IMY. Integritetsskydds myndigheten

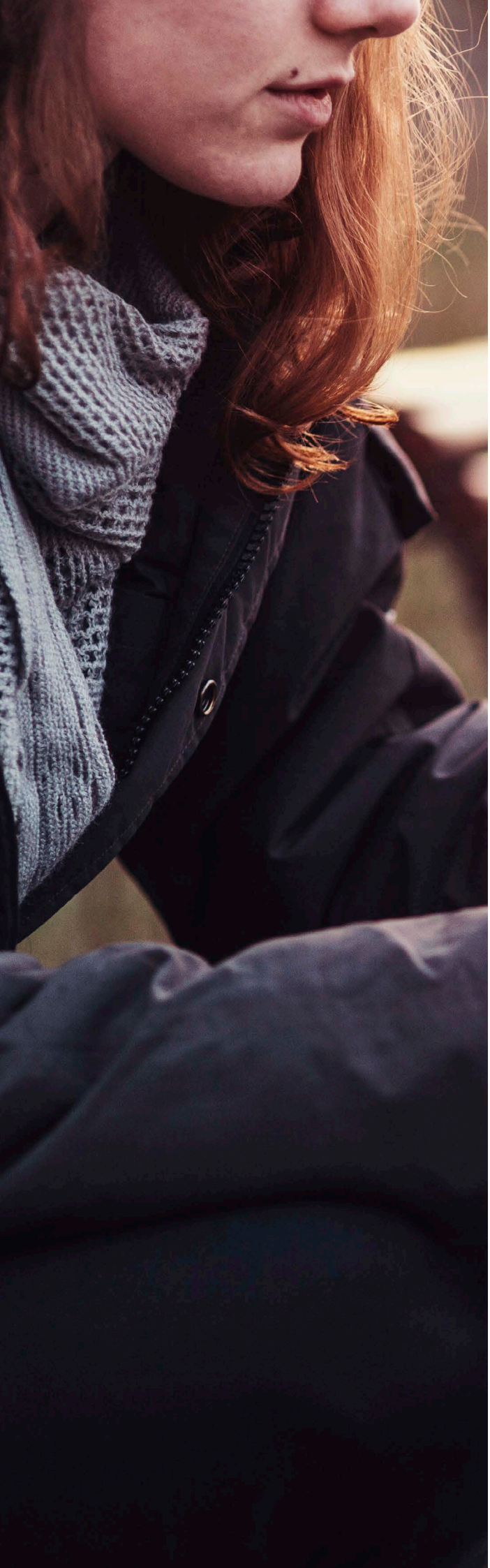
Anmälda personuppgiftsincidenter 2020

IMY rapport 2021:3

Innehållsförteckning

Del 1. Personuppgiftsincidenter 2020

Del 2. Anmälda personuppgiftsincidenter inom olika verksamhetsområden



Inledning

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

Denna rapport beskriver anmälda personuppgiftsincidenter under 2020. Statistiken över inflödet är uppdelad i två delar. Den första delen beskriver hur anmälda incidenter fördelar sig mellan olika verksamhetsområden, vad det är för typ av incidenter och vad den organisation som anmält uppger är skälet till att incidenten inträffat. Här beskrivs också förändringar mellan 2019 och 2020. Rapportens andra del redovisar statistik över anmälda personuppgiftsincidenter uppdelat på olika verksamhetsområden.

Rapporten är en del av IMY:s rapportserie där vi beskriver och analyserar inflödet till myndigheten.[2] Syftet är att bidra till en generell kunskapshöjning om integritet och dataskydd. Generella mönster och iakttagelser från inflödet till IMY beskrivs, som privata och offentliga verksamheter kan använda i sitt fortsatta dataskyddsarbete.

1. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
2. Tidigare rapporter i rapportserien behandlar bl.a. anmälda personuppgiftsincidenter 2018 (2019:1), anmälda personuppgiftsincidenter 2019 (2020:2), personuppgiftsincidenter som beror på antagonistiska angrepp 2019 (2020:3) och klagomål mot personsöktjänster med frivilligt utgivningsbevis (2020:1).

Metod

Anmälningar om personuppgiftsincidenter inkom och hanterades inledningsvis manuellt, men inkommer sedan mars 2020 till IMY huvudsakligen via e-tjänsten för anmälningar om personuppgiftsincidenter på IMY:s webbplats. IMY:s diariesystem läser automatiskt av kryssrutorna för inom vilket verksamhetsområde som incidenten inträffat, vilken typ av incident anmälan rör samt orsaken till incidenten. Systemet ställer sedan upp nyckelord för dessa kategorier utifrån vilka vi sedan kan ta fram statistik.

Totalt inkom 4 588 anmälningar om personuppgiftsincidenter till IMY 2020. Statistiken är framtagen på en bas av 4 471 anmälningar. Anledningen till att inte alla anmälningar om personuppgiftincidenter tagits med som grund för statistiken är att vissa anmälningar inkommit till myndigheten per post eller mejl istället för via myndighetens e-tjänst. Dessa anmälningar registreras manuellt och systemet har inte möjlighet att läsa av dem, varför inga nyckelord, och därmed heller ingen statistik, finns för dessa anmälningar. Detta är första året som IMY tar fram statistik efter att ärendegruppen digitaliserats. Tidigare har alla uppgifter statistikförts manuellt.

I tabell 1 (se sid. 12) redogörs för skillnaden i antalet anmälningar i genomsnitt per månad mellan 2019 och 2020 inom de olika verksamhetsområdena. Siffrorna för 2020 är en skattning och är beräknande utifrån hur många procent verksamhetsområdet står för sett till det totala inflödet. Utifrån procentsatsen har vi räknat ut totalt antal anmälningar under 2020 från verksamhetsområdet i fråga. Denna siffra har därefter dividerats med tolv.

De verksamhetsområden som redovisas utgår från de kategorier av verksamhetsområden som återfinns i blanketten för anmälan av personuppgiftsincident enligt dataskyddsförordningen. Kategorierna i rapporten skiljer sig dock i vissa fall från blankettens kategorier. Nedan listas de kategorier av verksamhetsområden som redovisas i rapporten.

- Hälso- och sjukvård
- Kommun
- Socialtjänst
- Skola och utbildning
- Finansiell sektor eller försäkring
- Näringslivet i övrigt
- Ideell organisation eller ekonomisk förening
- Statliga myndigheter och domstolar
- Övriga verksamhetsområden

Verksamhetsområdet *Skola och Utbildning* innefattar blankettens kategorier Skola: förskola, grundskola, gymnasium, Universitet eller högskola samt Annan eftergymnasial utbildning. Universitet eller högskola och Annan eftergymnasial utbildning har tidigare redovisats i främst verksamhetsområdena Statlig myndighet, Kommun och Näringslivet i övrigt beroende på huvudman. Blankettens kategori Forskning redovisas i rapporten utifrån huvudman. Verksamhetsområdet *Näringslivet i övrigt* innefattar även blankettens kategorier kreditupplysning och inkasso. Inom verksamhetsområdet *Statliga myndigheter och domstolar* redovisas blankettkategorierna statliga myndigheter, polis och rättsväsendet i övrigt. Även domstolarna redovisas inom denna kategori. Dessa verksamhetsområden har i tidigare rapporter redovisats i verksamhetsområdet statliga myndigheter.

I anmälningsblanketterna finns numera endast en kategori för förlust av personuppgifter. Tidigare har förlust varit uppdelat i kategorierna Förlust – övrigt och Förlust – stöld i både anmälningsblanketten och rapporterna. I årets rapport redovisas därför förlust av personuppgifter som orsak till incidenten som en kategori.

Sammanfattning

Antalet anmälda personuppgiftsincidenter var något lägre 2020 jämfört med 2019. Under 2020 anmäldes knappt 4 600 personuppgiftsincidenter till IMY, varav knappt 50 rörde brottsdatalagen. Under 2019 fick IMY totalt in knappt 4 800 anmälningar om personuppgiftsincidenter varav knapp 60 rörde brottsdatalagen. I genomsnitt under året anmäldes 87 incidenter per vecka, vilket är något lägre än de 90 incidenter som i genomsnitt anmäldes per vecka under 2019.

Offentlig sektor står för den största andelen av anmälda incidenter 2020, i synnerhet statliga myndigheter och domstolar samt hälso och sjukvården. Anmälningar från hälso- och sjukvården står för den största ökningen av antalet anmälda personuppgiftsincidenter under 2020.

Inom privat sektor har antalet anmälda incidenter 2020 minskat jämfört med 2019. Detta syns främst inom näringslivet, där antalet anmälda incidenter minskat med ett tjugotal anmälningar per månad. En möjlig förklaring till minskningen kan vara att Coronapandemin har tvingat verksamheter till snabba omställningar och omprioriteringar som påverkat hanteringen av personuppgiftsincidenter.

Den vanligaste incidenten 2020 är liksom föregående år felskickade mejl eller brev, som utgör 40 procent av incidenterna. Den vanligaste orsaken till de anmälda incidenterna är fortsatt den mänskliga faktorn, som uppges ha orsakat mer än hälften av de anmälda incidenterna 2020.

IMY:s bedömning är att det i Sverige fortfarande finns ett stort mörkertal i form av anmälningspliktiga incidenter som inte anmäls. Bedömningen baseras bland annat på utvecklingen i andra EU länder där anmälningsskyldigheten för personuppgiftsincidenter funnits längre.

Under 2020 har tre tillsynsärenden inletts baserat på anmälda personuppgiftsincidenter, vilket är något färre än föregående år. Totalt har myndigheten inlett tillsyn i åtta ärenden baserat på personuppgiftsincidenter, eller som rör verksamheters hantering av personuppgiftsincidenter.

Sedan mars 2020 är det möjligt att skicka in anmälningar om personuppgiftsincidenter digitalt i och med lanseringen av myndighetens e tjänst för anmälningar av personuppgiftsincidenter.

I början av 2021 fattade IMY beslut om en ny tillsynspolicy och tillsynsplan där ett övergripande fokus är att utreda klagomål från enskilda. Detta har medfört en ny klagomålshantering för myndigheten som innebär en fördjupad bedömning av samtliga klagomål. Den nya hanteringen medför att anmälda personuppgiftsincidenter kan påverka IMY:s bedömning i klagomålsärenden. Det kan till exempel handla om att IMY tar emot ett klagomål från en enskild som drabbats av en personuppgiftsincident. IMY kan då använda den anmälda personuppgiftsincidenten som underlag för att avgöra vilken åtgärd som är lämplig att vidta med anledning av klagomålsärendet.

Rekommendationer

Utifrån de personuppgiftsincidenter som hittills anmälts går det att ge generella rekommendationer som kan bidra till att förebygga incidenter och mildra konsekvenserna om en incident ändå inträffar. Flera av dessa rekommendationer har funnits med i IMY:s tidigare rapporter om anmälda personuppgiftsincidenter, men är fortfarande relevanta.

Rutiner för att upptäcka och anmäla incidenter kan ytterligare förbättras

Alla organisationer som hanterar personuppgifter behöver ha rutiner för att upptäcka, dokumentera, anmäla och hantera personuppgiftsincidenter. Det förhållandet att den mänskliga faktorn fortfarande uppges vara den vanligaste orsaken till en incident pekar på vikten av att ha fungerande rutiner på plats. I IMY:s nationella integritetsrapport 2019 uppgav knappt 80 procent av de intervjuade dataskyddsombuden att deras organisation har tagit fram rutiner för att anmäla personuppgiftsincidenter. Bland företag utan dataskyddsombud uppgav bara drygt 40 procent att de hade sådana rutiner. Bland företag utan dataskyddsombud fanns därmed stor förbättringspotential.[3] Även om situationen kan ha ändrats sedan undersökningen gjordes finns sannolikt ytterligare förbättringspotential för dessa verksamheter.

Löpande intern utbildning

Den stora andelen incidenter som anmäls och uppges bero på den mänskliga faktorn understryker betydelsen av att styrdokument och tekniska informationssäkerhetsåtgärder kompletteras med löpande utbildning och andra åtgärder för att öka kunskap och medvetenhet hos medarbetarna.

I IMY:s nationella integritetsrapport 2019 uppgav knappt hälften av dataskyddsombuden att dataskydd och informationssäkerhet ingår i introduktionsutbildningen till nya medarbetare i deras organisation. Endast 36 procent av dataskyddsombuden uppgav att medarbetarna i deras organisation får löpande utbildning i dataskydd och informationssäkerhet.

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

- Rutiner för hantering av personuppgifter i mejl. Till exempel att alltid kontrollera att korrekt mottagare är angiven innan ett brev eller mejl skickas ut, att använda funktionen dold kopia vid utskick som ska till flera mottagare. Känsliga eller integritetskänsliga personuppgifter ska helst inte skickas med mejl, om detta inte går att undvika ska man använda mejl som är skyddad med kryptering så att endast den avsedda mottagaren kan ta del av uppgifterna.
- att om personuppgifter lagras på flyttbara media som är särskilt sårbara för stöld eller förlust – till exempel usb-minnen, bärbara datorer och mobiltelefoner – bör informationen krypteras så att ingen obehörig kan ta del av den.
- att det för att förebygga antagonistiska angrepp är angeläget att inte öppna länkar eller bifogade filer från okända avsändare.

God behörighetsstyrning kan förebygga incidenter

Obehörig åtkomst och obehörigt röjande utgör de näst vanligaste orsakerna till anmälda personuppgiftsincidenter. En central del i arbetet med informationssäkerhet och dataskydd handlar om behörighetsstyrning. Enligt dataskyddsförordningen är den personuppgiftsansvariga verksamheten skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.[4] Alla organisationer som hanterar personuppgifter behöver ha stabila rutiner för att säkerställa att behörigheter tilldelas korrekt, att behörigheterna löpande kontrolleras och följs upp samt att åtkomstkontroller genomförs.

Incidenter kan ge viktiga signaler om utvecklingsbehov

En generell rekommendation är att de flesta organisationer kan vinna på att aktivt använda de personuppgiftsincidenter som upptäcks som ett underlag för att identifiera brister och utvecklingsbehov i det löpande och systematiska arbetet med dataskydd och informationssäkerhet.

3. IMY:s Nationella Integritetsrapport 2019 https://www.IMY.se/globalassets/dokument/rapporter/nationell-integritetsrapport-2019.pdf

4. Följer av artikel 32.1 i dataskyddsförordningen

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

Anmälningsplikt för vissa personuppgiftsincidenter

I dataskyddsförordningen finns en skyldighet för organisationer att anmäla vissa typer av personuppgiftsincidenter till IMY. En personuppgiftsincident är en säkerhetsincident som omfattar personuppgifter. Incidenten kan till exempel handla om att personuppgifter har blivit förstörda eller ändrade, gått förlorade eller kommit i orätta händer genom obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.[5] 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 personuppgiftsansvarige, så snart denne får vetskap om incidenten, bedöma vilken risk som incidenten kan medföra.[6] Riskbedömningen är en viktig del i hanteringen av personuppgiftsincidenten och underlättar för den personuppgiftsansvarige att ta ställning till lämpliga åtgärder för att effektivt begränsa och åtgärda incidenten. Den är också avgörande för att avgöra om incidenten ska anmälas till IMY samt om de registrerade ska informeras.[7]

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

Vid riskbedömningen bör den personuppgiftsansvariga ta hänsyn till de specifika omständigheterna i samband med incidenten. Några faktorer att tänka på vid riskbedömningen är bland annat typen av incident, personuppgifternas natur, känslighet och volym, hur lätt det är att identifiera enskilda personer samt konsekvensernas svårighetsgrad för enskilda individer.[9]

Om det är osannolikt att incidenten leder till en risk för de registrerades fri- och rättigheter behöver incidenten inte anmälas till IMY. Det kan till exempel vara när personuppgifter redan finns allmänt tillgängliga och utlämnandet av sådana uppgifter inte utgör en sannolik risk för den enskilde.[10] Oavsett om incidenten ska anmälas till IMY eller inte så är den personuppgiftsansvarige alltid skyldig att dokumentera incidenten internt.[11]

Information till de registrerade

Om det finns en hög risk att privatpersoners fri- och rättigheter kan påverkas till följd av en personuppgiftsincident är den ansvariga verksamheten skyldig att – förutom att anmäla det inträffade till IMY – också informera de registrerade om att incidenten inträffat.[12] I dataskyddsförordningen anges att den personuppgiftsansvarige ska informera de registrerade utan onödigt dröjsmål. Syftet med informationen är bl.a. att ge den enskilde möjlighet att vidta egna åtgärder för att skydda sig själv mot negativa konsekvenser av incidenten, till exempel genom att byta lösenord eller spärra bankkort.[13]

Den personuppgiftsansvarige ska åtminstone lämna följande information till de registrerade.[14]

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

5. 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.
6. Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 2018.
7. Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 2018.
8. Artikel 33 dataskyddsförordningen.
9. Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 2018.
10. Artikel 29-arbetsgruppen för uppgiftsskydd, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 2018.
11. Artikel 33.5 dataskyddsförordningen.
12. Artikel 34 dataskyddsförordningen.
13. Skäl 86 dataskyddsförordningen, Artikel 29-arbetsgruppen för uppgiftsskydd, *Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679*, 2018.
14. Artikel 34 dataskyddsförordningen.

IMY:s arbete med personuppgiftsincidenter

IMY övervakar dagligen inflödet av anmälda incidenter som inkommer till myndigheten. Anmälningarna gör det möjligt att bland annat bevaka de åtgärder som vidtas av de personuppgiftsansvariga för att motverka negativa effekter av incidenter, vilka typer av personuppgiftsincidenter som är vanligt förekommande samt observera vilka som anmäler och inte anmäler personuppgiftsincidenter. Informationen i de anmälda personuppgiftsincidenterna är ett viktigt underlag när vi i vår tillsynsplan identifierar riskområden som tillsyn bör inriktas mot samt identifierar behov av utbildningsinsatser inom olika kunskap- och verksamhetsområden.

IMY kan välja att inleda en tillsyn med anledning av en anmäld personuppgiftsincident. En tillsyn kan övervägas med anledning av exempelvis hanteringen av själva incidenten och anmälan, generella brister som incidenten indikerar, att incidenten bedöms som särskilt allvarlig eller tyder på mer systematiska brister. Att en anmälan om personuppgiftsincident inte föranleder någon åtgärd är inte detsamma som att IMY anser att allt har gått rätt till. Myndighetens tillsynsarbete utgår från vår tillsynspolicy och vår tillsynsplan och vi försöker planera våra tillsynsinsatser så att vi kan åstadkomma största möjliga nytta. Myndigheten har dock alltid möjlighet att inleda tillsyn mot en personuppgiftsansvarig. Uppgifter i media, klagomål eller personuppgiftsincidenter kan exempelvis föranleda att myndigheten inleder en tillsyn.

Oavsett om en anmälan leder till en tillsyn eller inte får den personuppgiftsansvarige alltid ett beslut från myndigheten med besked om att ärendet avslutas. I det fall tillsyn har inletts med anledning av den anmälda personuppgiftsincidenten finns även en hänvisning till tillsynsärendet med i beslutet. Ett tillsynsärende kan även inledas mot bakgrund av informationen i en anmäld incident efter att IMY beslutat att avsluta incidentärendet. Tillsyn är ett separat förförande i förhållande till den anmälda incidenten och bedrivs i ett eget ärende.

I början av 2021 fattade IMY beslut om en ny tillsynspolicy och tillsynsplan där ett övergripande fokus är att utreda klagomål från enskilda. Detta har medfört en ny klagomålshantering för myndigheten som innebär en fördjupad bedömning av samtliga klagomål. Den nya hanteringen medför att anmälda personuppgiftsincidenter kan påverka IMY:s bedömning i klagomålsärenden. Det kan till exempel handla om att IMY tar emot ett klagomål från en enskild som drabbats av en personuppgiftsincident. IMY kan då använda den anmälda personuppgiftsincidenten som underlag för att avgöra vilken åtgärd som är lämplig att vidta med anledning av klagomålsärendet. Om informationen i anmälan inte visar att personuppgiftsansvarige har vidtagit tillräckliga åtgärder för att avhjälpa riskerna eller den personuppgiftsansvarige inte har anmält personuppgiftsincidenten och den bedöms vara anmälningspliktig kan IMY komma att skicka ett informationsbrev eller inleda tillsyn med anledning av klagomålet.

Tillsynsärenden som rör personuppgiftsincidenter

Nedan listas sammanfattningar av pågående och avslutade tillsynsärenden som rör personuppgiftsincidenter. Under 2020 har tre tillsynsärenden inletts baserat på anmälda personuppgiftsincidenter, vilket är något färre än föregående år. Totalt har myndigheten inlett tillsyn i åtta ärenden baserat på personuppgiftsincidenter, eller som rör verksamheters hantering av personuppgiftsincidenter.

Mer om IMY:s tillsynsärenden finns att del av på IMY:s hemsida: https://www.imy.se/tillsyner/.

Pågående tillsynsärenden

Region Uppsala

IMY utreder bakgrunden till att regionen har skickat patientuppgifter med mejl utan kryptering efter att regionen anmält en personuppgiftsincident med anledning av hanteringen. Tillsynen inleddes i september 2019.

Tullverket

IMY granskar hur Tullverket använder mobiltelefoner i sin brottsbekämpande verksamhet samt omständigheterna kring den personuppgiftsincident som anmälts till IMY där personal på Tullverket har en använt en app i sina mobiltelefoner som för över personuppgifter till en molntjänst. Tillsynen inleddes i juni 2020.

Polismyndigheten

IMY granskar myndighetens rutiner för utskick av mejl med anledning av anmälda personuppgiftsincidenter som rör mejl som oavsiktligt hamnat hos fel mottagare. Tillsynen inleddes i april 2020.

Avslutade tillsynsärenden

Voice Integrate AB och Medhelp AB

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

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

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

För mer information om IMY:s granskning av incidenten kring 1177 se IMY:s rapport Integritetsskyddsmyndighetens kontroll av behandling av uppgifter om vårdsökande i samband med samtal till 1177 – en rapport.

Polismyndigheten

IMY har granskat Polismyndighetens personuppgiftsbehandling i belastningsregistret. Tillsynen inleddes mot bakgrund av att polisen anmält en personuppgiftsincident i vilken det framgår att polisen under en period hade skickat ett antal utdrag ur belastningsregistret till enskilda personer som innehållit för få eller för många uppgifter.

I tillsynsbeslutet konstaterar IMY att Polismyndigheten har åtgärdat det tekniska fel som orsakat incidenten. Ärendet avslutades utan ytterligare åtgärder i juni 2020.

Utbildningsnämnden i Stockholm Stad

Genom anmälningar om personuppgiftsincidenter från Utbildningsnämnden i Stockholms stad uppmärksammades IMY på att det funnits obehörig åtkomst till elevuppgifter i Stockholms stads skolplattform. Mot bakgrund av anmälningarna inledde IMY en tillsyn mot Utbildningsnämnden och deras behörighetsstyrning av vissa delar i Skolplattformen. Granskningen avsåg kraven på lämpliga tekniska och organisatoriska åtgärder enligt artikel 5.1 f och 32i dataskyddsförordningen och avsåg behörighetstilldelningen i respektive delsystem som omfattades av granskningen.

I tillsynsbeslutet konstaterar IMY att Utbildningsnämnden inte vidtagit tillräckliga lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, vilket bland annat inbegriper ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska säkerhetsåtgärderna. Myndigheten utfärdade en sanktionsavgift på fyra miljoner kronor för de överträdelser som konstaterats samt meddelade förelägganden om att genomföra en konsekvensbedömning för vissa av delsystemen och begränsa behörighetstilldelningar till enbart personer som har ett behov av att behandla personuppgifter för att utföra sina arbetsuppgifter. Ärendet avslutades i november 2020 och har överklagats.

Statens servicecenter

IMY mottog en anmälan av personuppgiftsincident från Statens servicecenter (SSC) avseende systemet Primula. Några veckor senare mottog IMY flera anmälningar avseende incidenten från myndigheter som SSC är personuppgiftsbiträde åt. Mot bakgrund av anmälningar inledde IMY en tillsyn i syfte att granska SSC:s hantering av personuppgiftsincidenter i systemet Primula.

IMY utfärdade en sanktionsavgift på 50 000 kronor för att SCC underlåtit att anmäla personuppgiftsincidenten till IMY (dåvarande Datainspektionen) inom 72 timmar efter att ha fått vetskap om den. IMY utfärdade också en sanktionsavgift på 150 000 kronor mot SCC för att ha dröjt med att underrätta såväl IMY som berörda myndigheter om personuppgiftsincidenten. Ärendet avslutades i april 2020.

Polismyndigheten, Ekobrottsmyndigheten, Skatteverket, Kustbevakningen, Tullverket, Åklagarmyndigheten och Kriminalvården

IMY har i sju tillsynsärenden granskat myndigheternas förmåga att bland annat upptäcka, rapportera och hantera personuppgiftsincidenter. Tillsynerna har fokuserat på rättsväsendet, mot bakgrund bland annat av att få incidenter var anmälda utifrån brottsdatalagen.

IMY konstaterade att rutinerna överlag såg bra ut och granskningen avslutades i december 2020 med att ge ett antal rekommendationer till respektive myndighet.

Del 1.
Personuppgiftsincidenter 2020

Anmälda personuppgiftsincidenter

IMY fick under perioden 1 januari – 31 december 2020 in totalt 4 588 anmälningar om personuppgiftsincidenter, varav knappt 50 incidenter avsåg brottsdatalagen. I genomsnitt under året anmäldes 87 incidenter per vecka, vilket är något lägre än de 90 incidenter som i genomsnitt anmäldes per vecka under 2019. Det totala inflödet har således inte ändrats i någon större utsträckning jämfört med föregående år.

Det stora inflödet av anmälningar innebär att de som anmält en incident ibland har behövt vänta länge på besked om att ärendet avslutats. Under andra halvåret av 2020 har myndigheten därför prioriterat att arbeta med att korta handläggningstiden för ärendegruppen. Vid årsskiftet var, med några få undantag, samtliga pågående ärenden yngre än två månader.

Under årets första elva veckor och under årets sista fyra månader låg det genomsnittliga veckoinflödet över årssnittet med ett tiotal anmälningar. I slutet av mars skedde en tydlig minskning av inflödet. Från slutet av mars fram till och med augusti 2020 var det genomsnittliga inflödet ett 70-tal anmälningar per vecka. IMY bedömer att den tillfälliga minskningen sannolikt beror på Coronapandemin, detta mot bakgrund av att minskningen av anmälda incidenter till myndigheten och införandet av restriktioner för att minska smittspridningen i samhället sammanföll i tid. En möjlig förklaring till minskningen kan vara att snabba omställningar och omprioriteringar i verksamheterna har påverkat förmågan att upptäcka och anmäla personuppgiftsincidenter.

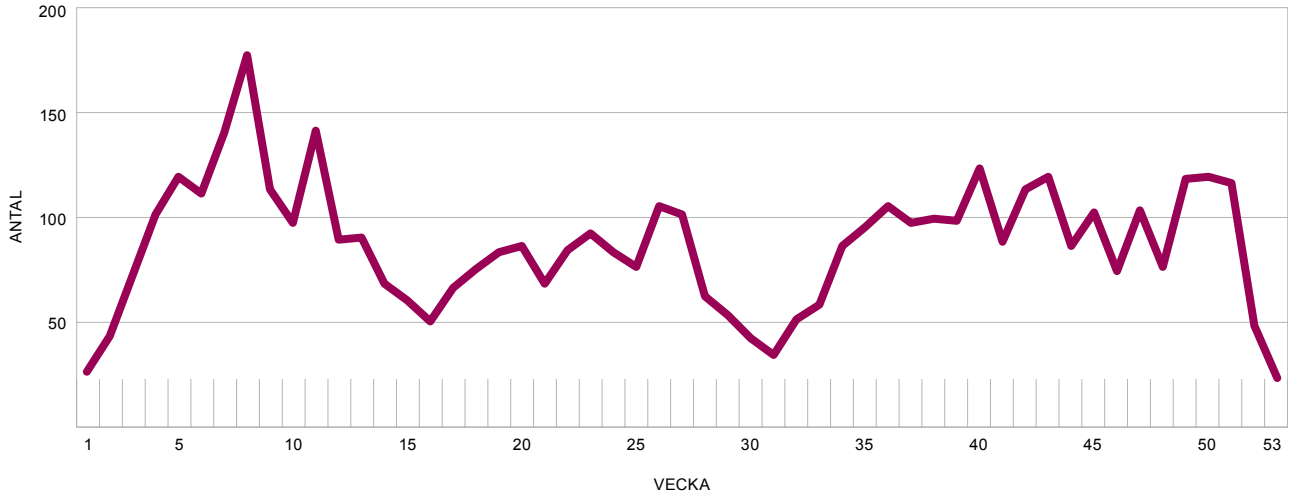


Bild 1. Antal anmälda personuppgiftsincidenter per vecka 2020.

Den absoluta merparten av de incidenter som anmälts under 2020 bedömer vi utgör faktiska personuppgiftsincidenter. En viss överrapportering i form av icke-anmälningspliktiga incidenter förkommer sannolikt fortfarande. Samtidigt gör IMY fortsatt bedömningen att det i Sverige fortfarande finns ett stort mörkertal i form av anmälningspliktiga incidenter som inte anmäls. Anmälningsplikten är fortfarande förhållandevis ny, och rutinerna för att upptäcka och anmäla incidenter inte fullt ut etablerade, vilket kan påverka såväl antal som vilka incidenter som anmäls till IMY.

Vid en jämförelse av anmälda incidenter per 100 000 invånare med andra europeiska länder placerade sig Sverige 2020 på tionde plats med 48 anmälda incidenter per 100 000 invånare. Föregående år placerade sig Sverige på åttonde plats med 57 incidenter per 100 000 invånare. Flest anmälningar har Danmark med 156 incidenter per 100 000 invånare, följt av Nederländerna med 150 och därefter Irland med 128 incidenter.[15] Att Nederländerna och Danmark har ett stort antal anmälda incidenter per invånare beror sannolikt bland annat på att länderna haft skyldighet att rapportera incidenter även före införandet av dataskyddsförordningen. Även Irland har sedan 2011 haft frivillig incidentanmälan. Erfarenheter från dessa EU-länder, där anmälningsskyldigheten för personuppgiftsincidenter funnits längre, tyder också på att antalet anmälningar kan öka över tid. I Nederländerna, där anmälningsskyldigheten infördes år 2016, ökade antalet anmälda incidenter kraftigt varje år under den första treårsperioden.[16] 2019 uppgick det totala antalet incidentanmälningar i Nederländerna till cirka 25 000.[17] Under 2020 ökade antalet med ytterligare närmare 1 000 anmälningar.[18]

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

15. DLA Piper GDPR Data Breach Survey: January 2021
16. EDPS-ENISA Conference: Towards assessing the risk in personal data breaches, 4 april 2019, Bryssel.
17. DLA Piper GDPR Data Breach Survey: January 2020
18. DLA Piper GDPR Data Breach Survey: January 2021

Fördelning på olika verksamhetsområden

Av de incidenter som anmäldes 2020 kom totalt 67 procent från offentlig sektor. Motsvarande siffra för 2019 var 61 procent.

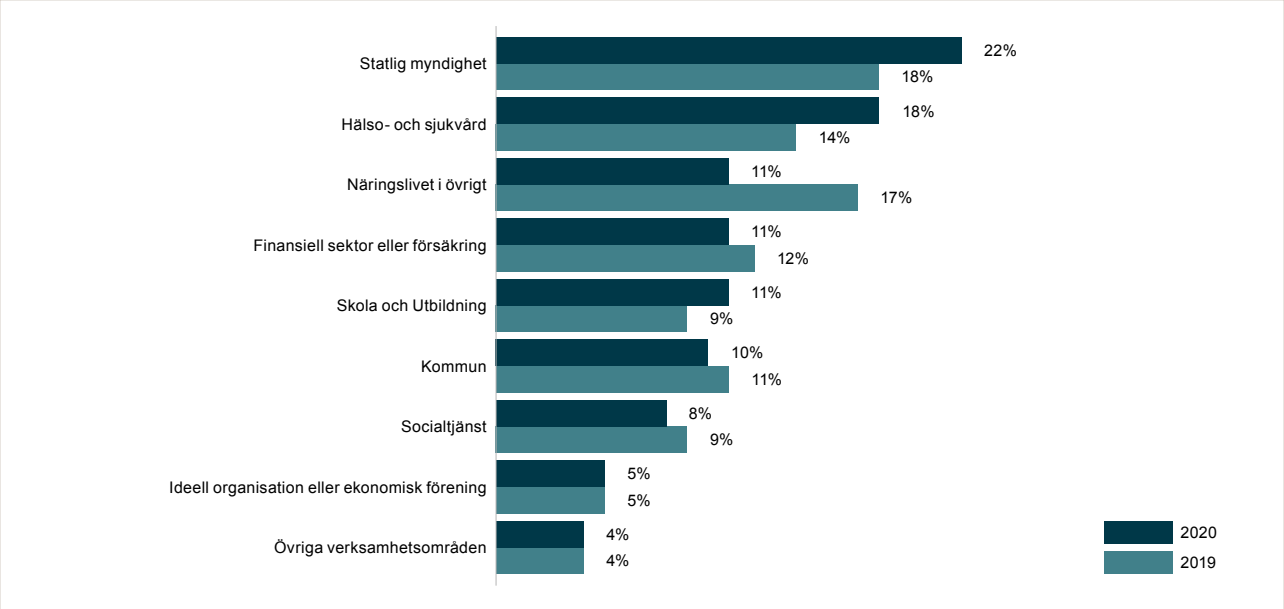


Bild 2. Andel anmälda personuppgiftsincidenter per verksamhetsområde 2019 och 2020.

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

Inom privat sektor har antalet anmälda incidenter 2020 minskat jämfört med 2019. Detta syns främst inom näringslivet, där antalet anmälda incidenter minskat med ett tjugotal anmälningar per månad. En möjlig förklaring till minskningen kan vara att Coronapandemin har tvingat verksamheter till snabba omställningar och omprioriteringar som påverkat hanteringen av personuppgiftsincidenter.

Nedan presenteras en jämförelse av antalet anmälda incidenter i genomsnitt per månad för olika verksamhetsområden mellan åren 2019 och 2020.

Ökningen av antalet anmälningar syns främst inom hälso- och sjukvården men även hos statliga myndigheter och domstolar syns en viss ökning. Av de anmälningar som inkommit från hälso- och sjukvården kommer ungefär 64 procent från offentlig sektor.

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

Verksamhetsområde	2019	2020	Skillnad	Skillnad (procent)
Näringslivet i övrigt	67	42	-25	- 37
Kommuner	45	38	-7	- 16
Finansiell sektor/försäkring	48	42	-6	- 12
Ideella organisationer	21	19	-2	- 10
Socialtjänst	33	31	-2	- 6
Övriga verksamheter	16	15	-1	- 6
Skola och Utbildning	36	42	6	17
Statliga myndigheter och domstolar	67	84	7	10
Hälso- och sjukvård	55	69	14	25

Tabell 1. Antal anmälda personuppgiftsincidenter i genomsnitt per månad per verksamhetsområde, 2019 och 2020.

Typ av incident

Felaktiga brevutskick, det vill säga brev eller mejl som innehåller personuppgifter och oavsiktligt hamnat hos fel mottagare, utgör den största delen av de anmälda incidenterna. Under 2020 utgjorde andelen felaktiga brevutskick 40 procent av samtliga anmälda incidenter. Felaktiga brevutskick har varit den vanligast förekommande personuppgiftsincidenten som anmälts till IMY sedan anmälningsplikten infördes i maj 2018.

Obehörig åtkomst är den näst största kategorin av anmälda personuppgiftsincidenter och utgjorde under 2020 knappt 30 procent av anmälningarna. Obehörig åtkomst handlar om att någon olovligen berett sig tillgång till personuppgifter, till exempel genom att behörigheter till ett it-system har tilldelats felaktigt eller för generellt. Det kan exempelvis handla om att personuppgifter har funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning. Även antagonistiska angrepp genom olika typer av hacking,[19] till exempel phishingattacker[20] eller malware,[21] förekommer inom kategorin obehörig åtkomst.

Obehörigt röjande står för 23 procent av anmälningarna 2020. Obehörigt röjande innebär att den personuppgiftsansvarige eller någon under den personuppgiftsansvariges ledning hanterat personuppgifter på ett sätt så att de kommit till obehörigas kännedom. Det kan till exempel handla om att personuppgifter avsiktligt eller oavsiktligt röjts för någon som saknar behörighet att ta del av dem eller att brister i ett tekniskt system gör att stora mängder personuppgifter kommit till fel mottagares kännedom.

Förlust utgör en relativt liten andel av anmälningarna, endast 8 procent. De anmälda incidenterna kan till exempel vara att tjänstedatorer glömts på allmän plats, att organisationen haft inbrott, blivit utsatta för ett antagonistiskt angrepp eller att ett tekniskt fel har medfört att personuppgifter gått förlorade.

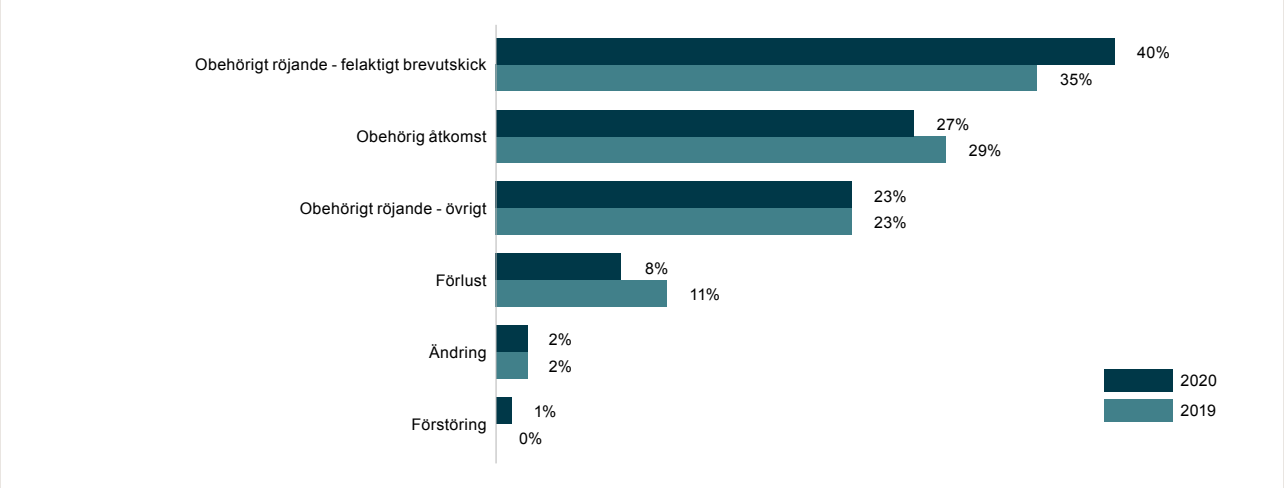


Bild 3. Andel av incidenterna fördelat på typ av incident 2019 och 2020.

19. *Hacking* innebär att någon bryter sig in i it-system utan användarens samtycke eller vetskap.
20. *Phishing* eller *nätfiske* är en metod för IT-brottslighet där internetanvändare luras att lämna ut känslig information som sedan kan användas till bedrägerier.
21. *Malware* eller *sabotageprogram* är skadlig programvara som installeras på en dator eller nätverk utan användarens samtycke för att till exempel samla in information.

Varför inträffade incidenten?

Den *mänskliga faktorn* utgör den vanligaste orsaken till anmälda personuppgiftsincidenter. I 59 procent av de incidentanmälningar som inkom under 2020 angavs den mänskliga faktorn som förklaring. Detta är en ökning i jämförelse med 2019 då motsvarande siffra var 51 procent. Incidenter som beror på den mänskliga faktorn består i huvudsak av individer som begått ett misstag vid hantering av personuppgifter i sina verksamheter. Det kan också handla om att individer, medvetet eller omedvetet, inte följer interna rutiner för hantering av personuppgifter. Omkring hälften av de incidenter som beror på den mänskliga faktorn handlar om felskickade brev och mejl.

Tekniska fel uppgavs vara orsaken till 11 procent av alla incidenter 2020, medan *antagonistiska angrepp* och *brister i organisatoriska rutiner och processer* stod 10 respektive 9 procent.

IMY släppte under 2020 en temarapport om anmälda personuppgiftsincidenter som orsakats av antagonistiska angrepp.[22] Rapporten innehåller bland annat rekommendationer, beskrivning av olika typer av antagonistiska angrepp samt statistik över de verksamhetsområden som anmält incidenter orsakade av antagonistiska angrepp.

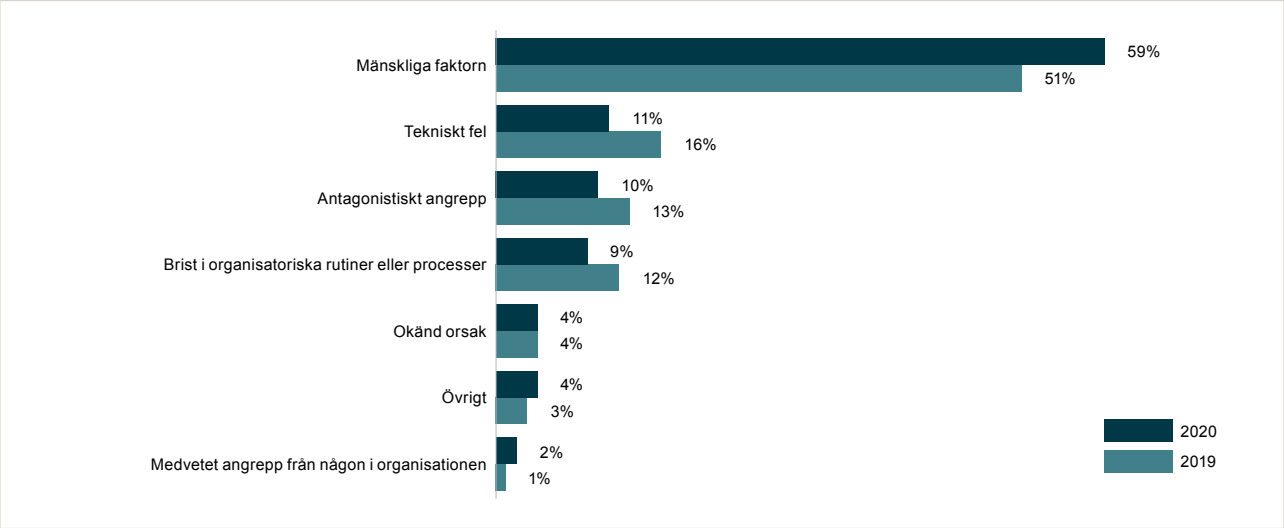


Bild 4. Andel av incidenterna fördelat på orsak 2019 och 2020.

22. Personuppgiftsincidenter som beror på antagonistiska angrepp 2019 (2020:3)

Del 2. Anmälda personuppgiftsincidenter inom olika verksamhetsområden

I denna del redovisas statistik över anmälda personuppgiftsincidenter uppdelat på olika verksamhetsområden. Det finns viss variation mellan olika verksamhetsområden när det gäller vilka incidenter som anmäls och orsakerna till dem. Det är svårt att dra slutsatser utifrån statistiken om varför fördelningen och förändringarna ser ut som de gör. Syftet med statistiken är främst att ge personuppgiftsansvariga inom olika verksamhetsområden möjlighet att se hur det ser ut i den egna branschen och skapa ett lärande genom att jämföra och reflektera vad den egna organisationen skulle kunna förbättra i sitt arbete med personuppgiftsincidenter och dataskydd.

Vanligast incident per verksamhetsområde

Verksamhetsområden där *felaktiga brevutskick* utgör den vanligaste incidenten är statliga myndigheter och domstolar, finansiell sektor och försäkring, socialtjänsten, kommuner, ideella organisationer samt hälso- och sjukvården. En möjlig förklaring till att felaktiga brevutskick är vanligast inom dessa verksamhetsområden skulle kunna vara att de i stor utsträckning skickar personuppgifter per post eller mejl. Andelen felaktiga brevutskick har dessutom ökat inom samtliga områden. Tydligast är ökningen inom kommuner där andelen anmälda incidenter som utgör felaktiga brevutskick har ökat med 21 procent. Inom övriga verksamhetsområden har felaktiga brevutskick ökat med en till åtta procent. En möjlig förklaring till ökningen hos kommuner kan vara kommunerna i större utsträckning har rutiner på plats för att upptäcka, dokumentera, anmäla och hantera personuppgiftsincidenter.

Inom näringslivet och Skola och utbildning är istället *obehörig åtkomst* den vanligast förekommande incidenten. Detta skulle kunna bero på att dessa verksamheter i mindre utsträckning kommunicerar mejl- eller brevledes med integritetskänsliga uppgifter till skillnad från övriga verksamhetsområden. Inom Skola och utbildning handlar det många gånger om användning av olika digitala verktyg och plattformar för kommunikation med föräldrar där skolresultat och annan information dokumenteras.

Incidenter av typen obehörig åtkomst har ökat med två till fem procent inom de flesta verksamhetsområden med undantag för Kommuner, Finansiell sektor och försäkring samt Statliga myndigheter och domstolar. Inom Finansiell sektor och försäkring samt Statliga myndigheter har obehörig åtkomst minskat med ungefär tio procent per område. Stört minskning, 14 procent, syns inom kommuner.

Vanligaste orsak till incident per verksamhetsområde

Inom i stort samtliga verksamhetsområden, med undantag för Näringslivet i övrigt, utgör *den mänskliga faktorn* den vanligaste orsaken till de anmälda incidenterna. Inom Näringslivet i övrigt står den mänskliga faktorn och antagonistiska angrepp för lika stor del, 30 procent, av de anmälda incidenterna. Andelen incidenter som orsakas av mänsklig faktor är störst hos Statliga myndigheter och Domstolar där 76 procent av incidenterna anges ha orsakats av mänskliga faktorn. Tydligast ökning av incidenter orsakade av mänskliga faktorn syns hos Statliga myndigheter och domstolar samt Finansiell sektor och försäkring. Inom dessa verksamhetsområden har incidenter orsakade av den mänskliga faktorn ökat med 16 respektive 17 procent. Hos övriga verksamhetsområden har inga större förändringar skett avseende andel anmälda incidenter som orsakats av mänskliga faktorn.

Näringslivet är fortsatt det verksamhetsområde där störst andel, 39 procent, av de anmälda incidenterna uppges ha orsakats av ett *antagonistiskt angrepp*. Näst störst andel finns hos Ideella organisationer och ekonomiska föreningar där 18 procent av de anmälda incidenterna anges ha orsakats av ett antagonistiskt angrepp. Inom Hälso- och sjukvård, Finansiell sektor och försäkring samt Statliga myndigheter och domstolar står de antagonistiska angreppen för mindre än fem procent av de anmälda incidenterna. Det kan ligga en reell skillnad bakom siffrorna, det vill säga att näringslivet skulle vara mer utsatta för antagonistiska angrepp än övriga verksamhetsområden. Det är dock svårt att dra slutsatser utifrån statistiken om vad skillnaderna beror på.

Typ av incident och orsak till incident uppdelat per verksamhetsområde

Nedan redovisas anmälda incidenter till IMY uppdelat på de olika verksamhetsområdena. För varje verksamhetsområde redovisas statistik över vilka typer av incidenter som anmälts från verksamhetsområdet i fråga samt vad som angetts som orsak till incidenterna.

Statliga myndigheter och domstolar

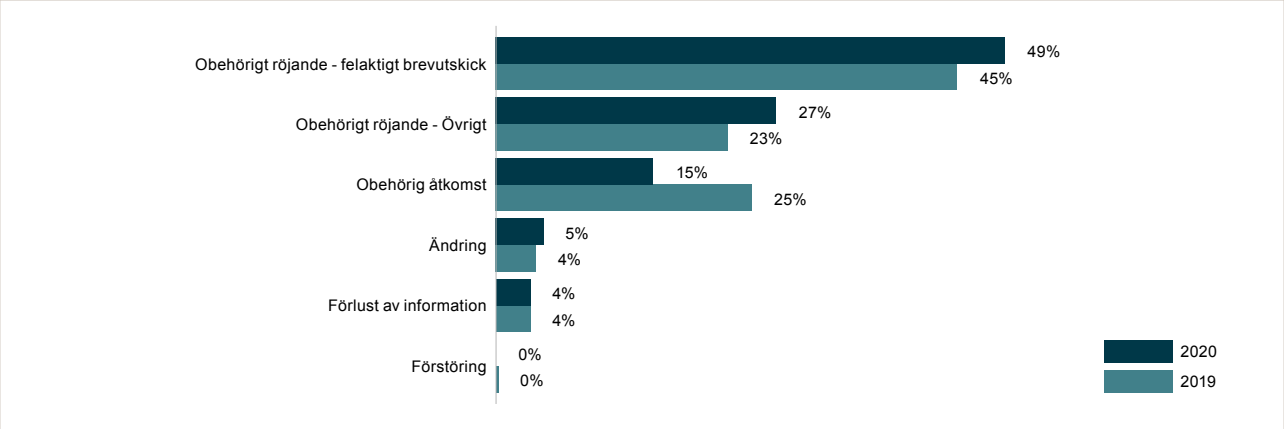


Bild 5. Fördelning av incidenter inom statliga myndigheter och domstolar 2020.

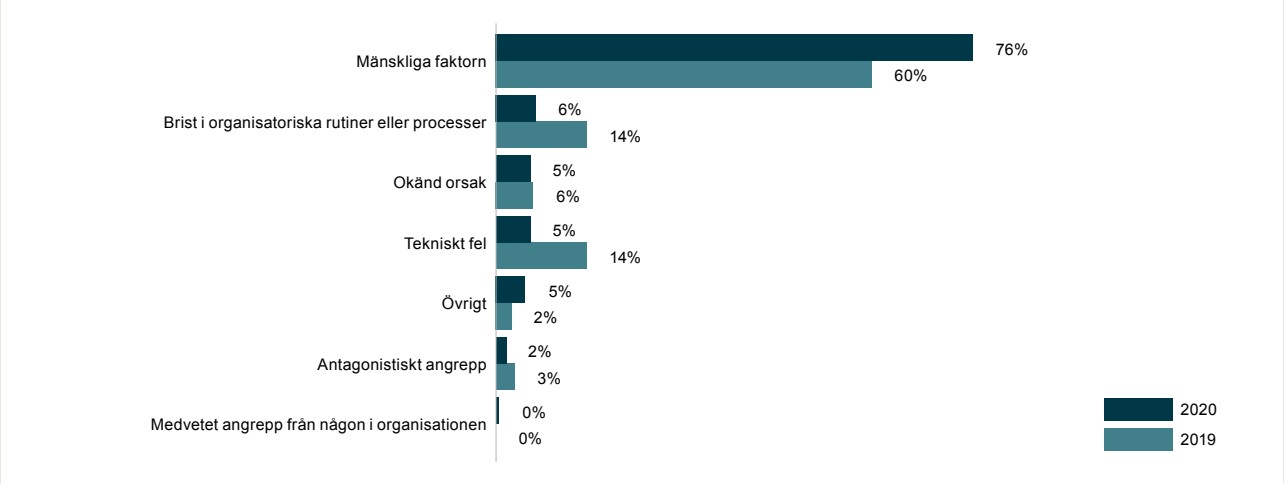


Bild 6. Fördelning av orsaker till incidenterna inom statliga myndigheter och domstolar 2020.

Finansiell sektor och försäkring

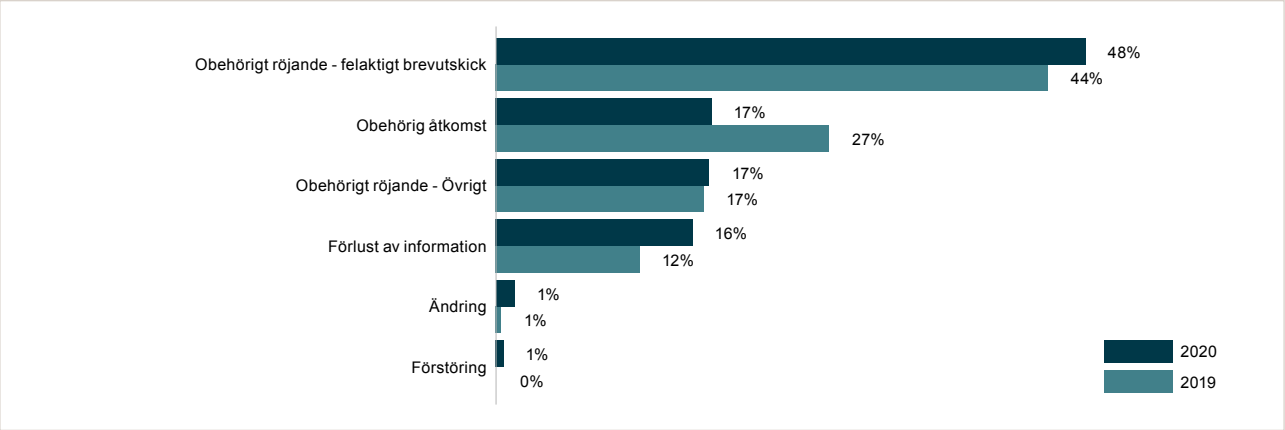


Bild 7. Fördelning av incidenter inom finansiell sektor och försäkring 2020.

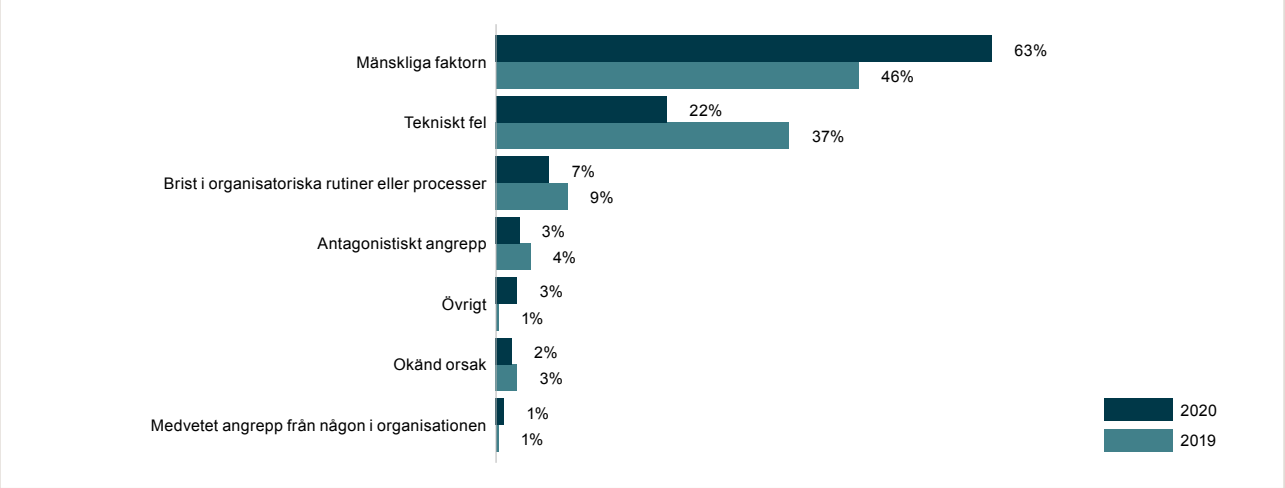


Bild 8. Fördelning av orsaker till incidenterna inom finansiell sektor och försäkring 2020.

Socialtjänsten

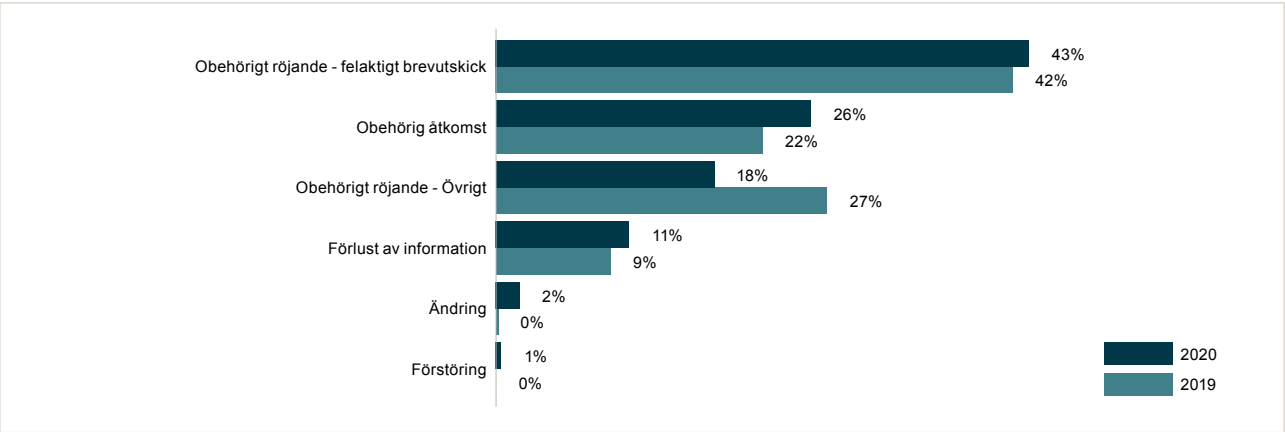


Bild 9. Fördelning av incidenter inom socialtjänsten 2020.

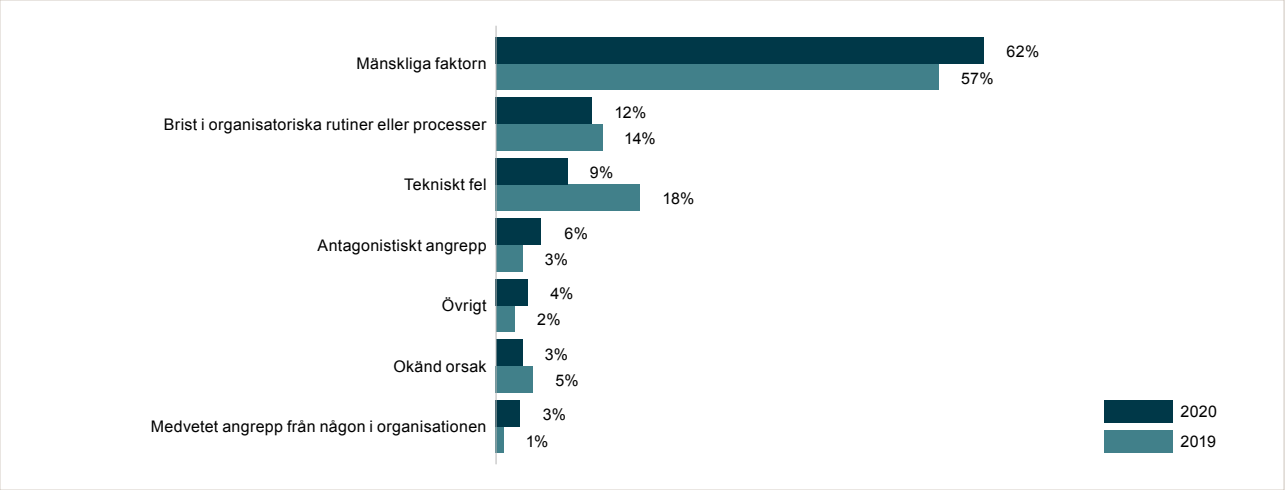


Bild 10. Fördelning av orsaker till incidenterna inom socialtjänsten 2020.

Ideella organisationer och ekonomiska föreningar

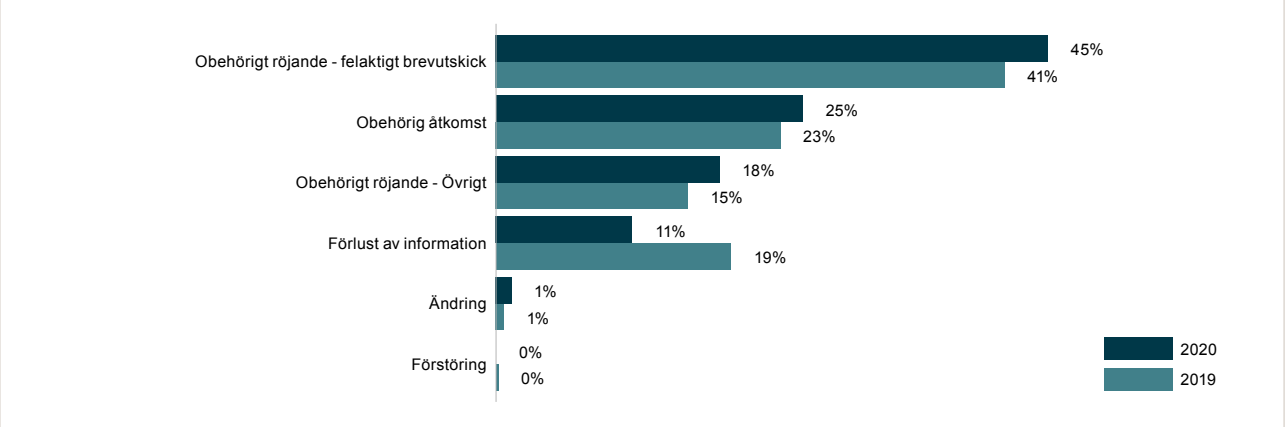


Bild 11. Fördelning av incidenter inom ideella organisationer och ekonomiska föreningar 2020. I sektorn ingår bland annat intresseföreningar, trossamfund och fackförbund.

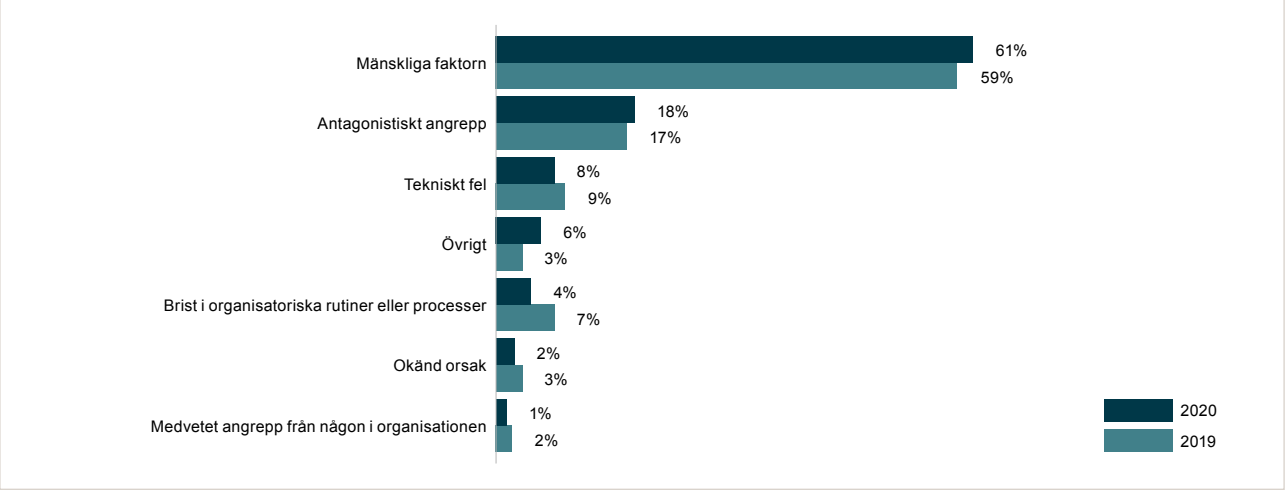


Bild 12. Fördelning av orsaker till incidenterna inom ideella organisationer och ekonomiska föreningar 2020. I sektorn ingår bland annat intresseföreningar, trossamfund och fackförbund.

Hälso- och sjukvården

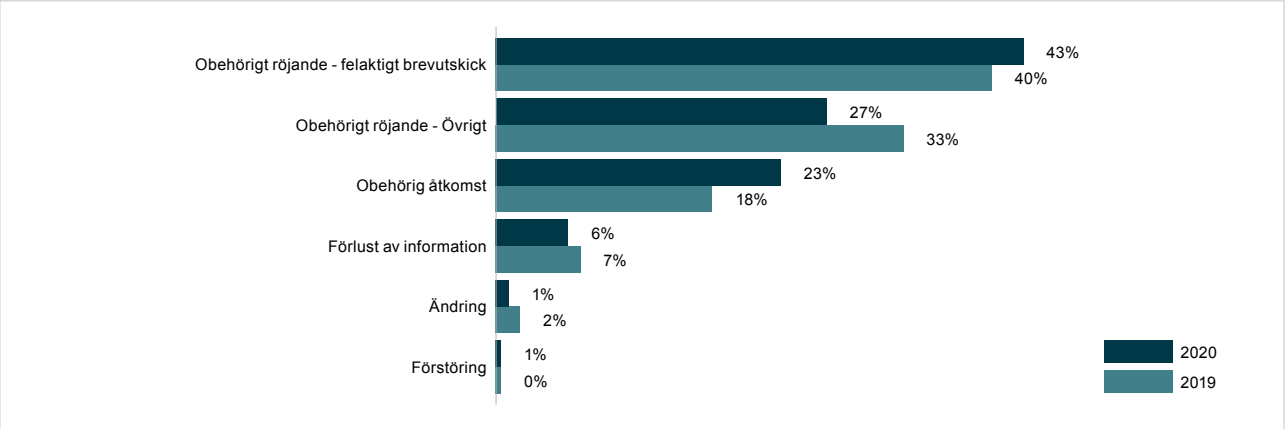


Bild 13. Fördelning av incidenter inom hälso- och sjukvården 2020.

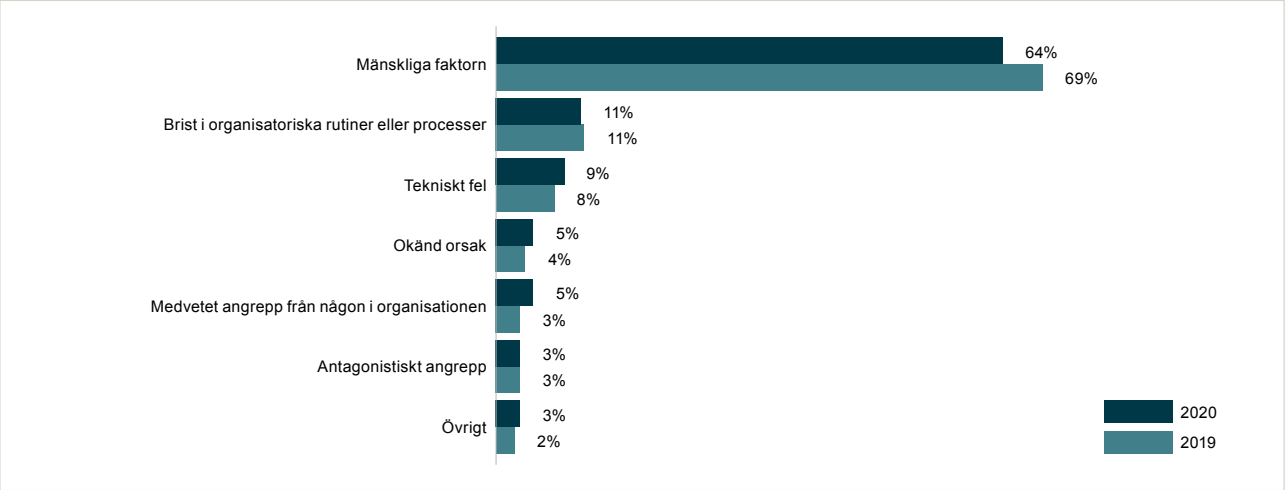


Bild 14. Fördelning av orsaker till incidenterna inom hälso- och sjukvården 2020.

Näringslivet i övrigt

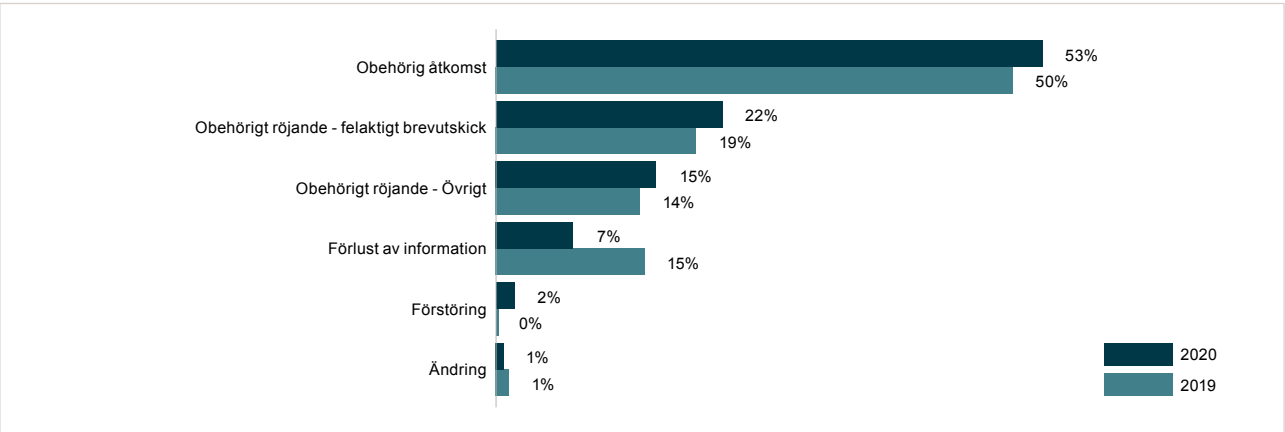


Bild 15. Fördelning av incidenter inom näringslivet i övrigt 2020.

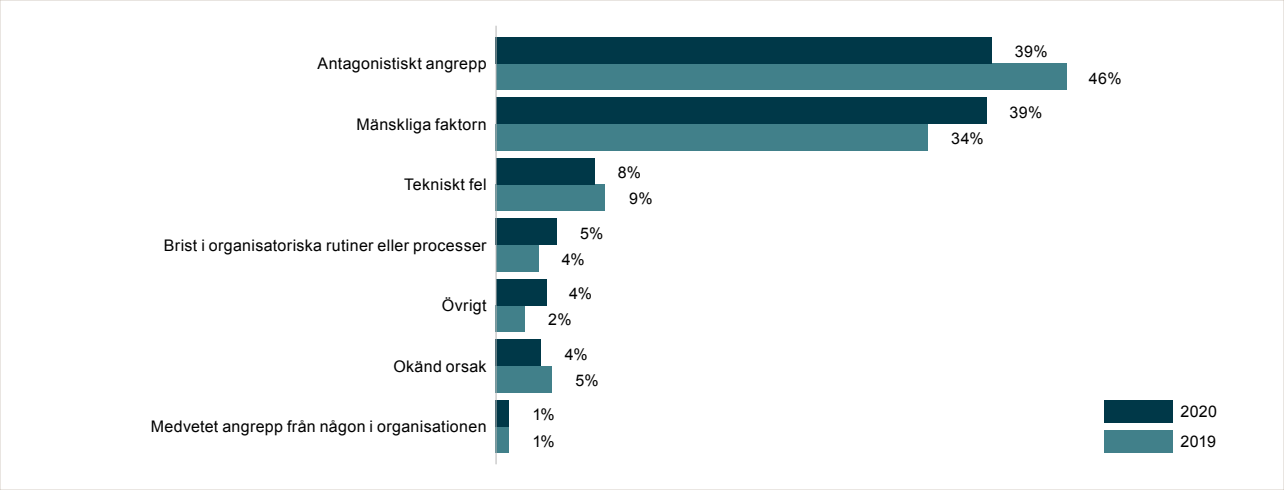


Bild 16. Fördelning av orsaker till incidenterna inom näringslivet i övrigt 2020.

Kommun

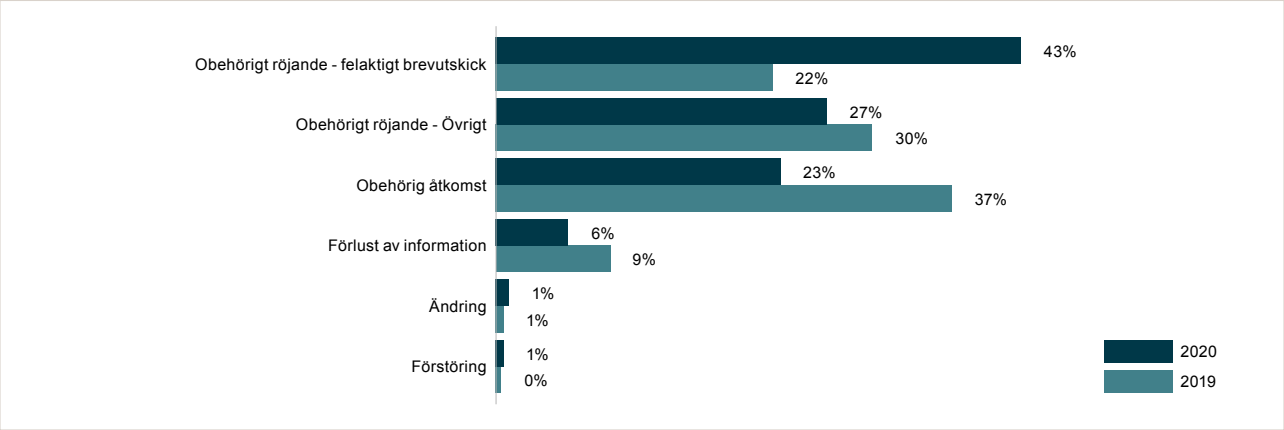


Bild 17. Fördelning av incidenter inom kommuner 2020.

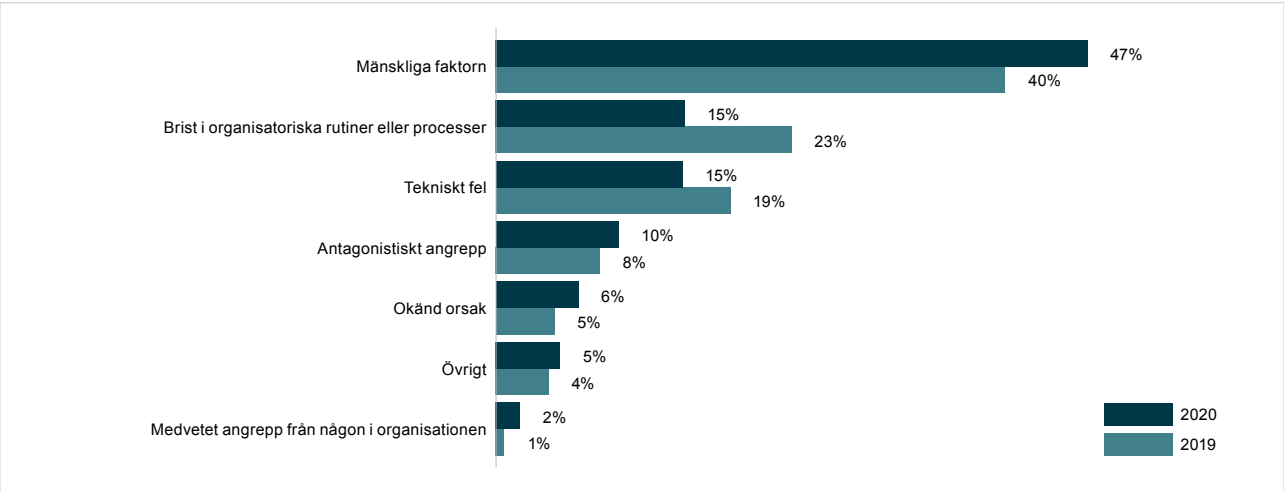


Bild 18. Fördelning av orsaker till incidenterna inom kommuner 2020.

Skola och utbildning

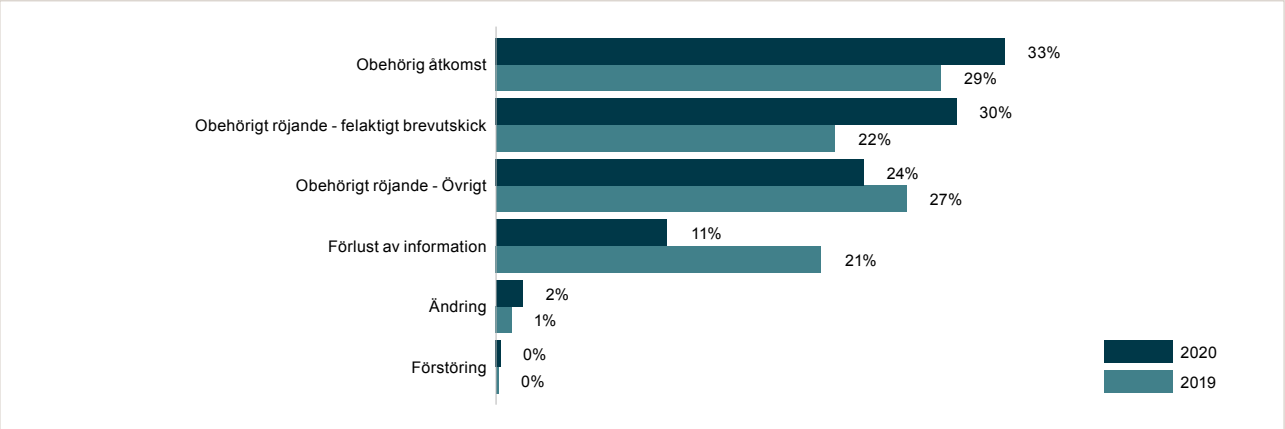


Bild 19. Fördelning av incidenter inom Skola och utbildning 2020.

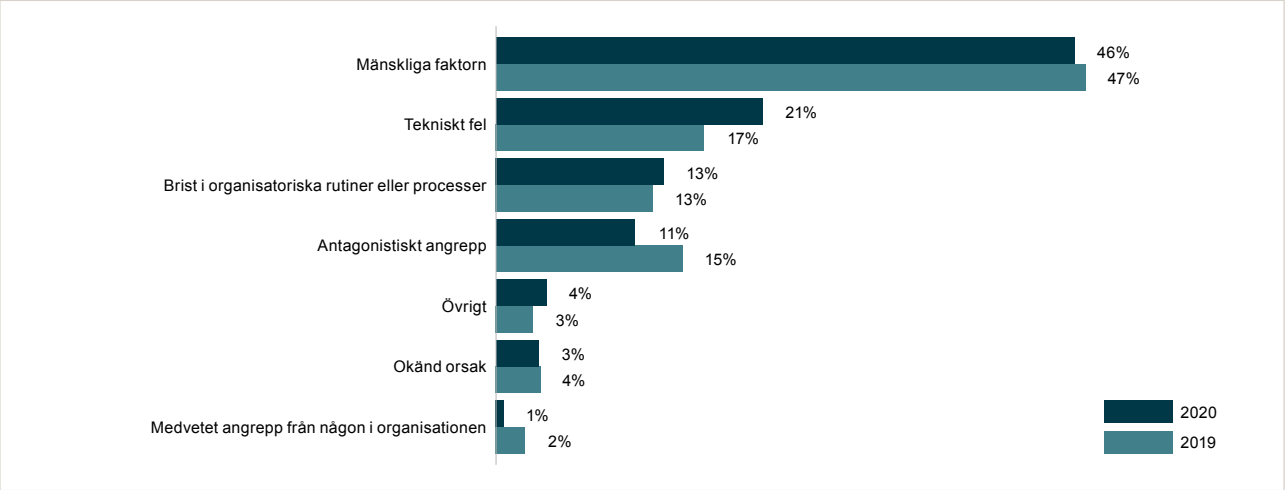


Bild 20. Fördelning av orsaker till incidenterna inom Skola och utbildning 2020.

IMY. Integritetsskydds myndigheten

Detta är Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten 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 Integritetsskyddsmyndigheten

E-post: imy@imy.se
Webb: www.imy.se
Tel: 08-657 61 00.
Postadress: Integritetsskyddsmyndigheten,
Box 8114, 104 20 Stockholm.