Anmälda personuppgiftsincidenter januari–september 2019

Datainspektionens rapport 2019:3

Datainspektionen

Anmälda personuppgiftsincidenter januari–september 2019
Datainspektionens rapport 2019:3
Denna rapport finns att ladda ner på www.datainspektionen.se

Innehåll

Inledning

Genom dataskyddsförordningen[1] (GDPR, The General Data Protection Regulation) infördes den 25 maj 2018 en skyldighet för privata och offentliga verksamheter som behandlar personuppgifter att rapportera vissa personuppgiftsincidenter till Datainspektionen. Den 1 augusti 2018 infördes i brottsdatalagen motsvarande anmälningsskyldighet för brottsbekämpande myndigheter.

I denna rapport ges en översikt över de personuppgiftsincidenter som anmälts till Datainspektionen under perioden 1 januari–30 september 2019.

I början av 2019 publicerade Datainspektionen den första rapporten över anmälda personuppgiftsincidenter.[2] Rapporten beskrev de incidenter som anmälts under perioden 25 maj–31 december 2018. Datainspektionen kommer även fortsättningsvis att regelbundet publicera rapporter som beskriver generella tendenser och rekommendationer utifrån incidentanmälningarna.

På en övergripande nivå kan konstateras att antalet anmälda personuppgiftsincidenter ökat under de första nio månaderna 2019. Totalt fick Datainspektionen under januari–september 2019 in 3 410 anmälningar om personuppgiftsincidenter, vilket motsvarar närmare 90 anmälda incidenter per vecka. Under 2018 anmäldes i genomsnitt 70 incidenter per vecka. Antalet anmälda incidenter har därmed ökat med närmare 30 procent under 2019 jämfört med 2018. Ökningen återfinns främst i offentlig sektor.

Det finns också vissa förändringar i vilken typ av incidenter som anmälts. Ett konkret exempel är att incidenter som rör felskickade brev minskat från 42 procent 2018 till 35 procent under 2019. Detta bedöms primärt bero på att viss överrapportering som förekom under 2018 nu har minskat.

Datainspektionens bedömning är att ökningen av antalet anmälda incidenter och förändringarna i vad som anmäls i stor utsträckning beror på en ökad medvetenhet och kunskap om anmälningsskyldigheten. Intrycket är att rutinerna för att anmäla incidenter nu blivit mer etablerade, i synnerhet inom offentlig sektor och större företag.

Samtidigt är bedömningen att det i Sverige fortfarande finns ett stort mörkertal i form av anmälningspliktiga incidenter som inte anmäls.

1 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

2 Datainspektionens rapport Anmälda personuppgifter 2018 https://www.datainspektionen.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2018.pdf

Detta bygger bland annat på erfarenheter från andra EU-länder där anmälningsskyldigheten för personuppgiftsincidenter i vissa fall funnits längre. I Nederländerna, där anmälningsskyldigheten infördes år 2016, ökade antalet anmälda incidenter kraftigt varje år under den första treårsperioden. Under 2019 beräknas det totala antalet incidentanmälningar i Nederländerna komma att uppgå till cirka 24 000.[3]

Vad är en personuppgiftsincident och varför ska den anmälas till Datainspektionen?

En personuppgiftsincident är en säkerhetsincident som rör personuppgifter. Incidenten kan till exempel handla om att personuppgifter har blivit förstörda eller ändrade, gått förlorade eller kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

En personuppgiftsincident kan innebära risker för den vars personuppgifter det handlar om. Riskerna kan handla om till exempel identitetsstöld, bedrägeri, finansiell förlust, diskriminering eller skadlig ryktesspridning. Om det *inte är osannolikt* att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter ska den anmälas till Datainspektionen inom 72 timmar från att den upptäckts.

Om det finns en *hög risk* att privatpersoners fri- och rättigheter kan påverkas till följd av en personuppgiftsincident är den ansvariga verksamheten skyldig att – förutom att anmäla det inträffade till Datainspektionen – också informera de registrerade om att incidenten inträffat. Det ger den enskilde möjlighet att vidta egna åtgärder, till exempel att byta lösenord.

Även när en incident inte anmäls ska den alltid dokumenteras internt. Datainspektionen får med jämna mellanrum frågor om vilken typ av incidenter som inte behöver anmälas till Datainspektionen, utan där det istället räcker med att dokumentera internt. Avgörande för när en incident ska anmälas är bedömningen av vilken risk incidenten inneburit för de registrerade. Riskbedömningen är också styrande för när de registrerade ska informeras om att en incident inträffat.

Inom ramen för Datainspektionens samarbete med andra dataskyddsmyndigheter inom EU pågår ett arbete med en fördjupad vägledning kring personuppgiftsincidenter. Ambitionen är att det EU-gemensamma arbetet ska resultera i ett mer konkret stöd till verksamheter när det gäller riskbedömningar i samband med en incident.

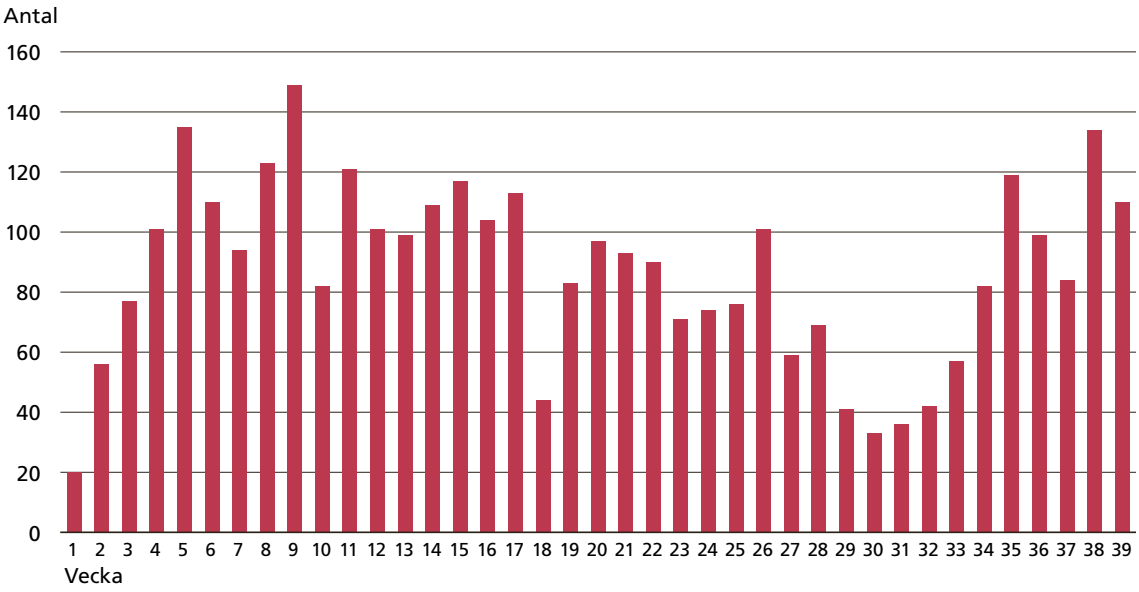
3 Rapport från den Nederländska dataskyddsmyndigheten september 2019 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht_datalekken_feiten_en_cijfers_1e_helft_2019.pdf

Ytterst syftar skyldigheten att anmäla personuppgiftsincidenter till att stärka integritetsskyddet. Genom anmälningsskyldigheten har kraven höjts på alla verksamheter som hanterar personuppgifter att ha rutiner på plats för att kunna upptäcka, rapportera och utreda incidenter. En inträffad incident som inte anmäls kan leda till sanktionsavgifter.

Anmälda personuppgiftsincidenter under januari–september 2019

Datainspektionen fick under perioden 1 januari–30 september 2019 in totalt 3 410 anmälningar om personuppgiftsincidenter, varav 3 376 utifrån dataskyddsförordningen och 34 utifrån brottsdatalagen. Mönstret är att antalet anmälningar minskar kraftigt under semesterperioder. För sommarperioden började antalet anmälningar att minska redan i maj. Under hösten har antalet anmälningar återgått till de nivåer som rådde i början av året.

Antal incidentanmälningar per vecka januari–september 2019



Den absoluta merparten av de incidenter som anmälts under 2019 bedöms utgöra reella personuppgiftsincidenter. Det förekommer fortfarande en viss överrapportering även om det under 2019 har minskat väsentligt jämfört med 2018. Om en organisation anmäler ett större antal incidenter som Datainspektionen bedömer inte är anmälningspliktiga kontaktar myndigheten den aktuella verksamheten för att ge vägledning kring anmälningsskyldigheten. Detta har hittills primärt rört vilka incidenter i form av felskickade brev som ska anmälas. Om ett felskickat brev eller e-post endast innehåller kontaktuppgifter till en eller mycket få registrerade och ingen känslig information röjs, är det typiskt sett inte nödvändigt att anmäla incidenten till Datainspektionen. Om ett felskickat brev eller e-post däremot innehåller till exempel uppgifter om ett stort antal människor, finansiell information eller känsliga personuppgifter, exempelvis om hälsa, ska incidenten anmälas till Datainspektionen.

Fördelning på olika samhällssektorer

Sammantaget står verksamheter inom offentlig sektor eller med offentligt uppdrag för nästan två tredjedelar, 64 procent, av alla incidentanmälningar som hittills inkommit under 2019. Under 2018 var motsvarande siffra 46 procent. Att en organisation eller en bransch anmäler många personuppgiftsincidenter behöver inte nödvändigtvis vara en indikation på bristande säkerhet. Ofta kan det tvärtom tyda på att verksamheten har strukturer och rutiner som ger en god förmåga att upptäcka och rapportera personuppgiftsincidenter.

Myndigheter och kommuner står tillsammans för 31 procent av anmälningarna, det vill säga ungefär en tredjedel. 2018 stod dessa för 23 procent av anmälningarna, ungefär en fjärdedel. Anmälningar från hälso- och sjukvård, skola och socialtjänst har ökat från att tillsammans stå för 23 procent 2018 till 33 procent 2019. Den absoluta merparten av de anmälda incidenterna från dessa verksamheter kommer från offentlig sektor.

I absoluta tal har antalet anmälningar från offentlig sektor nästan dubblerats, från 1 079 anmälningar under 25 maj 2018–31 december 2018 till 2 047 anmälningar under januari–september 2019. För privat sektor är antalet oförändrat; under 25 maj–31 december anmäldes 1 149 incidenter och under januari–september 2019 anmäldes 1 146 incidenter från privat sektor.

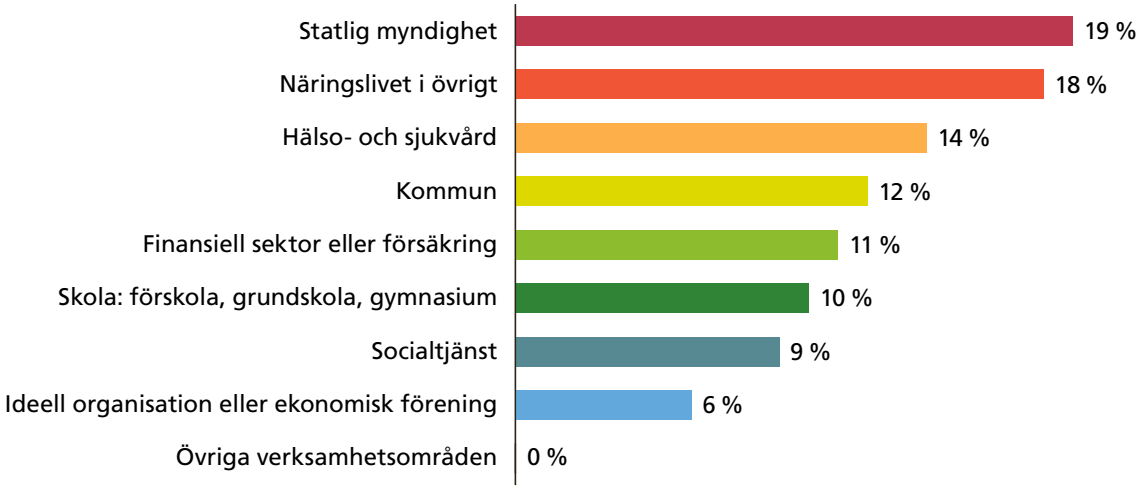
Ökningen av antalet anmälningar från offentlig sektor bedöms bero på ett flertal faktorer. Den främsta förklaringen är sannolikt att rutinerna för att upptäcka och rapportera incidenter nu blivit mer etablerade. Många verksamheter i offentlig sektor behandlar också stora mängder personuppgifter och ofta känsliga kategorier av personuppgifter, vilket kan bidra till att fler incidenter betraktas som anmälningspliktiga vid riskbedömningen. Även att det under 2019 skett flera incidenter i offentlig sektor som fått stor massmedial uppmärksamhet kan ha bidragit till en ökad medvetenhet och anmälningsbenägenhet.

Den privata sektorn står för drygt en tredjedel, 36 procent, av de incidenter som hittills anmälts under 2019. Motsvarande siffra under 2018 var 54 procent.

Av det totala antalet anmälningar kommer 11 procent från verksamheter inom den finansiella sektorn eller försäkringsbranschen. Under 2018 stod branschen för 25 procent av alla incidentanmälningar. Att dessa minskat under 2019 bedöms i första hand bero på den överrapportering som skedde från vissa större företag direkt efter att anmälningsskyldigheten infördes.

Därutöver står näringslivet i övrigt för 18 procent och ideella organisationer och föreningar för 6 procent.

Antal personuppgiftsincidenter per verksamhetsområde



Typ av incident

Felaktiga brevutskick. Den största delen av de anmälda incidenterna, 35 procent, avser fortfarande felaktiga brevutskick, det vill säga brev eller e-post som innehåller personuppgifter och oavsiktligt hamnat hos fel mottagare. Andelen anmälda incidenter av denna typ har minskat något, då det 2018 stod för 42 procent av anmälningarna. Datainspektionen bedömer att det i denna kategori, framför allt direkt efter att anmälningsskyldigheten infördes, inledningsvis fanns en överrapportering. Den minskade andelen anmälda felaktiga brevutskick bedöms primärt bero på ökad kunskap och medvetenhet om vilka incidenter som är anmälningspliktiga.

Obehörig åtkomst handlar om att någon olovligen berett sig tillgång till personuppgifter, till exempel genom att behörigheter till ett it-system har tilldelats felaktigt eller för generellt. Även så kallade phishingattacker[4] är vanligt förekommande i kategorin obehörig åtkomst. Ett annat återkommande exempel är att det upptäcks att personuppgifter har funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning.

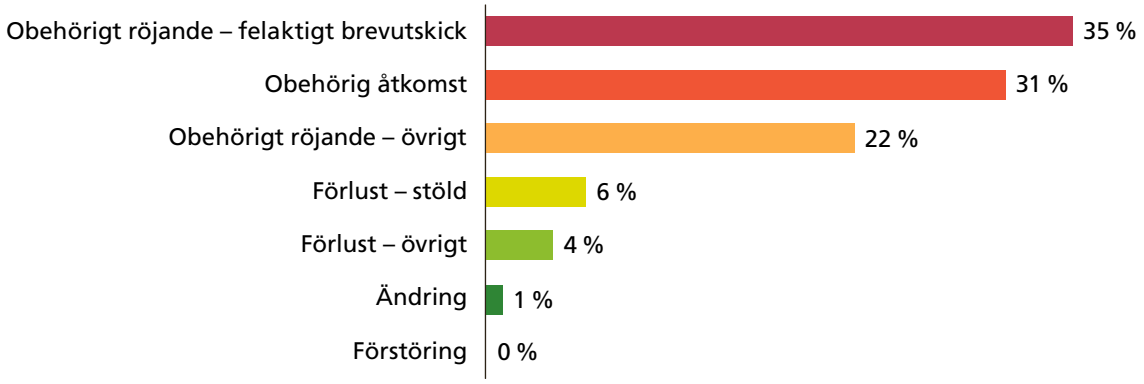
I likhet med 2018 är obehörig åtkomst den näst största kategorin av anmälda personuppgiftsincidenter men har ökat från 23 procent 2018 till 31 procent 2019. Ökningen kan bland annat bero på bättre kunskap om och rutiner kring att upptäcka och anmäla incidenter.

4 *Phishing* eller *nätfiske* är en metod för it-brottslighet där internetanvändare luras att lämna ut känslig information som sedan kan användas till bedrägerier.

Obehörigt röjande innebär att den personuppgiftsansvarige eller någon under den personuppgiftsansvariges ledning hanterat personuppgifter på ett sätt så att de kommit till obehörigas kännedom. Det kan till exempel handla om att personuppgifter avsiktligt eller oavsiktligt röjts för någon som saknar behörighet att ta del av dem eller att brister i ett tekniskt system gör att stora mängder personuppgifter kommit till fel mottagares kännedom. Denna kategori av anmälda personuppgiftsincidenter står för 22 procent anmälningarna vilket motsvarar ungefär samma nivå som 2018.

Stöld och förlust. I dessa kategorier handlar de anmälda incidenterna till exempel om att tjänstedatorer glömts i kollektivtrafiken, att organisationen haft inbrott eller varit utsatta för ett antagonistiskt angrepp genom till exempel malware[5] eller hacking[6]. Även om dessa incidenter är förhållandevis få till antalet är det typiskt sett större grupper av registrerade som berörs.

Vad har hänt?



Varför inträffade incidenten?

Den mänskliga faktorn. Personuppgiftsincidenter som beror på den mänskliga faktorn består i huvudsak av att individer begått ett misstag vid hantering av personuppgifter i sina verksamheter. Det kan också handla om att individer, medvetet eller omedvetet, inte följer interna rutiner för hantering av personuppgifter. Den mänskliga faktorn anges oftast som orsak till anmälda personuppgiftsincidenter och står för

5 *Malware* eller *sabotageprogram* är skadlig programvara som installeras på en dator eller nätverk utan användarens samtycke för att till exempel samla in information.

6 *Hacking* innebär att någon bryter sig in i it-system utan användarens samtycke eller vetskap.

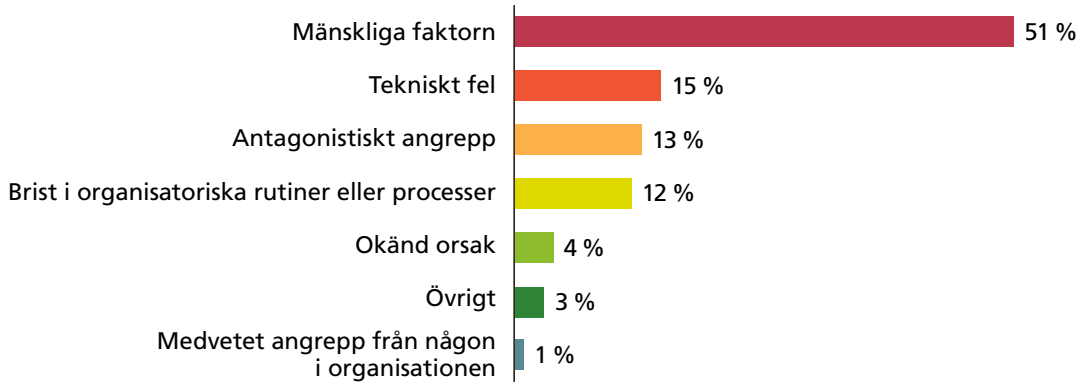
51 procent av anmälningarna. 2018 stod den mänskliga faktorn för 61 procent. Drygt hälften av de personuppgiftsincidenter som beror på den mänskliga faktorn handlar om felskickade brev och e-postmeddelanden.

Tekniskt fel som orsak till en incident kan till exempel handla om att behörighetsbegränsningar förlorats efter en systemuppdatering. En del av de incidenter som inträffat till följd av ett tekniskt fel har skett hos ett personuppgiftsbiträde med uppdrag hos flera olika personuppgiftsansvariga. Detta medför att flera anmälningar görs med anledning av en och samma incident, eftersom samtliga berörda personuppgiftsansvariga är skyldiga att anmäla incidenten. Tekniskt fel är tillsammans med brister i organisatoriska rutiner eller processer de orsaker till personuppgiftsincidenter som ökat sedan 2018.

Antagonistiska angrepp står för ungefär var sjunde anmälan. Ungefär 60 procent av de antagonistiska angreppen utgörs av phishingattacker. Näringslivet i övrigt står under 2019 för drygt hälften av alla incidentanmälningar som uppges bero på antagonistiska angrepp.

Brist i organisatoriska rutiner eller processer innebär att de rutiner och processer som finns i verksamheten inte fungerat eller varit otillräckliga. Drygt en av tio, 12 procent, av incidenterna uppges bero på detta. Datainspektionens bedömning är att det här finns ett mörkertal, eftersom en del av de incidenter som uppges bero på den mänskliga faktorn i själva verket bottnar i brister i organisatoriska rutiner och processer.

Varför inträffade incidenten?



Rekommendationer

Utifrån de personuppgiftsincidenter som anmälts under 2019 går det att ge några generella rekommendationer som kan bidra till att förebygga incidenter och mildra konsekvenserna om en incident ändå inträffar. Flera av dessa rekommendationer fanns med även i Datainspektionens rapport om anmälda personuppgiftsincidenter 2018, men är fortfarande relevanta.

- Alla organisationer som hanterar personuppgifter behöver ha rutiner för att upptäcka, dokumentera, anmäla och hantera personuppgiftsincidenter. När Datainspektionen i mars 2019 genomförde en undersökning riktad till dataskyddsombud uppgav knappt 80 procent att deras organisation har tagit fram rutiner för att anmäla personuppgiftsincidenter. Bland företag utan dataskyddsombud uppgav bara drygt 40 procent att de hade sådana rutiner. Här finns med andra ord fortfarande förbättringspotential[7].
- Den stora andelen incidenter som uppges bero på den mänskliga faktorn understryker betydelsen av att styrdokument och tekniska informationssäkerhetsåtgärder kompletteras med löpande utbildning och andra åtgärder för att öka kunskapen och medvetenheten hos personalen. I Datainspektionens undersökning riktad till dataskyddsombud uppgav knappt 50 procent att dataskydd och informationssäkerhet ingår i introduktionsutbildningen till nya medarbetare i deras organisation. Endast 36 procent av dataskyddsombuden uppgav att medarbetarna i deras organisation får löpande utbildning i dataskydd och informationssäkerhet[8].
- Grundläggande åtgärder som kontinuerligt kan behöva informeras om internt är till exempel
  - att alltid kontrollera att korrekt mottagare är angiven innan ett brev eller e-post skickas ut, att använda funktionen dold kopia (bcc) vid utskick som ska till flera mottagare samt att använda e-post som är skyddad med kryptering vid utskick av känsliga eller integritetskänsliga uppgifter.

7 Datainspektionens Nationella Integritetsrapport 2019
https://www.datainspektionen.se/globalassets/dokument/rapporter/nationell-integritetsrapport-2019.pdf

8 Datainspektionens Nationella Integritetsrapport 2019
https://www.datainspektionen.se/globalassets/dokument/rapporter/nationell-integritetsrapport-2019.pdf

- att om personuppgifter lagras på flyttbara media som är särskilt sårbara för stöld eller förlust – till exempel usb-minnen, bärbara datorer och mobiltelefoner – bör informationen krypteras så att ingen obehörig kan ta del av den.
- att det för att förebygga antagonistiska angrepp är angeläget att inte öppna länkar eller bifogade filer från okända avsändare.

- En central del i arbetet med informationssäkerhet och dataskydd handlar om behörighetsstyrning. Alla organisationer som hanterar personuppgifter behöver ha stabila rutiner för att säkerställa att behörigheter tilldelas korrekt, att behörigheterna löpande kontrolleras och följs upp samt att åtkomstkontroller genomförs.
- En generell rekommendation är att de flesta organisationer kan vinna på att aktivt använda de personuppgiftsincidenter som upptäcks som ett underlag för att identifiera brister och utvecklingsbehov till det löpande och systematiska arbetet med dataskydd och informationssäkerhet.

Datainspektionens arbete med personuppgiftsincidenter

När en anmälan om en personuppgiftsincident registrerats hos Datainspektionen gör myndigheten omgående en första bedömning av incidenten. I denna första bedömning granskar myndigheten bland annat

- hur allvarlig incidenten är, till exempel hur många registrerade som berörs, om incidenten rör känsliga personuppgifter eller särskilt sårbara grupper av registrerade och om incidenten beror på ett antagonistiskt angrepp
- hur incidenten har hanterats, till exempel om incidenten har anmälts i tid och om de registrerade har informerats när så ska ske, samt vilka åtgärder som vidtagits i övrigt
- om incidentanmälan är fullständig eller om anmälaren uppgett att de kommer att komplettera anmälan.

Om anmälan inte behöver kompletteras, incidenten har hanterats på ett tillfredsställande sätt och risken för enskildas fri- och rättigheter bedöms som låg avslutas ärendet vid Datainspektionen. Anmälaren får då ett brev från myndigheten med besked om att ärendet avslutas.

Datainspektionens bedömning är att den stora merparten av de incidentanmälningar som inkommit under 2019 kommer att avslutas utan ytterligare åtgärd. Hittills har cirka 60 procent av samtliga anmälningar som inkommit sedan den 25 maj 2018 avslutats.

Datainspektionen utvecklar arbetet med personuppgiftsincidenter löpande. Målsättningen är att i början av 2020 driftsätta en e-tjänst där personuppgiftsincidenter kan anmälas digitalt. Närmare information om datum för driftsättning av e-tjänsten kommer att publiceras på Datainspektionens webbplats.

En viktig del av Datainspektionens fortsatta arbete är att ta fram information som kan ge vägledning till företag, myndigheter och organisationer. Inom ramen för EU-samarbetet pågår arbete med en fördjupad vägledning kring personuppgiftsincidenter. Ambitionen är att ge mer konkret stöd till verksamheter i arbetet med att bedöma risken för de registrerade i samband med en incident. Riskbedömningen är avgörande för arbetet med personuppgiftsincidenter då den bland annat styr vilka incidenter som ska anmälas till dataskyddsmyndigheten och i vilka fall de registrerade ska informeras om att en incident inträffat. Det är ännu inte fastställt när det EU-gemensamma stöddokumentet kommer att vara klart.

Andra prioriteringar i det fortsatta utvecklingsarbetet handlar om att utveckla arbetet med att vidta skyndsamma åtgärder när incidenter inte hanterats på ett korrekt och lämpligt sätt. Slutligen är en central fråga för Datainspektionen att fånga upp fall där incidenter inträffat men där anmälan inte skett.

Pågående tillsynsärenden som rör personuppgiftsincidenter

För incidenter som bedöms som särskilt allvarliga gör Datainspektionen en fördjupad bedömning. Myndigheten har möjlighet att inleda tillsyn baserat på hanteringen av själva incidenten och anmälan, men också utifrån mer generella brister som incidenten indikerar. För närvarande pågår ett tiotal tillsynsärenden som inletts direkt baserat på anmälda personuppgiftsincidenter. Granskningarna avser

- **1177 Vårdguiden.** Datainspektionens granskar incidenten kring 1177 Vårdguiden. Granskningen omfattar sex tillsynsärenden och behandlar bland annat regionernas behandling av personuppgifter som rör sjukvårdsrådgivningen, kopplingen mellan regionerna och sjukvårdsrådgivningen via 1177 Vårdguiden samt ansvarsförhållandet mellan de olika aktörerna. Följande aktörer ingår i granskningen:
  - **Voice Integrate Nordic.** Tillsyn inleddes i mars 2019.
  - **Inera AB.** Tillsyn inleddes i mars 2019.
  - **MedHelp AB.** Tillsyn inleddes i mars 2019.
  - **Region Stockholm.** Tillsyn inleddes i juni 2019.
  - **Region Sörmland.** Tillsyn inleddes i juni 2019.
  - **Region Värmland.** Tillsyn inleddes i juni 2019.
- **Utbildningsnämnden Stockholm Stad.** Tillsynen inleddes i juni 2019 och granskar hur Stockholms stad hanterar skolpersonalens behörighet att ta del av uppgifter om elever.
- **Statens servicecenter.** Tillsynen inleddes i september 2019 och avser en granskning av myndighetens rutiner för att upptäcka och utreda personuppgiftsincidenter.
- **Region Uppsala.** Tillsynen inleddes i september 2019 och utreder bakgrunden till att regionen har skickat patientuppgifter utan kryptering.

Datainspektionen har också två pågående tillsynsärenden som fokuserar på de generella rutinerna för incidenthantering, men där tillsynsärendet inte har inletts utifrån en specifik personuppgiftsincident som anmälts:

- **Polisen.** Tillsynen inleddes i juni 2019. Granskningen syftar till att ta reda på om myndigheten har dokumenterade rutiner för att upptäcka, rapportera och hantera personuppgiftsincidenter.
- **Ekobrottsmyndigheten.** Tillsynen inleddes i juni 2019 Även denna granskning fokuserar på om myndigheten har dokumenterade rutiner för att upptäcka, rapportera och hantera personuppgifts-incidenter.

Slutligen har Datainspektionen en pågående tillsyn som rör en misstänkt incident som inte anmälts till myndigheten, utan istället kommit till myndighetens kännedom genom ett klagomål:

- **Umeå Universitet.** Tillsynen inleddes i augusti 2019. Universitetet har, för forskning, tagit emot känsliga personuppgifter från Polis-myndigheten. Enligt ett klagomål från Polismyndigheten till Datainspektionen har universitetet sedan skickat känsliga person-uppgifter via okrypterad e-post. Datainspektionen granskar nu universitetets hantering av känsliga personuppgifter.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm

Datainspektionen