Göteborgs Stad

Rutiner vid personuppgiftsincidenter

Granskningsrapport för Gryaab

2020-12-21

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2020-12-01	1	Utkast för granskning av DSK	Andréa Bergqvist
2020-12-21	2	Rapport åtgärdad efter kommentarer från DSK	Andréa Bergqvist

Innehåll

1 Inledning

1.1 Bakgrund

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Personuppgiftsansvariga verksamheter och personuppgiftsbiträden ska sträva efter att arbeta medvetet och proaktivt för att undvika personuppgiftsincidenter. Ansvarsskyldigheten i artikel 5.2 dataskyddsförordningen ålägger den personuppgiftsansvarige verksamheten att se till att de personuppgifter som behandlas inom ramen för verksamheten utförs i enlighet med dataskyddsförordningens bestämmelser. Inom Göteborgs stad är det varje enskild nämnd eller bolagsstyrelse som är personuppgiftsansvarig och således ansvarig för att verksamheten har god och regelriktig följsamhet mot dataskyddsförordningen.

Det är av stor vikt att verksamheten i god tid har skapat tydliga rutiner för att upptäcka personuppgiftsincidenter. En komplett och metodisk handlingsplan ska ha upprättats för de fall en personuppgiftsincident inträffar så att verksamheten snabbt kan och vet hur den ska agera. De uppmuntras därför att i god tid planera och införa processer för att skyndsamt kunna begränsa en incident, bedöma riskerna för enskilda och därefter avgöra om det är nödvändigt att anmäla incidenten till tillsynsmyndigheten. Vid behov ska även den drabbade registrerade informeras om inträffad incident. Anmälan till tillsynsmyndigheten bör utgöra en del av incidenthanteringsplanen.

Den övergripande och viktigaste uppgiften för stadens dataskyddsombud är att övervaka att personuppgiftsansvariga förvaltningar och bolag följer dataskyddsförordningen. Det innebär bland annat att dataskyddsombudet samlar in information om hur organisationen behandlar personuppgifter, kontrollerar att organisationen följer bestämmelser och interna styrdokument samt att dataskyddsombudet informerar och ger rådgivning om dataskyddsfrågor. Som ett led i detta arbete kommer därför periodiska granskningar och uppföljningar att genomföras. En grundläggande förutsättning för att detta ska vara möjligt är att den personuppgiftsansvarige bedriver ett eget förbättringsarbete inom dataskydd som kan granskas och följas upp. Vad gäller personuppgiftsincidenter ska den personuppgiftsansvarige verksamheten omedelbart efter inträffandet av en personuppgiftsincident eller annan incident kontakta dataskyddsombudet för att konsultera tillvägagångssätt, enligt Artikel 29-arbetsgruppen för skydd av personuppgifter och dess vägledning gällande ”Riktlinjer om dataskyddsombud”.

1.2 Granskningens utförande

1.2.1 Granskningsområdet

Granskningsområdet för denna rapport är verksamhetens rutiner och processer för personuppgiftsincidenter.

1.2.2 Syfte

Granskningens syfte är att säkerställa att verksamheten har arbetat med att ta fram fungerande rutiner för hanteringen av personuppgiftsincidenter, att personalen inom verksamheten är väl insatta i hur de ska agera vid inträffad incident och att verksamheten vid en inträffad incident är införstådd med de skyldigheter som åligger dem enligt dataskyddsförordningen. Syftet är också att se över vilka delar av rutinen som kräver förbättringsarbete framgent.

1.2.3 Tillvägagångssätt

Granskningen utförs i form av en skrivbordstillsyn där den personuppgiftsansvarige verksamheten har beretts tillfälle att inkomma med all nödvändig dokumentation som rör hanteringen av personuppgiftsincidenter. Metoden består av att dokumentgranska verksamhetens rutiner, processer och handlingsplan, samt att genom ett frågeställningsutskick få svar på ett antal grundläggande frågor som rör verksamhetens rutiner vid personuppgiftsincidenter.

1.2.4 Bilagor

Bilaga 1	Information om granskningen
Bilaga 2	Frågeställningsutskick
Bilaga 3	Säkerhetshandbok innehållandes rutiner vid personuppgiftsincidenter
Bilaga 4	Handlingsplan utbildningsinsatser
Bilaga 5	Personuppgiftsincidentregister

2 Tillämplig lagstiftning

2.1 Definitionen av en personuppgiftsincident

Det är viktigt att den personuppgiftsansvarige verksamheten kan fastställa vad en personuppgiftsincident är. Enligt artikel 4.12 dataskyddsförordningen definieras en personuppgiftsincident på följande sätt:

”En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Enligt dataskyddsförordningen har en personuppgiftsincident inträffat om personuppgifter på ett oavsiktligt eller olagligt sätt har förstörts, förlorats, ändrats eller röjts till någon obehörig. Det är varje personuppgiftsansvariges skyldighet att dels kunna identifiera en incident, dels agera korrekt och lagenligt när detta inträffar.

2.2 Den personuppgiftsansvariges skyldigheter

2.2.1 Ansvarsskyldighet

Den personuppgiftsansvarige verksamhetens ansvarsskyldighet regleras i artikel 5.2 och artikel 24 dataskyddsförordningen. Det är inte längre tillräckligt att enbart följa lagen utan den som är ansvarig för personuppgiftsbehandlingen måste också kunna visa hur och på vilket sätt man följer bestämmelserna i dataskyddsförordningen, bland annat genom att beakta risker för fysiska personers rättigheter och friheter. Detta kan verksamheten göra genom att visa att det finns tydliga rutiner för personuppgiftsincidenter, en upprättad handlingsplan samt dokumentation av samtliga inträffade incidenter. Dessa ska kontinuerligt ses över och uppdateras vid behov.

Dataskyddsförordningen ställer krav på att personuppgifter, med användning av lämpliga tekniska och organisatoriska åtgärder, ska behandlas på ett sätt som säkerställer kvalificerad säkerhet för personuppgifterna. Dessutom måste alla lämpliga tekniska skyddsåtgärder och organisatoriska åtgärder ha vidtagits för att omedelbart fastställa om en incident har ägt rum för att därefter kunna avgöra om rapporteringsskyldigheten ska fullgöras, enligt beaktandeskäl 87 i dataskyddsförordningen.

2.2.2 Rapporteringsskyldighet

Enligt artikel 33 dataskyddsförordningen ska den personuppgiftsansvarige utan onödigt dröjsmål inte senare än 72 timmar efter att ha fått vetskap om personuppgiftsincidenten, anmäla den till Datainspektionen i enlighet med ansvarsprincipen, såvida det inte är osannolikt att incidenten medför ***en risk*** för fysiska personers rättigheter och friheter. Den personuppgiftsansvarige ska därmed undersöka incidentens allvarlighet och väsentlighet. Det är omständigheterna i det enskilda fallet som avgör huruvida det är nödvändigt att anmäla incidenten till tillsynsmyndigheten och underrätta de personer som påverkas. Den personuppgiftsansvarige måste bedöma sannolikheten för i vilken grad den uppkomna incidenten påverkar fysiska personers rättigheter och friheter.

De konsekvenser som kan uppstå är fysisk, materiell eller immateriell skada enligt beaktandeskäl 85 i dataskyddsförordningen. Det kan exempelvis handla

om identitetsstöld, ekonomisk förlust och diskriminering. Datainspektionen kan utöva sina tillsynsbefogenheter för att se till att den personuppgiftsansvarige de facto har vidtagit lämpliga och nödvändiga åtgärder.

2.2.3 Informationsplikt

Den personuppgiftsansvarige verksamheten har en informationsplikt gentemot den registrerade så att den enskilde kan vidta nödvändiga försiktighetsåtgärder. Informationsplikten gäller när en personuppgiftsincident sannolikt kommer att medföra ***en hög risk*** för den registrerades rättigheter och friheter, enligt artikel 34 och skäl 86 i dataskyddsförordningen. Personuppgiftsansvarig ska i underrättelsen beskriva incidentens art samt ge en rekommendation till den drabbade om hur de potentiellt negativa effekterna kan mildras. Underrättelsen ska ske så snart det rimligtvis är möjligt.

2.2.4 Dokumentationsskyldigheten

Den personuppgiftsansvarige verksamheten har en skyldighet enligt artikel 33.5 dataskyddsförordningen att dokumentera samtliga inträffade incidenter oavsett risknivå. Dokumentationsskyldigheten är kopplad till ansvarsskyldigheten i artikel 5.2 i dataskyddsförordningen, som innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna för dataskydd efterlevs. Dokumentationen ska också innefatta omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska kunna uppvisas till tillsynsmyndigheten vid en eventuell granskning för kontroll av efterlevnad av artikel 33 i dataskyddsförordningen. En förutsättning för att tillsynsmyndigheten ska kunna följa upp en personuppgiftsincident baserat på dokumentation är att den är samlad och ger en rättvisande bild av händelseförloppet.

2.3 Konsekvenser om kraven inte efterlevs

Tillsynsmyndigheten kan besluta att en verksamhet som bryter mot reglerna i dataskyddsförordningen ska betala en administrativ sanktionsavgift. I Sverige uppgår sanktionsavgiften för myndigheter till högst 10 miljoner kronor för allvarligare överträdelser och högst 5 miljoner kronor för mindre allvarliga överträdelser. För företag är den högsta avgiften 20 miljoner euro eller fyra procent av bolagets globala årsomsättning. Sanktionsavgiftens storlek baseras på vilken bestämmelse som överträdelsen gäller samt på omständigheter i det enskilda fallet. De faktorer som avgör allvarlighetsgraden av överträdelsen är hur stor skada som har skett, om det är fråga om känsliga personuppgifter och om överträdelsen är avsiktlig. Tillsynsmyndigheten ska enligt artikel 83 i dataskyddsförordningen se till att sanktionsavgiften är effektiv, proportionerlig och avskräckande, vilket medför att verksamhetens storlek har betydelse vid bedömningen.

Om den personuppgiftsansvarige har behandlat den enskildes personuppgifter i strid med dataskyddsförordningen på ett sätt som har orsakat materiell eller immateriell skada, kan den enskilde väcka skadeståndstalan i allmän domstol för att begära ersättning. Vad som utgör ett skäligt skadeståndsanspråk baseras på vägledning från förarbeten till motsvarande bestämmelse i den tidigare gällande personuppgiftslagen och den rättspraxis som utvecklats kring den (se SOU 2017:39 s. 304 och rättsfallet NJA 2013 s. 1046).

3 Granskning av verksamheten

3.1 Verksamhetens rutiner vid personuppgiftsincidenter

Gryaab har redogjort för hur verksamheten hanterar personuppgiftsincidenter genom att bifoga organisationens rutiner vid personuppgiftsincidenter som finns i bolagets säkerhetshandbok, bolagets handlingsplan avseende utbildningsinsatser, andra relevanta dokument samt givit en kort beskrivning i frågeutskicket hur rutinerna ser ut.

Bolagets rutiner för personuppgiftsincidenter upprättades den 31: a maj 2018 i säkerhetshandboken. Målgruppen är anställda inom Gryaab. Av säkerhetshandboken framgår det att bolagets dataskyddsgrupp ansvarar för att både rutiner och personal hålls uppdaterade i frågor som rör personuppgiftsincidenter. Vidare har bolaget i rutinen fastställt när och hur en anmälan om personuppgiftsincident ska ske genom en tydlig beskrivning. Vid en inträffad intern incident ska en anmälan göras i bolagets system ENIA genom att man skapar en avvikelse. Vid inträffad extern incident ska leverantörer med flera kontakta bolaget via info@gryaab.se. Anmälan hanteras därefter av bolagets dataskyddsgrupp som gör en bedömning av personuppgiftsincidentens allvarlighetsgrad.

3.1.1 Identifiering av en incident

Vid inträffad incident är det av stor vikt att bolaget har en utbildad personalstyrka som har kompetens nog att kunna identifiera en personuppgiftsincident. Gryaab har i frågeutskicket svarat att samtliga anställda vid ikraftträdandet av dataskyddsförordningen maj 2018 har fått information om förändringarna som förordningen innebär. Gryaab har vidare svarat att information om personuppgiftsincidenter och hanteringen av dessa återfinns i organisationens verksamhetsbok. Vidare planerar Gryaab att hålla regelbundna webbutbildningar för personal som hanterar personuppgifter på regelbunden basis. Dataskyddsombudet har fått ta del av bolagets handlingsplan som rör utbildningsinsatser och där ett särskilt avsnitt berör utbildning inom personuppgiftsincidenter.

3.1.1.1 Analys

I bolagets säkerhetshandbok definieras och exemplifieras vad en personuppgiftsincident är. I rutinerna framgår det tydligt när och hur en anmälan ska göras vid en inträffad incident. Bolaget tydliggör också vikten av att anmälan ska göras omedelbart, vilket dataskyddsombudet ser som mycket positivt. Säkerhetshandboken finns tillgänglig för alla medarbetare och det informeras regelbundet om den. Det hänvisas till den både på möten, via intranät och liknande. Även vid nyanställning informeras arbetstagaren om handboken. Viss viktig information finns också tillgänglig på verksamhetens intranät. Det är positivt att medarbetarna regelbundet hålls informeras om rutinen. Gryaab har också angett i frågeutskicket att personalen i maj 2018 har fått information om den nya förordningen.

Gryaab har bifogat bolagets handlingsplan som rör utbildningsinsatser framgent där ett kort avsnitt handlar om personuppgiftsincidenter. Dataskyddsombudet ser det som positivt att bolaget planerar att göra insatser för att stärka personalens kompetens gällande personuppgiftsincidenter. Att personalen har kompetens om dataskyddsfrågor är grundläggande för att de ska kunna hantera uppkomna incidenter. Gryaab har i sin handlingsplan identifierat vissa befattningar som särskilt jobbar med personuppgifter där det är av stor vikt att utbildning sker. Dataskyddsombudet anser att det är positivt att bolaget gjort en handlingsplan där överblick och uppföljning av medarbetarnas kunskap är möjlig.

Det är också av stor vikt att dataskyddsgruppen som hanterar och gör bedömningen av inträffade personuppgiftsincidenter blir informerade i god tid. Av återkopplingen från bolaget framgår det att ansvariga får en direkt notifiering vid en anmälan som görs i systemet. Notisen skickas som e-post direkt när anmälan görs i systemet. Leverantörer och personuppgiftsbiträden instrueras dessutom att använda sig av bolagets info-mail för notifiering och anmälan av en personuppgiftsincident till bolaget, vilket dataskyddsombudet ställer sig kritisk till. Eftersom tidsaspekten vid en inträffad personuppgiftsincident är av stor vikt bör dessa kontakter rimligtvis ske direkt och per telefon för att därefter dokumenteras, detta för att den personuppgiftsansvarige ska undvika en alltför utdragen process som i sin tur kan leda till dels en högre risk för den enskildes fri- och rättigheter, dels en större risk att inte kunna uppfylla sin rapporteringsskyldighet inom 72 timmar till tillsynsmyndigheten. Bolaget bör därför uppdatera sina rutiner gällande personuppgiftsbiträdets skyldighet att informera bolaget om uppkomna incidenter. Hur personuppgiftsincidenter ska hanteras i biträdessituationer bör också framgå tydligt i aktuella personuppgiftsbiträdesavtal.

3.1.2 Anmälan av en incident till tillsynsmyndigheten

Gryaab har i frågeutskicket svarat att de bedömer riskerna för enskilda personer som har drabbats av en personuppgiftsincident baserat på typ av incident, personuppgifternas natur, känslighet och volym. Vidare har Gryaab svarat att vid bedömningen av när en incident ska rapporteras till Datainspektionen så

beaktar de huruvida incidenten berör en stor mängd personer, om känsliga uppgifter röjs eller om de anser att det finns andra faktorer som innebär en hög risk. Bolaget har också i sin säkerhetshandbok stadgat att incidenter som medför en risk för fysiska personers rättigheter och friheter ska anmälas till tillsynsmyndigheten inom 72 timmar från det att den upptäcks. Gryaab har angett att det är dataskyddsgruppen bestående av personer från IT, HR och registratur som är utsedda för att ansvara för personuppgiftsincidenter. Det saknas information i rutinen om när dataskyddsombudet ska meddelas.

3.1.2.1 Analys

Det är positivt att Gryaab i sin säkerhetshandbok har stadgat *när* rapporteringsskyldigheten de facto är ett krav, något som är viktigt att ha kännedom om. Bolaget har övergripande beskrivit de kriterier de använder sig av vid bedömningen kring huruvida det rör sig om personuppgiftsincident som omfattas av deras rapporteringsskyldighet. Det räcker med att incidenten utgör en risk för den enskildes rättigheter och friheter för att den personuppgiftsansvariges rapporteringsskyldighet ska inträda. Genom att ha regelbunden utbildning för personalen minskar bolaget risken för att personalen inte kan identifiera en incident. Däremot saknas det information om hur bolaget avgör om risk föreligger. Gryaab har kompletterat granskningen med deras rutiner för övrig riskbedömning, i förhållande till tex hälsa och miljö, men inte hur denna ska kunna användas för att avgöra risk ur dataskyddsförordningens mening. Dataskyddsombudet rekommenderar att bolaget ser över sina rutiner för riskbedömning i hänseende till personuppgiftsincidenter.

Vid frågan om vem som är kontaktperson gentemot tillsynsmyndigheten vid inträffad personuppgiftsincident bör Gryaab förtydliga att det är dem som personuppgiftsansvariga som är kontaktpersoner och således även skyldiga att informera tillsynsmyndigheten när deras rapporteringsskyldighet aktualiseras. Gryaab har inom bolaget utsett gruppchefen för AIT som är ansvarig kontaktperson för detta ändamål. Att bolaget anger att det finns en utsedd kontaktperson som sköter dialogen med tillsynsmyndigheten vid inträffade incidenter är positivt men också något som bör fastställas i verksamhetens rutiner. Gryaab bör också förtydliga att dataskyddsombudet ska kontaktas omedelbart vid misstanke om inträffad incident för rådgivning och stöttning kring hanteringen av personuppgiftsincidenten. Dataskyddsombudet finns också tillgänglig i de fall tillsynsmyndigheten eller de registrerade vill kontakta denna.

3.1.3 Information och vägledning till den registrerade

Gryaab har kortfattat angett att de bedömer riskerna för den enskilde som har drabbats av en personuppgiftsincident baserat på typ av incident, personuppgifternas natur, känslighet och volym.

3.1.3.1 Analys

Dataskyddsombudet gör bedömningen utifrån bolagets inkomna svar och dokument att det i dagsläget inte finns någon fastställd rutin för att hantera

informationsplikten gentemot den registrerade. De registrerade ska som huvudregel informeras om det är sannolikt att hör risk föreligger. Bolaget behöver således rutiner för att uppfylla sin informationsplikt gentemot den som utsätts för en personuppgiftsincident. Däri behöver bolaget för egen del tydliggöra hur de gör bedömningen utifrån dataskyddsförordningens rekvisit **hög** risk för den enskildes friheter och rättigheter. De kriterier som anges i svarsformuläret är ett tecken på att bolaget är på god väg för att kunna göra en korrekt riskbedömning. En bedömning måste göras av allvarligheten av faktisk eller potentiell påverkan på människors fri-och rättigheter och sannolikheten för att de inträffar. Frågor som kan ställas för att bedöma risken är till exempel: Hur allvarliga kan konsekvenserna bli? Hur sannolikt är det att enskilda drabbas? Om personuppgiftsincidenten är allvarlig är risken högre, likaså är risken också högre om sannolikheten för konsekvenser är stor.

Information till de registrerade krävs inte om något av undantagen i artikel 34.3 föreligger. Det handlar om att den personuppgiftsansvarige antingen:

- Har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som kan göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till uppgifterna, såsom kryptering,
- Har vidtagit ytterligare åtgärder som säkerställer att den höga risk för de registrerades rättigheter och friheter som avses inte längre kommer att uppstå, eller
- Att det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

Gryaab bör också förtydliga i rutinen att de registrerade ska meddelas utan onödigt dröjsmål vid en inträffad incident samt vilken information som ska lämnas. Enligt Dataskyddsförordningen artikel 34.2 finns det minimikrav för vilken information den personuppgiftsansvarige är skyldig att ge den registrerade:

- Beskriv orsaken till incidenten
- Namn och kontaktuppgifter till dataskyddsombudet eller annan kontakt
- Beskriv de sannolika konsekvenserna av incidenten
- Beskriv vad ni gjort, eller tänkt göra för att hantera konsekvenserna
- Beskriv vad ni har gjort för att mildra eventuella negativa konsekvenser

3.1.4 Dokumentation av incidenter

Gryaab anger att samtliga personuppgiftsincidenter har dokumenterats. Bolaget har också bifogat dokumentregister i form av ett Excel-ark där dessa incidenter har bokförts. Vissa incidenter dokumenteras mer utförligt i systemet.

3.1.4.1 Analys

Tillsynsmyndigheten ställer högra krav på dokumentationen vid en inträffad personuppgiftsincident. Därför är det positivt att Gryaab dokumenterar alla incidenter, även de som inte anmäls till tillsynsmyndigheten, och att bolaget har ett register där de bokförs. Gryaab har bifogat det Excel-ark där alla incidenter dokumenteras. I Excel-arket antecknas datum, vad som hänt, bedömning/åtgärd samt källa där incidenten dokumenteras utförligare. Eftersom dataskyddsombudet inte har åtkomst till systemet där incidenterna registreras, kan ingen bedömning göras om den dokumentation som sker där uppfyller alla krav i förordningen. Enligt dataskyddsförordningen ska den personuppgiftsansvarige dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Gryaab bör se över och säkerställa så att dokumentationen i systemet uppfyller de nämnda kraven.

3.2 Iakttagelser och risker

Inför granskningen har dataskyddsombudet efterfrågat allt underlag och dokumentation som verksamheten har avseende rutiner för personuppgiftsincidenter. Dataskyddsombudet har också efterfrågat detaljerade beskrivningar och svar i det frågeställningsutskick som har sänts ut till verksamheten. Bolaget har återkopplat med kortfattade svar i frågeställningen men inkommit med flera handlingar som underlag, vilket har underlättat för dataskyddsombudet att granska bolagets personuppgiftsincidenthantering.

Det är positivt att Gryaab har en säkerhetshandbok avseende rutiner för personuppgiftsincidenter. Det tyder på att bolaget har börjat arbeta aktivt med den här frågan och tar frågan på allvar. Det är vidare positivt att all personal informeras om rutinen och att bolaget initierat en utbildning av personalen.

3.3 Rekommendationer

Rutinerna behöver kompletteras ytterligare med hänsyn till den korta tidsfrist som dataskyddsförordningen medger vid en inträffad incident. Bolaget bör fundera på hur informationen om en inträffad incident från de som upptäcker incidenten, på ett mer skyndsamt sätt kan nå fram till de som ansvarar för bedömningen av en personuppgiftsincident. För detta krävs att personalen har kompetens nog att kunna identifiera en uppkommen personuppgiftsincident varför utbildningsinsatser inom det angivna området är direkt avgörande. Bolaget behöver även se över rutinerna kring hur personuppgiftsbiträden sköter kommunikationen med dem som personuppgiftsansvariga och att det vid inträffade incidenter anmäls till bolaget ett skyndsamt sätt.

Vidare behöver rutinerna förtydligas kring hur de olika bedömningarna ska genomföras med hänsyn till personuppgiftsansvariges ansvarsskyldighet som även innefattar rapporteringsskyldigheten och informationsplikten. Bolaget kan se över hur de kan använda det material de redan har för riskbedömning inom

andra områden och applicera det på personuppgiftsincidenthanteringen, eller ta fram en ny, fristående rutin för riskbedömning i detta hänseende.

De registrerade ska informeras om hög risk föreligger samt utan onödigt dröjsmål. Bolaget bör också se till så att informationen som ges till de registrerade följer minimikraven i förordningen. Det finns också behov av att se över dokumentationsskyldigheten så att den överensstämmer med vad dataskyddsförordningen kräver av en personuppgiftsansvarig verksamhet.

4 Sammanfattning

Dataskyddsförordningen innehåller korta tidsfrister när det kommer till personuppgiftsincidenter. När en incident inträffar är det därför viktigt att den personuppgiftsansvarige agerar snabbt och korrekt. I ett sådant läge är det viktigt att samtliga inblandade vet hur de ska gå tillväga och vad som behöver göras, vilket säkerställs genom tydliga rutiner och utbildning. Vid en eventuell tillsyn kommer bristfälliga rutiner att anses vara uppsåtliga och därmed föranleda till sanktionsavgifter. Personuppgiftsansvarige behöver också se till att vidta åtgärder för att skyndsamt bli informerade av både personal och personuppgiftsbiträden som får kännedom om en inträffad incident. Detta kan göras genom kompetensutveckling och tydligt upprättade rutiner som är lättillgängliga och som berörda parter har god kännedom om.