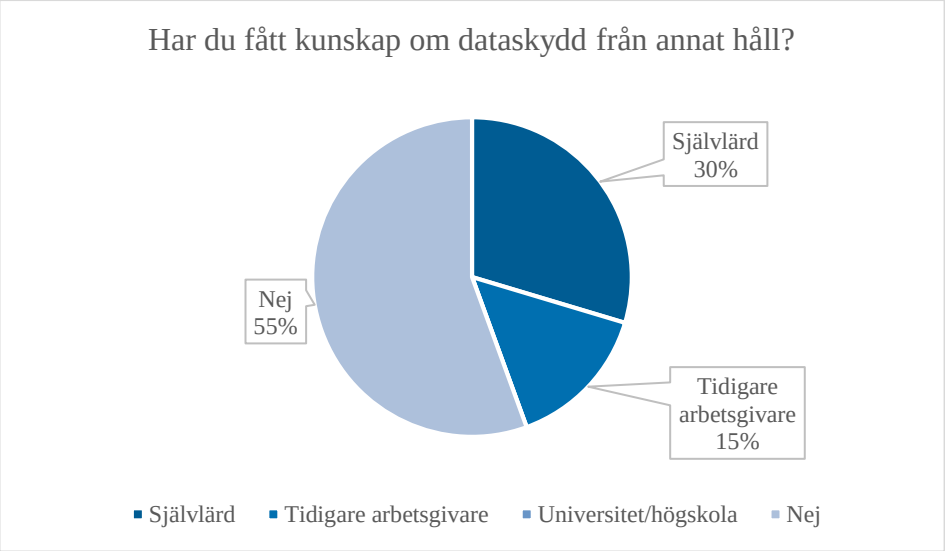
Utifrån nedanstående tabell ser man att cirka 73 procent uppgett att de har fått utbildning och 27 procent har svarat att de inte fått någon utbildning.



Av de inkomna svaren har de flesta, 62 procent, fått utbildning under 2018.



19 personer svarade nej på den inledande frågan om huruvida de erhållit utbildning från arbetsgivare och skulle därmed gå vidare till ”fråga 3 – Hur har du fått kunskap om dataskydd från annat håll?”. Antal svaranden på fråga 3 är dock 26 personer varför det förekommer viss felmarginal i svarsfrekvensen och därmed resultatet av den frågan. Med reservation för ovanstående ser utfallet ut enligt nedan.



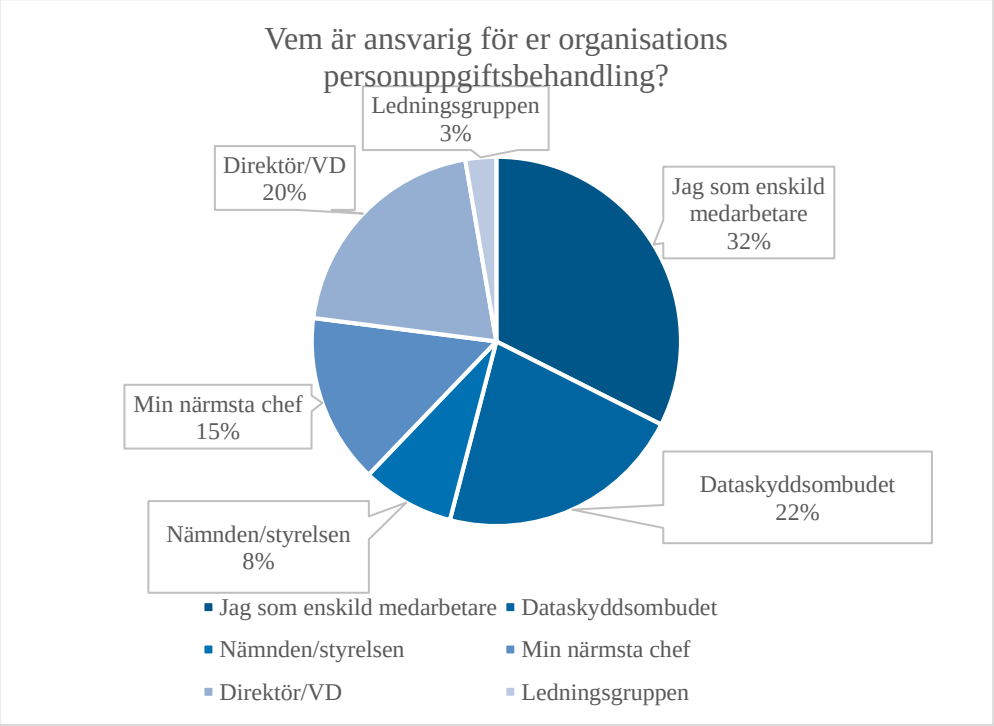
Personuppgiftsincidenter

På frågan om man vet hur man ska gå tillväga vid en personuppgiftsincident svarade samtliga 71 tillfrågade personer varav uppdelningen mellan jakande och nekande svar var relativt jämnt fördelat – 41 ja (ca 58 procent) respektive 30 nej (ca 42 procent).

Personuppgiftsansvaret

På frågan om vem som är ansvarig för organisationens personuppgiftsbehandlingar svarade totalt 65 personer men antalet faktiska svar i underlaget är 74 varför resultatet får bedömas mot bakgrund av det. Bedömer man resultatet mot unika svaranden blir procenttalen alltså något högre.

Det korrekta svaret på frågan är ”Nämnden/styrelsen”. Av diagrammet nedan kan man utläsa att över 30 procent av de svarande har angett att det är dem själva som enskild medarbetare som är ansvariga för organisationens personuppgiftsbehandlingar. Över 20 procent har angett att DSO är ansvarigt för personuppgiftsbehandlingen och nästan lika många har angett ”Direktör/VD”.



2.2.2 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).

Utifrån underlaget kan utläsas att 69 personer har svarat men det går inte att utläsa huruvida någon angett samtliga korrekta alternativ. En avvikelse som är värd att notera är att endast 50 personer av 69 svaranden har korrekt angett namn som en

personuppgift, vilket innebär att nästan 30 procent av någon anledning har missat att ange namn. I övrigt är det väldigt få som 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. Fyra av alternativen var rätt (medlemskap i fackförening, hälsa, filosofisk övertygelse, politiska åsikter) och två var felaktiga (lösenord till dator och mobilnummer). Totalt svarade 68 personer på frågan och för de ”vanligaste” känsliga personuppgifterna såsom medlem i fackförening, hälsa och politiska åsikter låg svarsfrekvensen på cirka 70–95 procent.

Av de felaktiga svarsalternativen svarade närmare 45 procent att ”Lösenord till dator” är 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 dataskyddsförordningen. Av dessa nio angivna alternativen är sex rätt och tre felaktiga. Totalt svarade 60 personer på frågan.

De tre första (korrekta) alternativen som gäller medlemsregister, molntjänster och utlämnande av personuppgifter har en svarsfrekvens på 70 procent respektive cirka 50 procent och 85 procent.

Värt att notera är att endast 25 procent har angett att mail till en kollega (”Anställd A skickar ett mail till Anställd B”) är att betrakta som en behandling och endast 20 procent har korrekt identifierat att läsa ett mail och sedan ta fram ett svar är en behandling. Runt hälften av de svaranden har felaktigt angett att gallring av en personakt avseende en avliden kollega är att betrakta som en behandling.

Personuppgiftsincidenter

På frågan om man vet hur man ska gå tillväga vid en personuppgiftsincident svarade cirka 58 procent 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.

63 personer svarade på frågan och cirka 77 procent respektive 54 procent identifierade korrekt de två första alternativen som en personuppgiftsincident.

Endast 7 svaranden, cirka 11 procent, angav korrekt att svarsalternativet virusangrepp på datorn är en personuppgiftsincident. Värt att notera är att det bara var fyra personer som angav det felaktiga alternativet.

2.2.3 Iakttagelser

Svarsfrekvensen

Varför vissa inte har svarat på alla frågor i enkäten 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 av dels ovanstående dels i ljuset av Renovas kärnuppdrag och verksamhet i stort.

Utbildningsinsatser

Sammanfattningsvis kan konstateras att 73 procent av de som svarade uppgav att de fått någon form av utbildning vilket också innebär att ett flertal inte har fått utbildning.

Det är positivt att lejonparten anser sig ha fått utbildning, men att en dryg fjärdedel av de anställda som ingår i sådan grupp i organisationen att de bör ha grundläggande kunskaper om dataskyddslagstiftningen inte ansett sig ha fått utbildning är problematiskt.

Vad siffrorna beror på är svårt att veta men eventuellt kan det kan bero på att de anställda inte uppfattat att de utbildningsinsatser som hållits varit utbildningar utan kanske sett dessa mer som informationstillfällen. Oavsett anledningen bör bolaget se över hur de kan fånga in även denna fjärdedel så att samtliga som berörs befinner sig på en acceptabel kunskapsnivå.

Att anställda anser sig vara självlärda kan vara både bra och dåligt. Bra om det är så att de faktiskt har fått adekvata kunskaper inom dataskydd genom att självmant läsa på och ta reda på vad som gäller, men dåligt om kunskaperna de erhållit på egen hand är bristfälliga eller kanske rent av felaktiga. Det blir svårt för organisationen att veta vilka kunskaper dessa personer faktiskt har och om de är adekvata då det idag inte finns någon uppföljning med kunskapstester.

Som tidigare påpekats bör utbildningsinsatser vara något som är levande och kontinuerligt då även de som fått utbildning, och särskilt de under 2018, bör få möjlighet att ta del av uppdaterad information eftersom området är så föränderligt. Varje val och bedömning gällande en behandling bidrar till att forma rättsläget varför det är viktigt att hålla sig a jour.

Personuppgiftsansvaret

Endast åtta procent av de svarande angav att det är styrelsen som är ansvarig för bolagets personuppgiftsbehandlingar.

Många hade angett att de själva som enskild medarbetare är ansvariga för organisationens personuppgiftsbehandling. Visserligen är man som anställd förpliktad att utföra sina arbetsuppgifter enligt de instruktioner och rutiner som

bolaget har, så det faktum 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 när det uppstår fel såsom vid 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.

Många hade även angett att det är dataskyddsombudet som är ansvarigt för personuppgiftsbehandlingen. Det kan tolkas som att det finns en föreställning om att det är dataskyddsombudet som, i någon form av ansvarig projektledare, ska driva dataskyddsarbetet framåt.

Ett dataskyddsombud ska enligt förordningen och vägledningar inte agera som projektledare utan närmast som en rådgivare och resurs för bolagets organisation kring dataskydd.

Det är 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.

Att nästan 30 procent inte angett att namn är en personuppgift är oroväckande. Möjligen kan någon eller några förklaras som rena misstag men det går inte att helt bortse från det inkomna resultatet.

Generellt var låg svarsfrekvens på cirka 50-60 procent för de korrekta svarsalternativen sånär som på personnummer där hela 98 procent angett det som en personuppgift.

Sett till de alternativ som angavs i frågan är 50-60 procent en tämligen låg siffra och en indikation på att kunskapsnivån behöver höjas generellt. Det är positivt att väldigt få angav något av de felaktiga alternativen vilken kan vittna om att det ändå finns viss förståelse för vad som bör utgöra en personuppgift eller ej. Kan man identifiera vad som inte är en personuppgift kan man möjligen ”bakvägen” komma fram till vad som faktiskt är en personuppgift, men det bör närmast ses som en klen tröst i sammanhanget.

Gällande de känsliga personuppgifterna ska poängteras att de allra flesta visste att medlemskap i fackförening, hälsa och politiska åsikter är känsliga personuppgifter vilket är positivt och helt i linje med vilka typer av personuppgifter som Renova behandlar, särskilt sett till HR-området.

Sett till bolagets kärnuppdrag och vad normala administrativa arbetsuppgifter består av, kan man dra slutsatsen att bolaget i det dagliga arbetet i princip aldrig kommer att behandla uppgifter om filosofiska övertygelser. Den bristande kunskapen kring att filosofisk övertygelse är att anse som en känslig personuppgift medför alltså inte en överhängande risk för verksamheten.

Att dryga 40 procent angav lösenord till dator som en känslig personuppgift kan bero på att man inte vet vad känsliga personuppgifter är enligt förordningens mening, men kan också bero på att man har en personlig inställning till vad som är känsligt och inte.

Det är såklart viktigt att vi skyddar lösenordet till datorn där vi har vår information och att så många angav detta alternativ som en känslig personuppgift är bra ur ett informationssäkerhetsperspektiv även om är ett inkorrekt svar på 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 förordningen.

Det var relativt många som prickade in flera av de korrekta alternativen. De flesta förstod att när vi lämnar ut personuppgifter, lagrar personuppgifter i molntjänster och innehar register och listor med personuppgifter är det en behandling. Detta tyder på att man 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.

Det felaktiga svarsalternativ som stack ut var alternativet där verksamhet Z glömt gallra en personakt gällande en avliden kollega. Dataskyddsförordningen är inte tillämplig på avlidna personer varför detta var ett felaktigt svarsalternativ. Att gallra personuppgifter på en fysisk levande person är en personuppgiftsbehandling så även om man missat att avlidna personer undantas

från förordningen så kan man ändå anse att det är positivt att många angett att detta är en personuppgiftsbehandling.

Personuppgiftsincidenter

Att 42 procent av svaranden har angett att de inte vet hur de ska gå till väga vid en personuppgiftsincident är anmärkningsvärt och här behövs informations- eller utbildningsinsatser genomföras gällande rutinerna.

De flesta verkar ha kännedom om att felaktiga behörigheter samt glömda papper i skrivare innehållande personuppgifter är att ses som personuppgiftsincidenter (cirka 78 respektive 54 procent). Varför endast ett fåtal angett svarsalternativet virusangrepp 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 och att det fortsatt finns en betydande andel som inte vet hur de ska gå till väga vid en incident ger anledning för Renova 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 en registrerad. Renova bör även av denna anledning se över kunskapen hos de anställda gällande personuppgiftsincidenter för att minimera risker för sanktionsavgifter.

3 Analys och sammanfattning

Närmare en tredjedel av de som svarat på enkäten har angett att de inte fått någon utbildning av bolaget. Resultatet på många av kunskapsfrågorna visar 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 vad som utgör känsliga personuppgifter.

Därtill bör organisationen utbilda och öva på personuppgiftsincidenter. 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 organisationen ska efterleva kraven enligt förordningen och minimera riskerna för eventuella beslut om sanktionsavgifter.