Anmälda personuppgiftsincidenter 2018

Datainspektionens rapport 2019:1

Datainspektionen

Anmälda personuppgiftsincidenter 2018
Datainspektionens rapport 2019:1
Denna rapport finns att ladda ner på www.datainspektionen.se

Innehåll

Inledning

Genom dataskyddsförordningen (GDPR, The General Data Protection Regulation) infördes den 25 maj 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 detta faktablad ges en kort översikt över de personuppgiftsincidenter som anmälts till Datainspektionen under perioden 25 maj – 31 december 2018.

Totalt fick Datainspektionen under perioden in 2 262 anmälningar om personuppgiftsincidenter. Den absoluta merparten anmälningar gjordes utifrån GDPR, färre än tio anmälningar gjordes utifrån brottsdatalagen.

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.

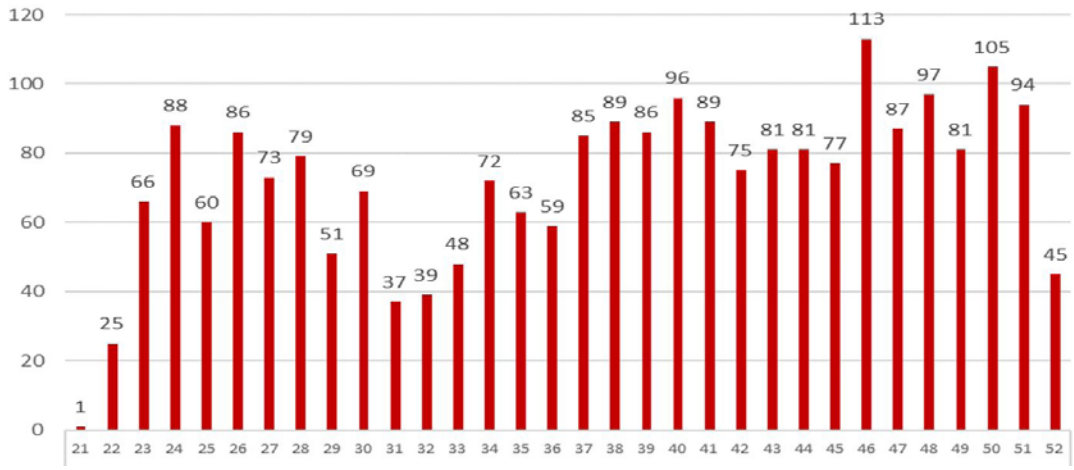
Ytterst syftar skyldigheten att anmäla personuppgiftsincidenter till att stärka integritetsskyddet. Genom anmälningsskyldigheten har kraven höjts på alla verksamheter som hanterar personuppgifter att ha rutiner på plats för att kunna upptäcka, rapportera och utreda incidenter. En inträffad incident som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

Anmälda personuppgiftsincidenter under 2018

Datainspektionen fick under perioden 25 maj – 31 december in totalt 2 262 anmälningar om personuppgiftsincidenter, varav 2 258 utifrån GDPR och 4 utifrån brottsdatalagen. Tendensen är att antalet anmälningar ökade successivt under året.

Framför allt i början efter att anmälningsskyldigheten infördes fanns en viss överrapportering, det vill säga att även incidenter som inte är anmälningspliktiga anmäldes. Den absoluta merparten av de incidenter som anmälts under året bedöms dock utgöra reella personuppgiftsincidenter.

Den successiva ökningen av anmälningar efter sommaren beror sannolikt på en inledande något avvaktande hållning till att anmäla personuppgiftsincidenter.



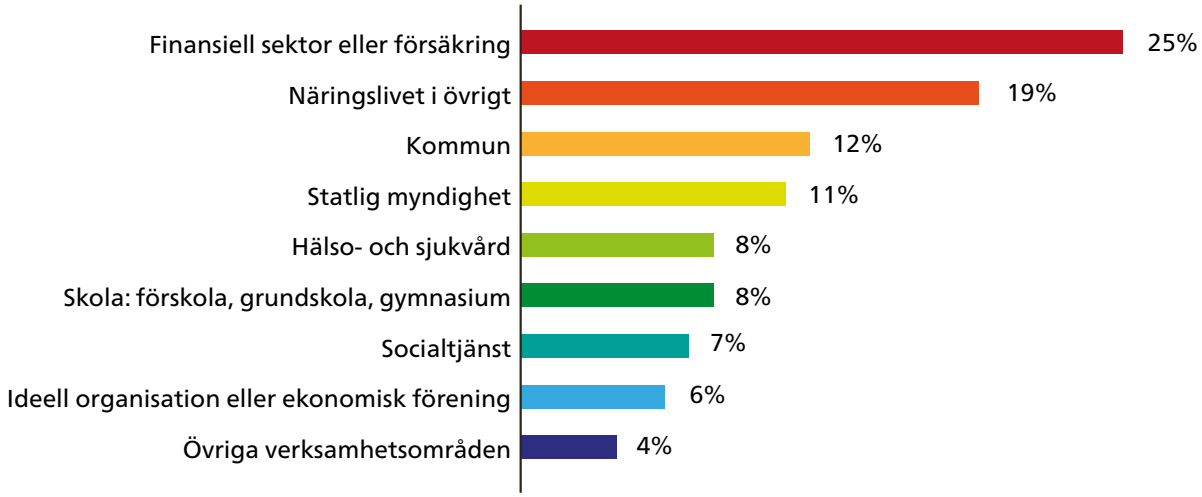
Inrapporterade personuppgiftsincidenter per vecka (v. 21–52)

Fördelning på olika samhällssektorer

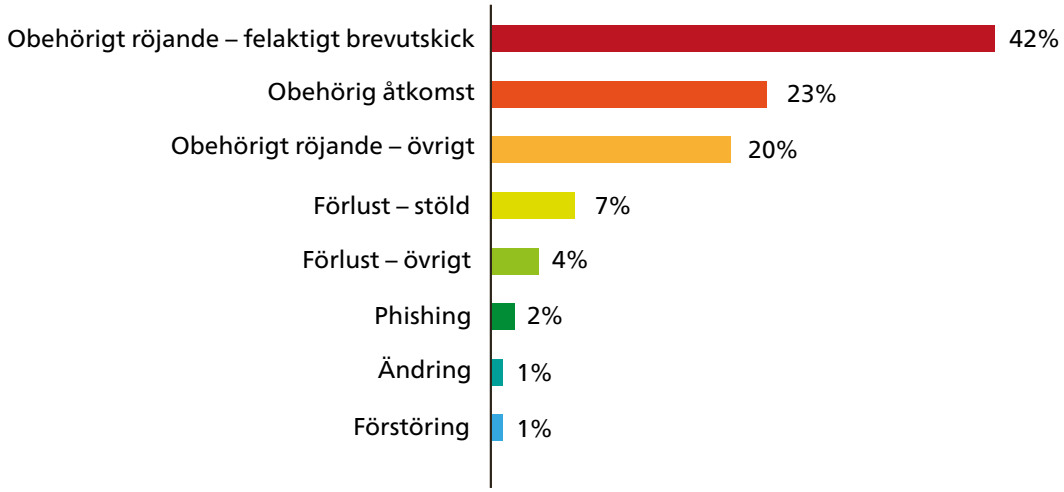
En fjärdedel av alla incidentanmälningar kom från verksamheter inom den finansiella sektorn eller försäkringsbranschen. Myndigheter och kommuner står tillsammans för 23 procent av anmälningarna, det vill säga ungefär en fjärdedel. Anmälningar från hälso- och sjukvård, skola och socialtjänst utgör tillsammans 23 procent, med 7 till 8 procent vardera. Därutöver står näringslivet i övrigt för 19 procent.

Att en organisation eller en bransch anmäler många personuppgiftsincidenter behöver inte nödvändigtvis vara en indikation på bristande säkerhet. I vissa fall kan det tvärtom tyda på att verksamheten har strukturer och rutiner som ger en god förmåga att upptäcka och rapportera personuppgiftsincidenter.

Vilket verksamhetsområde?



Vad har hänt?



Varför inträffade incidenten?

Typ av incident

Felaktiga brevutskick. Den största delen av de anmälda incidenterna, 42 procent, avser felaktiga brevutskick, det vill säga brev eller e-post som innehåller personuppgifter och oavsiktligt hamnat hos fel mottagare. Datainspektionen bedömer att det i denna kategori, framför allt direkt efter att anmälningsskyldigheten infördes, funnits en viss överrapportering. 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 om till exempel hälsa ska incidenten anmälas till Datainspektionen.

Obehörig åtkomst är den näst största kategorin av anmälda personuppgiftsincidenter och står för 23 procent. Denna kategori 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. Ett annat återkommande exempel är att det upptäcks att personuppgifter har funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning.

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 handla till exempel om att en stor mängd mottagare av ett e-postmeddelande med känslig information kunnat se vilka andra som fått samma e-postmeddelande. Ett annat scenario är att brister i ett tekniskt system gör att stora mängder personuppgifter kommit till fel mottagares kännedom.

Stöld, förlust och phishing. 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 phishing, malware eller hacking. Även om dessa incidenter är förhållandevis få till antalet är det typiskt sett större grupper av registrerade som berörs.

Varför inträffade incidenten?

Den mänskliga faktorn uppges vara den vanligaste orsaken bakom de anmälda personuppgiftsincidenterna. Drygt sextio procent av de anmälda personuppgiftsincidenterna under 2018 berodde på den mänskliga faktorn. Personuppgiftsincidenter som beror på den mänskliga faktorn består i huvudsak av individer som begått ett misstag vid hantering av personuppgifter i sina verksamheter. Majoriteten av de personuppgiftsincidenter som beror på den mänskliga faktorn handlar om felskickade brev och e-postmed-

delanden. Närmare en av tio anmälningar handlar också om brister i organisatoriska rutiner eller processer.

Antagonistiska angrepp står för ungefär var sjunde anmälan. Totalt handlar det om drygt 300 av de anmälda incidenterna som primärt rör stölder och phishing.

Rekommendationer

Utifrån de personuppgiftsincidenter som anmälts under 2018 går det att ge några generella rekommendationer som kan bidra till att förebygga incidenter och mildra konsekvenserna om en incident ändå inträffar.

- Grundläggande åtgärder 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.
- 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.
- För att förebygga antagonistiska angrepp förtjänar det att påminna om vikten av information om 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.
- 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.

Datainspektionens arbete med personuppgiftsincidenter

När en anmälan om en personuppgiftsincident inkommer till Datainspektionen gör myndigheten efter att ärendet registrerats, en första bedömning av incidenten. I denna första bedömning granskar myndigheten bland annat

- om incidentanmälan är fullständig eller om anmälaren uppgett att de kommer att komplettera anmälan
- 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
- 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.

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 där vi meddelar att vi avslutat ärendet.

Datainspektionens bedömning är att merparten av de incidentanmälningar som inkommit under 2018 kommer att avslutas utan ytterligare åtgärd. Hittills har cirka 600 av de totalt 2 262 incidentanmälningarna som inkom under 2018 avslutats.

Om det framkommer nya upplysningar i ärendet, eller om det inkommer ytterligare incidentanmälningar från samma personuppgiftsansvarig, kan Datainspektionen i ett senare skede komma att beakta incidenten i en tillsyn.

För incidenter som bedöms som mer allvarliga gör Datainspektionen en fördjupad bedömning. Så är fallet för omkring 100 av de incidenter som inkommit under 2018, för dessa pågår handläggningen fortfarande.

Datainspektionen har möjlighet att inleda tillsyn baserat på hanteringen av själva incidenten och anmälan, men också utifrån mer generella brister som incidenten indikerar. Under 2018 har ingen tillsyn inletts baserat på en personuppgiftsincident.

Datainspektionen utvecklar arbetet med personuppgiftsincidenter löpande. En viktig del av det fortsatta arbetet är att med incidentrapporteringen som grund ta fram information som kan ge vägledning till företag, myndigheter och organisationer. Genom att sprida kunskap om varför personuppgiftsincidenter inträffar, var riskerna är störst och

vilka förebyggande åtgärder som kan vidtas, kan Datainspektionen bidra till att förebygga ytterligare incidenter eller minska de negativa konsekvenserna av framtida incidenter.

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. Datainspektionen kommer också under 2019 att driftsätta en e-tjänst där personuppgiftsincidenter kan anmälas. Slutligen är en central fråga för Datainspektionen att fånga upp fall där incidenter inträffat men där anmälan inte skett.

Kontakta Datainspektionen

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

Datainspektionen