IMY. Integritetsskydds myndigheten

Rapport om anmälda personuppgiftsincidenter 2022

Den nationella bilden med en fördjupning om antagonistiska angrepp och en nordisk jämförelse 2019–2022

IMY rapport 2023:2

Innehållsförteckning

Kapitel 5. Vad är en personuppgiftsincident och när ska den anmälas till IMY?

Bilagor

Sammanfattning

En personuppgiftsincident inträffar när de uppgifter som en verksamhet ansvarar för drabbas av en säkerhetsincident som leder till ett brott mot konfidentialiteten, tillgängligheten eller integriteten. Om detta händer, och det är sannolikt att personuppgiftsincidenten utgör en risk för en enskild persons rättigheter och friheter, måste verksamheten anmäla incidenten till IMY utan onödigt dröjsmål och senast inom 72 timmar efter att ha fått kännedom om den.

Under 2022 tog IMY emot cirka 5 330 anmälningar om personuppgiftsincidenter, varav 70 procent kom från offentlig sektor och cirka 25 procent kom från privat sektor. Inom offentlig sektor anmäldes var fjärde incident inom statliga myndigheter, och var femte inom hälso- och sjukvård.

63 procent av anmälningar kan tillskrivas någon typ av obehörigt röjande: antingen genom felskick, 38 procent, eller genom annan felaktig hantering av personuppgifter, 25 procent.

Den mänskliga faktorn angavs som orsak i 59 procent av samtliga anmälningar om personuppgiftsincidenter 2022. Oftast handlade det om personer som begått ett misstag när de hanterat personuppgifter i sina verksamheter. Mer än hälften av de personuppgiftsincidenter som orsakades av den mänskliga faktorn är felskickade brev, mejl eller sms. Jämfört med föregående år ökade andelen anmälningar med den mänskliga faktorn som orsak inom hälso- och sjukvården.

IMY:s jämförelse av anmälningar om personuppgiftsincidenter i Norden 2019–2022 visar att Danmark är det land som har flest anmälda personuppgiftsincidenter, följt av Sverige och Finland. I förhållande till folkmängden har Sverige färre anmälningar än både Danmark och Finland. År 2022 rapporterade verksamheterna i Finland dubbelt så många personuppgiftsincidenter som i Sverige och verksamheterna i Danmark tredubbelt så många. Utifrån dessa siffror drar vi slutsatsen att det sannolikt finns en underteckning av personuppgiftsincidenter i Sverige och att det kan handlar om 10 000 oanmälda personuppgiftsincidenter.

Det förändrade säkerhetsläget med krig i Ukraina och Sveriges ansökan om medlemskap i Nato gjorde många oroliga för att Sverige skulle drabbas av fler cyberangrepp under 2022. Trots oron visar IMY:s undersökning att antagonistiska angrepp enligt dataskyddsförordningen minskade jämfört med föregående år. Flest antagonistiska angrepp, 140 fall, rapporterades av näringslivet (exklusive finansiell sektor eller försäkringar). Andra förhållandevis utsatta verksamheter fanns inom kommuner samt inom skola och utbildning, som vardera rapporterade cirka 40 anmälningar om antagonistiska angrepp som involverade personuppgifter.

IMY:s rekommendationer för att förebygga personuppgifts-incidenter

Årets sammanställning av anmälningar om personuppgiftsincidenter 2019–2022 visar att knappt sex av tio anmälningar varje år anses ha sin orsak på grund av den mänskliga faktorn. Eftersom dessa kan vara av allvarlig karaktär och innebära hög risk för enskildas friheter och rättigheter lämnar IMY rekommendationer som kan bidra till att förebygga incidenter och mildra konsekvenserna om en incident ändå inträffar.

En fördjupad beskrivning av IMY:s rekommendationer finns i bilaga 3.

Ett systematiskt informationssäkerhetsarbete är centralt

Att den mänskliga faktorn anges frekvent som orsak till personuppgiftsincidenter och att den kan leda till allvarliga incidenter innebär att det är en viktig faktor att beakta i er verksamhets systematiska informationssäkerhetsarbete. De organisatoriska och tekniska säkerhetsåtgärderna behöver vara integrerade i verksamhetens arbetssätt och skapa förutsättningar för att det ska vara lätt att göra rätt och svårt att göra fel.

Verksamhetens säkerhetsnivå i relation till riskerna för enskildas friheter och rättigheter

Säkerhetsnivån ska sättas i relation till vilka personuppgifter som behandlas och de specifika risker för enskildas friheter och rättigheter som föreligger i er verksamhet. Verksamheten kan därför inte rakt av kopiera andras säkerhetsåtgärder och säkerhetsarbetet måste pågå kontinuerligt då verksamheten, tekniken och därmed riskerna hela tiden förändras.

Minska risken för misstag

Ni kan minska risken att medarbetare begår misstag genom organisatoriska och tekniska åtgärder. Exempel på det är att tekniskt förhindra att medarbetare sparar information på löstagbara medier eller att förhindra dem att installera program och appar som inte godkänts av verksamheten. Lösningar som gör det enkelt för medarbetarna att lösenordsskydda och kryptera e-post och bifogade filer är också åtgärder som kan höja säkerheten.

Aktiv behörighetsstyrning

En annan viktig och grundläggande säkerhetsåtgärd är att ha en aktiv behörighetsstyrning. Behörigheterna ska vid varje tid vara anpassade så att varje medarbetare bara får tillgång till de personuppgifter som medarbetaren behöver för att kunna utföra sina arbetsuppgifter.

Processer som stärker det systematiska informationssäkerhetsarbetet

Alla verksamheter som hanterar personuppgifter behöver ha dokumenterade och implementerade riskhanterings- och personuppgiftsincidenthanteringsprocesser för att kunna förebygga, upptäcka och hantera personuppgiftsincidenter. Processerna ska också leda till ett kontinuerligt lärande.

Säkerhetskultur

För att få en god säkerhetskultur krävs att ledningen är engagerad i verksamhetens säkerhetsfrågor, vilket även inkluderar skyddet för personuppgifter. I en god säkerhetskultur kommuniceras även dragna lärdomar av inträffade incidenter, och hur dessa lärdomar sedan ska realiseras för att skapa en ännu bättre säkerhetskultur och därmed bidra till det systematiska säkerhetsarbetet.

Inledning

Integritetsskyddsmyndigheten är Sveriges nationella tillsynsmyndighet för behandling av personuppgifter. Varje år publicerar myndigheten en rapport om personuppgiftsincidenter på basis av de anmälningar som verksamheter och organisationer har rapporterat in. Syftet med rapporten är att förmedla iakttagelser och lägesbilder samt analyser och rekommendationer som privata och offentliga verksamheter kan använda i sitt interna dataskyddsarbete. Rapporten är en del av IMY:s rapportserie[1] och detta är den femte rapporten om personuppgiftsincidenter i serien.

På webbplatsen www.imy.se finns våra rapporter för nedladdning under rubriken Publikationer.

1. 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), klagomål mot personsöktjänster med frivilligt utgivningsbevis (2020:1) och anmälda personuppgiftsincidenter 2021 (2022:1).

Metod

I den här rapporten ger vi en lägesbild utifrån de anmälningar om personuppgiftsincidenter som kom in till IMY under 2022 och jämför med resultaten för

- 2021
- fyraårsperioden 2019–2022
- de nordiska länderna under fyraårsperioden 2019–2022.

I underlaget för årets rapport ingår sammantaget 5 331 anmälningar om personuppgiftsincidenter 2022. Incidentanmälningar 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 i e-blanketten beskriver den personuppgiftsansvariga omständigheterna kring den inträffade personuppgiftsincidenten.

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

- verksamhetsområdet för incidenten
- typen av incident
- orsaken till incidenten.

I vår undersökning utgår vi från dessa indelningar när vi beskriver utfallet för 2022, och även för föregående år. Notera att rapporten vilar på information om de anmälningar som varje år görs till IMY och inte på de personuppgiftsincidenter som faktiskt inträffar. Till exempel utgår vi från att inte alla anmälningspliktiga säkerhetsincidenter enligt dataskyddsoförordningen respektive brottsdatalagen upptäcks, och att alla som upptäcks inte alltid anmäls till IMY.

Mer information om metoden och kvaliteten i dataunderlaget framgår av bilaga 1 Dataunderlaget.

Rapportens disposition

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

Kapitel 1 beskriver inflödet av anmälningar om personuppgiftsincidenter till IMY. Bland annat redovisar vi statistik över det totala antalet anmälningar, vilken typ av personuppgiftsincident som anmäldes och orsaken till att incidenten inträffade enligt anmälaren. Vi beskriver även förändringen mellan 2021 och 2022 räknat i antal incidentanmälningar (i avrundade tal) och redovisar förändringen under 2019–2022.

Kapitel 2 handlar om hur mönstren ser ut inom olika verksamhetsområden. I den delen redovisar vi statistik över incidentanmälningar 2022 för olika verksamhetsområden och beskriver förändringar under 2019–2022. Tillhörande diagram redovisas samlade i bilaga 2.

Kapitel 3 presenterar jämförande analyser av anmälningar om personuppgifts-incidenter inom Norden under 2019-2022. Bland annat beskriver vi antal anmälningar per 100 000 invånare för respektive land under fyraårsperioden och resonerar kring hur stort mörkertalet kan vara i Sverige vad gäller anmälningspliktiga personuppgifts-incidenter som inte rapporteras till IMY.

Kapitel 4 ger en fördjupad analys av anmälningar om personuppgiftsincidenter som inträffade när någon obehörig försökte att ta del av uppgifter den inte hade rätt till, så kallade antagonistiska angrepp. Med tanke på det förändrade säkerhetsläget i Sverige och i Europa valde vi att undersöka ifall antalet anmälningar om antagonis-tiska angrepp ökade under 2022.

Kapitel 5 beskriver översiktligt vilka personuppgiftsincidenter som måste anmälas till IMY och hur IMY arbetar med de incidenter som anmäls till myndigheten. Vi beskriver även vilka pågående tillsynsärenden som fanns under 2022 och vilka som kunde avslutas.

Sist i rapporten finns tre bilagor: *Dataunderlaget, Diagram över anmälningar om personuppgiftsincidenter indelat efter verksamhetsområde* samt *Fördjupning av IMY:s rekommendationer.*

Kapitel 1.

Anmälningar om personuppgiftsincidenter 2022

I det här kapitlet beskriver vi inflödet av anmälningar om personuppgiftsincidenter till IMY 2022. Förutom inflödet över tid redovisar vi vanliga typer av incidenter och vilka orsaker som anmälarna oftast anger.

Kapitlets viktigaste resultat:

1. Antalet anmälningar om personuppgiftsincidenter minskade.
2. 70 procent av samtliga anmälningar om personuppgiftsincidenter rapporterades av verksamheter inom offentlig sektor. Var fjärde anmälan gjordes av statliga myndigheter.
3. 63 procent av anmälningarna handlar om att personuppgifter röjdes.
4. Den mänskliga faktorn orsakade sex av tio incidenter. Tekniska fel, brister i organisatoriska rutiner eller processer samt antagonistiska angrepp orsakade var tionde incident vardera.

Anmälningarna minskade

Anmälningar om personuppgiftsincidenter görs antingen utifrån bestämmelser inom dataskyddsförordningen (GDPR) eller utifrån brottsdatalagen (BDL). Under 2022 anmäldes sammantaget 5 331 personuppgiftsincidenter till IMY. Det är en minskning mot föregående år med 7,6 procent eller cirka 440 fall.

Det minskade antalet anmälda incidenter ska ses mot bakgrund av det relativt höga inflöde av icke anmälningspliktiga personuppgiftsincidenter från offentlig sektor som IMY registrerade det föregående året. En bidragande faktor till överteckningen 2021 kan ha varit de granskningar media gjorde under året, speciellt inom den offentliga sektorn, och som medförde att fler personuppgiftsincidenter anmäldes direkt i anslutning till medierapporteringen.

Tabell 1

Antal anmälningar om personuppgiftsincidenter 2019–2022

	2019	2020	2021	2022
Dataskyddsförordningen	4 702	4 542	5 726	5 291
Brottsdatalagen	55	48	41	40
Samtliga	4 757	4 590	5 767	5 331

Sammanställning över antalet anmälningar om personuppgiftsincidenter som rapporterats av olika verksamheter utifrån bestämmelserna i dataskyddsförordningen och brottsdatalagen för 2019–2022.[2]

Tabell 1 visar antalet anmälningar om personuppgiftsincidenter per år under 2019–2022, indelat efter anmälningar efter dataskyddsförordningen och brottsdatalagen. Dataskyddsförordningen och brottsdatalagen utgår från samma principer:

Personuppgifter får bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål, och fler personuppgifter än nödvändigt får inte behandlas. Brottsbekämpande myndigheter ska följa brottsdatalagen vid behandling av personuppgifter som sker inom ramen för den brottsbekämpande verksamheten. För andra uppgifter som inte direkt innebär brottsbekämpning, till exempel gränskontroll eller tullkontroll, gäller dataskyddsförordningen.

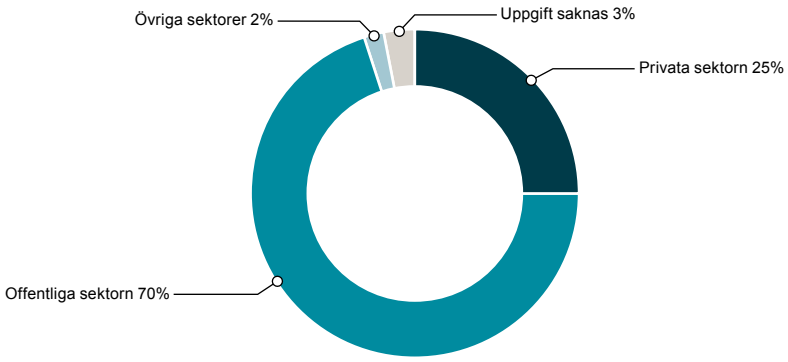
Av tabell 1 framgår att den absoluta merparten av anmälningar om personuppgiftsincidenter de senaste fyra åren handlade om anmälningspliktiga säkerhetsincidenter enligt dataskyddsförordningen. Endast ett förhållandevis litet antal anmälningar görs varje år utifrån brottsdatalagen. Antalet anmälningar utifrån brottsdatalagen minskade under fyraårsperioden; från 55 anmälningar 2019 till 40 anmälningar 2022.

2. Rapportens beräkningar utgår från det totala antalet anmälda personuppgiftsincidenter per år som redovisas i tabell 1.

Sju av tio personuppgiftsincidenter rapporteras av offentlig sektor

Diagram 1

Andel anmälningar om personuppgiftsincidenter 2022, fördelat på sektorer



Cirkeldiagrammet redogör för andelen inrapporterade personuppgiftsincidenter fördelat på offentlig sektor (N = 3 717), privat sektor (N = 1 355) och övriga sektorer (N = 124) under 2022. Dessutom redovisas andelen fall 2022 som saknar sektorstillhörighet (N = 135).

Diagram 1 visar den procentuella fördelningen av anmälningar om personuppgifts-incidenter indelat efter sektor. Den övervägande merparten av alla inrapporterade personuppgiftsincidenter 2022 anmäldes av verksamheter inom offentlig sektor; 70 procent. Anmälningar från verksamheter inom privat sektor stod för 25 procent av samtliga incidentanmälningar. Det kan jämföras med föregående år 2021 när offentlig sektor anmälde 66 procent av alla inrapporterade personuppgiftsincidenter och privat sektor 29 procent.

Att offentlig sektor fortsatt står för majoriteten av anmälningar om personuppgifts-incidenter beror sannolikt på flera faktorer. Många verksamheter inom offentlig sektor behandlar stora mängder personuppgifter och ofta även känsliga personuppgifter. Det kan bidra till att fler incidenter betraktas som anmälningspliktiga vid risk-bedömningen och leda till en viss grad av överteckning av icke anmälningspliktiga personuppgiftsincidenter.

Det är alltid den personuppgiftsansvariga som ansvarar för att hantera respektive säkerhetsincident korrekt. Det innebär ett ansvar att rapportera anmälningspliktiga incidenter, alltså att göra en självständig bedömning om incidenten är anmälnings-pliktig eller inte, men också att dokumentera incidenten internt inom organisationen.[3] När IMY lämnar generell vägledning vid inträffade personuppgiftsincidenter har vi vid gränsfallssituationer lämnat rådet att det är bättre att anmäla incidenten inom 72 timmar, och sedan eventuellt göra en komplettering som visar att den inte var anmälningspliktig, än att inte göra en anmälan alls.

3. I dataskyddsförordningen finns en skyldighet för organisationer att anmäla vissa typer av incidenter till IMY, så kallade personuppgiftsincidenter. Mer information om anmälningsplikten och IMY:s arbete med personuppgifts-incidenter redovisas i kapitel 5.

Var fjärde personuppgiftsincident rapporteras av statliga myndigheter

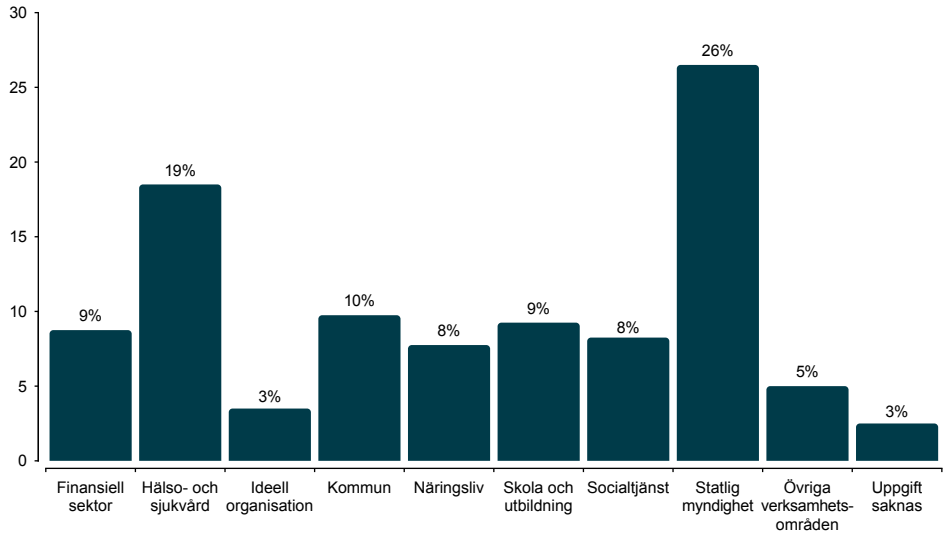
I rapporten delar vi in anmälningar om personuppgiftsincidenter i nio olika verksamhetsområden:

- finansiell sektor eller försäkringar
- hälso- och sjukvård
- ideell organisation eller ekonomisk förening
- kommun
- näringsliv
- skola och utbildning
- socialtjänst
- statlig myndighet
- övriga verksamhetsområden.

Observera att finansiell sektor eller försäkringar särredovisas. Det betyder att de inte ingår i gruppen näringsliv. Vissa verksamhetsområden innehåller undergrupper. Vi hänvisar till bilaga 1 för en mer utförlig beskrivning av verksamhetsområdena med tillhörande undergrupper.

Diagram 2

Fördelning i procent av anmälningar om personuppgiftsincidenter fördelat på verksamhetsområde 2022



Stapeldiagram över andelen inrapporterade personuppgiftsincidenter fördelat på nio verksamhetsområden under 2022: finansiell sektor eller försäkringar (N = 466), hälso- och sjukvård (N = 987), ideell organisation eller ekonomisk förening (N = 179), kommun (N = 527), näringsliv (N = 420), skola och utbildning (N = 490), socialtjänst (N = 435), statlig myndighet (1 403), övriga verksamhetsområden (N = 265) samt uppgift saknas (N = 159).

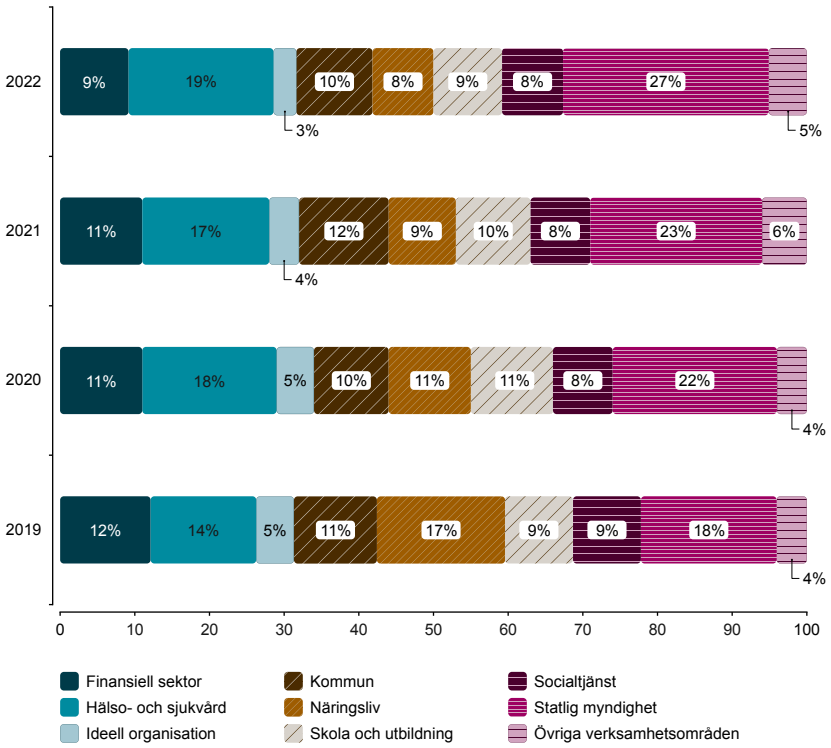
Diagram 2 visar den procentuella fördelningen bland incidentanmälningar indelat efter verksamhetsområde. Av diagrammet framgår att flest personuppgiftsincidenter 2022 anmäldes av statliga myndigheter respektive hälso- och sjukvård, 26 procent respektive 19 procent.

Sett till antalet anmälningar finns det stora skillnader mellan verksamhetsområdena. Verksamheter inom området ideella organisationer rapporterade relativt sett få personuppgiftsincidenter, cirka 180 anmälningar, jämfört med statliga myndigheter som anmälde flest incidenter, cirka 1 400 anmälningar. Tillsammans anmälde statliga myndigheter, hälso- och sjukvård samt kommuner mer än hälften av alla anmälningspliktiga säkerhetsincidenter enligt dataskyddsförordningen och brottsdatalagen, cirka 2 900 incidentanmälningar.

Näringslivet rapporterar allt färre personuppgiftsincidenter

Diagram 3

Anmälningar om personuppgiftsincidenter efter verksamhetsområde i procent 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket incidentanmälningar från de nio verksamhetsområdena bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter 2019–2022.

Diagram 3 visar den procentuella fördelningen av anmälda personuppgiftsincidenter enligt dataskyddsförordningen och brottsdatalagen indelat efter verksamhetsområden 2019–2022. Diagrammet visar att andelen anmälda incidenter per verksamhetsområde har varit relativt stabilt under fyraårsperioden. Det finns dock två undantag:

- Inom statliga myndigheter har andelen ökat från år till år: Andelen ökade 9 procentenheter mellan 2019 och 2022, en ökning med cirka 580 anmälningar.
- Inom näringslivet har andelen i stället minskat från år till år: Andelen minskade med 9 procentenheter mellan 2019 och 2022, en minskning med cirka 380 anmälningar.

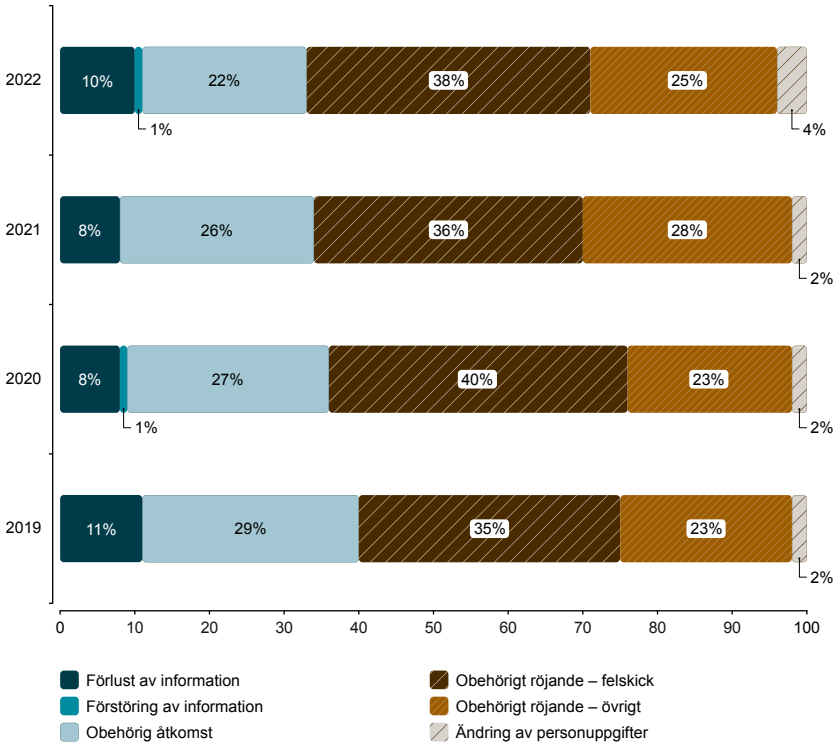
Det behöver inte nödvändigtvis vara en indikation på bristande säkerhet att en organisation eller en bransch (verksamhetsområde) anmäler många personuppgiftsincidenter. Tvärtom kan det ofta tyda på att verksamheten har strukturer och rutiner som ger en god förmåga att upptäcka och rapportera personuppgiftsincidenter.

På motsvarande sätt behöver det inte vara en signal om en hög grad av informationssäkerhet när ett område rapporterar få personuppgiftsincidenter. Det kan exempelvis handla om att verksamheter inte rapporterar anmälningspliktiga personuppgiftsincidenter av rädsla för att bli föremål för IMY:s tillsynsverksamhet och eventuella sanktionsavgifter.

Sex av tio personuppgiftsincidenter handlar om att personuppgifter röjs

Diagram 4

Andel anmälningar om personuppgiftsincidenter fördelat på typ av incident 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika typer av incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter 2019–2022.

Diagram 4 visar att den procentuella fördelningen av inrapporterade incidenter under 2019–2022 indelat efter typ av incident. Diagrammet visar att sammantaget 63 procent av samtliga incidentanmälningar under 2022 kan tillskrivas någon form av obehörigt röjande: antingen genom felskick eller genom annan felaktig hantering av personuppgifter. Även anmälningar om att någon berett sig själv olovlig tillgång till personuppgifter var vanliga. 2022 handlade 22 procent av alla inrapporterade personuppgiftsincidenter om obehörig åtkomst.

Obehörigt röjande på grund av felskick

Felskick är brev, mejl eller sms som innehåller personuppgifter och som oavsiktligt hamnat hos fel mottagare. Den typen av personuppgiftsincidenter var vanligast under 2022, när felskick representerade 38 procent av samtliga incidenter som anmäldes till IMY. Jämfört med föregående år innebär det att felskicken minskade med cirka 50 anmälningar.

Obehörigt röjande av andra anledningar

Den näst vanligaste typen av personuppgiftsincidenter 2022 stod övriga fall av obehörigt röjande för. Obehörigt röjande innebär att den personuppgiftsansvariga eller någon under den personuppgiftsansvarigas ledning har 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 gjort att personuppgifter kommit till fel mottagares kännedom. Den typen av incidenter utgjorde 25 procent av samtliga anmälda personuppgiftsincidenter 2022, vilket innebar en minskning med 3 procentenheter, eller cirka 280 anmälningar, jämfört med föregående år.

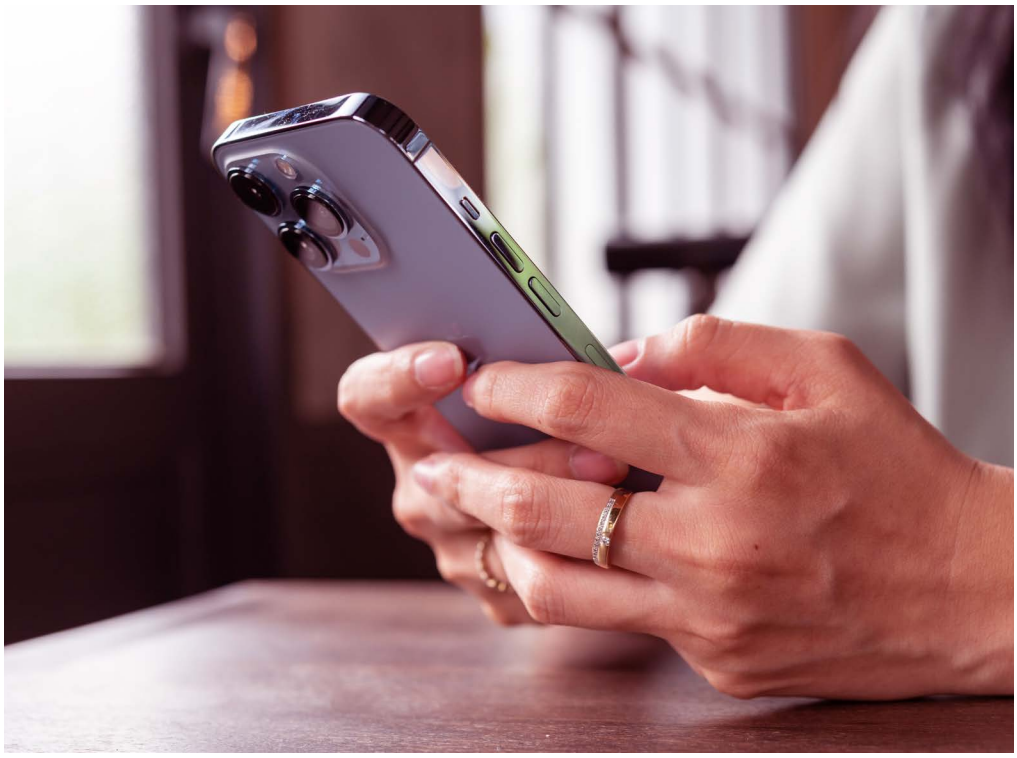
Obehörig åtkomst

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 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 hackning[4], som till exempel *spoofing*[5], *phishing-attacker*[6] eller *malware*[7], förekommer inom kategorin obehörig åtkomst. 2022 var den typen av incidenter 22 procent av samtliga incidentanmälningar. Det var en minskning från föregående år med 4 procentenheter, eller cirka 330 anmälningar.

Förlust

Förlust handlar om att information gått förlorad på något sätt, till exempel genom att en tjänstedator 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 kan också vara att en enhet med den personuppgiftsansvarigas kunddatabas förlorats eller stulits, eller att den personuppgiftsansvarigas databas har krypterats av så kallat *ransomware*. Förlust innebär att uppgifterna fortfarande existerar, men att den personuppgiftsansvariga har förlorat kontrollen eller åtkomsten till dem, eller inte längre har uppgifterna. Förlust utgjorde en relativt liten andel av anmälningarna, 10 procent 2022 – en ökning med 2 procentenheter eller cirka 70 anmälningar jämfört med föregående år.

4. 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.
5. 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.
6. 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.
7. Malware eller sabotageprogram är skadlig programvara som installeras på en dator eller nätverk utan användarens samtycke för att till exempel samla in information.



Ändring av personuppgifter

Ändring av personuppgifter innebär att personuppgifter ändrats på något sätt. Att personuppgifter ändras förekom förhållandevis sällan; 4 procent av incident-anmälningarna under 2022 rörde ändring av personuppgifter. Det var en ökning med 2 procentenheter jämfört med föregående år eller cirka 100 anmälningar.

Förstöring av information

Förstöring innebär att någon eller något har förstört information. Det kan exempelvis vara en dator eller hårddisk som har gått sönder. Den gemensamma nämnaren är att uppgifterna inte längre existerar eller är i ett sådant format att den personuppgifts-ansvariga inte längre kan använda dem. Det är ovanligt att personliga data förstörs. Mindre än 100 incidentanmälningar om förstöring av information anmäldes till IMY under 2022.

En tydlig trend: Obehörigt röjande alltid vanligast typ

Sett över 2019–2022 har ett grundläggande mönster uppstått för de olika typerna av personuppgiftsincidenter som anmäls. Den inbördes fördelningen mellan de olika typerna är relativt stabil med endast mindre variation mellan åren.

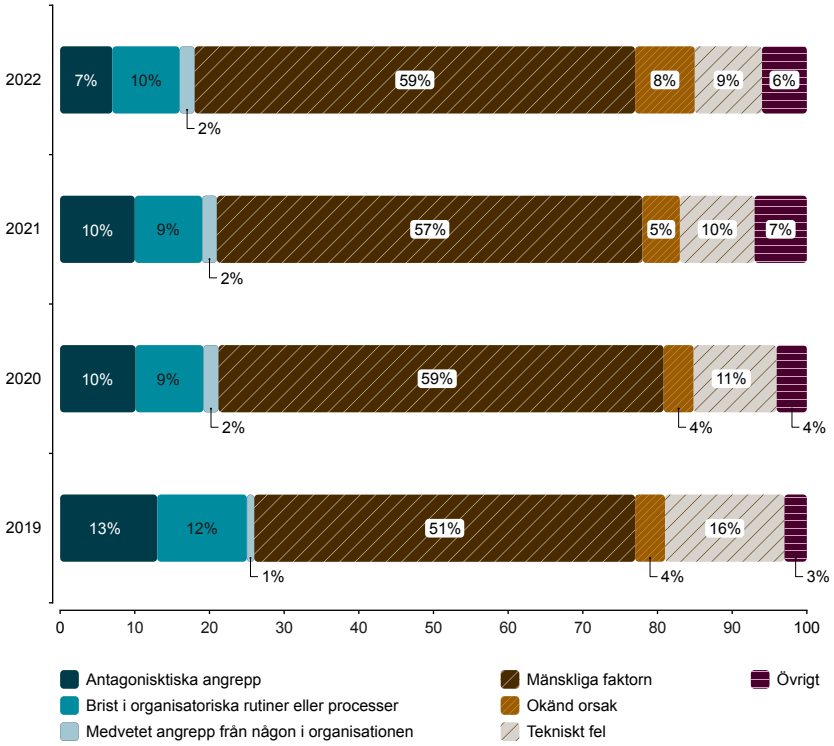
Så här brukar fördelningen se ut under ett normalår:

- 60 procent av anmälningarna gäller obehörigt röjande i någon form.
- 25–30 procent av anmälningarna gäller obehörig åtkomst.
- 10 procent av anmälningarna gäller förlust av information.

Sex av tio personuppgiftsincidenter orsakas av den mänskliga faktorn

Diagram 5

Andel anmälningar om personuppgiftsincidenter fördelat på orsak för incident 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika orsaker bakom incidentanmälningar bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter 2019–2022.

Diagram 5 visar hur olika orsaker bakom inrapporterade incidenter har fördelat sig under fyraårsperioden 2019–2022. Diagrammet visar att den mänskliga faktorn fortsatte att vara den vanligaste orsaken till alla rapporterade fall av personuppgifts-incidenter. Under 2019–2022 stod den mänskliga faktorn varje år för över hälften av alla rapporterade fall.

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. Bakom mer än hälften av de incidenter som orsakas av den mänskliga faktorn ligger någon form av felskick, alltså felskickade brev, mejl eller sms. Men det kan också handla om att individer, medvetet eller omedvetet, inte följer interna rutiner för hantering av personuppgifter.

2022 var den mänskliga faktorn orsaken bakom 59 procent av samtliga incident-anmälningar. Motsvarande siffra 2021 var 57 procent. Trots att andelen ökat med

2 procentenheter mot föregående år, minskade antalet anmälda personuppgiftsincidenter under 2022 med cirka 140 anmälningar.

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 9 procent av alla anmälda incidenter 2022, vilket räknat i antal fall innebar en minskning med cirka 100 anmälningar.

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.[8] 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*[9]. 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 7 procent av samtliga säkerhetsincidenter som anmäldes enligt dataskyddsförordningen 2022, eller cirka 340 fall. Jämfört med föregående år innebär det en minskning med 4 procentenheter eller cirka 220 anmälningar.

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 10 procent av samtliga incidentanmälningar 2022. Det är en ökning med cirka 20 anmälningar.

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 som den inte hade rätt till.

Under 2022 kunde 2 procent av incidenterna tillskrivas medvetna angrepp av någon i organisationen. Förändringen mot föregående år är förhållandevis liten, cirka 10 anmälningar.

8. IMY (tidigare Datainspektionen) släppte under 2020 en temarapport om anmälda personuppgiftsincidenter som orsakats av antagonistiska angrepp. Rapporten innehåller bland annat rekommendationer, beskrivningar av olika typer av antagonistiska angrepp och statistik över de verksamhetsområden som anmält incidenter orsakade av antagonistiska angrepp. Datainspektionens rapport (2020:3), Personuppgiftsincidenter som beror på antagonistiska angrepp 2019.
9. Ransomware är en typ av skadlig programvara som också kallas malware. Det rör sig om utpressning där angriparen genom skadlig programvara krypterar filer i någons datorsystem. För att få tillgång till dekrypteringsnyckel krävs företag, organisationer eller andra verksamhet på en lösensumma.

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. 2022 utgjorde incidenter med okänd orsak 8 procent av samtliga fall som rapporterades till IMY, vilket kan jämföras med föregående år när 5 procent av incidenterna saknade fastställd orsak. Det innebär att antalet fall ökade med cirka 140 anmälningar.

Övrigt

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

Under 2022 markerades 6 procent av incidentanmälningarna som Övrigt. Det är en minskning med cirka 80 anmälningar jämfört med 2021.

En tydlig trend: Mänskliga faktorn alltid vanligast orsak

Sett över 2019–2022 har ett grundläggande mönster uppstått för orsakerna bakom de personuppgiftsincidenter som anmäls. Den inbördes fördelningen mellan de olika orsakerna är relativt stabil med endast mindre variation mellan åren.

Så här brukar fördelningen se ut under ett normalår:

- 60 procent av anmälningar orsakas av den mänskliga faktorn.
- 10 procent av anmälningar orsakas av olika tekniska fel.
- 10 procent av anmälningar orsakas av brister i organisatoriska rutiner eller
- 10 procent av anmälningar orsakas av antagonistiska angrepp.

Exempel på inrapporterade antagonistiska angrepp 2022

Personuppgiftsincidenter som orsakas av att någon obehörig utanför organisationen försöker ta del av uppgifter den inte har rätt till klassas i IMY:s statistik som antagonistiska angrepp. 7 procent av samtliga anmälningar om säkerhetsincidenter enligt dataskyddsförordningen och enligt brottsdatalagen 2022 handlade om antagonistiska angrepp, det vill säga cirka 340 anmälningar. Här presenterar vi några exempel på vad dessa anmälningar handlade om.

Anmälningar som gjordes av verksamheter inom näringslivet

- Ett bolag blev utsatt för ett riktat cyberangrepp mot bolagets it-miljö. Angriparen fick åtkomst till systemet, påbörjade förberedelser för olovlig kopiering av data och inledde kryptering av informationen (på engelska *ransomware*). Den personuppgiftsansvariga hann avbryta attacken innan den fullbordades.
- En antagonist skickade mejl med skadlig kod (på engelska *phishing*) till den personuppgiftsansvariga. En anställd öppnade den bifogade filen varpå antagonisten tog över e-postkontot.
- Databasen till ett bolags it-leverantör blev utsatt för så kallade *SQL-injections*, där angriparen lyckades få ut uppgifter om de anställda.

Anmälningar som gjordes av verksamheter inom hälso- och sjukvård

- En vårdgivare blev utsatt för ett inbrott nattetid, där angriparen bröt sig in i ett kassaskåp som innehöll dokument och handlingar med personuppgifter.
- En antagonist kom genom hackning över en vårdanställds arbetsmejl. Antagonisten skickade sedan mejl som innehöll skadlig kod (på engelska phishing) till de anställda på organisationen, varpå medarbetare öppnade mejlet som innehöll koden. Incidenten ledde förutom ominstallation och översikt av informationssäkerheten till att tvåstegsautentisering applicerades på de anställdas mejlkonton.
- En tidigare anställd hos vårdgivaren blev inte borttagen från systemet korrekt och exporterade vårdgivarens patientregister.

Kapitel 2.

Anmälningar om personuppgiftsincidenter indelat efter verksamhetsområde

I det här kapitlet beskriver vi de vanligaste personuppgiftsincidenterna som anmäldes till IMY 2022 uppdelat på verksamhetsområden. Vi jämför de olika verksamhetsområdena med varandra och hur anmälningarna har utvecklats under fyraårsperioden.

Kapitlets viktigaste resultat:

- Felskick – alltså felskickade brev, mejl eller sms – var den vanligaste typen av personuppgiftsincidenter inom flera verksamhetsområden 2022. Andelen felskick var störst inom den finansiella sektorn och försäkringsbranschen samt inom hälso- och sjukvården.
- Den mänskliga faktorn var den vanligaste orsaken för personuppgiftsincidenter inom alla områden 2022. Andelen anmälningar ökade inom hälso- och sjukvården jämfört med föregående år.
- Andelen anmälningar som handlar om obehörig åtkomst – alltså att någon olovligen berett sig tillgång till personuppgifter – var störst inom näringsliv, skola och utbildning samt kommuner.

Tillhörande diagram redovisas i bilaga 2.

Felskick fortsatt vanligaste typen av incident

Felskick är den vanligaste typen av de personuppgiftsincidenter som anmäldes till IMY under 2022. Som felskick betecknas händelser där personlig information oavsiktligt hamnat hos fel mottagare genom brev, mejl, sms eller liknande. Under 2022 stod felskick för en stor del av samtliga säkerhetsincidenter som rapporterads till IMY. Närmare fyra av tio personuppgiftsincidenter av samtliga cirka 5 330 handlade om felskick, vilket visas i diagram 4.

Felskick var också den vanligaste personuppgiftsincidenten inom flera verksamhetsområden, vilket framgår av diagrammen i bilaga 2. En möjlig förklaring kan vara att verksamheterna i stor utsträckning skickar personuppgifter per post eller mejl.

Inom följande områden handlade knappt 40 procent eller mer av personuppgiftsincidenterna 2022 om felskick:

- finansiell sektor eller försäkring (57 procent, en ökning med 5 procentenheter)
- hälso- och sjukvård (43 procent, en ökning med 8 procentenheter)
- statlig myndighet och domstol (40 procent, en minskning med 1 procentenhet)
- socialtjänst, (39 procent, oförändrat)
- ideell organisation eller ekonomisk förening (38 procent, en minskning med 16 procentenheter).

Intressanta observationer

Under 2019–2022 ökade andelen felskick inom den finansiella sektorn och försäkringsbranschen konstant från år till år. Av diagram 10 i bilaga 2 framgår att felskick inom den finansiella sektorn och försäkringsbranschen utgjorde 44 procent av samtliga anmälda personuppgiftsincidenter 2019 jämfört med 57 procent 2022. Det är en ökning med 13 procentenheter.

Hälso- och sjukvården gjorde 2022 cirka 420 anmälningar där personuppgiftsincidenter oavsiktligt hade röjts på grund av felskick, vilket motsvarar en ökning med 8 procentenheter mot föregående år. Det framgår av diagram 12 i bilaga 2. Eftersom hälso- och sjukvården hanterar känsliga uppgifter om enskilda, bör varje incident anses som potentiellt allvarligt.

Den största förändringen från 2021 till 2022 skedde inom ideella organisationer och ekonomiska föreningar. Där minskade antalet anmälda personuppgiftsincidenter med 16 procentenheter. Notera dock att det handlar om relativt små tal.

Mänskliga faktorn dominerar som orsak

Den övervägande delen av samtliga incidenter som rapporterades till IMY under 2019–2022 förorsakades av den mänskliga faktorn, vilket framgår av diagram 5. Vi vet också en stor del av de incidenterna handlar om någon form av felskick, alltså felskickade brev, mejl eller sms.

Den mänskliga faktorn var den vanligaste orsaken för personuppgiftsincidenter inom alla verksamhetsområden och den absolut dominerande faktorn inom flera av dem, vilket framgår av diagrammen i bilaga 2.

Inom följande områden handlade 60 procent eller mer av incidenterna 2022 om den mänskliga faktorn:

- hälso- och sjukvård (71 procent, en ökning med 12 procentenheter)
- statlig myndighet (64 procent, en minskning med 6 procentenheter)
- finansiell sektor eller försäkring (63 procent, en minskning med 2 procentenheter)
- ideell organisation eller ekonomisk förening (60 procent, en minskning med 8 procentenheter)
- socialtjänst (61 procent, en minskning med 1 procentenhet).

Intressanta observationer

Hälso- och sjukvården utmärkte sig genom en ökad andel anmälningar om personuppgiftsincidenter som berodde på den mänskliga faktorn. 2022 gjordes cirka 700 anmälningar från verksamheter inom området. Eftersom hälso- och sjukvården hanterar känsliga uppgifter om enskilda bör varje incident anses som potentiellt allvarlig.

Inom statliga myndigheter samt ideella organisationer eller ekonomiska föreningar minskade andelen anmälningar som berodde på den mänskliga faktorn jämfört med föregående år. Vi har ingen information ifall verksamheterna inom dessa områden genomfört särskilda åtgärder för att begränsa den mänskliga faktorn, och i så fall vilka.

Obehörig åtkomst vanligast i näringsliv, skola och utbildning samt kommuner

22 procent av alla incidentanmälningar 2022 handlade om obehörig åtkomst, alltså att någon olovligen berett sig tillgång till personuppgifter, vilket framgår av diagram 4. Det kan ha hänt på olika sätt. Till exempel genom att behörigheter till ett it-system tilldelats felaktigt eller alltför generellt, eller att personuppgifter funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning. Men även antagonistiska angrepp genom olika typer av hackning förekommer inom kategorin obehörig åtkomst.

Vissa verksamhetsområden har en högre andel incidentanmälningar av den typen, vilket framgår av bilaga 2.

Inom följande områden handlade cirka 25 procent eller mer av incidenterna 2022 om att någon skaffat sig tillgång till personlig information som personen inte har rätt till. Av informationen i parentesen framgår den andelsmässiga fördelningen för 2022 inom respektive område och antal fall:

- näringsliv (44 procent eller cirka 190 fall)
- skola och utbildning (30 procent eller cirka 140 fall)
- kommun (28 procent eller cirka 150 fall).

Intressanta observationer

Inom områdena näringsliv, skola och utbildning samt kommun finns av allt att döma verksamheter som har brister i det systematiska dataskyddsarbetet. Systematiskt dataskydd är att arbeta förebyggande och kontinuerligt med dataskydd i verksamheten för att stärka integriteten för de personer vars personuppgifter verksamheten behandlar.

Att detta inte sker i alla verksamheter framgår även av IMY:s enkätstudien *Dataskyddsarbetet i praktiken*.[10] Studien genomfördes våren 2022 och dataskyddsombudsombud för 800 verksamheter deltog genom att besvara enkätfrågor. Rapporten visar att endast fyra av tio dataskyddsombud som ingår i studien anser att den egna organisationen arbetar kontinuerligt och systematiskt med dataskyddsfrågor.

10. IMY rapport 2023:1, Dataskyddsarbetet i praktiken. En studie av förutsättningar för arbetet med dataskyddsfrågor i verksamheter som är skyldiga att ha dataskyddsombud.

Kapitel 3.

Anmälningar om personuppgiftsincidenter i Norden

I det här kapitlet jämför vi anmälningar om personuppgiftsincidenter i Norden under 2019–2022.

Kapitlets viktigaste resultat:

- Danmark har flest anmälningar om personuppgiftsincidenter. Därefter kommer Sverige och Finland.
- I förhållande till folkmängden har Sverige färre anmälningar om personuppgiftsincidenter än Danmark och Finland men fler än Norge och Island.
- Det finns sannolikt en underteckning av personuppgiftsincidenter i Sverige.

En mer utförlig beskrivning av vårt tillvägagångssätt finns i bilaga 1.

Danmark har flest anmälda personuppgiftsincidenter

De nordiska länderna har en lång tradition av samarbete och samverkan, och våra respektive samhällen är uppbyggda på liknande sätt även om det förstås finns skillnader. Sedan den europeiska dataskyddsförordningen trädde i kraft 2018 har tillsynsmyndigheterna inom Norden träffats regelbundet i nordiska dataskyddsmöten för att utbyta erfarenheter. Det faller sig därför naturligt att jämföra Sverige med övriga Norden när det gäller personuppgiftsincidenter utifrån den europeiska dataskyddsförordningen.

Tabell 2
Antal anmälningar om personuppgiftsincidenter per land, 2019–2022

Land	2019	2020	2021	2022	Samtliga under fyraårsperioden
Danmark	7 242	8 772	8 554	8 812	33 380
Finland*	3 840	4 275	4 786	5 446	18 347
Sverige	4 702	4 542	5 726	5 291	20 257
Norge	1 893	2 008	2 255	2 237	8 393
Island	266	218	147	123	754
Färöarna**	2	7	18	37	64

Sammanställning över antalet anmälningar om personuppgiftsincidenter som är anmälningspliktiga utifrån anmälningsskyldigheten enligt dataskyddsförordningen (artikel 4, avsnitt 12). *Innehåller anmälda personuppgiftsincidenter från privat sektor på Åland (ett mindre tal). Uppgifter om anmälda personuppgiftsincidenter för offentlig sektor på Åland saknas här. **Motsvarigheten till dataskyddsförordningen (dátuverndarlógin) trädde i kraft 1 januari 2021 på Färöarna.[11]

Tabell 2 visar antal inrapporterade personuppgiftsincidenter per land under 2019–2022. Av diagrammet framgår att nivån på det antal incidenter som varje år rapporteras varierar i omfattning mellan de nordiska länderna. Flest antal personuppgiftsincidenter räknat över fyraårsperioden anmäldes av verksamheter i Danmark, cirka 33 000 incidenter, följt av verksamheter i Sverige med cirka 20 000 incidenter och av verksamheter i Finland med cirka 18 000 incidenter. Minst antal personuppgiftsincidenter rapporterades av verksamheter på Färöarna, sammantaget cirka 60 fall under fyraårsperioden.

11. Løgtingslóg um vernd av persónupplýsingum (Dátuverndarlógin).

Anmälningar om personuppgiftsincidenter per 100 000 invånare

De nordiska länderna liknar varandra i många avseenden, men de skiljer sig väsentligt i folkmängd. För att kunna jämföra de nordiska länderna beräknar vi antalet anmälningar om personuppgiftsincidenter per 100 000 invånare. Det ger oss ett intryck av hur många anmälningspliktiga säkerhetsincidenter utifrån dataskyddsförordningen som rapporteras i respektive land i förhållande till landets folkmängd. Trots att personuppgiftsincidenter per capita kan ses som ett trubbigt mått så ger det oss möjligheten att jämföra de nordiska länderna och att ställa nya, mer kvalificerade följdfrågor samt att föra djupare resonemang om det okända antal anmälningspliktiga incidenter som inte rapporteras till IMY (det vill säga om underteckning och mörkertal).

Tabell 3

Antal anmälningar om personuppgiftsincidenter per 100 000 invånare för respektive land 2019–2022

Land	2019	2020	2021	2022
Danmark**	124	155	146	149
Finland*	69	77	86	98
Färöarna*	4	13	34	68
Sverige*	46	44	55	50
Norge**	35	37	42	41
Island**	75	60	40	33

Sammanställning över antalet anmälningar om personuppgiftsincidenter per 100 000 invånare i Norden för 2019, 2020, 2021 och 2022. Information för Åland saknas i sammanställningen. * Beräkningen gjordes utifrån uppgifter om folkmängden 31 december respektive år. ** Beräkningen gjordes utifrån uppgifter om folkmängden 1 januari efterföljande år. För att skapa jämförbarhet användes siffran för folkmängden 1 januari 2020 för att representera folkmängden 31 december 2019 och så vidare.

Tabell 3 visar antalet anmälningar om personuppgiftsincidenter per år och per 100 000 invånare i respektive land under 2019–2022. Tabellen visar att antalet anmälda incidenter låg högst i Danmark 2022 med knappt 150 anmälda personuppgiftsincidenter per 100 000 invånare och i Finland med knappt 100 fall. I Sverige rapporterades 50 incidenter 2022. Trots sin förhållandevis stora folkmängd rapporterade alltså verksamheterna i Sverige färre personuppgiftsincidenter än verksamheterna i Danmark, i Finland och på Färöarna, men fler än i Norge och på Island.

Skillnader mellan olika länder kan bero på variationer i de verksamheter som finns inom respektive land. Eftersom personuppgiftsincidenter ska anmälas till det land där ett företag har sitt huvudkontor, ökar antalet anmälningar i länder där många internationella företag finns. Ett exempel för detta är Irland som med sina drygt 5 miljoner invånare hade cirka 130 incidenter per 100 000 invånare 2021.[12]

12. En mer detaljerad redovisning av antalet anmälda personuppgiftsincidenter per 100 000 invånare för länderna inom EU 2021 finns i IMY:s rapport 2022:1, Anmälda personuppgiftsincidenter 2021, s. 25.

Andra faktorer som kan påverka antalet anmälningar är den nationella dataskydds-myndighetens arbete, både i form av vägledningar, tillsyn och administrativa sanktionsavgifter. Just oro för sanktionsavgifter kan vara en bidragande faktor som kan tänkas få verksamheter att avstå från att rapportera anmälningspliktiga händelser. Men även brister i verksamheternas systematiska dataskyddsarbete kan bidra till de nationella skillnaderna.

För att kunna besvara frågan varför verksamheterna i Sverige, Finland och Norge varje år rapporterar färre incidenter utifrån dataskyddsförordningen än i Danmark, skulle det behövas en fördjupad studie som tar hänsyn till alla relevanta variabler och faktorer som kan påverka utfallet.

Befolkningsmängden i Norden 2022

- Sverige: 10,5 miljoner
- Danmark: 6 miljoner
- Finland: 5,6 miljoner
- Norge: 5,5 miljoner
- Island: 0,37 miljoner
- Färöarna: 0,054 miljoner.

Sannolik underteckning i Sverige

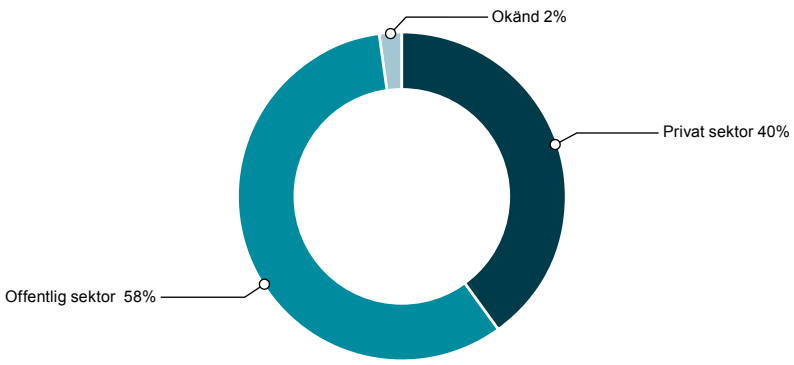
Sammanställningen av antalet anmälningar om personuppgiftsincidenter per 100 000 invånare i Norden förstärker bilden av att det sannolikt förekommer en underteckning av anmälningspliktiga personuppgiftsincidenter till IMY – särskilt när vi jämför Sverige med Danmark och Finland. År 2022 rapporterade verksamheterna i Finland dubbelt så många incidenter som i Sverige och verksamheterna i Danmark tredubbelt så många.

I nuläget finns det inte någon tillräckligt (bra) statistik för att kunna gå till botten med frågan om hur omfattande den troliga underteckningen är och vilka verksamheter den i så fall gäller. För att ge mer kvalificerade svar behövs ett fortsatt statistikutvecklingsarbete – både i Sverige, Norden och EU – så att vi kan jämföra data och göra mer djupgående analyser.

Vi kan dock få en indikation genom att jämföra våra svenska siffror över fördelningen av anmälda personuppgiftsincidenter med liknande siffror i Danmark.

Diagram 6

Andel anmälningar om personuppgiftsincidenter i Danmark 2022, fördelat på sektorer



Cirkeldiagram som redogör för den andelsmässiga fördelningen mellan inrapporterade personuppgifts-incidenter fördelat efter offentlig sektor (N = 5 119), privat sektor (N = 3 545) och okänd (N = 148) i Danmark under 2022. Samtliga anmälda personuppgiftsincidenter 2022 i Danmark var 8 812.

Diagram 6 visar andelen anmälningar om personuppgiftsincidenter i Danmark 2022 indelat efter sektor.[13] Diagrammet visar att fördelningsmönstret i Danmark skiljer sig från det svenska som redovisas i diagram 1. Det handlar framför allt om en högre grad av jämvikt mellan anmälningar från offentlig sektor och privat sektor, cirka 60 procent respektive 40 procent. Det kan jämföras med de 70 procent inom offentlig sektor och 25 procent inom privat sektor som anmäldes i Sverige 2022. I likhet med Sverige kom dock flest incidentrapporter från den offentliga sektorn även i Danmark.

I avsaknad av mer djupgående undersökningar och gemensam (nordisk respektive europeisk) statistik är det svårt att veta vad denna skillnad faktiskt beror på. En hypotes kan vara att offentlig sektor i Sverige generellt skickar digitala brev i större omfattning än man gör i Danmark, vilket skulle innebära en ökad risk i Sverige för att personuppgifter råkar skickas fel. Mot det antagandet talar att mer än 50 procent av anmälda personuppgiftsincidenter i Danmark beror på felskick (enligt information från den danska tillsynsmyndigheten), jämfört med mindre än 40 procent i Sverige.

13. Dataunderlaget till diagrammen togs fram av den ansvariga danska tillsynsmyndigheten *Datatilsynet*.

Kapitel 4.

Personuppgiftsincidenter i ljuset av ett förändrat säkerhetsläge

I det här kapitlet redogör vi för hur personuppgiftsincidenter påverkas av det förändrade säkerhetsläget med krig i Europa och oro för cyberangrepp. Vi undersöker de antagonistiska angreppen, det vill säga att någon obehörig utanför organisationen försöker ta del av uppgifter den inte har rätt till.

Kapitlets viktigaste resultat:

- Trots farhågorna minskade de antagonistiska angrepp som anmäls till IMY under 2022.
- Näringslivet rapporterade flest antagonistiska angrepp. Därefter kommer hälso- och sjukvården.

Personuppgiftsincidenter är säkerhetsincidenter

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter.[14] Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter, det vill säga till att någon får eller förskaffar sig tillgång till information den inte har rätt till.[15]

Sammantaget 70 procent av de säkerhetsincidenter enligt dataskyddsförordningen och brottsdatalagen som anmäldes till IMY 2022 kom från den offentliga sektorn, det vill säga från verksamheter som statliga myndigheter, socialtjänsten, hälso- och sjukvården och kommuner som inte sällan hanterar känsliga uppgifter om individen. En fjärdedel av samtliga personuppgiftsincidenter som IMY har kännedom om rapporterades inom statliga myndigheter, vilket visas i diagram 2.

Vikten av en god informationssäkerhet inom statliga myndigheter, alltså säker lagring av känslig information och personuppgifter, uppmärksammades av Myndigheten för samhällsskydd och beredskap (MSB) år 2020. MSB hade identifierat ett behov av tydligare styrning av statliga myndigheters informationssäkerhetsarbete och uppdaterade därför flera viktiga föreskrifter inom området. De nya, skärpta föreskrifterna trädde i kraft 1 oktober 2020 och handlar om

- informationssäkerhet för statliga myndigheter[16]
- säkerhetsåtgärder i informationssystem i statliga myndigheter[17]
- rapportering av it-incidenter för statliga myndigheter.[18]

Föreskrifterna ställer bland annat krav på att statliga myndigheter ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete och rapportera it-incidenter som allvarligt kan påverka säkerheten. MSB utfärdade dessutom nya föreskrifter om säkerhetsåtgärder i informationssystem (it-säkerhet). Myndigheten poängterade att även andra offentliga och privata organisationer har nytta av föreskrifterna och vägledningarna i sitt systematiska informationssäkerhetsarbete.

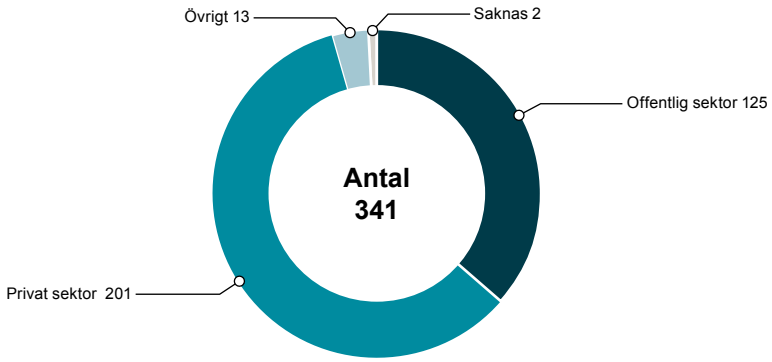
14. En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, artikel 4.12 dataskyddsförordningen.
15. Vissa organisationer har krav på sig att rapportera skilda typer av it-incidenter, men rapporteringskraven och var incidenten ska rapporteras varierar beroende på vilken reglering som organisationen berörs av. Förutom bestämmelserna i dataskyddsförordningen finns bland annat bestämmelser i krisberedskapsförordningen, säkerhetsskyddsförordningen och NIS-direktivet om anmälningsplikten för andra typer av incidenter. Mer information finns i faktarutan Generellt om incidentrapportering på sida 40 i denna rapport.
16. Föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
17. Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).
18. Föreskrifter om rapportering av IT-incidenter för statliga myndigheter (MSBFS 2020:8).

Antagonistiska angrepp under krigsåret 2022

Säkerhetsläget i Sverige och övriga Europa har ändrats sedan Ryssland den 24 februari 2022 inledde sin invasion av Ukraina. Sedan dess har Ukraina utsatts för omfattande cyberangrepp och farhågan har varit att även cyberangrepp mot samhällsviktiga verksamheter i Sverige skulle komma att öka under 2022.[19]

Diagram 7

Antal anmälningar om personuppgiftsincidenter som orsakades av antagonistiska angrepp 2022 indelat efter sektor



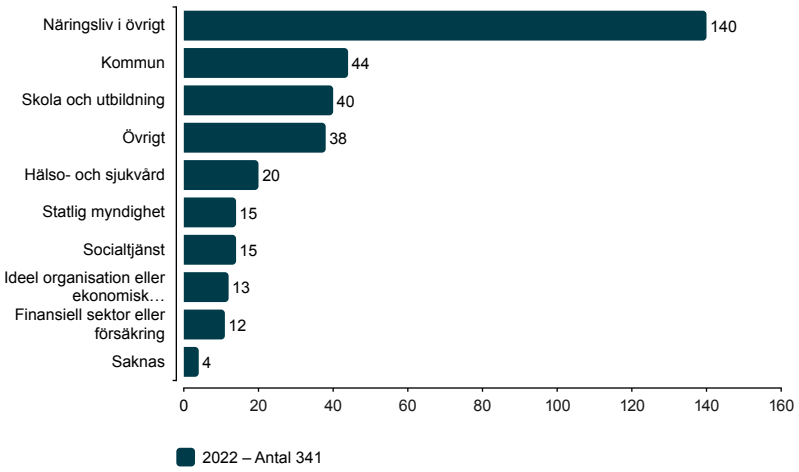
Cirkeldiagrammet redogör för antalet anmälningar av personuppgiftsincidenter med antagonistiska angrepp som orsak och fördelat på offentlig sektor, privat sektor och övriga sektorer under 2022. Dessutom redovisas antalet antagonistiska angrepp 2022 som saknar sektorstillhörighet.

Diagram 7 visar antalet anmälningar om antagonistiska angrepp som rörde personuppgifter 2022 indelat efter olika sektorer. Diagrammet visar att merparten av anmälningarna om personuppgiftsincidenter som beror på någon obehörig utanför organisationen försöker ta del av uppgifter den inte har rätt till rapporterades av verksamheter inom privat sektor, cirka 200 fall. Offentlig sektor anmälde 125 incidenter som involverade personuppgifter.

19. MSB rapport, När kriget kom nära. Årsrapport it-incidentrapportering 2022.

Diagram 8

Antal anmälningar om personuppgiftsincidenter som orsakades av antagonistiska angrepp 2022 indelat efter verksamhetsområde



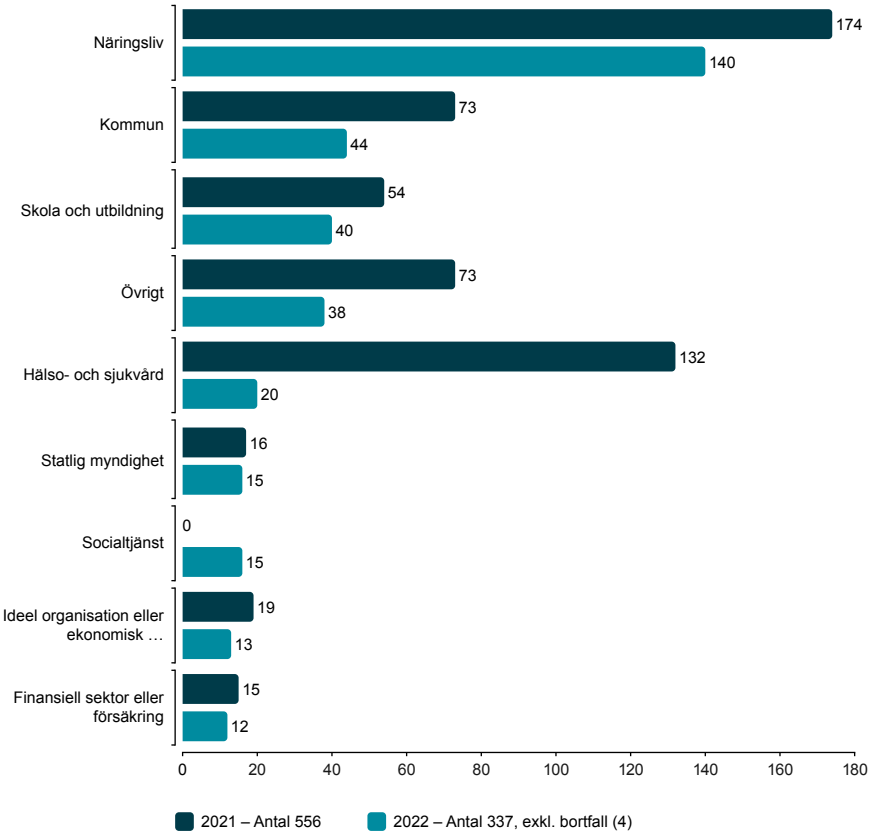
Stapeldiagrammet redovisar antalet anmälningar om personuppgiftsincidenter som orsakats av antagonistiska angrepp indelat efter nio verksamhetsområden under 2022. Dessutom redovisas antalet fall där information saknas om tillhörighet till något av de nio verksamhetsområdena.

Diagram 8 visar antalet anmälningar om personuppgiftsincidenter som orsakades av antagonistiska angrepp 2022 indelat efter verksamhetsområde. Diagrammet visar att merparten av samtliga anmälningar om antagonistiska angrepp rapporterades inom näringslivet, 140 fall. Andra förhållandevis utsatta verksamheter fanns inom kommuner samt skola och utbildning, som vardera rapporterade cirka 40 anmälningar om antagonistiska angrepp som involverade personuppgifter.

Antagonistiska angrepp i ett längre tidsperspektiv

Diagram 9

Antal personuppgiftsincidenter som orsakades av antagonistiska angrepp 2022 och 2021 indelat efter verksamhetsområde



Liggande stapeldiagrammet redovisar och jämför antalet anmälda personuppgiftsincidenter 2022 och 2021, uppdelat på nio olika verksamhetsområden.

Diagram 9 visar antalet anmälningar om personuppgiftsincidenter som orsakades av antagonistiska angrepp 2021 och 2022 fördelat på verksamhetsområde. Diagrammet visar att flest anmälningar om antagonistiska angrepp gjordes inom näringslivet med cirka 310 personuppgiftsincidenter de senaste två åren, följt av hälso- och sjukvården med cirka 130 incidenter under samma period. Socialtjänsten och statliga myndigheter gjorde sammantaget relativt få anmälningar om antagonistiska angrepp under 2021 och 2022, 25 och 30 anmälningar.

Trots farhågor minskade de antagonistiska angreppen under 2022

Tabell 4

Sammanställning av anmälningar om antagonistiska angrepp bland samtliga anmälda personuppgiftsincidenter för 2019–2022

	2019	2020	2021	2022
Samtliga anmälningar om personuppgiftsincidenter respektive år	4 757	4 588	5 767	5 331
Anmälningar om antagonistiska angrepp av samtliga incidenter för respektive år (antal)	616	459	566	341
Anmälningar om antagonistiska angrepp av samtliga incidenter för respektive år (andel)	13 procent	10 procent	10 procent	6 procent
Förändring i antal anmälningar om antagonistiska angrepp mot föregående år		–157	+107	– 225

Tabellen redovisar andelen anmälningar om personuppgiftsincidenter som beror på antagonistiska angrepp och som rapporterades till IMY utifrån anmälningsplikten i dataskyddsförordningen och utifrån anmälningsplikten i brottsdatalagen.

Tabell 4 visar andelen anmälningar om antagonistiska angrepp bland anmälda personuppgifter 2019–2022. Tabellen visar dessutom antalet anmälningar om antagonistiska angrepp och förändringen jämfört med respektive föregående år.

Av sammanställningen framgår att anmälningar om antagonistiska angrepp – oron till trots – minskade med 4 procentenheter 2022 jämfört med 2021.[20] Det motsvarar cirka 220 fall. Sett över fyraårsperioden har personuppgiftsincidenter som beror på antagonistiska angrepp och som behöver anmälas utifrån dataskyddsförordningen minskat med 6 procentenheter. Antal anmälningar om antagonistiska angrepp som togs emot av IMY var som högst 2019 med över 600 rapporterade händelser.[21]

20. Även MSB observerade att antalet inrapporterade it-incidenter som ses som antagonistiska angrepp minskade 2022 jämfört med 2021. MSB rapport, När kriget kom nära. Årsrapport it-incidentrapportering 2022, s. 20.
21. 2019 genomförde IMY (dåvarande Datainspektionen) en fördjupad undersökning av antagonistiska angrepp. Analysen visade bland annat att en betydande andel, nästan nio av tio, av de anmälda personuppgiftsincidenten som berodde på it-angrepp kom från privat sektor. En tänkbar förklaring att privat sektor är mer utsatt för och har större fokus på it-angrepp än offentlig sektor. Datainspektionens rapport 2020:3, Personuppgiftsincidenter som beror på antagonistiska angrepp 2019.

Kapitel 5.

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

I det här kapitlet 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 2022.

Anmälningsplikt för vissa personuppgiftsincidenter

I dataskyddsförordningen finns en skyldighet för organisationer att anmäla vissa typer incidenter, så kallade 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.[22] 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 fått vetskap om händelsen, bedöma vilken risk personuppgiftsincidenten kan medföra för den enskilde.[23] 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 och om de registrerade ska informeras.[24]

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.[25] Sedan mars 2020 är det möjligt att skicka in anmälningar om personuppgiftsincidenter digitalt i myndighetens e-tjänst för anmälningar av personuppgiftsincidenter.

Vid riskbedömningen ska den personuppgiftsansvariga ta hänsyn till de specifika omständigheterna i samband med incidenten. Några faktorer att ta hänsyn till 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.[26]

Om det är osannolikt att incidenten leder till en risk för de registrerades friheter 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.[27] Oavsett om incidenten ska anmälas till IMY eller inte, så är den personuppgiftsansvariga alltid skyldig att dokumentera incidenten internt.[28]

22. En personuppgiftsincident är enligt artikel 4.12 i dataskyddsförordningen en säkerhetsincident som leder till oavsiktlig eller olaglig förstörning, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.
23. Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 2018.
24. Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 2018.
25. Artikel 33 dataskyddsförordningen.
26. Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 2018.
27. Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 2018.
28. Artikel 33.5 dataskyddsförordningen.

Generellt om incidentrapportering

Vissa organisationer har krav på sig att rapportera skilda typer av it-incidenter,[29] men rapporteringskraven och var incidenten ska rapporteras varierar beroende på vilken reglering som organisationen berörs av. Förutom bestämmelserna i dataskyddsförordningen finns bland annat bestämmelser i krisberedskapsförordningen[30], säkerhetsskyddsförordningen[31] och NIS-direktivet[32] om anmälningsplikten för andra typer av incidenter.

Samma incident kan under vissa omständigheter vara anmälningspliktig till flera olika myndigheter. Statliga myndigheter[33] och leverantörer av samhällsviktiga och digitala tjänster[34] rapporterar exempelvis IT-incidenter till Myndigheten för samhällsskydd och beredskap (MSB). Om det rör sig om en incident som faller under rapporteringsskyldigheten i säkerhetsskyddsförordningen är det i stället till Säkerhetspolisen, och i vissa fall även till Försvarsmakten det ska rapporteras till. Är incidenten relaterad till en brottslig gärning, ska incidenten rapporteras till MSB och Polismyndigheten. Om IT-incidenten dessutom påverkar personuppgifter så att den är rapporteringspliktig enligt dataskyddsförordningen, ska den rapporteras till Integritetsskyddsmyndigheten (IMY), utom i de fall där incidenten ska rapporteras i enlighet med säkerhetsskyddslagen.

29. Se vidare MBS:s föreskrifter om obligatorisk it-incidentrapportering för statliga myndigheter (MSBFS 2016:2).
30. Förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (2015:1052).
31. Säkerhetsskyddsförordning (2021:955).
32. Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
33. Förordning om statliga myndigheters beredskap (2022:524).
34. Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

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 anmäla det inträffade till IMY och informera de registrerade om att incidenten inträffat.[35] 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 skydda sig själv mot negativa konsekvenser av incidenten, till exempel genom att byta lösenord eller spärra ett bankkort.[36]

Den personuppgiftsansvariga ska åtminstone lämna följande information[37] till de registrerade:

- 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 personuppgiftsansvariga har genomfört eller föreslagit för att åtgärda incidenten, inbegripet i förekommande fall åtgärder för att mildra dess potentiella negativa effekter.

35. Artikel 34 dataskyddsförordningen.
36. Skäl 86 dataskyddsförordningen, Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 2018.
37. Artikel 34 dataskyddsförordningen, även artikel 33.3 b, c och d dataskyddsförordningen.

IMY:s arbete med personuppgiftsincidenter

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

- vad de personuppgiftsansvariga gör för att motverka negativa effekter av incidenter
- vilka typer av personuppgiftsincidenter som är vanliga
- vilka verksamheter som anmäler personuppgiftsincidenter.

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

IMY kan inleda tillsyn

IMY kan välja att inleda en tillsyn med anledning av en anmäld personuppgifts-incident. 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 personupp-giftsincident 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 2022 har fem tillsynsärenden inletts baserade på anmälda personuppgifts-incidenter, vilket är betydligt färre än de trettiotal som inleddes under 2021. Det minskade antalet har främst sin förklaring i att majoriteten av tillsynerna som inleddes 2021 var mot flera bolag i en och samma koncern. Årets siffra kan jämföras med de tre tillsyner som inleddes baserade på anmälda personuppgiftsincidenter under 2020.

Mer om IMY:s tillsynsärenden: https://www.imy.se/tillsyner/.

Pågående tillsynsärenden under 2022

I det följande avsnittet redogörs för nya och pågående tillsynsärenden under 2022 baserade på inrapporterade personuppgiftsincidenter.

Avanza

IMY har inlett 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 inlett 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 webbplatsen i vissa fall kunnat hämta in 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 inlett 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 kontrollera användarnas personuppgifter.

Polismyndigheten

IMY har inlett 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.[38]

Vklass

IMY har inlett tillsyn mot lärplattformen Vklass efter att IMY har tagit emot ett sextiotal anmälningar om personuppgiftsincidenter från skolor och kommuner. Enligt incidentanmälningarna ska någon ha laddat ner personuppgifter om skolelever och lärare från lärplattformen.

I granskningen ställer IMY ett antal frågor till företaget bakom lärplattformen för att bland annat ta reda på vad som inträffat, hur företaget upptäckte incidenten, omfattningen av incidenten och vilka organisatoriska och tekniska säkerhetsåtgärder som vidtagits före och efter incidenten.

Användning av Facebook-pixel hos apotek och vårdgivare

IMY har inlett fyra tillsyner mot Apoteket AB, Apotea AB, Apohem AB respektive Kry International AB för att utreda de personuppgiftsincidenter som respektive bolag anmält och som rör överföring av personuppgifter till Facebook. I respektive anmälan framgår att bolagen haft en så kallad Facebook-pixel på sin webbshop, vilket har

38. IMY fattade beslut i ärendet 16 januari 2023. IMY riktar kritik mot polisens e-posthantering och rekommenderar att polisen ska genomföra ytterligare åtgärder för att höja skyddsnivån. Mer information finns på IMY:s webbplats: https://www.imy.se/tillsyner/polisen-e-post/.

medfört att bolagen överfört personuppgifter till Facebook. IMY ställer ett antal frågor som bland annat rör vilken typ av personuppgifter som förts över till Facebook, vad syftet är med överföringen av uppgifter, vilken rättslig grund som använts för överföringen och hur bolagen bedömt riskerna med att dela personuppgifter från sin webbshop med Facebook.

Avslutade tillsynsärenden under 2022

I det följande avsnittet redogörs för avslutade tillsynsärenden under 2022 baserade på inrapporterade personuppgiftsincidenter.

Region Uppsala

IMY inledde 2019 tillsyn mot sjukhusstyrelsen i Region Uppsala och regionstyrelsen i Region Uppsala med anledning av två anmälningar om personuppgiftsincidenter. IMY konstaterar att regionen inte har genomfört tillräckliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för de personuppgifter som behandlas.

Den ena granskningen rör känsliga personuppgifter och personnummer som skickats via mejl. Själva överföringen av mejlen var krypterad men inte informationen i mejlen. Det rör dels mejl med patientuppgifter som skickats automatiserat till berörda vård-förvaltningar inom regionen, dels mejl med patientuppgifter som skickats manuellt till forskare och läkare inom regionen. För de konstaterade bristerna i den granskningen utfärdar IMY en administrativ sanktionsavgift på 300 000 kronor till regionstyrelsen i Region Uppsala.

Myndigheten har granskat säkerheten för de personuppgifter som behandlats, men har inte granskat lagligheten i själva tredjelandsöverföringen. För de konstaterade bristerna som den granskningen påvisat utfärdar IMY en sanktionsavgift på 1,6 miljoner kronor till sjukhusstyrelsen i Region Uppsala.

Tullverket

IMY inledde 2020 tillsyn mot Tullverket med anledning av en personuppgiftsincident. Ett par medarbetare vid Tullverkets tullkriminalverksamhet har använt molntjänsten Google Foto i sina tjänstemobiler. Tjänstemännen hade kopplat sina privata Google Foto-konton till sina tjänstemobiler som automatiskt synkat de foton och filmer som tagits i tjänsten till molntjänsten. Tullverket har angett att användningen av Google Foto inte var tillåten inom myndigheten.

IMY konstaterar att Tullverket har haft bristfälliga rutiner och tekniska spärrar, vilket gjort att uppgifter från brottsutredningar överförts från tjänstemobiler till en amerikansk molntjänst. IMY utfärdar en administrativ sanktionsavgift på 300 000 kronor till Tullverket.

Den andra granskningen rör hur Akademiska sjukhuset i Uppsala skickar mejl med patientuppgifter till patienter och remittenter i tredjeland, alltså länder utanför EU. IMY:s granskning omfattar även lagringen av patientuppgifter i sjukhusets mejlserver.

Bilaga 1.

Dataunderlaget

I den här bilagan redovisar vi grundläggande information om dataunderlaget för statistiken, indelningen i kategorier och undergrupper samt mer information om den nordiska jämförelsen.

Dataunderlaget för statistiken

Inflödet varierar

När dataskyddsförordningen började gälla i maj 2018 infördes en skyldighet för privata och offentliga verksamheter som behandlar personuppgifter att rapportera vissa personuppgiftsincidenter till IMY.[39] Kort därefter infördes motsvarande anmälningsskyldighet för brottsbekämpande myndigheter i brottsdatalagen.[40] Antalet anmälda personuppgiftsincidenter har sedan dess varierat från år till år.

Tabell 5

Antal anmälningar om personuppgiftsincidenter 2019–2022

	2019	2020	2021	2022
Dataskyddsförordningen	4 702	4 542	5 726	5 291
Brottsdatalagen	55	48	41	40
Samtliga	**4 757**	**4 590**	**5 767**	**5 331**

Sammanställning över antalet anmälningar om personuppgiftsincidenter som rapporterats av olika verksamheter utifrån bestämmelserna i dataskyddsförordningen och utifrån bestämmelserna i brottsdatalagen för 2019–2022.

Tabell 5 visar inflödet av anmälda personuppgiftsincidenter enligt dataskyddsförordningen och brottsdatalagen för 2019–2022. De beräkningar vi gör i rapporten utgår från det totala antalet för anmälda personuppgiftsincidenter per år i tabellen.

Inflödet var som störst under 2021 med närmare 5 770 incidenter och hade ökat med närmare 1 170 fall mot föregående år, 2020. 2022 minskat däremot inflöde av anmälda personuppgifter mot toppnoteringen från 2021. 2022 anmäldes totalt närmare 5 330 incidenter, vilket är en volymminskning med cirka 440 incidenter mot 2021.

Avrundade tal

Observera att rapportens diagram som redovisar fördelningar i procent bygger på avrundade tal, vilket kan leda till att totalen bli något större eller något mindre än 100 procent. För att öka läsbarheten använder vi även avrundade tal i delar av löptexten, vilket tydliggörs i texten.

Bortfall

Det finns mindre partiella bortfall hos de data som ligger till grund för rapporten. Partiella bortfall beror på att anmälningar om personuppgiftsincidenter av någon anledning inte matas in med all information i IMY:s ärendehanteringssystem. Ärenden som

39. 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).
40. Dataskyddsförordningen infördes 25 maj 2018 och brottsdatalagen 1 augusti 2018.

saknar information (nyckelord) kan inte analyseras i alla avseenden. 2022 varierade det partiella bortfallet 2,5–3 procent:

- 135 fall saknade information om sektorstillhörighet (2,5 procent)
- 144 fall saknade information om typ av personuppgiftsincident (2,7 procent)
- 155 fall saknade information om orsak för personuppgiftsincidenten (2,9 procent)
- 159 fall saknade information om verksamhetsområde (3 procent).

Bortfallet är relativt litet och påverkar inte resultaten i våra statistiska sammanställningar på ett avgörande sätt.

Överteckning, underteckning och mörkertal

Denna rapport bygger på de incidentanmälningar som kommer in till IMY varje år. Det innebär att det finns ett mörkertal av incidenter som av olika skäl inte kommer till myndighetens kännedom. Antalet incidenter som faktiskt inträffar varje år är alltså större än vad som redovisas i rapporten.

Vi bedömer att merparten av de cirka 5 330 personuppgiftsincidenter som anmäldes till IMY under 2022 utgörs av faktiska incidenter, det vill säga att det handlade om anmälningspliktiga händelser som rapporterades korrekt och enligt bestämmelserna i dataskyddsförordningen respektive i brottsdatalagen.

Vi har noterat att en viss överteckning i form av icke-anmälningspliktiga säkerhetsincidenter ibland förekommer – särskilt inom den offentliga sektorn. Överteckningen kan möjligen förklaras med att verksamheter inom exempelvis hälso- och sjukvård hanterar känsliga personuppgifter och därför av försiktighet hellre rapporterar icke-anmälningspliktiga incidenter än att försumma sin anmälningsplikt. Enligt vår bedömning är överteckningen försumbar 2022.

Utifrån de relativt låga anmälningsvolymer som rapporteras från den privata sektorn jämfört med den offentliga sektorn, bedömer vi att det troligtvis förekommer en viss underteckning av anmälningspliktiga incidenter från näringslivet (exklusive finansiell sektor eller försäkringar).

Dessutom utgår vi ifrån att inte alla personuppgiftsincidenter som inträffar upptäcks, vilket leder till att det sannolikt finns ett mörkertal av oupptäckta personuppgiftsincidenter. Vi känner inte till omfattningen av detta mörkertal. Rapportens jämförelse med andra länder inom Norden visar att underteckningen av anmälningspliktiga incidenter och mörkertalet av icke upptäckta händelser tillsammans kan utgöra relativt stora volymer – uppskattningsvis 10 000 incidenter jämfört med antalet anmälda personuppgiftsincidenter per år i Danmark.

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 flervalsalternativ som den personuppgiftsansvariga fyller i utifrån sin egen bedömning av omständigheterna för incidenten.
IMY gör ingen egen bedömning om den beskrivning som ges är ”rätt” eller ”fel”, utan utgår från vad den personuppgiftsansvariga har angett.

IMY:s diariesystem läser automatiskt av svaren i anmälan och registrerar bland annat
- det verksamhetsområde där incidenten inträffade
- typen av incident
- orsaken 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 2022:
- finansiell sektor eller försäkringar
- hälso- och sjukvård
- ideell organisation eller ekonomisk förening
- kommun
- näringsliv
  - näringslivet (exklusive finansiell sektor eller försäkringar)
  - kreditupplysning
  - inkasso
- skola och utbildning
  - annan eftergymnasial utbildning
  - forskning
  - förskola, grundskola, gymnasium
  - universitet eller högskola
- socialtjänst
- statlig myndighet
  - statliga myndigheter
  - polis
  - rättsväsendet i övrigt
- övrigt.

Typ av incident

Denna kategori består av sex typer av personuppgiftsincidenter:

- förlust av information
- förstöring av information
- obehörigt röjande – felskick
- 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 tre olika sektorer där personuppgiftsincidenterna har inträffat:

- offentlig sektor
- privat sektor
- övriga.

Nordisk jämförelse

Data till den nordiska jämförelsen togs fram med hjälp av de nationella dataskydds-myndigheterna i Danmark, Norge, Finland, Island och Färöarna. Dataskydds-myndigheterna sammanställde grundläggande information om antalet personuppgifts-incidenter för 2019–2022. De nordiska tillsynsmyndigheterna levererade också uppgifter om folkmängden för respektive år eller hjälpte IMY att få fram rätt information. När det gäller Åland så inkluderar Finlands redovisning av antalet anmälda personuppgiftsincidenter inom privat sektor de incidenter som anmäldes av verksamheter inom privat sektor på Åland. Dessa är få till antalet. Vi saknar uppgifter om anmälda personuppgiftsincidenter i den offentliga sektorn från dataskydds-myndigheten på Åland.

Jämförelsen baseras på antalet personuppgiftsincidenter som har rapporterats till de nordiska ländernas tillsynsmyndigheter utifrån anmälningsskyldigheten enligt dataskyddsförordningen artikel 4.12.

Kvaliteten på nationella data säkerställdes av respektive tillsynsmyndighet. Sammanställningen av all data, olika beräkningar och analysen av personuppgiftsincidenter under fyraårsperioden gjordes av IMY.

Bilaga 2.

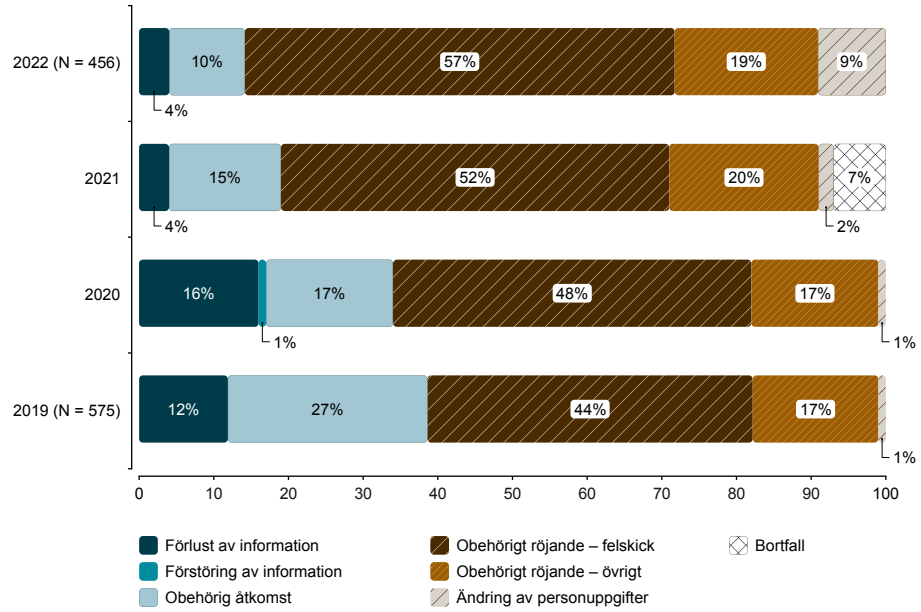
Diagram över anmälningar om personuppgifts-incidenter indelat efter verksamhets-område

I den här bilagan redovisar vi anmälningar om personuppgiftsincidenter till IMY för 2019–2022. Vi redovisar statistik för varje verksamhetsområde för sig, indelat efter typ av incident som anmäldes från respektive område samt vad som uppgavs som orsak till incidenten. I enstaka fall saknas information för 2019, vilket framgår tydligt av diagramtexten. För 2019 respektive 2022 redovisar vi även antalet som ingår i urvalet (N).

Finansiell sektor eller försäkring

Diagram 10

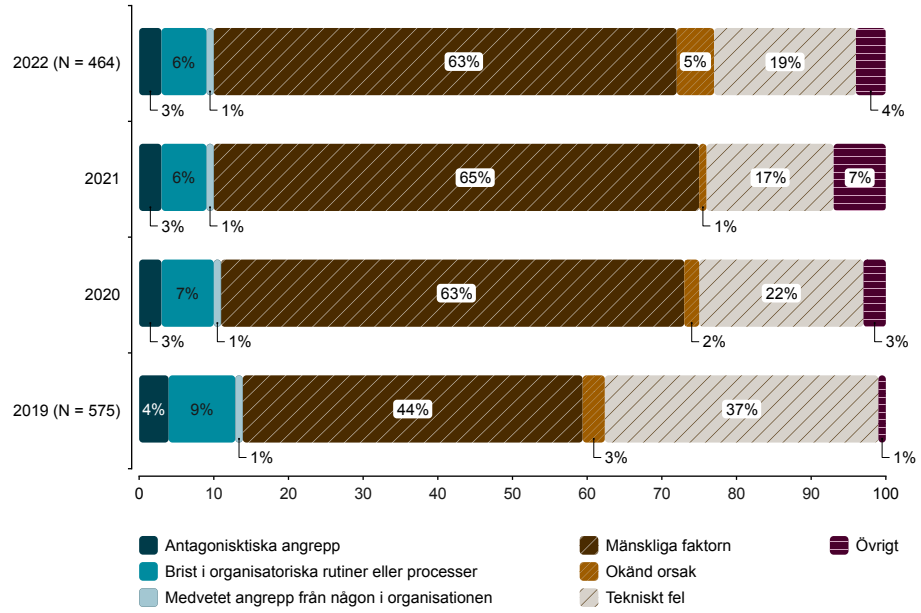
Andel anmälningar om personuppgiftsincidenter indelat efter typ av incident under 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika typer av incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet finansiell sektor eller försäkring 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Diagram 11

Andel anmälningar om personuppgiftsincidenter fördelat på orsak för incident 2019–2022

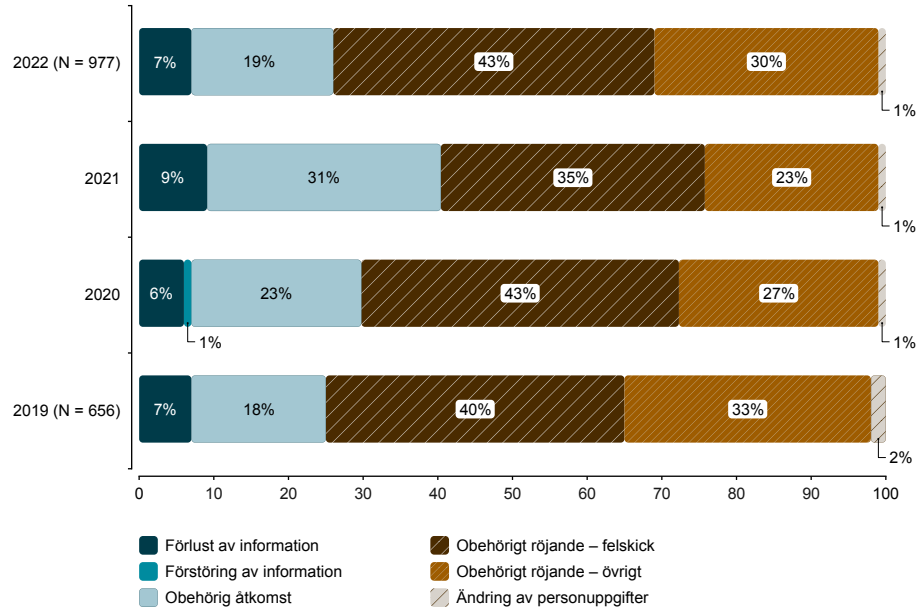


Liggande fraktionsstapeldiagram som jämför hur mycket olika orsaker bakom incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet finansiell sektor eller försäkring 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Hälso- och sjukvård

Diagram 12

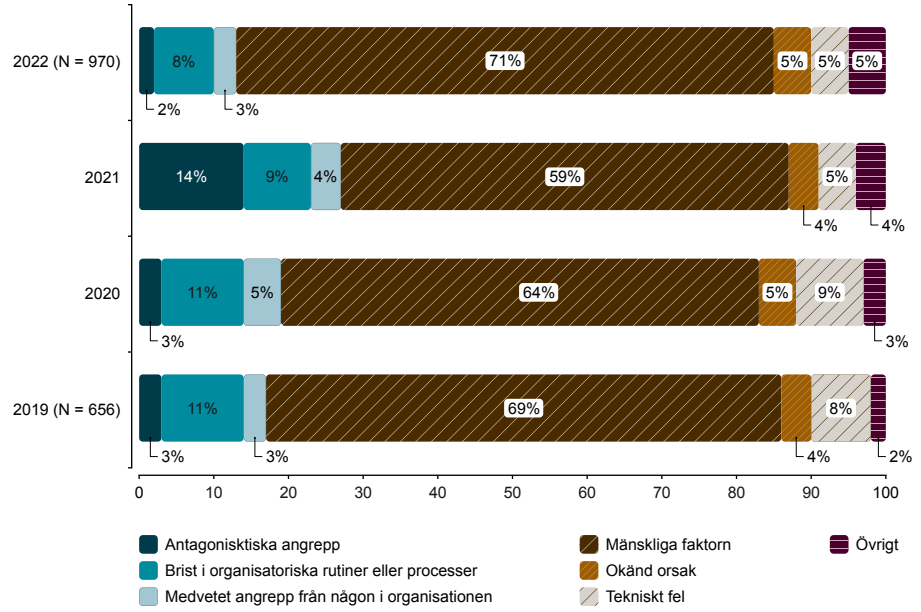
Andel anmälningar om personuppgiftsincidenter indelat efter typ av incident under 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika typer av incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet hälso- och sjukvård 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Diagram 13

Andel anmälningar om personuppgiftsincidenter fördelat på orsak för incident 2019–2022

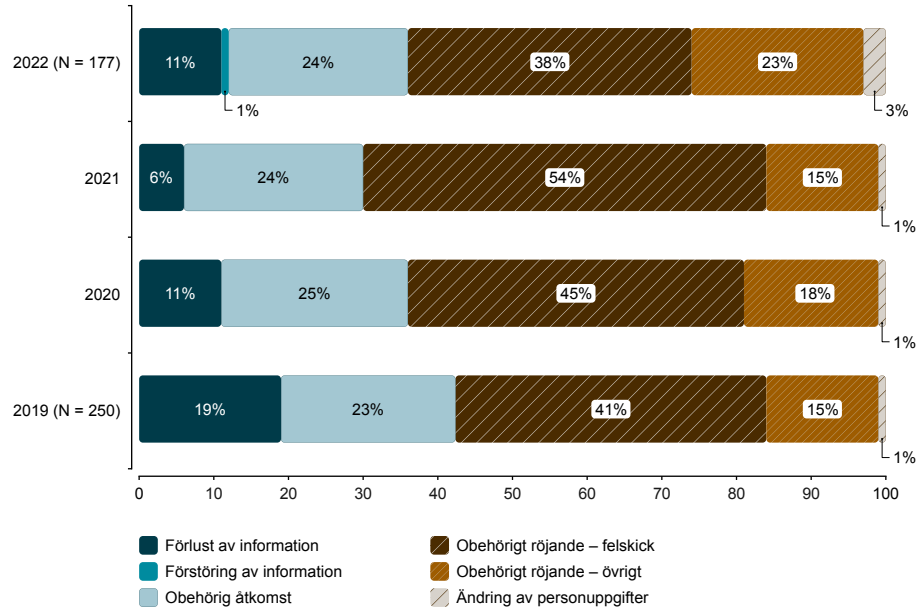


Liggande fraktionsstapeldiagram som jämför hur mycket olika orsaker bakom incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet hälso- och sjukvård 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Ideell organisation eller ekonomisk förening

Diagram 14

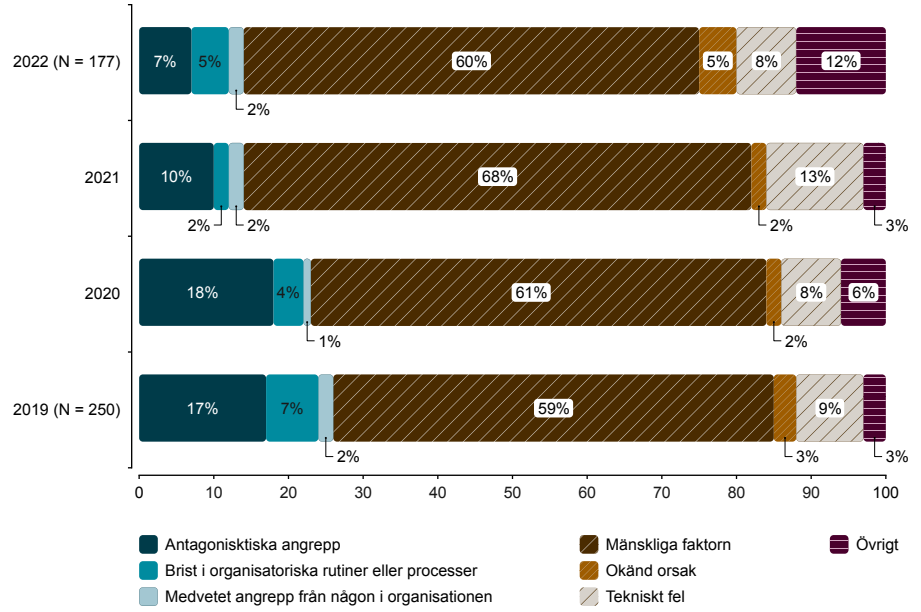
Andel anmälningar om personuppgiftsincidenter indelat efter typ av incident under 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika typer av incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet ideell organisation eller ekonomisk förening 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Diagram 15

Andel anmälningar om personuppgiftsincidenter fördelat på orsak för incident 2019–2022

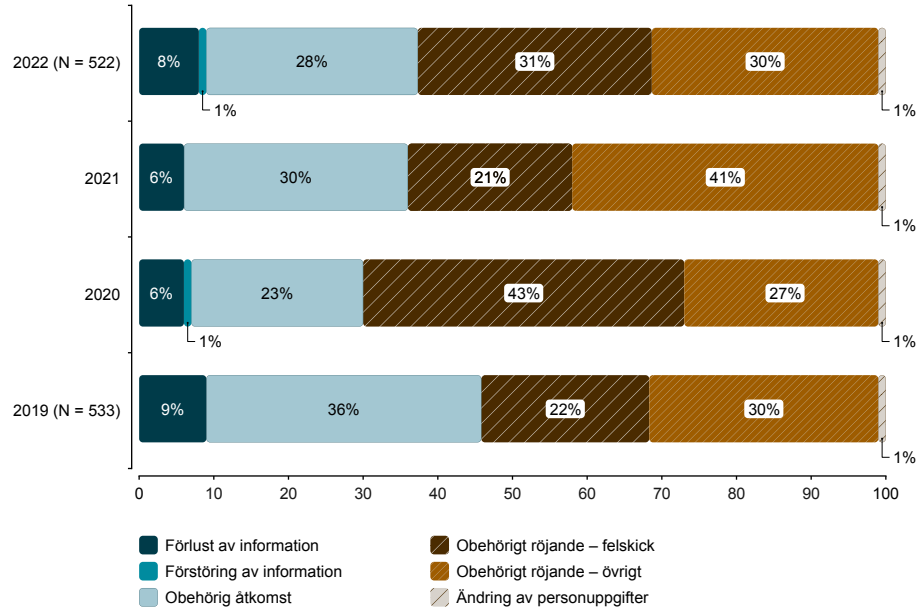


Liggande fraktionsstapeldiagram som jämför hur mycket olika orsaker bakom incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet ideell organisation eller ekonomisk förening 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Kommun

Diagram 16

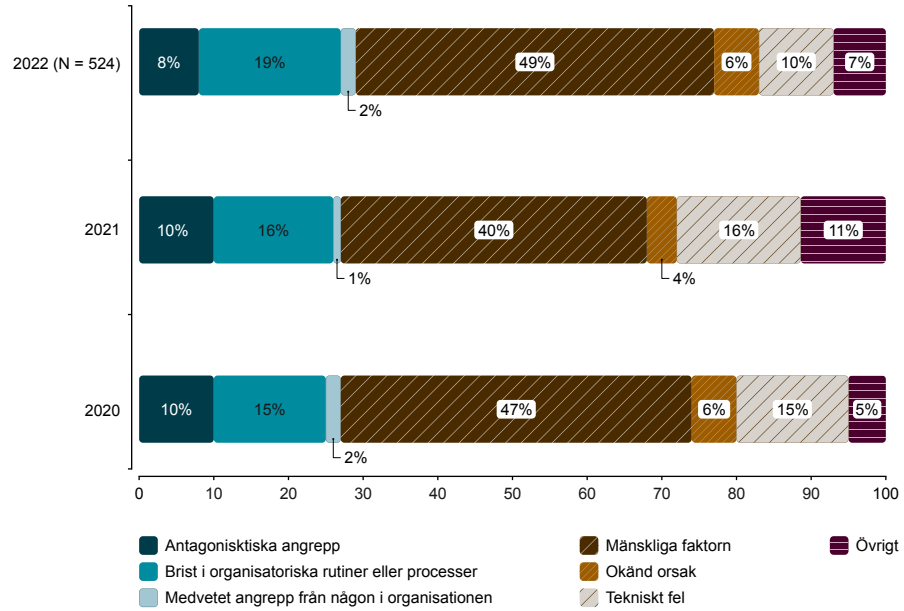
Andel anmälningar om personuppgiftsincidenter indelat efter typ av incident under 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika typer av incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet kommun 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Diagram 17

Andel anmälningar om personuppgiftsincidenter fördelat på orsak för incident 2019–2022

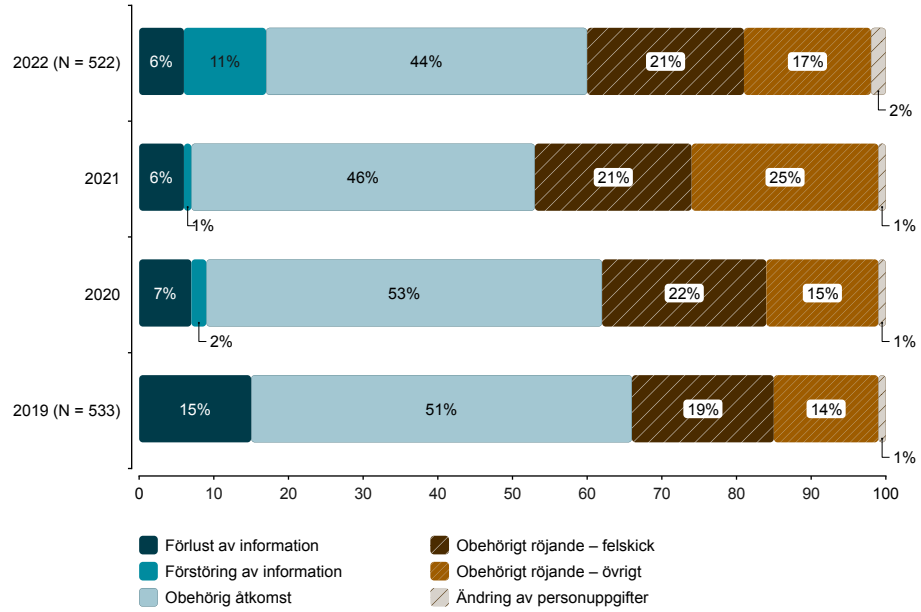


Liggande fraktionsstapeldiagram som jämför hur mycket olika orsaker bakom incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet kommun 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren. Information för 2019 har inte sammanställts i tidigare rapporter och saknas därför i detta diagram.

Näringsliv

Diagram 18

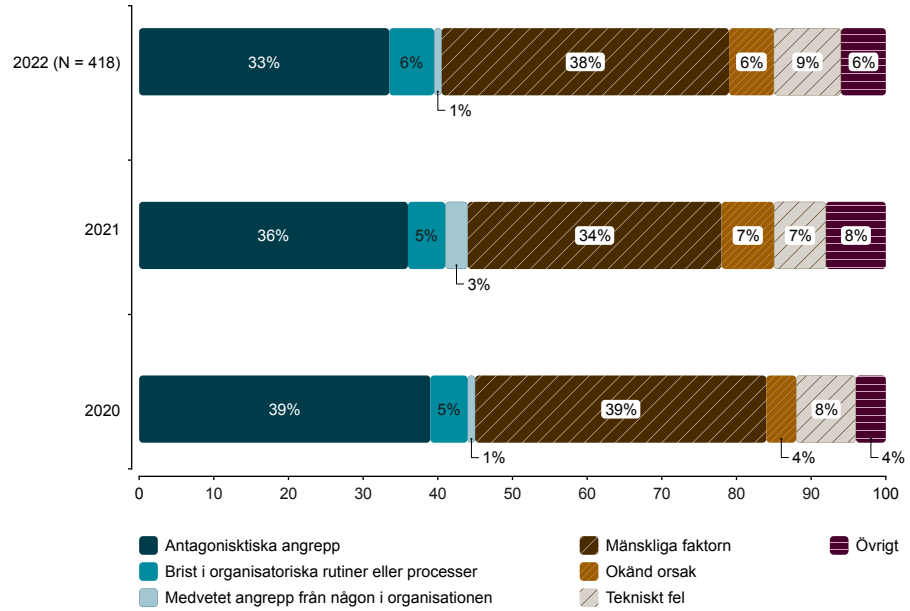
Andel anmälningar om personuppgiftsincidenter indelat efter typ av incident under 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika typer av incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet näringsliv 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Diagram 19

Andel anmälningar om personuppgiftsincidenter fördelat på orsak för incident 2020–2022

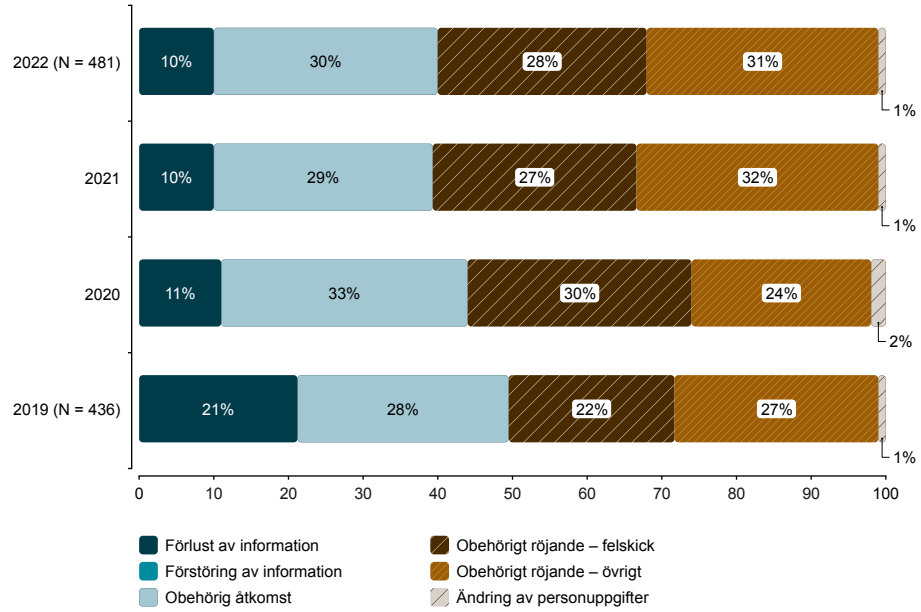


Liggande fraktionsstapeldiagram som jämför hur mycket olika orsaker bakom incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet näringsliv 2020–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren. Information för 2019 har inte sammanställts i tidigare rapporter och saknas därför i detta diagram.

Skola och utbildning

Diagram 20

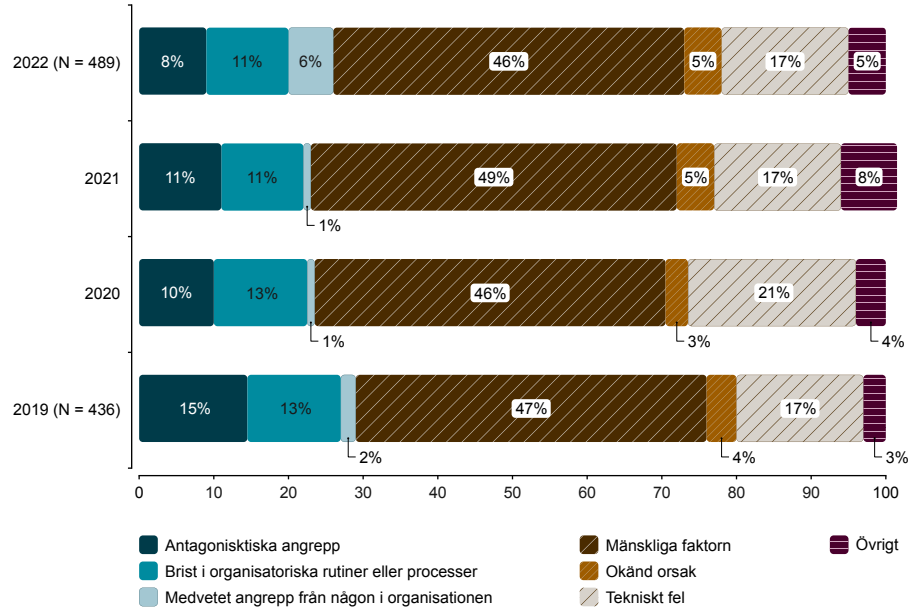
Andel anmälningar om personuppgiftsincidenter indelat efter typ av incident under 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika typer av incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet skola och utbildning 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Diagram 21

Andel anmälningar om personuppgiftsincidenter fördelat på orsak för incident 2019–2022

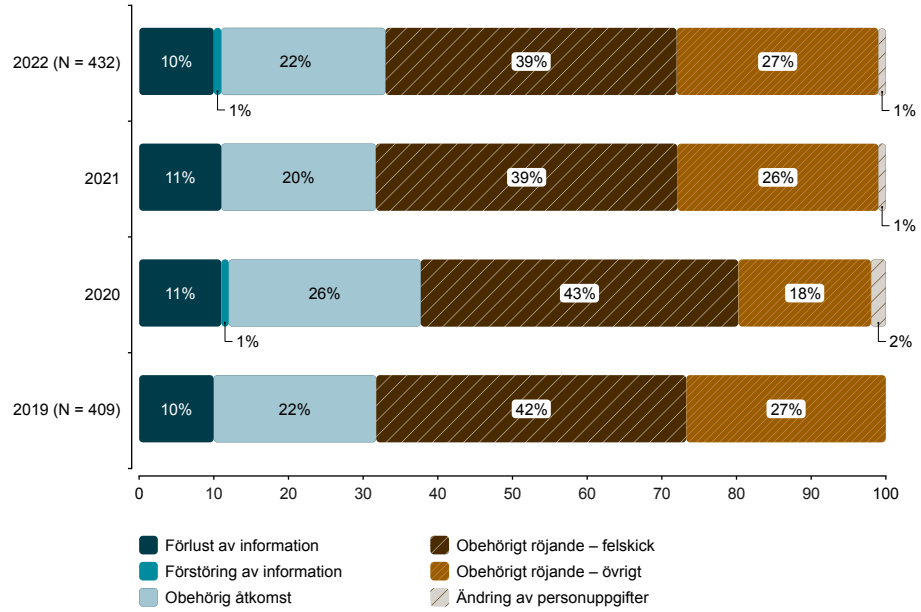


Liggande fraktionsstapeldiagram som jämför hur mycket olika orsaker bakom incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet skola och utbildning 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Socialtjänst

Diagram 22

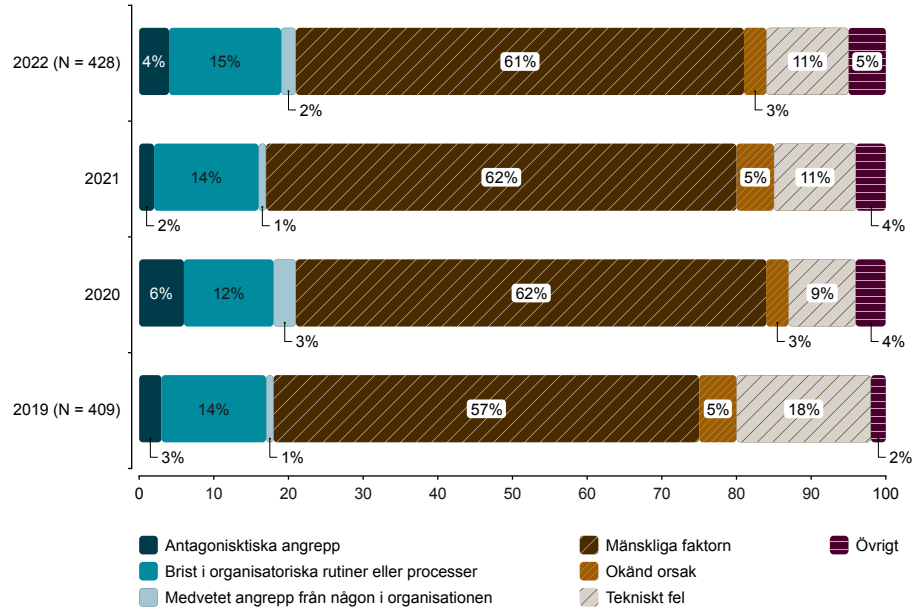
Andel anmälningar om personuppgiftsincidenter indelat efter typ av incident under 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika typer av incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet skola och utbildning 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Diagram 23

Andel anmälningar om personuppgiftsincidenter fördelat på orsak för incident 2019–2022

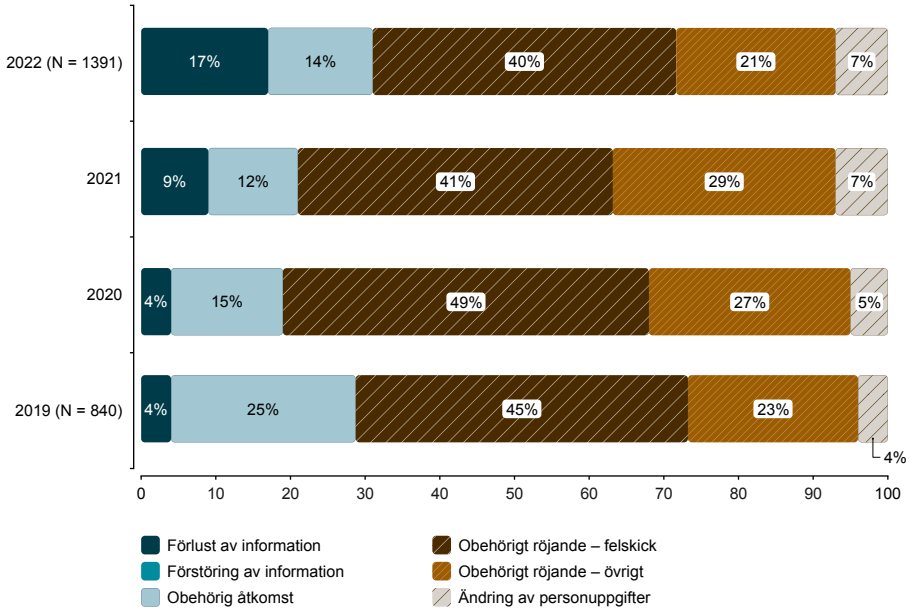


Liggande fraktionsstapeldiagram som jämför hur mycket olika orsaker bakom incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet skola och utbildning 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Statlig myndighet

Diagram 24

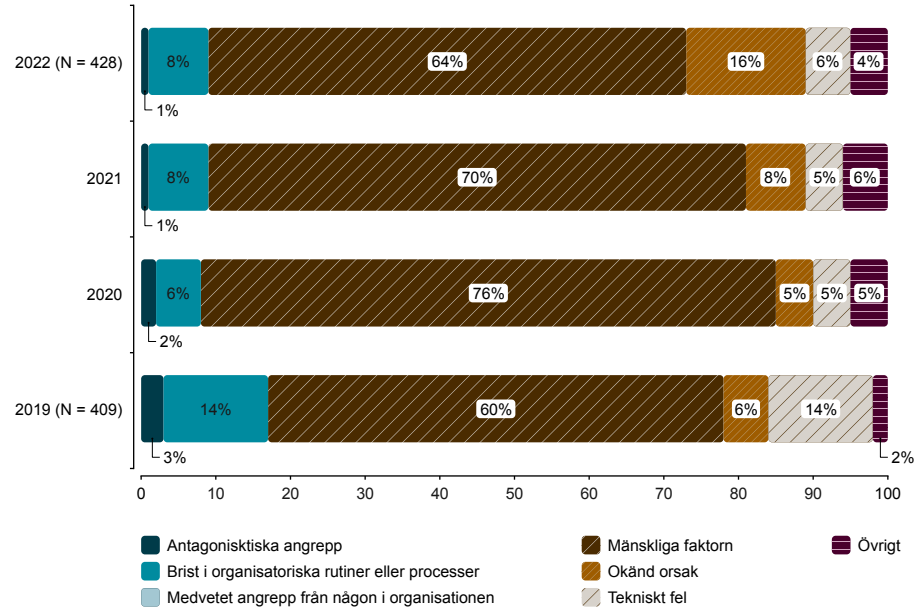
Andel anmälningar om personuppgiftsincidenter indelat efter typ av incident under 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika typer av incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet statlig myndighet år 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Diagram 25

Andel anmälningar om personuppgiftsincidenter fördelat på orsak för incident 2019–2022



Liggande fraktionsstapeldiagram som jämför hur mycket olika orsaker bakom incidenter bidrar andelsmässigt till samtliga inrapporterade personuppgiftsincidenter inom verksamhetsområdet statlig myndighet 2019–2022. Notera att det totala antalet inrapporterade personuppgiftsincidenter har varierat mellan åren.

Bilaga 3.

Fördjupning av IMY:s rekommendationer

Vad kan verksamheten göra för att minska risken för att personuppgifter oavsiktligt sprids?

Ett systematiskt informationssäkerhetsarbete är centralt

Den mänskliga faktorn anges såväl i år som tidigare år vara den vanligaste orsaken till personuppgiftsincidenterna.

Att den mänskliga faktorn anges som orsak kan innebära att det är frågan om en enstaka personuppgiftsincident som sker på grund av ett mänskligt misstag, men det kan också vara strukturella problem i verksamheten där incidenterna riskerar att upprepa sig. Incidenterna som orsakas av den mänskliga faktorn kan vara av mindre allvarlig karaktär, men incidenter kan också vara mycket allvarliga och innebära hög risk för enskildas fri- och rättigheter.

Att den mänskliga faktorn anges frekvent som orsak till personuppgiftsincidenter och att den kan leda till allvarliga incidenter innebär att det är en viktig faktor att beakta i er verksamhets systematiska informationssäkerhetsarbete.

Oavsett orsak till personuppgiftsincidenten måste säkerhetsnivån sättas i relation till riskerna för de enskildas friheter och rättigheter och hur sannolika och allvarliga dessa risker är. Det framgår av artikel 32.1 i dataskyddsförordningen om säkerhet i samband med behandling. Personuppgiftsansvariga och personuppgiftsbiträden ska i detta arbete beakta behandlingens art, omfattning, sammanhang och ändamål. Förenklat kan sägas att art handlar om vad det är för typ av behandling och vilken typ av uppgifter som behandlas, exempelvis känsliga personuppgifter. Omfattning handlar om antal registrerade, hur många uppgifter det är rörande varje registrerad, hur många som har åtkomst till uppgifterna och så vidare. Sammanhang är här den kontext personuppgifterna behandlas i och vilken grad av konfidentialitet och förtrolighet som den registrerade rimligen kan förvänta sig och ändamål är syftet med behandlingen av personuppgifterna. Utifrån dessa faktorer och tillsammans med den senaste utvecklingen och genomförandekostnaderna ska verksamheten vidta lämpliga organisatoriska och tekniska åtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till risken för de registrerade fysiska personernas rättigheter och friheter.

Det innebär att er verksamhet inte rakt av kan kopiera säkerhetsåtgärder som andra använder, utan varje verksamhet måste bedöma vilken nivå som krävs i den egna verksamheten. Det är inte heller möjligt att införa säkerhetsåtgärder och sedan slå sig till ro. Verksamheten förändras, tekniken förändras, riskerna förändras och därför krävs det att säkerhetsarbetet pågår kontinuerligt.

Det ska vara lätt att göra rätt och svårt att göra fel

Behandlar ni personuppgifter i er verksamhet behöver ni arbeta systematiskt med ert informationssäkerhetsarbete, då det är en viktig del av dataskyddet.

Ett systematiskt informationssäkerhetsarbete innebär att kontinuerligt planera, genomföra, utvärdera och förbättra sitt informationssäkerhetsarbete. Er verksamhet bör redan från början, det vill säga när en personuppgiftbehandling planeras, ha med såväl dataskydd som informationssäkerhet i sin helhet i utvecklingsprocessen.

Dessa delar bör därför vara naturliga delar i verksamhetens projektmodell och förändringsprocess. Inbyggt dataskydd innebär att er verksamhet tar hänsyn till integritetsskyddsreglerna redan när it-system och processer utformas. Lämpliga säkerhetsåtgärder ska skydda de registrerades rättigheter och säkerställa att skyddet av deras personuppgifter byggs in i behandlingen. Vilka åtgärder som är lämpliga beror på sammanhanget och de risker som finns med den aktuella behandlingen. Hänsyn behöver tas till behandlingens art, omfattning, sammanhang och ändamål.

Verksamheten ska sedan fortsätta detta arbete med att skapa, implementera, kontrollera och följa upp de organisatoriska och tekniska åtgärder som krävs för att få ett lämpligt skydd för behandlingen av informationen och personuppgifterna – i förhållande till de risker den medför.

Er verksamhet kan minska risken att medarbetare begår misstag genom att exempelvis göra det omöjligt för enskilda medarbetare att installera program och appar som inte godkänts av verksamheten eller spara information på löstagbara lagringsmedia. Lösningar som gör det enkelt för medarbetarna att lösenordsskydda och kryptera e-post och bifogade filer är också en åtgärd som kan vara viktig för att höja säkerheten. En annan åtgärd kan vara att ha begränsningar för bilagor till mejl.

En annan viktig och grundläggande säkerhetsåtgärd är att ha en aktiv behörighetsstyrning. Behörigheterna ska vid varje tid vara anpassade så att varje medarbetare bara får tillgång till de personuppgifter som medarbetaren behöver för att kunna utföra sina arbetsuppgifter.

De organisatoriska och tekniska säkerhetsåtgärderna behöver vara integrerade i verksamhetens arbetssätt och skapa förutsättningar för att det ska vara lätt att göra rätt och svårt att göra fel.

Processer som stärker det systematiska informationssäkerhetsarbetet

Alla verksamheter som hanterar personuppgifter behöver ha en dokumenterad och implementerad personuppgiftsincidenthanteringsprocess för att kunna förebygga, upptäcka och hantera personuppgiftsincidenter.

Personuppgiftsincidenthanteringsprocessen bör även innehålla aktiviteter för att informera och kommunicera både internt och externt till berörda, registrerade och till IMY.

En personuppgiftsincidenthanteringsprocess ska också ge verksamheten verktyg och rutiner för att snabbt begränsa de konsekvenser som påverkar de enskildas rättigheter och friheter. Processen bör också bidra till ett kontinuerligt lärande för att säkerställa att liknande personuppgiftsincidenter inte inträffar igen.

Den dokumentation som enligt artikel 33.5 i dataskyddsförordningen ska tas fram bidrar till att verksamheten i det uppföljande arbetet kan upptäcka och analysera vad som kan vara anledningen till att den mänskliga faktorn orsakar personuppgiftsincidenter. På så sätt kan verksamheten fånga upp och identifiera utvecklingsbehov av nya organisatoriska och tekniska säkerhetsåtgärder, eller uppdatera redan befintliga.

I er verksamhets riskhanteringsprocess ska de förbyggande, förhindrande och upptäckande åtgärderna identifieras. Vidare ska risker för fysiska personers rättigheter och friheter identifieras och åtgärdsplaner tas fram. Åtgärdsplanerna ska sedan genomföras och följas upp. Är det ofta den mänskliga faktorn som orsakar personuppgiftsincidenter är det viktigt att även de riskerna identifieras och att åtgärder för att motverka mänskliga misstag planeras.

Säkerhetskultur

Säkerhetskultur är de gemensamma värderingar, kunskaper, attityder och uppfattningar som både chefer och anställda inom en verksamhet har om förhållandet till skyddet för personuppgifter.

Verksamheten bör arbeta med att ha en god säkerhetskultur. Genom en god säkerhetskultur ökar medvetenheten om säkerhetsfrågor och behov i hela organisationen.

För att få en god säkerhetskultur krävs att ledningen är engagerad i verksamhetens säkerhetsfrågor, vilket även inkluderar skyddet för personuppgifter.

En god säkerhetskultur innebär också att varje medarbetare vet vad de ska göra i olika situationer och att säkerhetsfrågor kontinuerligt finns med på agendan vid olika typer av möten. I en god säkerhetskultur kommuniceras även dragna lärdomar av tidigare inträffade incidenter, och hur dessa lärdomar sedan ska realiseras för att skapa en ännu bättre säkerhetskultur och därmed bidra till det systematiska säkerhetsarbetet.

Verksamheten ska uppmuntras till att rapportera brister och säga ifrån när de upptäcker fel eller brister som kan riskera säkerheten. Det handlar om att upptäcka brister och sårbarheter för att se om de organisatoriska och tekniska

åtgärderna är tillräckliga eller om de behöver uppdateras, men också för att verksamheten ska vara medveten om vilka risker som finns.

Skapa en aktiv medvetenhet och en förmåga hos medarbetarna att skydda informationen och personuppgifterna genom att kontinuerligt utbilda och följa upp att utbildningen fungerar som tänkt.

IMY. Integritetsskydds myndigheten

Detta 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