

Anmälda personuppgiftsincidenter 2021

IMY rapport 2022:1



Innehållsförteckning

Sammanfattning	3
Rekommendationer	4
Inledning	6
Del 1. Vad är en personuppgiftsincident och när ska den anmälas till IMY?	8
Del 2. Personuppgiftsincidenter 2021	12
Del 3. Redovisning av personuppgiftsincidenter 2021 per verksamhetsområde	20
Del 4. Sverige jämfört med andra länder under 2021	23

Bilagor

Bilaga 1: Hur ser materialet ut och vilka indelningar finns?	25
Bilaga 2: Figurer för anmälda personuppgiftsincidenter per verksamhetsområde	29

Sammanfattning

2021 anmäldes 5 767 personuppgiftsincidenter till IMY. Det är en ökning med 26 procent jämfört med 2020 då 4 588 anmäldes. Av incidentanmälningarna 2021 rörde 41 brottsdatalagen. Motsvarande siffra för 2020 var 50 anmälningar.

Den vanligaste typen av personuppgiftsincidenter som anmäldes till IMY 2021 var felaktiga brevutskick, 36 procent. Det är en minskning mot föregående år då andelen felaktiga brevutskick utgjorde 40 procent av de anmälda incidenterna. Räknat i antal innebar det en ökning med ungefär 250 fall från 2020 till 2021. Exempel på felaktiga brevutskick är brev, mejl eller sms som innehåller personuppgifter och som oavsiktligt hamnat hos fel mottagare.

Den vanligaste orsaken till personuppgiftsincidenter 2021 kan, precis som tidigare år, härledas till den mänskliga faktorn, 57 procent. Motsvarande siffra 2020 var 59 procent. Räknat i antal anmälda personuppgiftsincidenter innebar det en ökning med ungefär 600 fall från 2020 till 2021.

Störst andel av anmälda personuppgiftsincidenter 2021 kom från offentlig sektor, 66 procent. Inom offentlig sektor anmäldes nästan var fjärde incident inom området Statliga myndigheter och domstolar, och nästan var femte inom området Hälso- och sjukvård.

Inom de flesta sektorerna minskade andelen incidenter som rapporterades bero på obehörig åtkomst och andelen antagonistiska angrepp

2021 jämfört med 2020. Hälso- och sjukvården och kommunal sektor uppvisade dock en avvikande utveckling med en ökad andel incidenter som berodde på obehörig åtkomst. Inom hälso- och sjukvården rapporterades dessutom en väsentligt högre andel antagonistiska angrepp mot föregående år.

Under 2021 inledde IMY ett trettiotal tillsynsärenden baserat på anmälda personuppgiftsincidenter.

I förhållande till befolkningens mängden och jämfört med andra länder inom det Europeiska ekonomiska samarbetsområdet (EES) rapporterade Sverige 55 personuppgiftsincidenter per 100 000 invånare under perioden 28 januari 2021 och 27 januari 2022. Nederländerna, Liechtenstein, Danmark och Irland rapporterade flest incidenter, mellan 130 till 150 incidenter per 100 000 invånare. 2020 hade Sverige 48 anmälningar per 100 000 invånare.

IMY bedömer att det fortfarande finns ett stort mörkertal i form av anmälningspliktiga incidenter som inte anmäls. Bedömningen baseras bland annat på utvecklingen i andra länder, där anmälningsskyldigheten för personuppgiftsincidenter funnits längre.

Europeiska dataskyddsstyrelsen (EDPB) antog nya riktlinjer under 2021 som syftar till att ge personuppgiftsansvariga rekommendationer och vägledning utifrån konkreta exempel på personuppgiftsincidenter.

IMY:s rekommendationer för att förebygga incidenter

Utifrån de personuppgiftsincidenter som kommit till myndigheten har IMY formulerat några generella rekommendationer. Rekommendationerna kan bidra till att förebygga personuppgiftsincidenter och mildra konsekvenserna om en incident ändå inträffar.

Ta stöd av nya riktlinjer från EDPB

Europeiska dataskyddsstyrelsen (EDPB) har antagit en slutgiltig version av riktlinjer som innehåller exempel på personuppgiftsincidenter. Syftet med riktlinjerna är att ge personuppgiftsansvariga vägledning och rekommendationer utifrån konkreta exempel på personuppgiftsincidenter. Riktlinjerna kan ge den personuppgiftsansvariga bra stöd och vägledning om hur olika typer av incidenter lämpligen bör hanteras och vilka säkerhetsåtgärder som behöver vidtas.

Skydda verksamheter mot obehörig åtkomst och antagonistiska angrepp

Bättre tekniska och organisatoriska åtgärder kan förebygga antagonistiska angrepp och därmed stärka skyddet för personuppgifter. Det är viktigt att alla verksamheter fortsätter att på ett systematiskt sätt arbeta med dataskydd och utveckla sin förmåga att förebygga, upptäcka och hantera antagonistiska angrepp så att personuppgifter skyddas. Detta är extra viktigt i verksamheter som hanterar känsliga personuppgifter och annan känslig information, som hälso- och sjukvården och inom kommuner.

Säkerställ en god lösenordshygien

För att förhindra obehörig åtkomst är det viktigt med en god lösenordshygien. Organisationen bör ha rutiner för skapandet och hantering av lösenord. Det kan även vara lämpligt att införa multifaktorautentisering som en teknisk åtgärd för att förhindra obehörig åtkomst.

Förebygg incidenter med god behörighetsstyrning

Obehörig åtkomst och obehörigt röjande utgör de näst vanligaste orsakerna till anmälda personuppgiftsincidenter. 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. Enligt dataskyddsförordningen är den personuppgiftsansvariga skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till risken.

Ha rutiner för när anställda avslutar sin anställning

Organisationer bör ha rutiner för hur arbetsmaterial, inloggningar och behörigheter ska hanteras när en anställd avslutar sin tjänst. Inaktivera inloggningar och konton så snart personen har lämnat organisationen.

Utbilda kontinuerligt

Den stora andelen incidenter som anmäls och uppges bero på den mänskliga faktorn understryker betydelsen av att tekniska informationssäkerhetsåtgärder kompletteras med organisatoriska åtgärder, såsom styr- och stöddokument, löpande utbildning och andra åtgärder för att öka kunskapen och medvetenheten hos medarbetarna.

Grundläggande åtgärder som kontinuerligt kan behöva informeras om är till exempel:

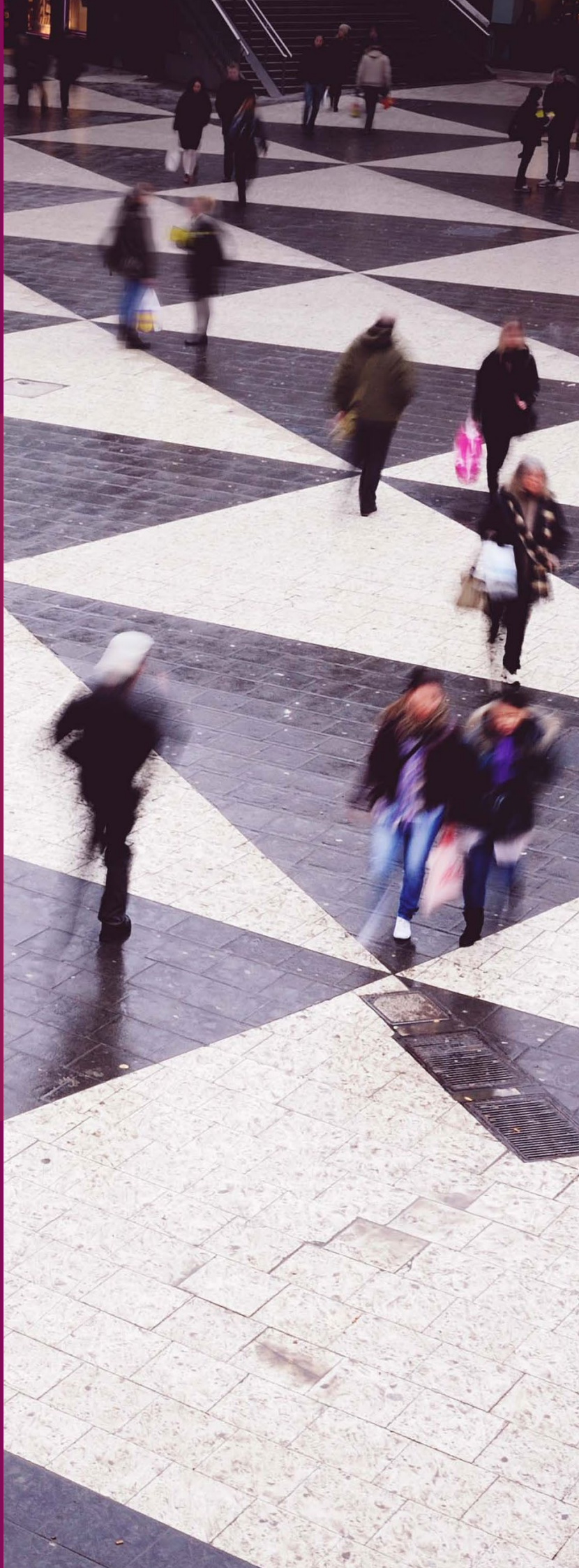
- Rutiner för hantering av personuppgifter i mejl. Till exempel att alltid kontrollera att korrekt mottagare är angiven innan ett brev eller mejl skickas ut, att använda funktionen dold kopia vid utskick som ska till flera mottagare. Känsliga eller integritetskänsliga personuppgifter ska helst inte skickas med mejl. Om detta inte går att undvika ska man använda mejl som är skyddade med kryptering så att endast den avsedda mottagaren kan ta del av uppgifterna.
- 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 är det angeläget att inte öppna länkar eller bifogade filer från okända avsändare. Den personuppgiftsansvariga bör verka för att höja säkerhetsmedvetandet och utbilda anställda i att känna igen tecken på när ett elektroniskt meddelande inte är autentiskt.

Rutiner för att upptäcka och anmäla incidenter kan förbättras

Alla organisationer som hanterar personuppgifter behöver ha rutiner för att upptäcka, dokumentera, anmäla och hantera personuppgiftsincidenter. Att den mänskliga faktorn år efter år uppges vara den vanligaste orsaken till en incident understryker vikten av att ha fungerande rutiner och uppdaterade styrdokument.

Incidenter kan ge viktiga signaler om utvecklingsbehov

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 i det löpande och systematiska arbetet med dataskydd och informationssäkerhet.





Inledning

Integritetsskyddsmyndigheten¹ (IMY) är Sveriges nationella tillsynsmyndighet för behandling av personuppgifter. Vi granskar att bestämmelserna i dataskyddsförordningen (GDPR) och brottsdatalagen (BDL), kamerabevakningslagen och annan reglering på dataskyddsområdet följs. Det gör vi framförallt genom tillsyn. Vi arbetar för att skydda individers personuppgifter, till exempel om hälsa och ekonomi så att de hanteras korrekt och inte hamnar i orätta händer.

IMY publicerar varje år en rapport om personuppgiftsincidenter som beskriver inflödet till myndigheten. Syftet med rapporten är att förmedla iakttagelser och lägesbilder samt analyser och rekommendationer som privata och offentliga verksamheter kan använda i sitt fortsatta dataskyddsarbete.

2021 års rapport om personuppgiftsincidenter ingår i IMY:s rapportserie.² På webbplatsen www.imy.se finns våra rapporter för nedladdning under rubriken Publikationer.

1. Tidigare Datainspektionen.

2. Tidigare rapporter i rapportserien behandlar bl.a. anmälda personuppgiftsincidenter 2018 (2019:1), anmälda personuppgiftsincidenter 2019 (2020:2), personuppgiftsincidenter som beror på antagonistiska angrepp 2019 (2020:3) och klagomål mot personsöktjänster med frivilligt utgivningsbevis (2020:1).

Metod

Detta är IMY:s fjärde årsrapport om personuppgiftsincidenter. I den här undersökningen beskriver vi de personuppgiftsincidenter som anmäldes till IMY under 2021, och jämför utfallet med resultat från motsvarande undersökning för 2020.

I underlaget ingår 5 767 anmälda personuppgiftsincidenter 2021. Incidenterna delas in i olika kategorier för att skapa statistik och för att kunna beskriva förändringar över tid.

När personuppgiftsincidenter anmäls till IMY sker det i regel via e-tjänsten på IMY:s webbplats. Där finns olika e-blanketter som fylls i av personuppgiftsansvariga för att anmäla att en personuppgiftsincident har inträffat. Med hjälp av bland annat rullgardinsmenyer med flervalsalternativ beskriver den personuppgiftsansvariga omständigheterna kring den inträffade personuppgiftsincidenten.

IMY:s diariesystem läser därefter automatiskt av svaren i anmälan och registrerar bland annat:

- verksamhetsområde inom vilket incidenten inträffade
- typ av incident
- orsak till incidenten.

I vår undersökning utgår vi från dessa och andra indelningar när vi beskriver utfallet för 2021, och även för tidigare år.

Mer om metoden och kvaliteten i dataunderlaget finns att läsa i bilaga 1 *Hur ser materialet ut?*

Rapportens disposition

Rapporten inleds med en sammanfattning och IMY:s rekommendationer för att förebygga incidenter.

I del ett ger vi en översiktlig beskrivning av vad som utgör personuppgiftsincidenter som måste anmälas och hur vi arbetar med de incidenter som anmäls. Dessutom redovisar vi pågående och avslutade tillsynsärenden under 2021.

Del två handlar om inflödet av personuppgiftsincidenter till IMY. I del två redovisar vi statistik över det totala antalet rapporterade fall, vad det är för typ av personuppgiftsincident som inträffade och vad som uppges vara orsaken till att incidenten inträffade. Där det är relevant beskriver vi även förändringen mellan 2020 och 2021 räknat i antal fall.

Den tredje delen handlar om hur mönstren ser ut för olika verksamhetsområden. I denna del redovisar vi statistik över anmälda personuppgiftsincidenter uppdelat på olika verksamhetsområden för 2021 och jämför med föregående år. För läsbarhetens skull redovisar vi de tillhörande figurerna samlade i bilaga 2.

I den fjärde avslutande delen av rapporten ges en internationell jämförelse över personuppgiftsincidenter inom det Europeiska ekonomiska samarbetsområdet (EES).

Sist i rapporten finns två bilagor: *Hur ser materialet ut?* och *Figurer för personuppgiftsincidenter per verksamhetsområde*.



Del 1. Vad är en personuppgiftsincident och när ska den anmälas till IMY?

I denna del beskriver vi vad en personuppgiftsincident är och när verksamheter har en skyldighet att anmäla incidenter till IMY. Vi beskriver även vårt arbete med personuppgiftsincidenter och redogör för pågående och avslutade tillsynsärenden under 2021.



Vad är en personuppgiftsincident och när ska den anmälas till IMY?

Anmälningsplikt för vissa personuppgiftsincidenter

I dataskyddsförordningen finns en skyldighet för organisationer att anmäla vissa typer av personuppgiftsincidenter till IMY. En personuppgiftsincident är en säkerhetsincident som omfattar personuppgifter. Incidenten kan till exempel handla om att personuppgifter har blivit förstörda eller ändrade, gått förlorade eller kommit i orätta händer genom obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.³ 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. När en personuppgiftsincident har inträffat ska den personuppgiftsansvariga, så snart denna får vetskap om incidenten, bedöma vilken risk som incidenten kan medföra.⁴ Riskbedömningen är en viktig del i hanteringen av personuppgiftsincidenten och underlättar för den personuppgiftsansvariga att ta ställning till lämpliga åtgärder för att effektivt begränsa och åtgärda incidenten. Den är också avgörande för att avgöra om incidenten ska anmälas till IMY samt om de registrerade ska informeras.⁵

Om det *inte är osannolikt* att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter ska den anmälas till IMY inom 72 timmar från att den upptäckts.⁶ Sedan mars 2020 är det möjligt att skicka in anmälningar om personuppgiftsincidenter digitalt i och med lanseringen av myndighetens e-tjänst.

Vid riskbedömningen bör den personuppgiftsansvariga ta hänsyn till de specifika omständigheterna i samband med incidenten. Några faktorer att tänka på vid riskbedömningen är bland annat typen av incident, personuppgifternas natur, känslighet och volym, hur lätt det är att identifiera enskilda personer samt konsekvensernas svårighetsgrad för enskilda individer.⁷

Om det är osannolikt att incidenten leder till en risk för de registrerades fri- och rättigheter behöver incidenten inte anmälas till IMY. Det kan till exempel vara när personuppgifter redan finns allmänt tillgängliga och utlämnandet av sådana uppgifter inte utgör en sannolik risk för den enskilde.⁸ Oavsett om incidenten ska anmälas till IMY eller inte så är den personuppgiftsansvarige alltid skyldig att dokumentera incidenten internt.⁹

Information till de registrerade

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 IMY – också informera de registrerade om att incidenten inträffat. I dataskyddsförordningen anges att den personuppgiftsansvariga ska informera de registrerade utan onödigt dröjsmål. Syftet med informationen är bland annat att ge den enskilde möjlighet att vidta egna åtgärder för att skydda sig själv mot negativa konsekvenser av incidenten, till exempel genom att byta lösenord eller spärra ett bankkort.¹⁰

Den personuppgiftsansvarige ska åtminstone lämna följande information till de registrerade.¹¹

- En beskrivning av incidentens art.
- Namnet på och kontaktuppgifterna till dataskyddsombudet eller annan kontaktpunkt.
- En beskrivning av de sannolika konsekvenserna av incidenten.
- Åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda incidenten, inbegripet i förekommande fall åtgärder för att mildra dess potentiella negativa effekter.

3. En personuppgiftsincident är enligt artikel 4.12 i dataskyddsförordningen en säkerhetsincident som leder till oavsiktligt 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.

4. Artikel 29-arbetsgruppen för uppgiftsskydd, *Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679*, 2018.

5. Artikel 29-arbetsgruppen för uppgiftsskydd, *Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679*, 2018.

6. Artikel 33 dataskyddsförordningen.

7. Artikel 29-arbetsgruppen för uppgiftsskydd, *Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679*, 2018.

8. Artikel 29-arbetsgruppen för uppgiftsskydd, *Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679*, 2018.

9. Artikel 33.5 dataskyddsförordningen.

10. Skäl 86 dataskyddsförordningen, Artikel 29-arbetsgruppen för uppgiftsskydd, *Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679*, 2018.

11. Artikel 34 dataskyddsförordningen.

IMY:s arbete med personuppgiftsincidenter

IMY följer löpande inflödet av personuppgiftsincidenter som anmäls till myndigheten. Anmälningarna gör det bland annat möjligt att följa:

- vilka åtgärder som vidtas av de personuppgiftsansvariga för att motverka negativa effekter av incidenter
- vilka typer av personuppgiftsincidenter som är vanligt förekommande
- vilka verksamheter som anmäler personuppgiftsincidenter.

Informationen i de anmälda personuppgiftsincidenterna är ett viktigt underlag när vi i vår tillsynsplan identifierar riskområden som tillsyn bör inriktas mot.

IMY kan inleda tillsyn

IMY kan välja att inleda en tillsyn med anledning av en anmäld personuppgiftsincident. En tillsyn kan övervägas med anledning av exempelvis:

- hanteringen av själva incidenten och anmälan
- generella brister som incidenten indikerar
- att incidenten bedöms som särskilt allvarlig.

Det är inte ovanligt att en personuppgiftsincident också följs av klagomål till IMY. Ett klagomål kan medföra att tillsyn inleds. Även uppgifter i media eller tips kan föranleda att myndigheten inleder en tillsyn. Myndigheten kan då granska om en personuppgiftsincident har inträffat och om incidenten har rapporterats eller dokumenterats på ett korrekt sätt.

Att en anmälan om personuppgiftsincident inte föranleder någon åtgärd är inte detsamma som att IMY anser att allt har gått rätt till.

Oavsett om en anmälan leder till en tillsyn eller inte får den personuppgiftsansvariga alltid ett beslut från myndigheten med besked om att ärendet avslutats. Om tillsyn har inletts med anledning av den anmälda personuppgiftsincidenten finns även en hänvisning till tillsynsärendet i beslutet.

Tillsynsärenden som rör personuppgiftsincidenter

Under 2021 har ett trettiotal tillsynsärenden inletts baserade på anmälda personuppgiftsincidenter, vilket är betydligt fler än de tre tillsynsärenden som inleddes 2020. Det ökande antalet tillsynsärenden 2021 har främst sin förklaring i att tillsyn inletts mot flera bolag inom en och samma koncern med anledning av inrapporterade personuppgiftsincidenter.

Mer om IMY:s tillsynsärenden finns att ta del av på IMY:s webbplats: <https://www.imy.se/tillsyner/>.

Pågående tillsynsärenden under 2021

Avanza

IMY har inletts tillsyn mot Avanza med anledning av en inrapporterad personuppgiftsincident. Incidenten handlar om att personuppgifter, på grund av felaktiga inställningar, under en längre tid löpande förts över till Facebook. IMY granskar vad som har skett och vilka rutiner bolaget har för att ha kontroll på användarnas personuppgifter.

Diskrimineringsombudsmannen

IMY har inletts tillsyn mot Diskrimineringsombudsmannen (DO) med anledning av en personuppgiftsincident som DO lämnat in som rör ett webbformulär för att lämna in tips och klagomål. Enligt DO har ett analysverktyg, som används för att förbättra användarvänligheten på webbplats, i vissa fall kunnat inhämta och lagra personuppgifter, bland annat från det formulär på DO:s webbplats som besökare kan använda för att lämna in tips och klagomål. IMY granskar det som inträffat.

Länsförsäkringar

IMY har inletts tillsyn mot ett antal av Länsförsäkringars olika bolag med anledning av inkomna personuppgiftsincidenter. I anmälningarna framgår att personuppgifter, på grund av felaktiga inställningar, under en längre tid löpande förts över till Facebook. IMY granskar vad som skett och vilka rutiner bolagen har för att ha kontroll på användarnas personuppgifter.

Polismyndigheten

IMY har inletts tillsyn mot Polismyndigheten. IMY granskar Polismyndighetens rutiner för utskick av mejl med anledning av anmälda personuppgiftsincidenter som rör mejl som oavsiktligt hamnade hos fel mottagare.

Region Uppsala

IMY har inlett tillsyn med anledning av en personuppgiftsincident från Region Uppsala. IMY granskade bakgrunden till att Region Uppsala skickat patientuppgifter med mejl utan kryptering.¹²

Tullverket

IMY har inlett tillsyn mot Tullverket. IMY granskar hur Tullverket använder mobiltelefoner i sin brottsbekämpande verksamhet samt omständigheterna kring den personuppgiftsincident som anmälts till IMY där personal på Tullverket har använt en app i sina mobiltelefoner som för över personuppgifter till en molntjänst.

Avslutade tillsynsärenden under 2021

Voice Integrate AB och MedHelp AB

IMY inledde 2019 tillsyn mot MedHelp AB och Voice Integrate AB (Voice).¹³ Tillsynen av bolagen är en del av IMY:s granskning med anledning av incidenten kring 1177 som omfattade sex tillsynsärenden, tre företag och tre regioner. Incidenten, där inspelade samtal till rådgivningsnumret 1177 legat tillgängliga utan lösenordsskydd eller annan säkerhet på en webbserver hos Voice Integrate Nordic AB (Voice), uppmärksammades först i media. Tillsynen mot personuppgiftsansvariga MedHelp AB och personuppgiftsbiträdet Voice grundade sig på de anmälningar som bolagen lämnat in med anledning av incidenten. I granskningen utreddes ansvarsförhållandena kring personuppgiftsbehandlingen när vårdsökande tog kontakt med sjukvårdsrådgivningen på telefon genom att ringa 1177. Samtliga tillsynsärenden avslutades i juni 2021.

IMY beslutade att MedHelp AB ska betala en administrativ sanktionsavgift på 12 miljoner kronor, varav åtta miljoner kronor avsåg säkerhetsincidenten med exponerade ljudfiler med inspelade telefonsamtal till 1177 mot internet utan skydd, tre miljoner kronor avsåg att MedHelp utfört personuppgiftsbehandling genom att anlita ett personuppgiftsbiträde med verksamhet i Thailand (MediCall), 500 000 kronor avsåg att MedHelp inte lämnat nödvändig information till vårdsökande som ringde 1177 och 500 000 kronor avsåg att MedHelp inte hade säkerhetskopierat ljudfiler i sin it-miljö. Beslutet omfattade också två förelägganden. Beslutet har överklagats.

IMY beslutade att Voice skulle betala en administrativ sanktionsavgift på 650 000 kronor. IMY konstaterade att personuppgifter i ljudfiler med inspelade telefonsamtal till 1177 hade exponerats mot internet utan skydd i Voice:s lagringsserver Voice NAS. Voice hade därvid i egenskap av personuppgiftsbiträde till MedHelp underlåtit att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som var lämplig för att förhindra obehörigt röjande av personuppgifterna eller obehörig åtkomst till personuppgifterna. Beslutet har överklagats.

12. IMY fattade beslut den 26 januari 2022 i ärendet och utfärdade två administrativa sanktionsavgifter, en på 300 000 kronor mot regionstyrelsen i Region Uppsala och en på 1,6 miljoner mot sjukhusstyrelsen i Region Uppsala. Mer information finns på IMY:s webbplats: <https://www.imy.se/tillsyner/region-uppsala-personuppgiftsincidenter/>

13. För mer information om IMY:s granskning av incidenten kring 1177 se IMY:s rapport (DI-2021-5220), Integritetsskyddsmyndighetens kontroll av behandling av uppgifter om vårdsökande i samband med samtal till 1177 – en rapport.

Del 2. Redovisning av personuppgiftsincidenter 2021

I denna del beskriver vi inflödet av personuppgiftsincidenter till IMY år 2021 jämfört med år 2020. Förutom inflödet över tid redovisar vi vanliga typer av incidenter och vad som oftast anges som deras orsak.



Anmälda personuppgiftsincidenter

Anmälningar av personuppgiftsincidenter utifrån dataskyddsförordningen ökade med en fjärdedel 2021 samtidigt som anmälningar utifrån brottsdatalagen minskade med nästan en femtedel mot föregående år. I genomsnitt rapporterades 111 fall till IMY per vecka 2021, och nästan en fjärdedel av incidenterna inträffade inom området Statliga myndigheter och domstolar.

Inflödet ökade med 26 procent

Anmälningar om personuppgiftsincidenter görs antingen utifrån bestämmelser i dataskyddsförordningen (GDPR) eller i brottsdatalagen (BDL). Tabell 1 visar att den absoluta merparten av incidentanmälningar både 2020 och 2021 handlade om incidenter enligt GDPR. Ett förhållandevis litet antal anmälningar till IMY görs utifrån BDL. 2021 avsåg endast 41 anmälningar brottsdatalagen, vilket är en minskning med 18 procent mot föregående år då 50 incidentanmälningar avsåg BDL.

Det ökade inflödet av incidentanmälningar 2021 kan möjligtvis förklaras av en viss överrapportering från offentlig sektor av incidenter som inte är anmälningspliktiga. En annan bidragande faktor kan vara de granskningar media gjorde under 2021, speciellt inom den offentliga sektorn, som medförde att fler incidenter anmäldes direkt i anslutning till medierapporteringen.¹⁴

14. Till exempel: <https://sverigesradio.se/artikel/skrivfel-orsak-till-att-ip-adresser-skickades-till-google>

	2020	2021	Skillnad	Skillnad (procent)
Dataskyddsförordningen	4 538	5 726	+1 188	+26
Brottsdatalagen	50	41	-9	-18
Totalt	4 588	5 767	1 179	+26

Tabell 1. Anmälda personuppgiftsincidenter 2020 och 2021, fördelat på dataskyddsförordningen och brottsdatalagen.

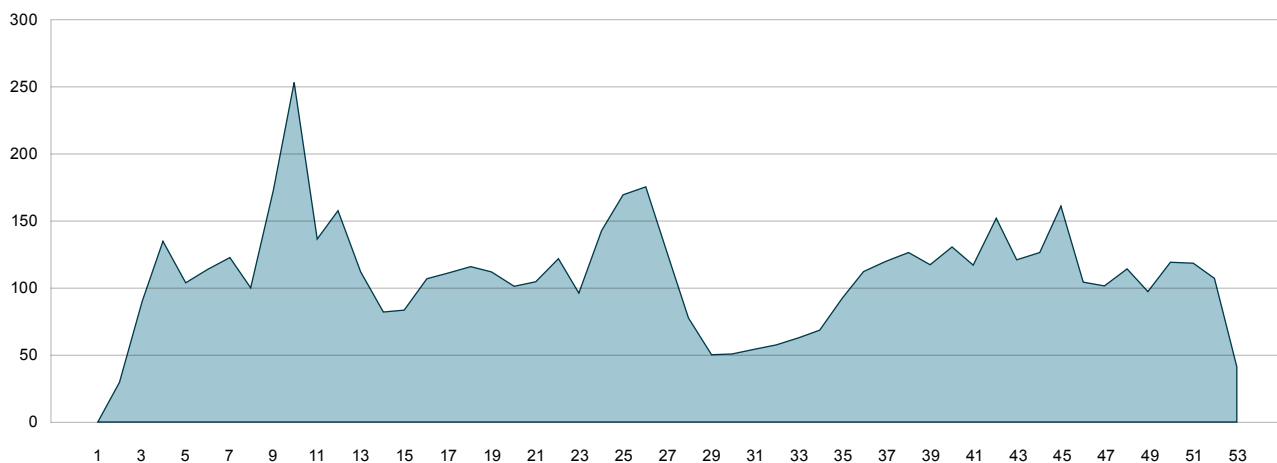


Inflödet i genomsnitt under 2021

När vi studerar 2021 års inflöde ser vi att det var ojämnt fördelat under året, vilket visas i figur 1. I genomsnitt anmäldes 111 personuppgiftsincidenter per vecka. Det är en ökning med 26 procent mot föregående år, då i snitt 87 incidenter anmäldes per vecka.

Inflödet var förhållandevis lågt i början och i slutet av året och under sommaren. Variationen i inflödet kan sannolikt förklaras med att semesterperioder på vintern och sommaren fick tillflödet att bromsa in tillfälligt. Under de sex sommarveckorna i juli och augusti anmäldes ungefär 50 till 70 fall per vecka.

Toppen under vecka 9 och 10 kan förklaras av att flera offentliga aktörer anmälde personuppgiftsincidenter med anledning av uppgifter som hade kommit fram i granskningar som gjordes av media.



Figur 1. Antal anmälda personuppgiftsincidenter per vecka 2021.



Fördelning på olika verksamhetsområden

IMY:s tidigare undersökningar av personuppgiftsincidenter visar att majoriteten av alla incidenter som anmäls till myndigheten inträffar inom den offentliga sektorn. Av figur 2 framgår att totalt 66 procent av de incidenter som rapporterades 2021 kom från offentlig sektor, det är mer än dubbelt så många som från den privata sektorn. 2020 rapporterade offentlig sektor 67 procent av alla personuppgiftsincidenter.



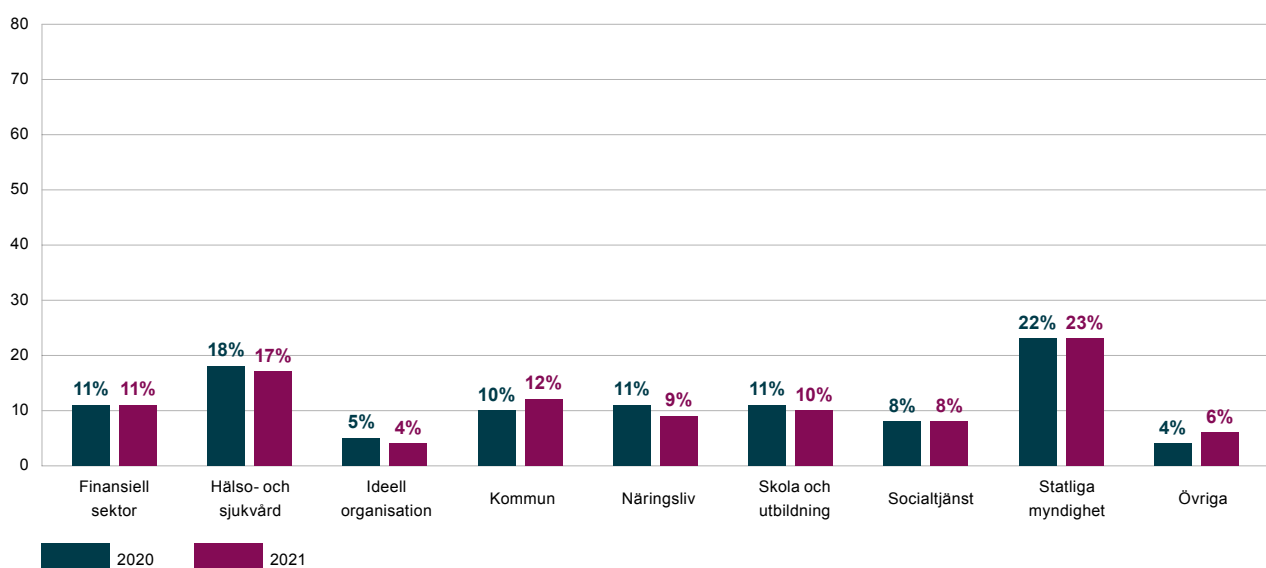
Figur 2. Andel av anmälda personuppgiftsincidenter 2021, fördelat på sektorer. Anmälda incidenter som inte kunde ordnas in i någon sektor redovisas i figuren som 'uppgift saknas'.

Att offentlig sektor fortsatt står för den största andelen beror sannolikt på ett flertal faktorer. Många verksamheter inom offentlig sektor behandlar stora mängder personuppgifter och ofta även känsliga personuppgifter, vilket kan bidra till att fler incidenter betraktas som anmälningspliktiga vid riskbedömningen. En annan möjlig förklaring är att rutinerna blivit mer etablerade för att rapportera incidenter internt och anmäla dem till IMY. Även det faktum att det skett flera incidenter i offentlig sektor som fått stor massmedial uppmärksamhet kan ha bidragit till en ökad medvetenhet och anmälningsbenägenhet. Att en organisation eller en bransch anmäler många personuppgiftsincidenter behöver alltså 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.

Statliga myndigheter anmäler flest personuppgiftsincidenter

Figur 3 visar de olika verksamhetsområdenas andel av samtliga anmälda personuppgiftsincidenter de senaste två åren. Följande tre verksamhetsområden anmälde flest personuppgiftsincidenter 2021:

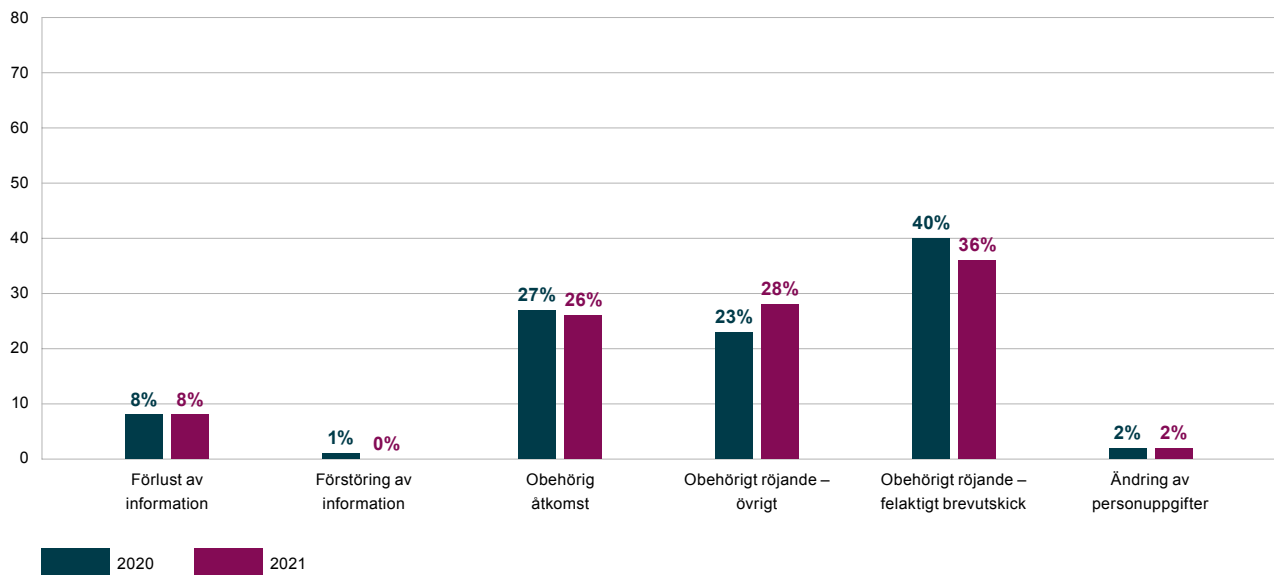
- Statlig myndighet och domstol (23 procent)
- Hälso- och sjukvård (17 procent)
- Kommun (12 procent).



Figur 3. Fördelning av anmälda personuppgiftsincidenter på verksamhetsområde 2020 och 2021 i procent. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Typ av personuppgiftsincident

Personuppgifter kan på olika sätt röjas för någon som saknar behörighet. Två av tre rapporterade incidenter 2021 handlade om någon form av obehörigt röjande antingen genom felaktiga brevutskick eller genom annan felaktig hantering av personuppgifter. Men även fall där någon berett sig olovlig tillgång till personuppgifter var vanliga; 2021 handlade var fjärde incident om obehörig åtkomst.



Figur 4. Andel av anmälda personuppgiftsincidenter fördelat på typ av incident 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Obehörigt röjande på grund av felaktigt brevutskick

Felaktiga brevutskick är brev, mejl eller sms som innehåller personuppgifter och oavsiktligt hamnat hos fel mottagare. Under 2021 utgjorde felaktiga brevutskick 36 procent av samtliga personuppgiftsincidenter som anmälades till IMY. Det är en minskning mot föregående år då andelen felaktiga brevutskick utgjorde 40 procent av de anmälda incidenterna. Om vi redovisar förändringen i antal så har det skett en ökning med ungefär 250 fall.

Obehörigt röjande av andra anledningar

Den näst vanligaste typen av personuppgiftsincidenter 2021 stod övriga fall av obehörigt röjande för. Obehörigt röjande innebär att den personuppgiftsansvariga eller någon under den personuppgiftsansvarigas ledning hanterat personuppgifter 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 personuppgifter kommit till fel mottagares kännedom. Denna typ av incidenter ökade jämfört med tidigare år och utgjorde 28 procent av samtliga anmälda personuppgiftsincidenter 2021. Sett till antal innebär det en ökning med närmare 500 fall, från ungefär 1 100 till 1 600.

Obehörig åtkomst

Obehörig åtkomst handlar om att någon olovligt berett sig tillgång till personuppgifter, till exempel genom att behörigheter till ett it-system har tilldelats felaktigt eller alltför generellt. Det kan exempelvis handla om att personuppgifter har funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning. Även antagonistiska angrepp genom olika typer av hackning¹⁵,

som till exempel spoofing¹⁶, phishingattacker¹⁷ eller malware¹⁸, förekommer inom kategorin obehörig åtkomst. 2021 utgjorde denna typ av incidenter 26 procent av samtliga incidentanmälningar. Räknet i antal innebär det en ökning med ungefär 300 fall mot 2020.

Förlust

Förlust handlar om att information gått förlorad på något sätt, till exempel genom att en tjänstедator blivit stulen eller glömts på allmän plats, att organisationen haft inbrott eller blivit utsatt för ett antagonistiskt angrepp. Dessutom kan tekniska fel leda till att personuppgifter går förlorade. Förlust utgjorde en relativt liten andel av anmälningarna, endast 8 procent 2021. Jämfört med 2020 innebär detta ändå en ökning i antal med ungefär 100 fall.

Ändring av personuppgifter

Ändring av personuppgifter innebär att personuppgifter ändrats på något sätt. Att personuppgifter ändras förekommer i förhållandevis liten utsträckning; 2 procent av incidentanmälningarna under 2021 rörde ändring av personuppgifter.

Förstöring av information

Förstöring innebär att någon eller något har förstört information. Endast några få incidentanmälningar om förstöring av information har kommit in till IMY under 2020 och 2021.

15. Hackning innebär i ett angripssammanhang att någon bryter sig in i it-system utan användarens samtycke eller vetskap och är att betrakta som ett dataintrång.

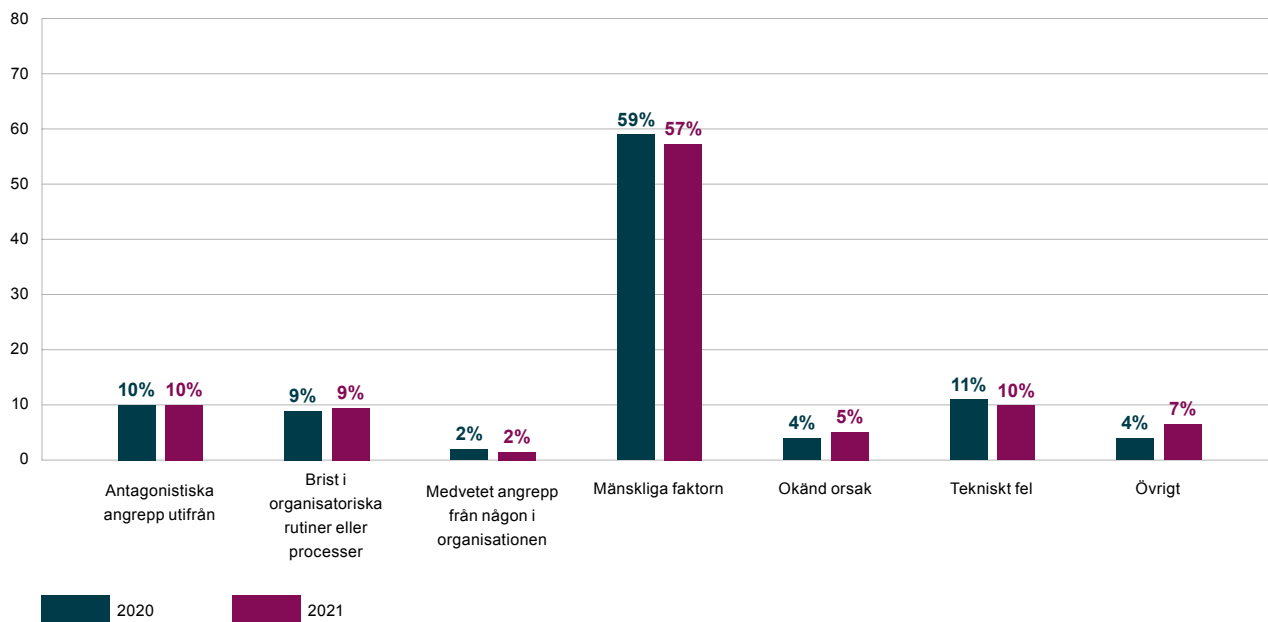
16. Spoofing är en metod där någon utnyttjar någon annans identitet på internet för att genomföra skadliga eller bedrägliga handlingar, till exempel när en angripare försöker efterlikna kända avsändare.

17. Phishing eller nätfiske är en metod för it-brottslighet där internetanvändare luras att lämna ut personlig information, som exempelvis inloggningsuppgifter, som sedan kan användas för att ta över konton och genomföra bedrägerier.

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

Orsaker till personuppgiftsincidenter

Under 2021 fortsatte den mänskliga faktorn att vara den vanligaste orsaken till alla rapporterade fall av personuppgiftsincidenter till IMY. De senaste två åren stod den mänskliga faktorn för mer än hälften av alla rapporterade fall.



Figur 5. Andel av anmälda personuppgiftsincidenter fördelat på orsak 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Den mänskliga faktorn

Incidenter som beror på den mänskliga faktorn består i huvudsak av individer som 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. Omkring hälften av de incidenter som beror på den mänskliga faktorn handlar om felskickade brev, mejl eller sms.

2021 angavs den mänskliga faktorn som orsak i 57 procent av samtliga incidentanmälningar som registrerades av IMY. Motsvarande siffra 2020 var 59 procent. Räknat i antal anmälda personuppgiftsincidenter innebär det en ökning med ungefär 600 fall.

Tekniska fel

Tekniska fel handlar ofta om fel i programvara, till exempel att kunder inte kan logga in på sina konton.

Tekniska fel uppgavs vara orsaken till 10 procent av alla anmälda incidenter 2021, vilket innebär att det har skett en ökning i antal med ungefär 100 fall från 2020 till 2021.

Antagonistiska angrepp

Personuppgiftsincidenter som har sin förklaring i att någon obehörig utanför organisationen försöker ta del av uppgifter den inte har rätt till klassas i IMY:s statistik som antagonistiska angrepp.¹⁹ Metoderna som används för att komma över information varierar. Till exempel kan det handla om fall av digitala angrepp med hjälp av exempelvis phishing eller ransomware. Men det kan också handla om fysiska stölder som lett till att information gått förlorad till exempel på grund av inbrott i organisationens lokaler eller att en dator blivit stulen.

Antagonistiska angrepp stod för 10 procent av anmälningarna 2021 och ökade i antal med ungefär 100 fall jämfört med 2020.

19. IMY (tidigare Datainspektionen) släppte under 2020 en temarapport om anmälda personuppgiftsincidenter som orsakats av antagonistiska angrepp. Rapporten innehåller bland annat rekommendationer, beskrivning av olika typer av antagonistiska angrepp samt statistik över de verksamhetsområden som anmält incidenter orsakade av antagonistiska angrepp. Datainspektionens rapport (2020:3), Personuppgiftsincidenter som beror på antagonistiska angrepp 2019.

Brister i organisatoriska rutiner eller processer

Incidenter som beror på brister i organisatoriska rutiner eller processer kan exempelvis handla om att verksamhetens rutiner inte är tillräckligt tydliga eller att de är bristfälliga i fråga om mejlhantering eller behörighetstilldelning.

Incidenter som beror på brister i organisatoriska rutiner och processer stod för 9 procent av samtliga rapporterade fall 2021, vilket i antal innebär en ökning med ungefär 100 fall.

Medvetna angrepp från någon i organisationen

Att personuppgiftsincidenter förorsakas av medvetna angrepp från någon i organisationen förekommer i förhållandevis liten utsträckning och endast få fall rapporteras varje år sedan anmälningsplikten infördes. Incidenterna kan handla om att en anställd har delat med sig av sekretessbelagd information eller inloggningsuppgifter till obehörig, eller att en anställd har tagit del av uppgifter den anställda inte hade rätt till.

Under 2021 kunde 2 procent av incidenterna tillskrivas medvetna angrepp av någon i organisationen.

Okänd orsak

Ibland händer det att personuppgiftsincidenter anmäls till IMY utan att orsaken till felet är fastställd vid tidpunkten för anmälan och att en utredning fortfarande pågår.

2021 utgjorde incidenter med okänd orsak 5 procent av samtliga fall som rapporterades till IMY.

Övrigt

Övriga personuppgiftsincidenter kan vara sådant som anmälaren inte tycker passar in i någon av de andra kategorierna i anmälningsblanketten, som till exempel inbrott i bilen eller att information skickats okrypterat i mejl mellan anställda. Under de senaste två åren har detta förekommit allt oftare.

Under 2021 markerades 7 procent av incidentanmälningarna som övrigt. Det är en ökning med ungefär 200 fall jämfört med 2020.

Del 3. Redovisning av personuppgiftsincidenter 2021 per verksamhetsområde

I denna del beskriver vi kortfattat de vanligaste personuppgiftsincidenter uppdelat på olika verksamhetsområden. Den uppdelade statistiken kan användas som underlag vid reflektioner över arbetet med personuppgiftsincidenter och dataskydd i den egna organisationen. I bilaga 2 finns tillhörande figurer.



Anmällda personuppgiftsincidenter inom olika verksamhetsområden

Inom de flesta områdena minskade andelen incidenter som rapporterades bero på obehörig åtkomst och andelen antagonistiska angrepp 2021 jämfört med 2020. Hälso- och sjukvården och kommunal sektor uppvisade dock en avvikande utveckling med en ökad andel incidenter som berodde på obehörig åtkomst.

Felaktiga brevutskick vanligast

2021 stod felaktiga brevutskick för mer än en tredjedel av samtliga incidentanmälningar till IMY, vilket visas i figur 4. Felaktiga brevutskick var också den vanligaste personuppgiftsincidenten inom ett flertal verksamhetsområden, vilket framgår av figurerna i bilaga 2.

Inom följande verksamhetsområden handlade omkring 40 procent eller mer av fallen om felaktiga brevutskick under 2021:

- Ideell organisation eller ekonomisk förening (54 procent)
- Finansiell sektor eller försäkring (52 procent)
- Statlig myndighet och domstol (41 procent)
- Socialtjänst (39 procent).

En möjlig förklaring till att felaktiga brevutskick är vanligast inom dessa områden kan vara att de i stor utsträckning skickar personuppgifter per post eller mejl.

Den mänskliga faktorn orsakar många incidenter

Den mänskliga faktorn anges oftast som förklaring för att en incident inträffade. Generellt sett hade mer än hälften av alla personuppgiftsincidenter den mänskliga faktorn som sin orsak under 2021, vilket framgår av figur 5. Mönstret återfinns också i alla verksamhetsområden med undantag för Näringslivet där även antagonistiska angrepp var en viktig orsak, vilket framgår av figur 16 i bilaga 2.

Under 2021 låg den mänskliga faktorn bakom mer än hälften av fallen inom följande områden:

- Statlig myndighet och domstol (70 procent)
- Ideell organisation eller ekonomisk förening (68 procent)
- Finansiell sektor eller försäkring (65 procent)
- Socialtjänst (62 procent)
- Hälso- och sjukvård (59 procent).

Obehörig åtkomst

2021 rapporterades en fjärdedel av alla personuppgiftsincidenter inom kategorin obehörig åtkomst, vilket framgår av figur 4. Obehörig åtkomst handlar om att någon olovligen berett sig tillgång till personuppgifter. Det kan ha skett genom att behörigheter till ett it-system tilldelats felaktigt eller alltför generellt, att personuppgifter funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning eller genom antagonistiska angrepp med hjälp av hackning.

Inom följande verksamhetsområden utgjorde obehörig åtkomst 30 procent eller mer av samtliga inom området rapporterade fall, vilket framgår av bilaga 2:

- Näringsliv i övrigt (46 procent)
- Hälso- och sjukvård (31 procent)
- Kommun (30 procent).

En möjlig förklaring bakom incidenterna skulle kunna vara att dessa verksamheter i mindre utsträckning kommunicerar mejl- eller brevledes med integritetskänsliga uppgifter.

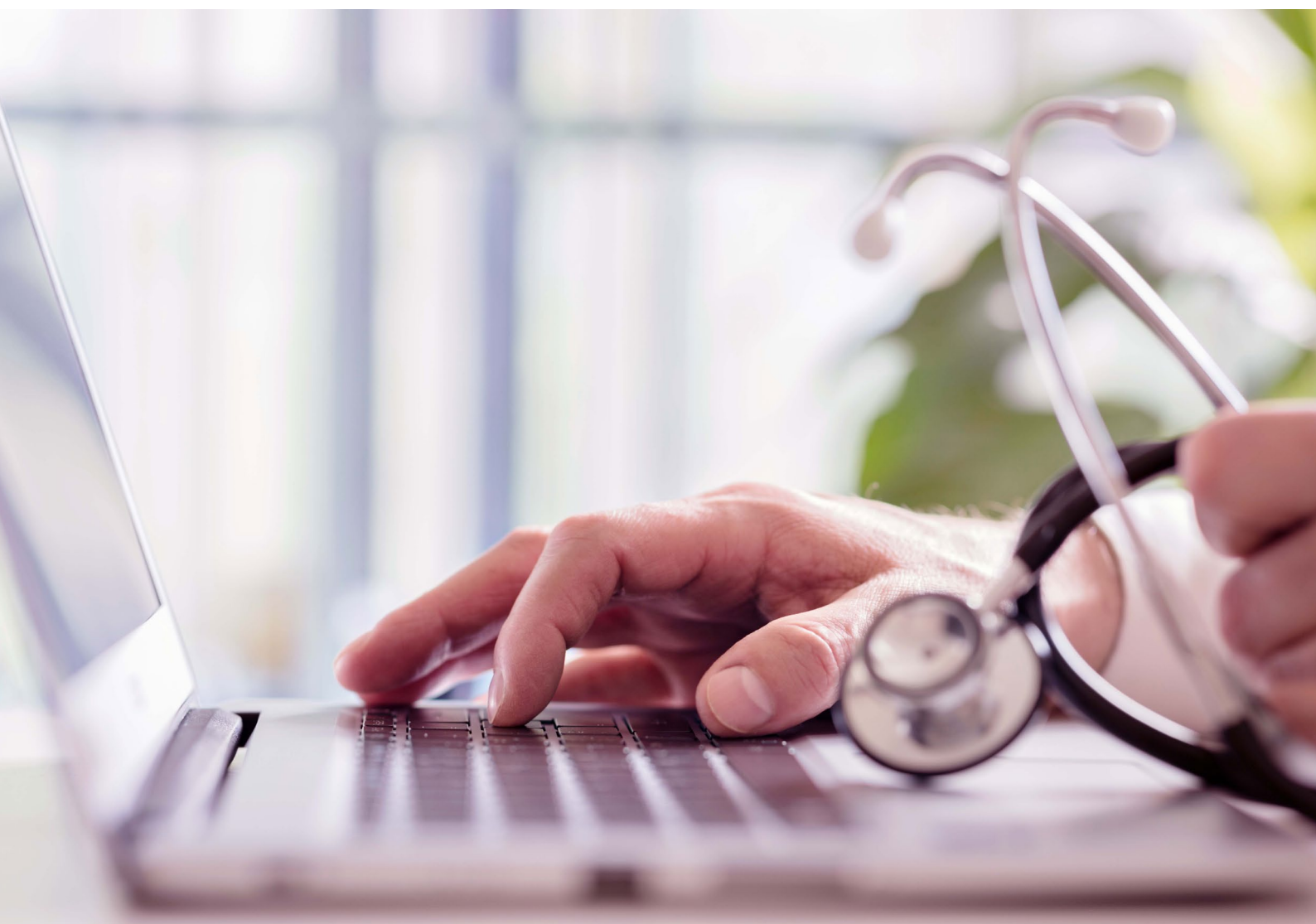
Inom de flesta sektorerna minskade andelen incidenter som rapporterades bero på obehörig åtkomst och andelen antagonistiska angrepp 2021 jämfört med 2020. Hälso- och sjukvården och kommunal sektor uppvisade dock en avvikande utveckling med en ökad andel incidenter som berodde på obehörig åtkomst. Inom hälso- och sjukvården rapporterades dessutom en väsentligt högre andel antagonistiska angrepp mot föregående år. Eftersom hälso- och sjukvården och kommunal sektor i stor utsträckning hanterar känsliga personuppgifter riskerar en incident att medföra stor skada för de registrerade. Det är därför viktigt att ta riskerna på allvar.

I juni 2020 flaggade Myndigheten för samhällsskydd och beredskap (MSB) för att särskilt hälso- och sjukvården kunde komma att bli utsatt för fler antagonistiska angrepp framöver, till exempel genom att utsättas för attacker med så kallad ransomware. MSB började under 2020 att genomföra en riktad informationsinsats mot hälso- och sjukvården om förebyggande åtgärder och rekommendationer för att minska risken för att bli utsatt för sådana attacker.

Utifrån den avvikande utveckling som noteras för 2021 inom framför allt hälso- och sjukvårdsområdet men även kommunsektorn ser IMY att det kan finnas särskilda behov av att se över tekniska och organisatoriska åtgärder för att förhindra obehörig åtkomst inom dessa verksamhetsområden. Men även andra områden bör systematiskt arbeta för att förebygga eventuella angrepp och därmed obehörig åtkomst.

I rapporten om personuppgiftsincidenter som beror på antagonistiska angrepp²⁰ sammanställde IMY ett antal generella rekommendationer som bör uppmärksammas i sammanhanget.

20. Datainspektionens rapport 2020:3, Personuppgiftsincidenter som beror på antagonistiska angrepp 2019.





Del 4. Sverige jämfört med andra länder under 2021

I denna del presenterar vi en kort beskrivning av utvecklingen för personuppgiftsincidenter enligt GDPR inom det Europeiska ekonomiska samarbetsområdet (EES) och Storbritannien. EES består av EU:s 27 medlemsländer plus Norge, Island och Liechtenstein.²¹ Den internationella statistiken inom området kan av olika orsaker vara osäker. Till exempel kan det finnas ett mörkertal beroende på graden av underrapportering i olika länder.



21. Statistiken i detta avsnitt går tillbaka till advokatbyrån DLA Pipers senaste sammanställning över sanktionsavgifter och personuppgiftsincidenter inom EES: DLA Piper GDPR fines and data breach survey: January 2022. DLA Pipers rapport avser perioden 28 januari 2021 till 27 januari 2022 och ställdes samman av DLA Pipers team för cybersäkerhet och dataskydd.

Internationell jämförelse

Inom EES anmäldes runt 130 000 incidenter under perioden 28 januari 2021 till 27 januari 2022. Baserat på utvecklingen i andra länder är IMY:s bedömning att det fortfarande finns ett stort mörkertal av anmälningspliktiga incidenter som inte anmäls.

Stor variation mellan länderna

I förhållande till befolkningens mängden rapporterade Sverige 55 personuppgiftsincidenter per 100 000 invånare 2021 jämfört med andra länder inom EES.²² Föregående år hade Sverige 48 anmälda incidenter per 100 000 invånare. Flest anmälningar per 100 000 invånare 2021 rapporterades till tillsynsmyndigheterna i Nederländerna, Liechtenstein och Danmark, vilket framgår av tabell 2.

Att Nederländerna och Danmark har ett stort antal anmälda incidenter per 100 000 invånare beror sannolikt på att länderna haft skyldighet att rapportera incidenter även före införandet av dataskyddsförordningen. Även Irland har sedan 2011 haft frivillig incidentanmälan. Erfarenheter från dessa länder, som hade mellan 130 till 150 rapporterade personuppgiftsincidenter per 100 000 invånare, talar för att antalet anmälningar kan komma att öka även i andra länder inom EES.

Eftersom incidenter ska anmälas till det land där ett företag har sitt huvudkontor, ökar också antalet anmälningar i länder där många internationella företag finns, till exempel på Irland. Andra faktorer som kan påverka antalet incidentanmälningar är den nationella dataskyddsmyndighetens arbete, både i form av vägledning, tillsyn och administrativa sanktionsavgifter. Även olika länders tradition och erfarenhet av inrapportering till statliga myndigheter kan påverka.

Sammanställningen i tabell 2 visar en stor spännvidd mellan länder högt upp på listan och länder längre ned. Så rapporterades till exempel 100 gånger fler personuppgiftsincidenter i Nederländerna, med runt 150 fall per 100 000 invånare, än i Grekland, med under 1,5 fall. Den stora variationen tyder på att det sannolikt finns en underrapportering av personuppgiftsincidenter till de nationella dataskyddsmyndigheterna i ett antal länder.

Stigande trend trots mörkertal inom EES

Inom EES anmäldes runt 130 000 personuppgiftsincidenter enligt GDPR under perioden 28 januari 2021 till 27 januari 2022.²³ Det betyder att i genomsnitt 356 fall dagligen rapporterades till de nationella dataskyddsmyndigheterna under perioden, vilket är en ökning med 8 procent jämfört med föregående period 2020. Det faktiska antalet personuppgiftsincidenter kan dock ligga väsentligt högre med tanke på ett sannolikt mörkertal.

	Antal incidenter per 100 000 invånare	Skillnad mot 2020
Nederländerna	151	1
Liechtenstein	136	6
Danmark	131	-2
Irland	130	-1
Finland	86	0
Tyskland	79	3
Slovenien	72	-3
Luxemburg	58	-1
Sverige	55	1
Norge	44	1
Island	44	-5
Polen	34	1
Malta	22	-1
Estland	15	1
Belgien	14	2
Litauen	14	3
Ungern	14	0
Österrike	10	-3
Cypern	8	-1
Frankrike	7	3
Slovakien	5	*
Lettland	5	-2
Spanien	4	-2
Italien	3	1
Kroatien	2	-1
Tjeckien	2	-4
Grekland	1	0

Tabell 2. Antal anmälda personuppgiftsincidenter per 100 000 invånare mellan 28 januari 2021 och 27 januari 2022.

* Information saknas.

Källa: DLA Piper GDPR fines and data breach survey: January 2022.

22. DLA Piper GDPR fines and data breach survey: January 2022, s. 17.

23. DLA Piper GDPR fines and data breach survey: January 2022, s. 4.

Bilaga 1. Hur ser materialet ut och vilka indelningar finns?

I denna bilaga redovisar vi grundläggande information om dataunderlaget för statistiken och rapportens kategorier.





Dataunderlaget för statistiken

Antal anmälda personuppgiftsincidenter de senaste två åren

2020 och 2021 anmäldes olika många personuppgiftsincidenter till IMY, 4 588 respektive 5 767. Det är en volymökning med ungefär 1 200 fall.

När vi i rapporten gör jämförelser baserat på en andelsmässig fördelning är det viktigt att komma ihåg att volymerna har varierat över tid. Som en följd kan det hända att en kategori minskade andelsmässigt, trots att antalet fall inom kategorin ökade. Den mänskliga faktorn angavs till exempel som orsak i 57 procent av samtliga anmälningar som registrerades av IMY 2021, motsvarande siffra 2020 var 59 procent. Räknat i antal anmälda personuppgiftsincidenter 2021 innebar det en ökning med ungefär 600 fall jämfört med 2020.

Överrapportering och mörkertal

Genom dataskyddsförordningen (GDPR)²⁴ infördes i maj 2018 en skyldighet för privata och offentliga verksamheter som behandlar personuppgifter att rapportera vissa personuppgiftsincidenter till IMY. Kort efter infördes motsvarande anmälningsskyldighet för brottsbekämpande myndigheter i brottsdatalagen.²⁵ IMY bedömer att merparten av de personuppgiftsincidenter som anmäldes under 2021 utgörs av faktiska incidenter. En viss överrapportering i form av icke-anmälningsskyldiga incidenter förekommer sannolikt fortfarande.

Samtidigt gör IMY bedömningen att det i Sverige fortfarande finns ett stort mörkertal i form av anmälningsskyldiga incidenter som inte anmäls. Anmälningsskyldigheten är fortfarande förhållandevis ny och rutinerna för att upptäcka och anmäla personuppgiftsincidenter är inte fullt ut etablerade. Detta kan påverka såväl antal som vilka incidenter som anmäls till IMY.

24. 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).

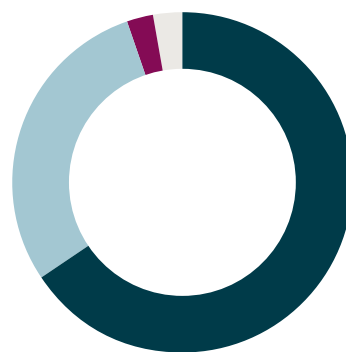
25. Dataskyddsförordningen infördes den 25 maj 2018 och brottsdatalagen den 1 augusti 2018.



Bortfall finns

En del av bortfallet kan härledas till att IMY i mars 2020 lanserade en e-tjänst för anmälningar av personuppgiftsincidenter. Det stora flertalet anmälningar lämnas sedan dess till myndigheten digitalt. Ibland förekommer det dock att anmälningar görs per post eller mejl. Dessa anmälningar registreras manuellt och systemet har då inte möjlighet att läsa av dem, varför inga nyckelord och därmed heller ingen statistik finns för dessa anmälningar. Bortfallet är marginellt och påverkar inte statistiken.

För att skapa statistik utifrån anmälningarna sorterar vi dataunderlaget efter olika kategorier. Vid varje sortering finns ett mindre bortfall. Dessa kan uppstå på grund av att uppgifter är ofullständiga av något skäl. Ett sådant exempel ser vi när vi delar in dataunderlaget i sektorer, figur 6. Då saknar 154 stycken anmälningar information om vilken sektor de tillhör.



Offentliga sektorn	3790
Privata sektorn	1674
Övriga sektorer	149
Uppgift saknas	154
Totalt	5767

Figur 6. Antal anmälda personuppgiftsincidenter 2021, fördelat på sektor.

Redovisade kategorier

När personuppgiftsincidenter anmäls till IMY sker det i regel via e-tjänsten på IMY:s webbplats. Där finns olika e-blanketter som fylls i av personuppgiftsansvariga för att anmäla att en personuppgiftsincident har inträffat. I blanketten förekommer rullgardinsmenyer med flervalsoalternativ som den personuppgiftsansvariga fyller i utifrån sin egen bedömning av omständigheterna kring incidenten. IMY gör ingen egen bedömning om den beskrivning som ges är "rätt" eller "fel", utan utgår från vad personuppgiftsansvariga har angett.

IMY:s diariesystem läser automatiskt av svaren i anmälan och registrerar bland annat:

- verksamhetsområde inom vilken incidenten inträffade
- typ av incident
- orsak till incidenten.

Verksamhetsområde

I rapporten utgår vi i huvudsak från de verksamhetsområden som finns i e-tjänstens blankett på IMY:s webbplats för anmälan av personuppgiftsincident enligt dataskyddsförordningen. I vissa fall har vi dock grupperat verksamhetsområden för att kunna ge en mer överskådlig bild av utvecklingen.

Här listas de verksamhetsområden som redovisas i rapporten och de undergrupper som en del verksamhetsområden inkluderar 2021:

- Finansiell sektor eller försäkringar
- Hälso- och sjukvård
- Ideell organisation eller ekonomisk förening
- Kommun
- Näringsliv i övrigt
 - Näringslivet i övrigt
 - Kreditupplysning
 - Inkasso
- Skola och utbildning
 - Skola: förskola, grundskola, gymnasium
 - Universitet eller högskola
 - Annan eftergymnasial utbildning
- Socialtjänst
- Statlig myndighet och domstol
 - Statliga myndigheter
 - Polis
 - Domstolar
 - Rättsväsendet i övrigt
- Övrigt

Typ av incident

Denna kategori består av sex typer av personuppgiftsincidenter:

- förlust av information
- förstöring av information
- obehörigt röjande - felaktigt brevutskick
- obehörigt röjande - övrigt
- obehörig åtkomst
- ändring av personuppgifter.

Orsaken till incidenten

Inom denna kategori redovisar vi sju olika skäl till personuppgiftsincidenter:

- antagonistiskt angrepp
- brist på organisatoriska rutiner eller processer
- medvetet angrepp från någon i organisationen
- mänskliga faktorn
- okänd orsak
- tekniskt fel
- övrigt.

Sektor

Inom denna kategori redovisar vi sju olika skäl till personuppgiftsincidenter:

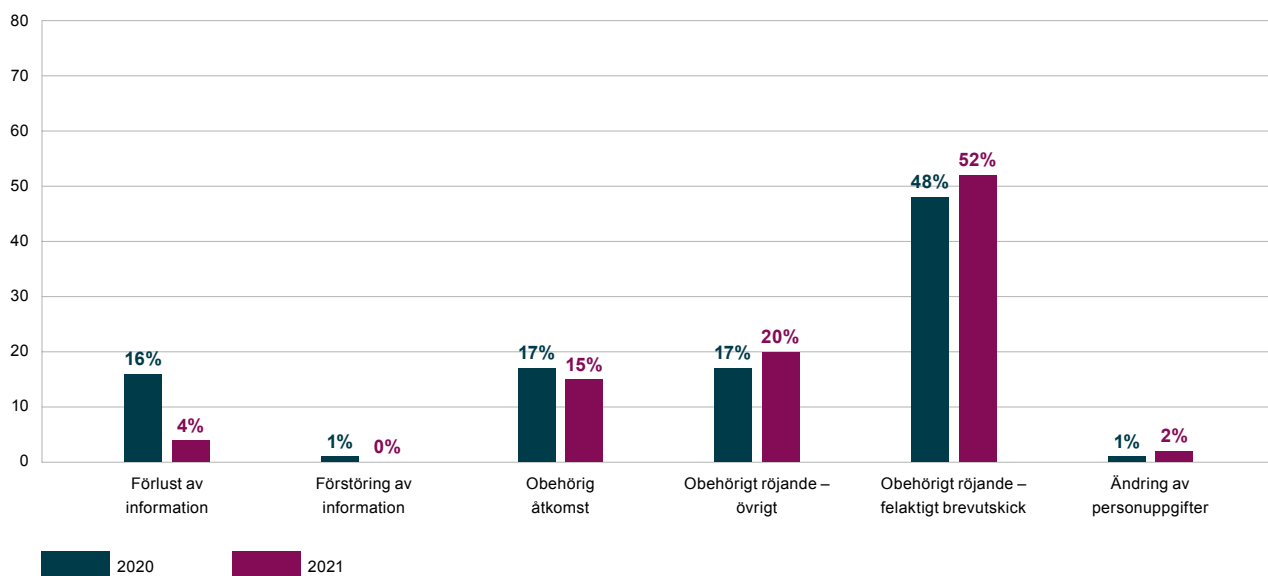
- Offentliga sektorn
- Privata sektorn
- Övriga

Bilaga 2. Figurer för anmälda personuppgiftsincidenter per verksamhetsområde

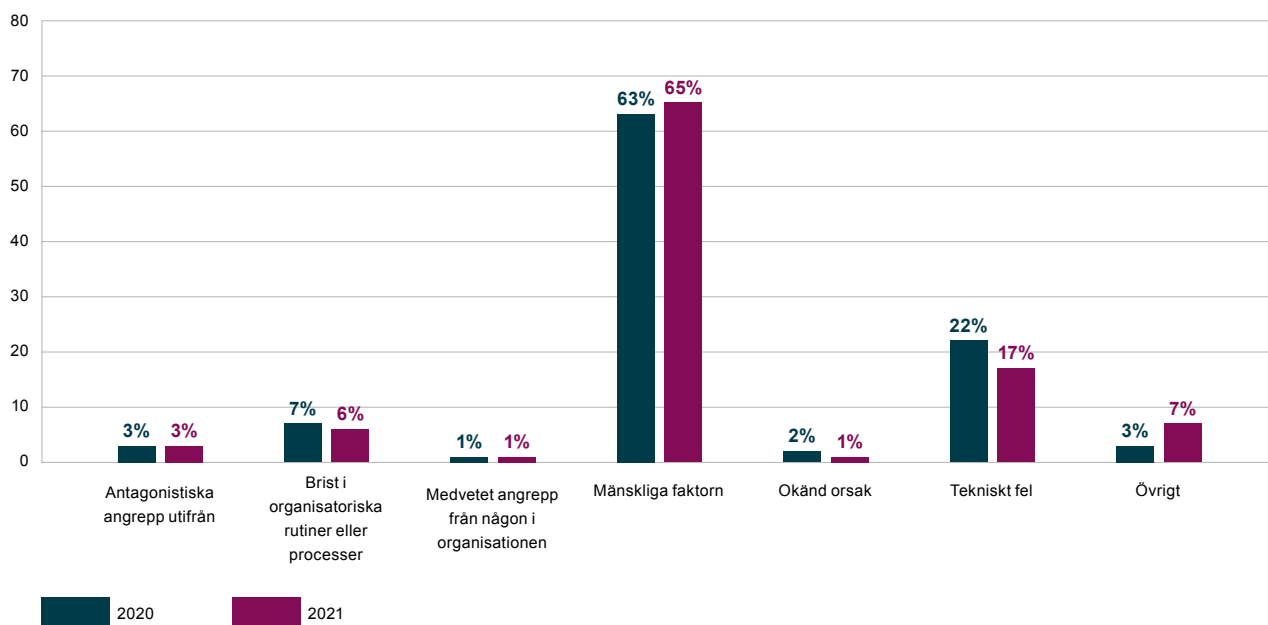
I denna bilaga redovisar vi anmälda personuppgiftsincidenter till IMY för 2020 och 2021. Vi redovisar statistik för varje verksamhetsområde för sig, uppdelad på typ av incident som anmälts från området i fråga samt vad som har angetts som orsak till incidenten.



Finansiell sektor eller försäkring

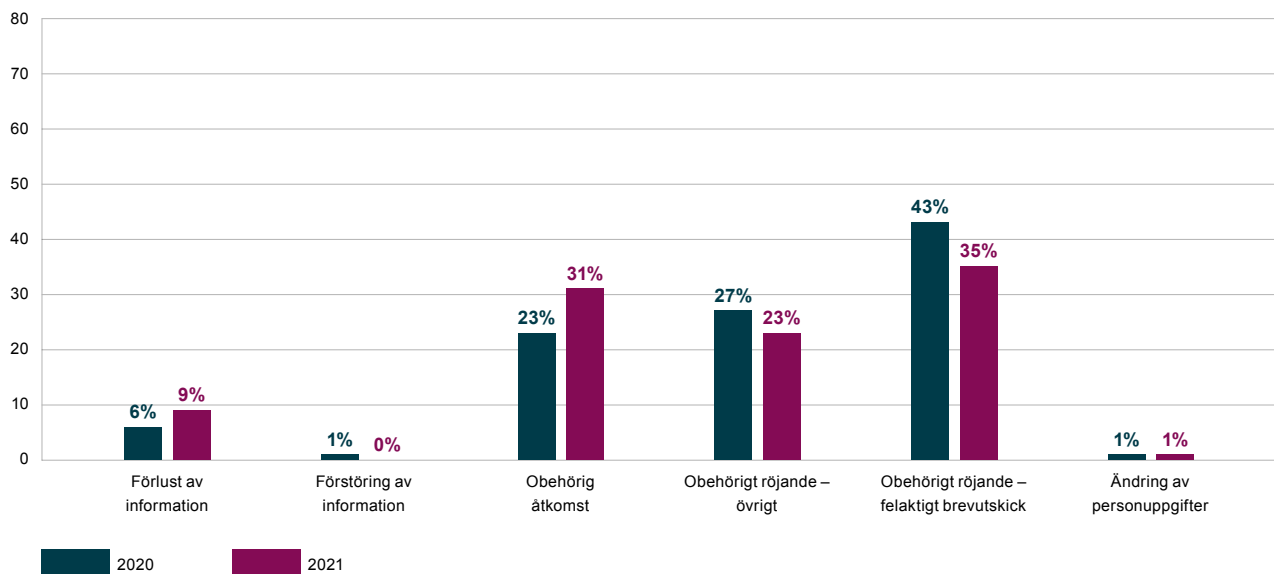


Figur 7. Typ av incident för Finansiell sektor eller försäkring i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

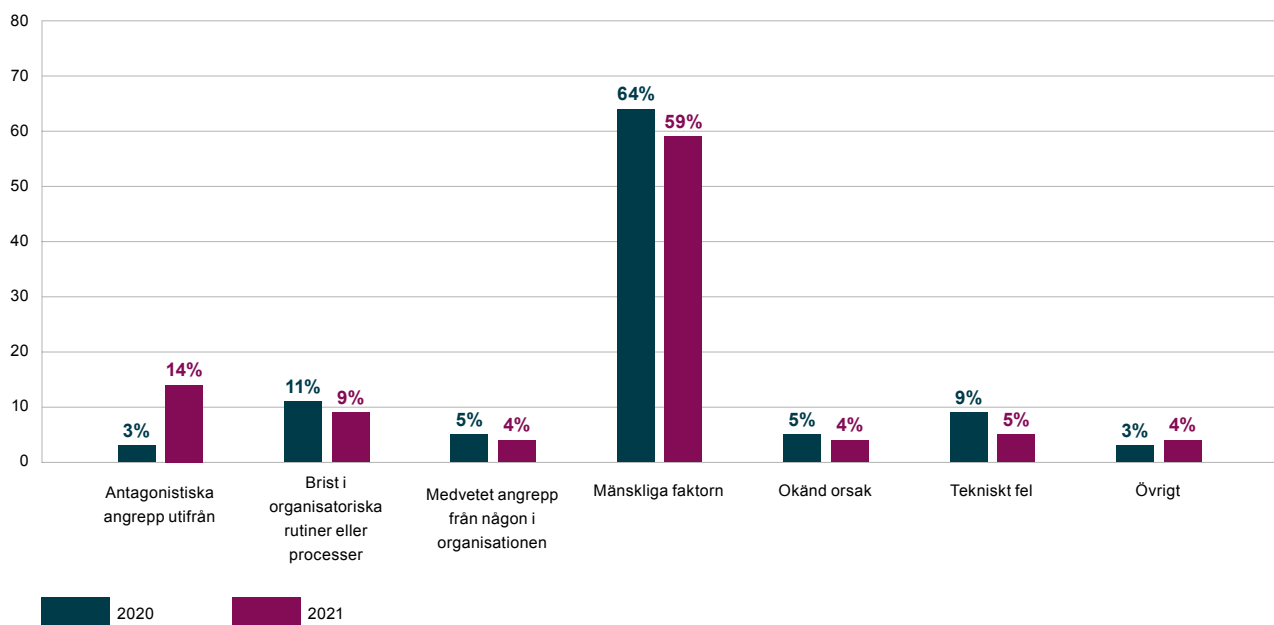


Figur 8. Orsak till incidenten för Finansiell sektor eller försäkring i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Hälso- och sjukvård

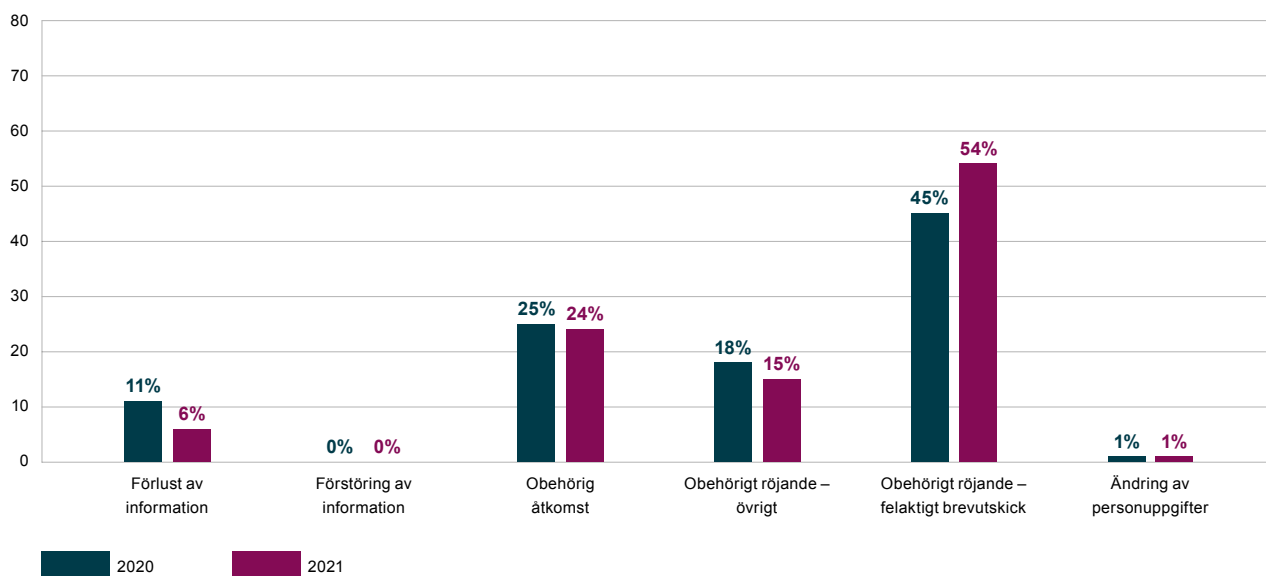


Figur 9. Typ av incident för Hälsö- och sjukvård i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

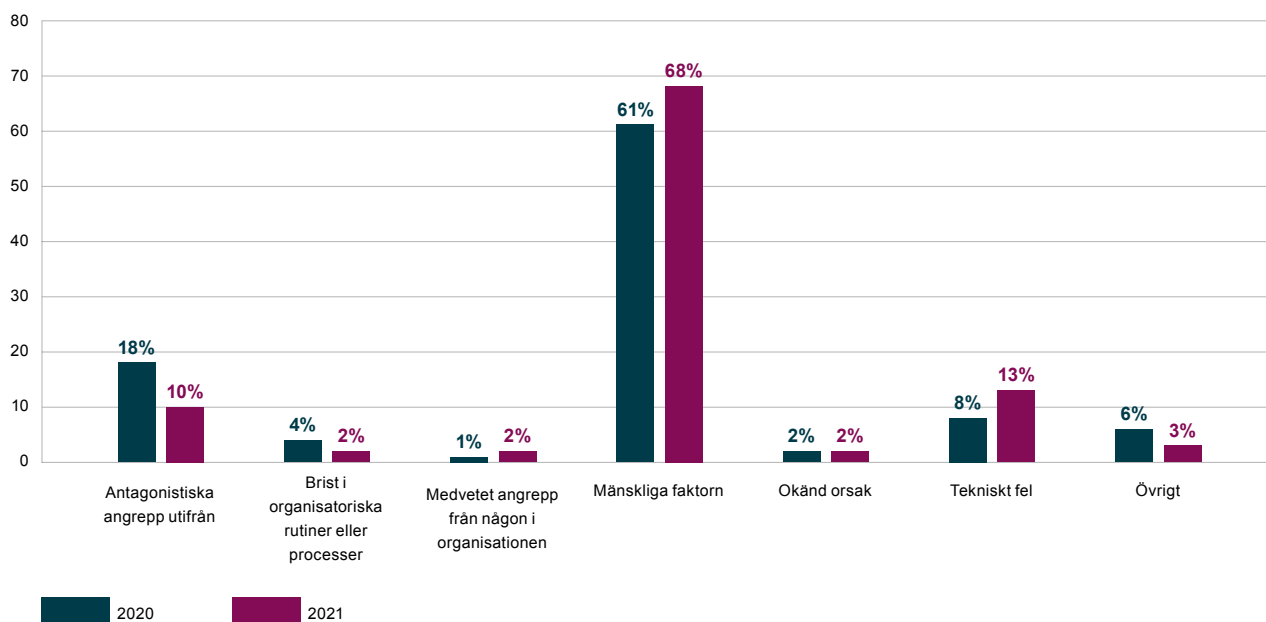


Figur 10. Orsak till incidenten för Hälsö- och sjukvård i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Ideell organisation eller ekonomisk förening

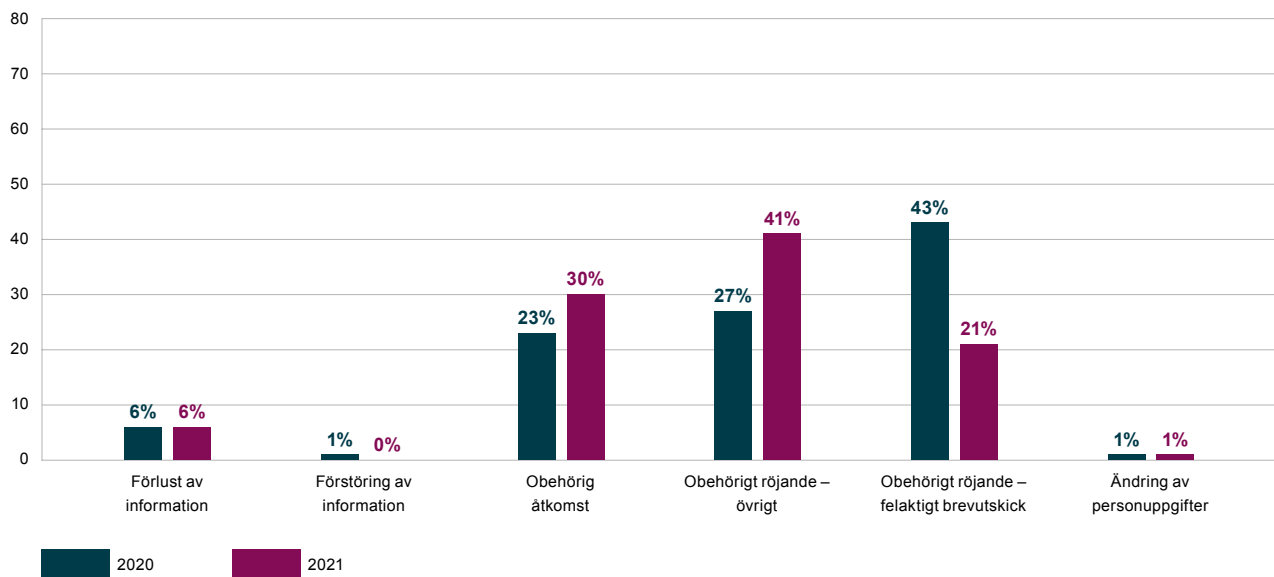


Figur 11. Typ av incident för Ideell organisation eller ekonomisk förening i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

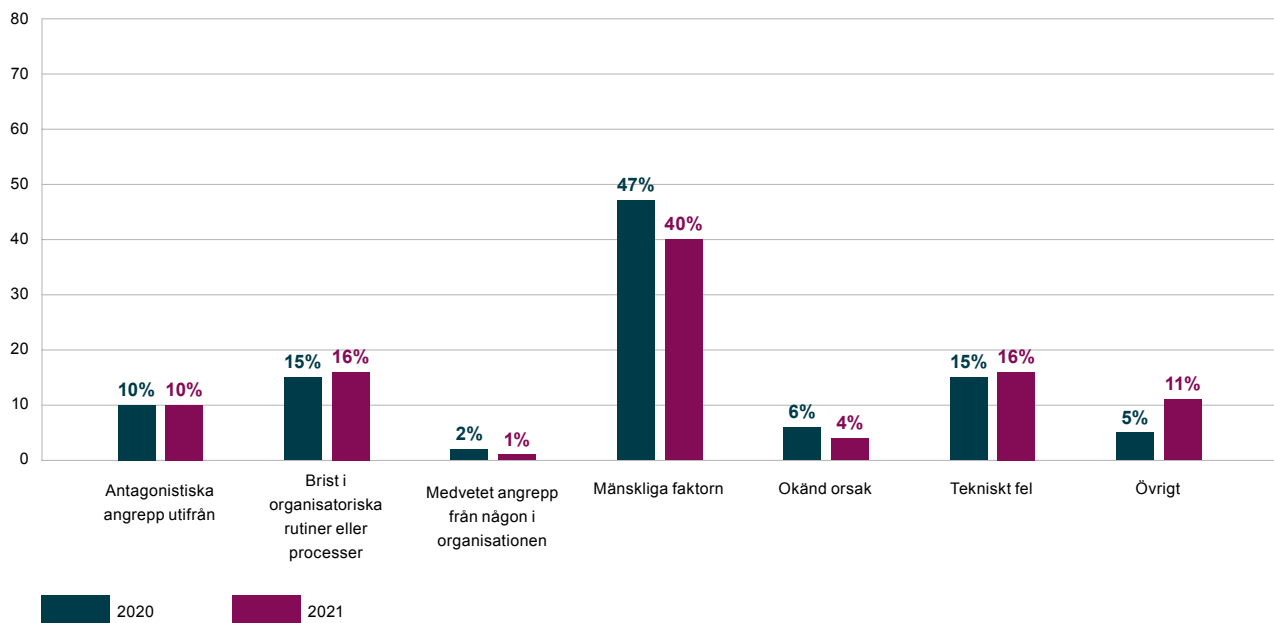


Figur 12. Orsak till incidenten för Ideell organisation eller ekonomisk förening i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Kommun

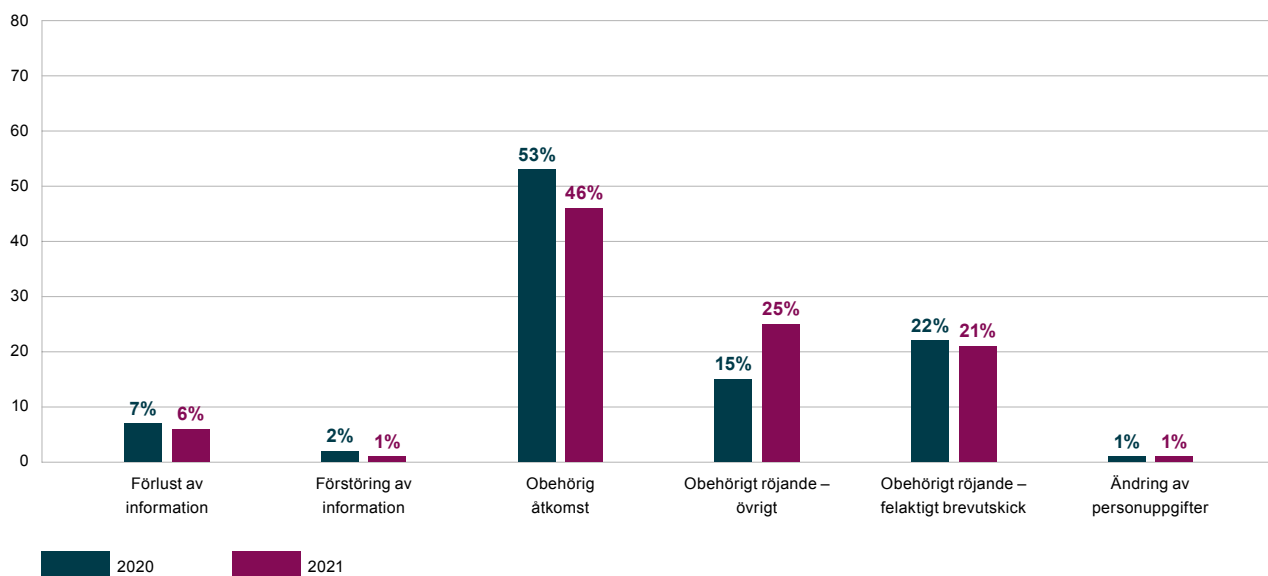


Figur 13. Typ av incident för Kommun i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

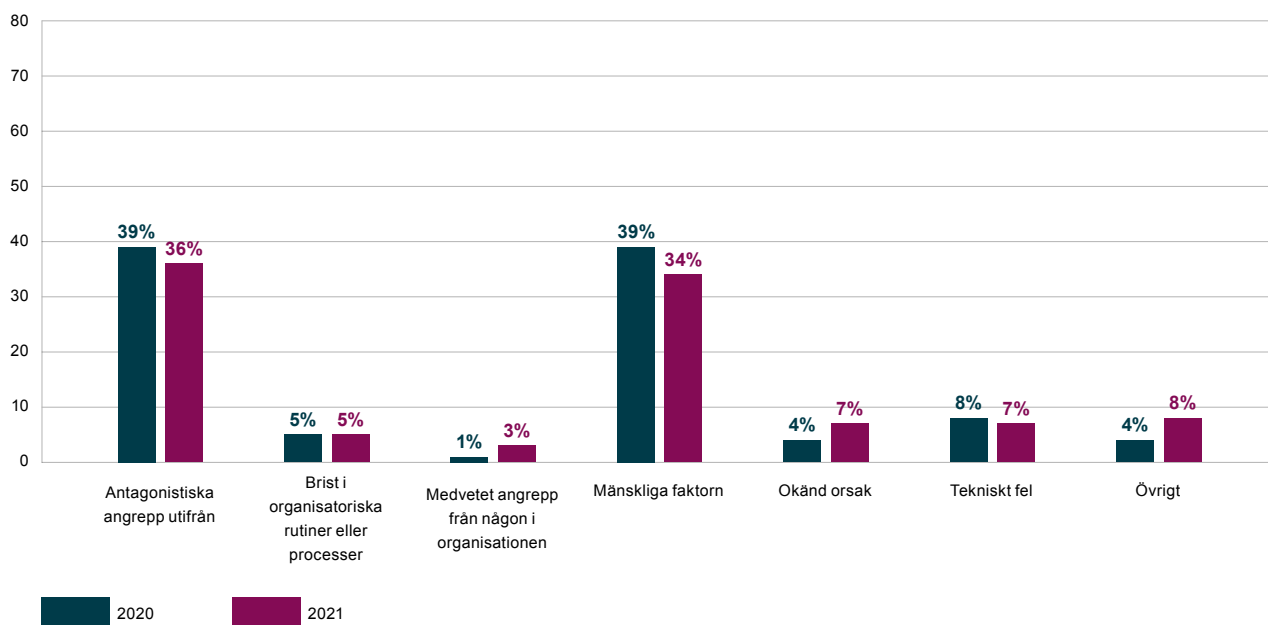


Figur 14. Orsak till incidenten för Kommun i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Näringsliv i övrigt

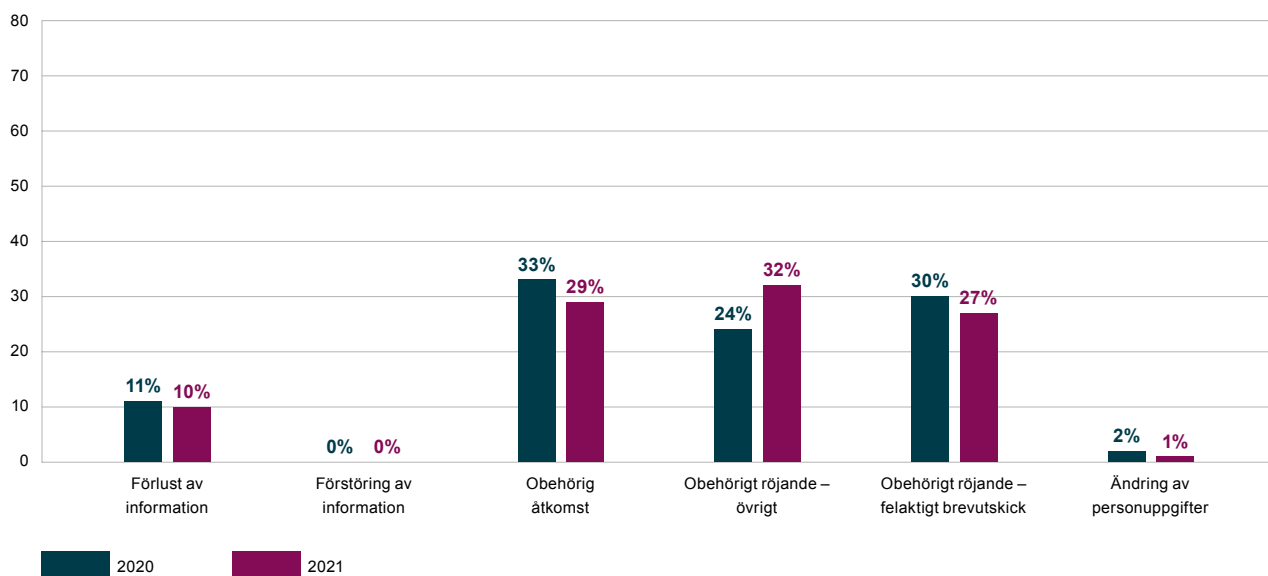


Figur 15. Typ av incident för Näringsliv i övrigt i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

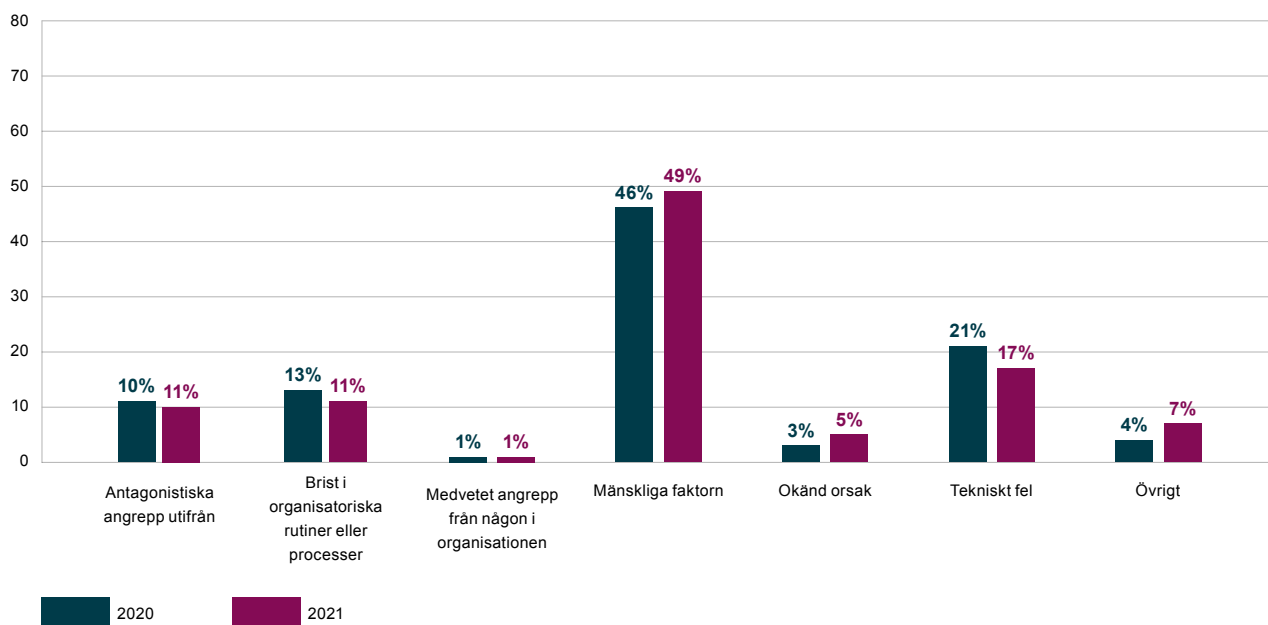


Figur 16. Orsak till incidenten för Näringsliv i övrigt i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Skola och utbildning

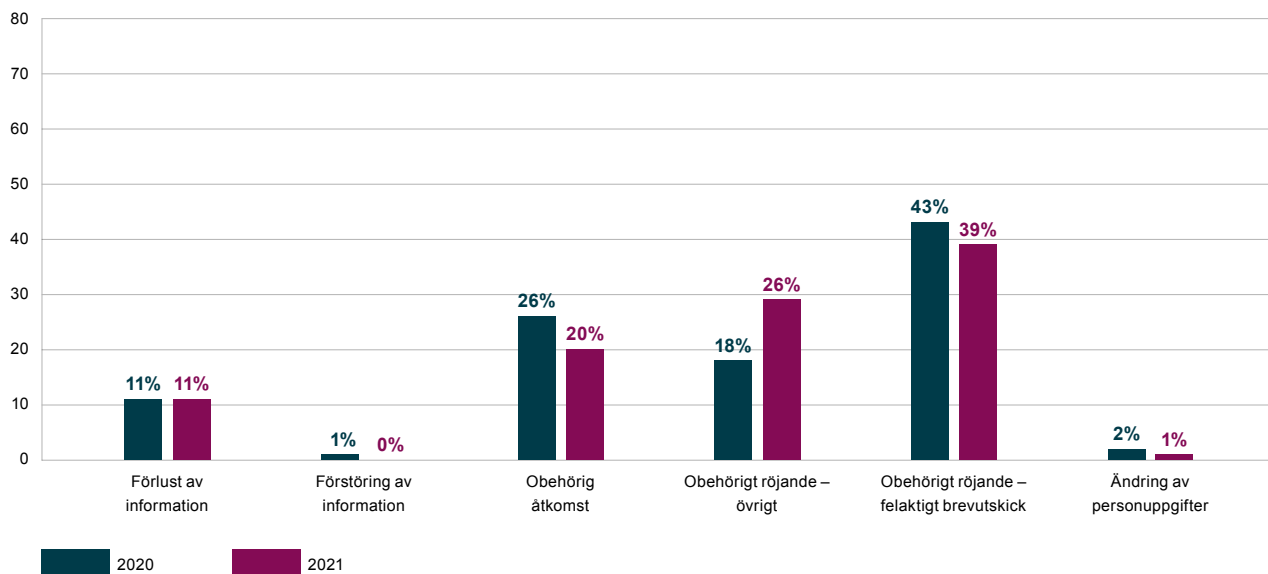


Figur 17. Typ av incident för Skola och utbildning i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

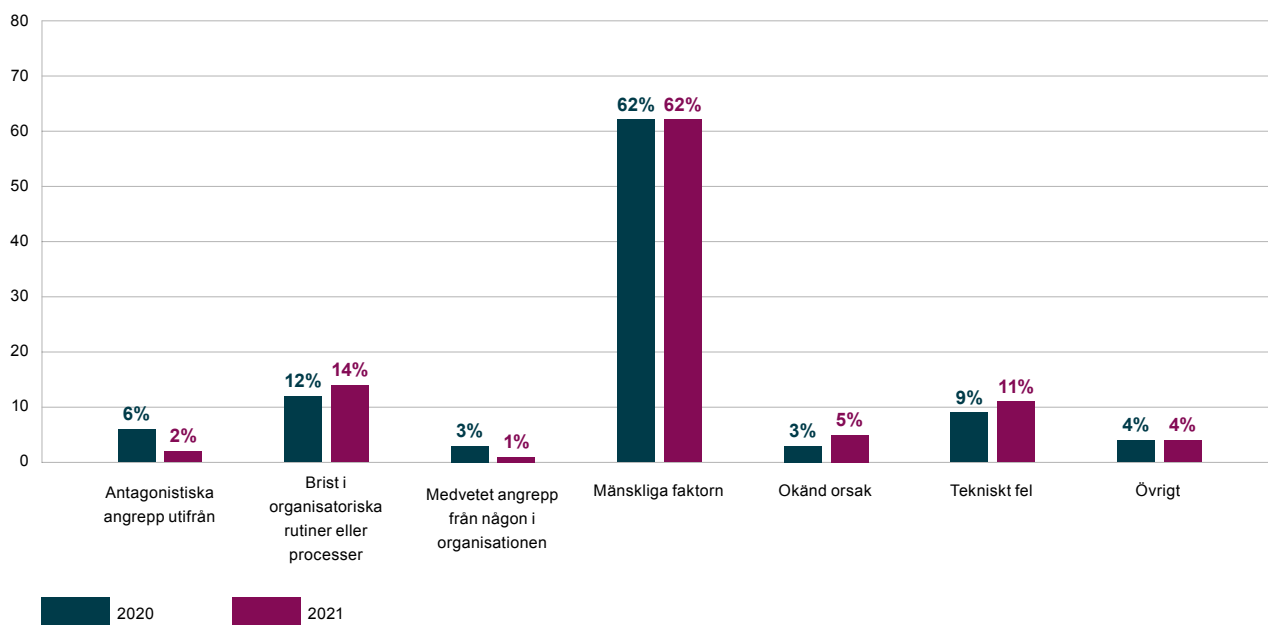


Figur 18. Orsak till incidenten för Skola och utbildning i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Socialtjänst

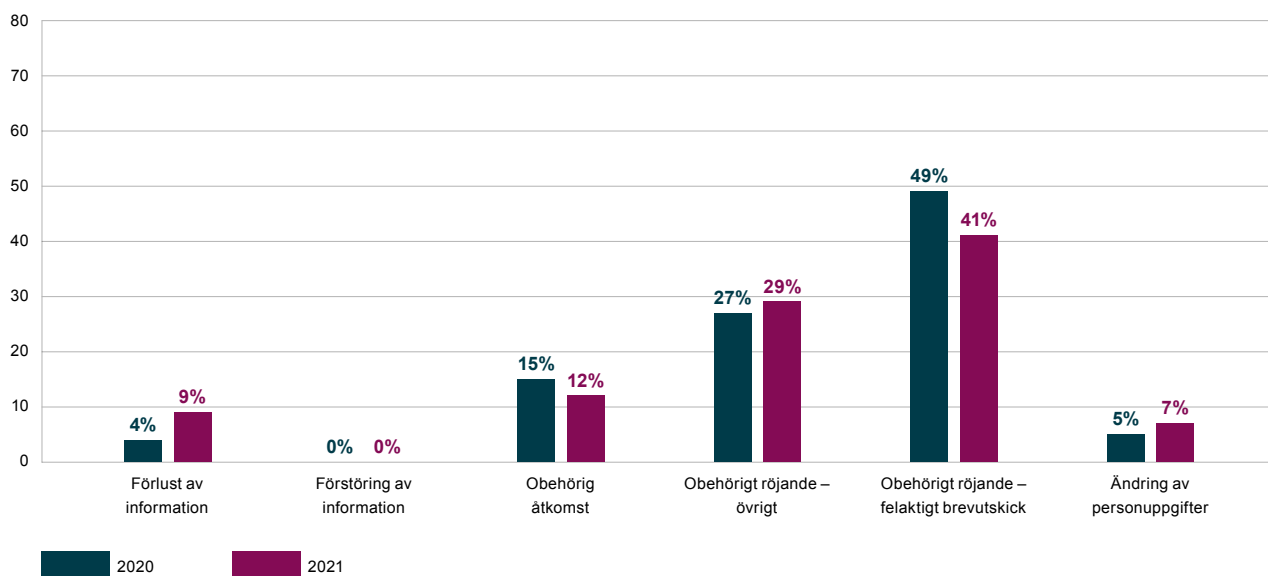


Figur 19. Typ av incident för Socialtjänst i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

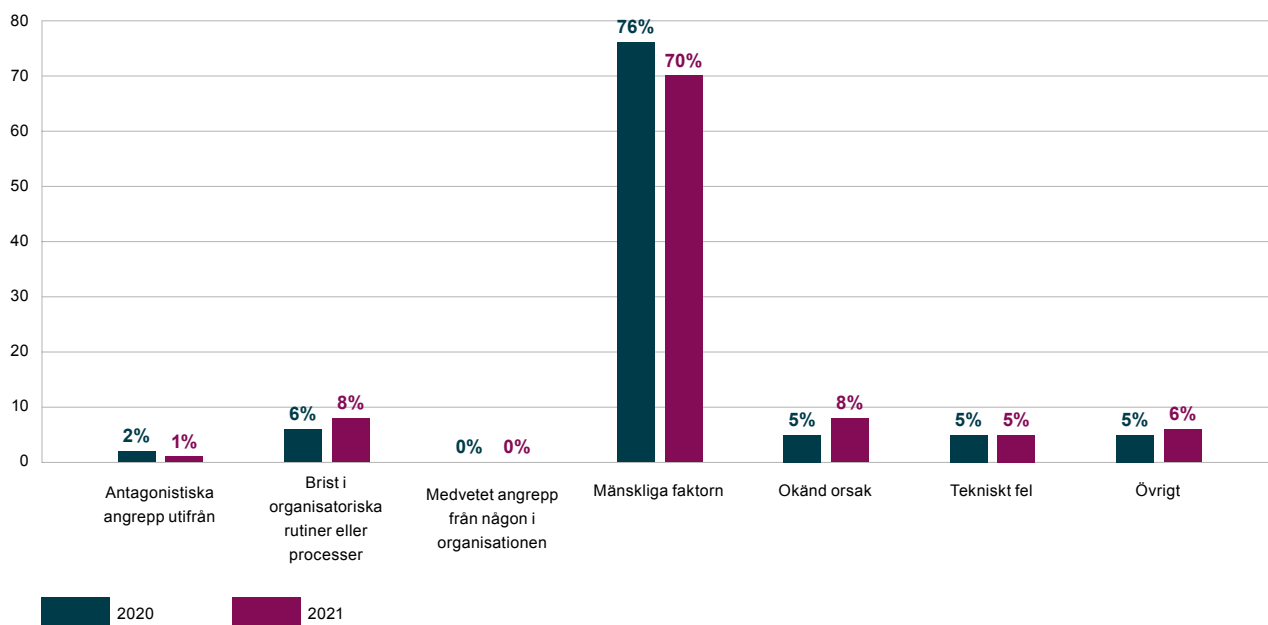


Figur 20. Orsak till incidenten för Socialtjänst i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Statlig myndighet och domstol



Figur 21. Typ av incident för Statlig myndighet och domstol i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.



Figur 22. Orsak till incidenten för Statlig myndighet och domstol i procent för 2020 och 2021. Observera att det totala antalet anmälda personuppgiftsincidenter har varierat mellan åren.

Det här är IMY

Integritetsskyddsmyndigheten (IMY) arbetar för att skydda medborgarnas alla personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer. Det är vi som granskar att företag, myndigheter och andra aktörer följer GDPR – dataskyddsförordningen. Vi utbildar och vägleder dem som behandlar personuppgifter. Vi påverkar även lagstiftningen. Vi vill se en hållbar och integritetsvänlig digitalisering. Vi är övertygade om att det går att värna medborgarnas trygghet och samhällets säkerhet, utan omotiverad kartläggning och övervakning. Tillsammans med övriga dataskyddsmyndigheter i EU arbetar vi för att medborgarnas personuppgifter ska ha samma skydd i hela unionen. Vi arbetar även för att kreditupplysning och inkassoverksamhet ska bedrivas på ett korrekt sätt. Vår vision är ett tryggt informationssamhälle, där vi tillsammans värnar den personliga integriteten.

Kontakta IMY

E-post: imy@imy.se

Webb: www.imy.se

Tel: 08-657 61 00

Postadress: Integritetsskyddsmyndigheten
Box 8114, 104 20 Stockholm