Göteborgs Stad

Rutiner vid personuppgiftsincidenter

Granskningsrapport för Boplats Göteborg AB

2020-12-14

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2020-12-01	1	Utkast för granskning av DSK	Andréa Bergqvist
2020-12-14	2	Slutgiltig version 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 komma 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 med svar ifrån verksamheten
Bilaga 3	Rutin vid personuppgiftsincidenter

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 Tillsynsmyndigheten 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. Tillsynsmyndigheten 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 bolag 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

Boplats har redogjort för hur verksamheten hanterar personuppgiftsincidenter genom att dels besvara frågeutskicket, dels hänvisa till den fastställda rutinen för personuppgiftsincidenter. Boplats har också bifogat tillhörande relevanta dokument samt register med inträffade personuppgiftsincidenter. Rutinen skapades 2019-04-18 och uppdaterades 2020-09-02.

Målgruppen för rutinen är de anställda i Boplats verksamhet. Alla anställda är ansvariga för att rapportera misstänkta personuppgiftsincidenter enligt handlingsplanen. Rutinen beskriver två tillvägagångssätt – ett för när Boplats är personuppgiftsbiträde och ett när Boplats är personuppgiftsansvariga.

När Boplats är personuppgiftsbiträde för behandlingen ska den som är personuppgiftsansvarig enligt personuppgiftsbiträdesavtalet kontaktas. Personuppgiftsansvarige tar över ansvaret för incidenthantering och Boplats är enbart behjälpliga vid behov.

När Boplats är personuppgiftsansvariga finns en handlingsplan framtagen för hur personuppgiftsincidenter ska hanteras. Handlingsplanen följer en ordning där varje steg säkrar hanteringen av incidenten. En incidentkoordinator utses av IT-chefen för att se till att arbetet löper vidare. Därefter informeras säkerhetsansvarig, strategisk kommunikatör, VD samt dataskyddsombudet om det inträffade. De olika stegen – informera, stoppa incidenten, säkra spårbarhet, bedöma allvarlighetsgrad, dokumentera, meddela tillsynsmyndigheten samt meddela de registrerade följer i kronologisk ordning.

3.1.1 Identifiering av en incident

Vid inträffande av en incident är det av stor vikt att personalstyrkan har tillräckligt med kompetens för att kunna identifiera en personuppgiftsincident. Boplats har i frågeutskicket svarat att utbildning har skett på personalmöte och att de har efterfrågat vidare utbildning ifrån sitt dataskyddsombud under hösten 2020. Bolaget förtydligar i sin rutin att det är viktigt att de som har kontakt med bostadssökande och allmänheten ska vara särskilt uppmärksam på de kommunikationskanaler som Boplats använder sig av.

I sin rutin ger bolaget också exempel på incidenter som är specifika för Boplats för att förtydliga vad det kan handla om för situationer.

3.1.1.1 Analys

Bolaget har en tydlig rutin med handlingsplan för hur en personuppgiftsincident ska hanteras vilket dataskyddsombudet anser vara positivt. Rutinen beskriver tydligt tillvägagångssätt och ansvar, hur dokumentation sker och när meddelande till tillsynsmyndigheten respektive registrerade ska ske.

Handlingsplanen beskriver både situationen när Boplats är personuppgiftsansvarig men också när Boplats är personuppgiftsbiträde. Det är även viktigt i biträdessituationer att incidenter anmäls så fort man får vetskap om dem, varför det är positivt att bolaget har förtydligat att personuppgiftsansvarige ska meddelas när en biträdessituation föreligger. Det ska också vara tydligt i de aktuella personuppgiftsbiträdesavtalen vilket ansvar som föreligger vid inträffande av en incident.

Det saknas information om hur rutinen förmedlas till personalen och hur den uppdateras. Det framkommer att utbildning har skett på personalmöte för att personalen ska kunna hantera incidenter. I revisionshistoriken framkommer att rutinen reviderats 2020, men inte om eventuella ändringar har kommunicerats till personalen. Att rutinen är reviderad tyder på att den ses över, men det måste också kommuniceras ut i alla led om eventuella ändringar och förbättringar.

Huruvida nyanställda får information om rutinen och hur de får utbildning gällande personuppgiftsincidenter framkommer inte heller i det material som Boplats presenterat. Det är personalen som är i första ledet för att upptäcka personuppgiftsincidenter och måste ha tillräckligt med kunskap för att kunna identifiera personuppgiftsincidenter, för att därefter kunna informera rätt person. Därför är det av vikt att bolaget ser till att personalen utbildas kontinuerligt och att rutinen både ses över och kommuniceras ut. Att ha verksamhetsspecifika exempel på personuppgiftsincidenter i rutinen är positivt, då det förtydligar för personalen vilka situationer det kan handla om.

Efter samråd mellan dataskyddsombudet och bolaget genomfördes en grundläggande utbildning i dataskydd för personalen på Boplats i oktober 2020. Det är positivt att Boplats har identifierat ett utbildningsbehov och efterfrågat detta av dataskyddsombudet. Kunskap inom dataskydd och personuppgiftshantering bör uppdateras kontinuerligt hos alla berörda inom verksamheten.

3.1.2 Anmälan av en incident till tillsynsmyndigheten

Boplats har angett i frågeutskicket att de bedömer huruvida tillsynsmyndigheten ska meddelas vid en personuppgiftsincident, om det är troligt att incidenten kommer att medföra en risk för de registrerades rättigheter. Risken bedöms utifrån Boplats informationsklassning, Boplats riktlinje för informationssäkerhet samt Boplats rutin för incidenthantering.

I rutinen anges också att en personuppgiftsincident ska anmälas snarast, senast inom 72 timmar. En anmälan kan kompletteras i efterhand.

Det framkommer tydligt i underlaget och rutinen att olika personer har olika ansvarsområden. IT-chefen utser en incidentkoordinator som ska ha kontakt med tillsynsmyndigheten. Vd:n ska hållas informerad och fattar avgörande beslut om möjligt.

3.1.2.1 Analys

Att Boplats har uppgett att tillsynsmyndigheten ska meddelas när det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerades rättigheter är korrekt och positivt att det framkommer tydligt i rutinen. Det visar på att Boplats är medvetna om när det föreligger rapporteringsskyldighet för bolaget.

Boplats anger att det finns flera underlag att ta till hjälp för att avgöra huruvida en risk för de registrerade föreligger, vilket är positivt. Dataskyddsombudet har också fått ta del av dessa dokument. Att Boplats gör bedömningen med hjälp av dessa dokument minskar riskerna för felaktig hantering av personuppgiftsincidenter. Det framkommer också i rutinen ett antal frågeställningar som Boplats använder sig av för att bedöma allvarlighetsgraden på incidenten, vilket är positivt.

Dataskyddsombudet anser det är positivt att det i rutinen anges att anmälan till tillsynsmyndigheten ska ske inom 72 timmar, då tidsaspekten är mycket viktig vid en inträffad incident. Dock framkommer det först i punkt 6 i rutinen. Anmälan ska ske inom 72 timmar från att man upptäckt incidenten, varpå det är av största vikt redan i ett tidigt skede att incidenten rapporteras av personalen till rätt person som därefter ska anmälas. Tidsaspekten vid en inträffad personuppgiftsincident är av stor vikt, varpå det bör förtydligas för personalen att upptäckta incidenter ska anmälas så fort det går. Boplats uppger att ett bestämt tillvägagångssätt för att personalen att anmäla en incident inte är optimalt, då olika situationer kan kräva olika kommunikationssätt.

Slutligen är det positivt att Boplats i sin rutin beskriver ansvarsfördelningen för berörda personer. Bolaget bör dock förtydliga att det är dem som personuppgiftsansvariga som är kontaktpersoner och som har ansvaret för att anmäla incidenten till tillsynsmyndigheten när rapporteringsskyldigheten aktualiseras. Det framkommer att det är incidentkoordinatorn som ska vara kontaktperson gentemot tillsynsmyndigheten, men inte huruvida det är den som ska anmäla incidenten.

3.1.3 Information och vägledning till den registrerade

I rutinen för personuppgiftsincidenter har Boplats angett att de drabbade ska meddelas om incidenten är allvarlig, det vill säga om det är hög risk (sannolikhet och konsekvens) att deras rättigheter kan påverkas. Det är även två exempel angivna som förtydligar vilka incidenter det kan handla om.

I svarsunderlaget uppger Boplats att man gör bedömningen av allvarlighetsgrad på risken utifrån hur många registrerade som påverkats, hur många uppgifter som påverkats, vilka grupper av registrerade, vilken sorts personuppgifter, om

personuppgifterna var krypterade, för vem uppgifterna var exponerade och hur länge samt vilka konsekvenser incidenten kan ha för de drabbade. Riskerna bedöms även här utifrån Boplats informationsklassificering och Boplats riktlinje för informationssäkerhet.

3.1.3.1 Analys

Att Boplats anger att det föreligger en informationsplikt till de registrerade för dem som personuppgiftsansvariga när det rör sig om en hög risk för att de registrerades rättigheter påverkas är korrekt. Dataskyddsombudet ser det som positivt att man i rutinen ger exempel på incidenter som man anser vara av hög risk, då det kan hjälpa personalen att veta vilken typ av situation de ska vara extra uppmärksamma på.

Bedömningen av allvarlighetsgraden på incidenten görs utifrån ett antal angivna frågeställningar. Genom att besvara dessa frågeställningar ges en helhetsbild av det inträffade och sannolikhet och konsekvens för hög risk för de registrerades fri- och rättigheter kan fastställas. Det är positivt att det i rutinen framkommer hur riskbedömningen görs samt att bolaget hänvisar till tillhörande kompletterande dokument. Bolaget har även bifogat dessa dokument så att dataskyddsombudet kunnat läsa igenom dem. Dokumenten visar på att bolaget är förberedda för att hantera frågor om informationssäkerhet och dataskydd.

Av materialet som presenteras saknas information om att det är Boplats som personuppgiftsansvarig som är ansvarig för att kontakta de registrerade om det föreligger en hög risk vid en personuppgiftsincident. Boplats bör förtydliga detta i rollbeskrivningen och ansvarsfördelningen. De registrerade ska enligt Dataskyddsförordningen informeras direkt och utan onödigt dröjsmål om personuppgiftsincidenten sannolikt leder till hög risk.

Det finns enligt artikel 34.1 Dataskyddsförordningen också följande minimikrav på information som ska lämnas till de registrerade:

- Beskriv orsaken till personuppgiftsincidenten klart och tydligt.
- Namn och kontaktuppgifter till dataskyddsombudet eller annan kontakt som är insatt.
- Beskriv de sannolika konsekvenserna av personuppgiftsincidenten.
- Beskriv vad Boplats har gjort eller tänker göra för att hantera personuppgiftsincidenten.
- I förekommande fall: beskriv vad ni har gjort för att mildra eventuella negativa effekter.

För att rätt information ges i rätt tid till de registrerade bör minimikraven anges i rutinen för personuppgiftsincidenter. Rutinen bör också förtydligas med att de registrerade ska informeras utan onödigt dröjsmål.

3.1.4 Dokumentation av incidenter

Boplats uppger att alla incidenter dokumenteras i deras personuppgiftsincidentregister. Även om en incident inte anmäls till

tillsynsmyndigheten så ska den dokumenteras. Om en incident inte anmäls så ska detta motiveras. Alla handlingar förvaras i Boplats digitala arkiv.

Det framkommer också att det vid större incidenter ska skrivas en utförlig rapport om vad som inträffat, som ska bifogas i registret som bilaga.

3.1.4.1 Analys

Det är positivt att det framgår i rutinen att alla personuppgiftsincidenter ska dokumenteras, även de som inte ska anmälas till tillsynsmyndigheten. Tillsynsmyndigheten ställer höga krav på dokumentation vid en inträffad personuppgiftsincident och ska ha möjlighet att ta del av den vid förfrågan. Förhoppningen är att tydlig information om hur dokumentationen ska gå till ökar chanserna för en bra dokumentationsrutin hos företaget. Dataskyddsombudet ser det vidare som positivt att det finns ett personuppgiftsregister där alla incidenter samlas. I registerdokumentet finns frågor att besvara så som hur upptäcktes incidenten, varför inträffade den, inom vilket verksamhetsområde inträffade den, vilka grupper tillhör de registrerade, hur många registrerade påverkades etc. Det innebär att bolaget har en rutin för att dokumentera inträffade incidenter vilket dataskyddsombudet ser som positivt.

3.2 Iakttagelser och risker

Det är bra att bolaget har en framtagen rutin med handlingsplan för hantering av personuppgiftsincidenter. Att det finns fler dokument att ta till hjälp vid en riskbedömning ser dataskyddsombudet som något positivt, som förhoppningsvis gör att bedömningen sker på rätt sätt. Registret är tydligt formulerat med bra frågor som gör att incidenterna dokumenteras korrekt.

Boplats har identifierat ett utbildningsbehov som har tillgodosetts under hösten. Det är positivt att bolaget ser till så att personalen får kunskap om personuppgiftsincidenter. Dataskyddsombudet saknar beskrivning av hur kunskapen tillgodoses framgent samt vid nyanställning.

3.3 Rekommendationer

Rutinerna behöver kompletteras med beskrivning över vilken information som ska ges till de registrerade, så att bolaget uppfyller de fastställda minimikraven, och *när* de ska informeras. Vidare bör det förtydligas att personalen snarast vid misstanke om, risk för eller inträffande av incident bör meddela ansvariga. Även hur informationen ska ges vid en biträdessituation bör förtydligas så att incidenten kommer till ansvarigas kännedom så snabbt som möjligt.

Det är viktigt att bolaget säkerställer att även ny personal får kunskap om personuppgiftsincidenter och tillgång till relevanta dokument. Det är väsentligt att all personal kan identifiera personuppgiftsincidenter så att informationen snabbt kommer till de ansvarigas vetskap. Utifrån informationen om utbildning av personalen kan dataskyddsombudet inte avgöra huruvida all personal har

tillräcklig kompetens för att bedöma en personuppgiftsincident och rekommenderar att detta ses över av bolaget även efter utbildningstillfället. Även uppföljning av kunskap och nya utbildningstillfällen bör ses över. Vid revidering av rutiner och tillhörande dokument bör berörd personal också informeras, och det bör säkerställas vem som har ansvaret för detta.

4 Sammanfattning

Boplats får anses vara förberedda för att hantera en personuppgiftsincident med hjälp av en rutin och därtill hörande hjälpdokument. Det finns utpekade ansvarsroller, som med lite extra förtydligande beskriver vem som gör vad. Det är viktigt när en incident inträffar att alla vet vad dem ska göra och att det sker så snabbt som möjligt eftersom tidsfristerna enligt Dataskyddsförordningen är korta. Med rätt och kontinuerlig utbildning ser Boplats till att berörd personal har kunskap om vad en personuppgiftsincident är, vem som ska meddela vem och hur dokumentationen ska gå till. Förtydligande gör att man minimerar riskerna för att en incident inte hanteras korrekt och rätt person inte meddelas i tid.