Nationell integritetsrapport 2019

Datainspektionens rapport 2019:2

Datainspektionen

Nationell integritetsrapport 2019
Datainspektionens rapport 2019:2
Tryckt hos Brand Factory i maj 2019
Denna rapport finns att ladda ner på www.datainspektionen.se

Förord

Sveriges ambitioner när det gäller digitalisering är höga: det övergripande målet i den nationella digitaliseringsstrategin är att vi ska vara bäst i världen på att använda digitaliseringens möjligheter. För att utvecklingen ska vara hållbar är ett viktigt delmål att alla medborgare ska kunna känna digital trygghet. Alla ska våga lita på digitala tjänster och både vilja och kunna bidra till användningen av dessa.

Privata och offentliga verksamheter har en viktig uppgift i att främja och förstärka digital innovation – och samtidigt kontinuerligt arbeta med att minimera risker.

I och med att EU:s dataskyddsförordning (GDPR) började gälla den 25 maj 2018 genomfördes den största integritetsstärkande reformen någonsin. En röd tråd i reformen är ett förstärkt skydd för individers grundläggande rättigheter i samband med att personuppgifter behandlas. Samtidigt som individens rättigheter förstärkts, har ansvaret för de som hanterar personuppgifter blivit ännu tydligare. Privata och offentliga verksamheter som hanterar personuppgifter har ett stort ansvar att sätta sig in i regelverken, följa dem och kunna visa vilka bedömningar som gjorts och åtgärder som vidtagits för att stärka skyddet av personuppgifter.

Denna rapport är Datainspektionens första nationella integritetsrapport. Rapporten är en del i vårt arbete med att följa och beskriva utvecklingen när det gäller frågor som rör integritet och dataskydd. Eftersom det gått ett år sedan dataskyddsförordningen började gälla, fokuserar rapporten på hur långt arbetet kommit med att införa det nya regelverket i företag, myndigheter och andra organisationer. Rapporten innehåller också ett inledande avsnitt om medborgarnas kunskap, attityder och beteenden när det gäller integritet och dataskydd.

Som rapporten visar har många privata och offentliga verksamheter åstadkommit mycket under det första året sedan dataskyddsförordningen trädde i kraft. Samtidigt är tre av fyra medborgare i någon mån oroliga för hur deras personuppgifter används – och bara hälften av dataskyddsombuden bedömer att den verksamhet de ansvarar för har ett kontinuerligt och systematiskt arbete med dataskydd. Det finns med andra ord mycket kvar att göra.

Målgruppen för rapporten är i första hand beslutsfattare i offentliga och privata verksamheter, förtroendevalda och personer som på olika sätt arbetar med dataskydd och informationssäkerhet. För Datainspektionen kommer rapporten att vara ett viktigt underlag, både för att utveckla vårt stödjande arbete och för att göra prioriteringar i tillsynsverksamheten. Vår förhoppning är att rapporten ska ge vägledning även för många andra i det fortsatta arbetet mot det som är Datainspektionens vision: *Ett tryggt informationssamhälle – tillsammans värnar vi den personliga integriteten.*

Stockholm i maj 2019
Lena Lindgren Schelin
Generaldirektör

Innehåll

Inledning

Den 25 maj 2018 började EU:s generella dataskyddsförordning[1] (The General Data Protection Regulation, GDPR) att gälla. Förberedelserna för dataskyddsförordningen och den första tiden med det nya regelverket har inneburit ett intensivt arbete i stora delar av det svenska samhället. Många privata och offentliga verksamheter har drivit ett ambitiöst arbete för att anpassa sina verksamheter till förordningen. Ett antal nya och förändrade skyldigheter har tillkommit och för många har arbetet varit utmanande, särskilt eftersom det i stora delar saknas närmare uttolkning av regelverken och praxis inte hunnit skapas.

Uppmärksamheten kring dataskyddsförordningen har varit omfattande, inte minst de sista veckorna i maj 2018. Få människor undgick förmodligen att dataskyddsförordningen började gälla den 25 maj. Floden av e-postbrev där medborgarna informerades om privata och offentliga verksamheters integritetspolicy, eller ombads samtycka till fortsatt behandling av personuppgifter, gjorde GDPR till ett omtalat begrepp.

För Datainspektionen har dataskyddsförordningen medfört stora förändringar i uppdrag, befogenheter och förutsättningar. Datainspektionens huvuduppdrag är att arbeta för att människors rättigheter skyddas i samband med behandling av personuppgifter. En viktig del av myndighetens verksamhet handlar om att granska att regler och lagar följs. Genom dataskyddsförordningen har myndigheten fått skarpare befogenheter i tillsynsverksamheten, bland annat rätten att besluta om administrativa sanktionsavgifter. Samtidigt har den förebyggande och stödjande delen i Datainspektionens uppdrag fått ökad betydelse. Varje dag får vi ett stort antal frågor från medborgare, men också myndigheter, företag och andra organisationer som behöver vägledning i arbetet med att tolka och införa de nya dataskyddsreglerna i sitt arbete.

En del av Datainspektionens uppdrag handlar om att följa, analysera och beskriva sådan utveckling som påverkar skyddet av personuppgifter. Ett år efter att dataskyddsförordningen började gälla har vi nu tagit fram vår första nationella integritetsrapport. Syftet med den nationella integritetsrapporten 2019 är att ge en bild av hur långt privata och offentliga verksamheter i Sverige kommit i arbetet med integritet och dataskydd.

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).

I rapporten presenteras resultaten från tre undersökningar; en enkät riktad till dataskyddsombud[2], en till företag utan dataskyddsombud och en till medborgare. Undersökningen riktad till medborgare fokuserar på inställning, attityder och beteenden när det gäller insamling och användning av personuppgifter i främst digitala kanaler.

Rapporten inleds med en sammanfattning, där de viktigaste resultaten presenteras. I några fall görs reflektioner kopplat till tidigare forskning och undersökningar inom integritetsskyddsområdet. Sammanfattningen avslutas med ett antal slutsatser som Datainspektionen bedömer ger värdefulla insikter i det fortsatta arbetet med att utveckla Sveriges integritets- och dataskydd.

Därefter följer ett avsnitt om integritet och dataskydd ur medborgarnas perspektiv. Där presenteras resultaten från undersökningen riktad till medborgare mer i detalj, följt av en översiktlig beskrivning av de frågor och klagomål som medborgare skickat till Datainspektionen under det första året med dataskyddsförordningen.

Rapportens tredje och sista del fokuserar på integritet och dataskydd ur verksamheternas perspektiv – företag, myndigheter och andra organisationer som hanterar personuppgifter och därmed omfattas av dataskyddsförordningen. Här ges också en översiktlig beskrivning av de frågor som verksamheter ställer till Datainspektionen, samt de personuppgiftsincidenter som anmälts under dataskyddsförordningens första år.

2 Myndigheter, företag och andra organisationer som behandlar personuppgifter måste i vissa fall utse ett dataskyddsombud. Ombudets roll är att kontrollera att dataskyddsförordningen följs och ge råd och information om dataskydd inom organisationen. Mer information om dataskyddsombud finns på www.datainspektionen.se/dso

Sammanfattning och slutsatser

Integritet och dataskydd ur medborgarnas perspektiv

Knappt ett år efter att dataskyddsförordningen började gälla visar Datainspektionens undersökning att den nya lagstiftningen är väl känd.

- Drygt åtta av tio medborgare känner till dataskyddsförordningen och att den innebär förstärkta rättigheter för individerna.

Kännedomen om vilka rättigheterna är varierar dock. Mest känd är rätten till information, som förenklat innebär att en verksamhet som behandlar en individs personuppgifter tydligt ska informera om hur uppgifterna används. Minst känd är rättigheten att få personuppgifter återlämnade eller överförda till ett annat företag, så kallad dataportabilitet.

Tre av fyra är i någon utsträckning oroliga för hur deras personuppgifter används

Medborgarna känner till att förordningen finns och att den ger individerna förstärkta rättigheter. På en övergripande nivå finns även en medvenhet om olika integritetsrisker kopplat till personuppgiftshantering.

- Nio av tio medborgare känner till att internetvanor och surfbeteende samlas in och i vissa fall kan säljas vidare till andra företag för att anpassa reklam.
- Åtta av tio känner till att appar i vissa fall kan innebära att företag kan följa en persons fysiska förflyttningar.
- Betydligt färre, bara tre av tio, upplever sig ha kunskap om hur deras personuppgifter används.
- Tre av fyra uppger att de i någon utsträckning känner oro för hur deras personuppgifter används.

Att så många känner till att personuppgifter samlas in men samtidigt upplever sig ha dålig kunskap om hur de används, är sannolikt en bidragande förklaring till att det finns en förhållandevis utbredd oro rörande personuppgiftshantering. Störst oro känner medborgarna för att kriminella eller andra obehöriga ska komma åt deras personuppgifter. En mer diffus känsla av att inte ha kontroll över sina personuppgifter bidrar också till oro.

Finansiella uppgifter och hälsoppgifter anses särskilt känsliga, och det finns en uttalad och återkommande oro kring att använda sitt bankkort på nätet. Även insamling av personuppgifter för riktad reklam skapar oro.

Förtroendet för olika verksamheters hantering av personuppgifter varierar i stor utsträckning.

- Störst förtroende har medborgarna för personuppgiftshanteringen inom vård, myndigheter och banker.
- Lägst förtroende åtnjuter appar, sociala medier och sökmotorer.

Trots en utbredd oro för hur personuppgifter används är det färre som vidtar åtgärder för att skydda sin integritet

Eftersom tre av fyra i någon mån är oroliga för hur deras personuppgifter hanteras, är det rimligt att medborgarna vidtar åtgärder för att skydda sina personuppgifter. Av undersökningsresultaten framgår också att ungefär hälften vidtar olika typer av aktiva åtgärder.

- Hälften av svenskarna gör ibland eller alltid aktiva val för att förhindra att deras surfvanor och surfbeteende kartläggs.
- Hälften avstår ibland eller ofta från att använda en digital tjänst om de upplever osäkerhet kring hur deras personuppgifter kommer att hanteras.
- Fyra av tio läser ibland eller alltid användarvillkoren innan de registrerar sig på en webbplats eller laddar ned en app.

Även om en del medborgare i vissa situationer medvetet skyddar sina personuppgifter är det många som fortsätter att använda tjänster på nätet utan att i någon större utsträckning skydda sina personuppgifter. Glappet mellan attityd och faktiskt beteende när det gäller att skydda personuppgifter benämns i forskningen ofta för integritetsparadoxen. Forskningen visar även på olika tänkbara förklaringar till att medborgarna trots en upplevd oro är förhållandevis generösa med att dela med sig av sina personuppgifter. En förklaring kan vara att fördelarna värderas högre än riskerna vid användning av digitala tjänster. Det kan också vara så att medborgarna inte upplever att de har något val när det gäller att dela med sig av personuppgifter för att få tillgång till en tjänst. Även brist på kunskap kan spela in.[3]

3 Se till exempel Sara Leckner, SOM-institutet: ”Sprickor i fasaden”, Vem är positiv till insamling av användargenererad data på internet?” 2018, Sid 56

Olika demografiska grupper har olika kunskap och vidtar olika typer av åtgärder

I ett stort antal av frågorna som medborgare svarat på i Datainspektionens undersökning är demografiska skillnader återkommande. Såväl ålder, kön, utbildning som var man bor i landet tycks spela roll för graden av kunskap, oro och vilka aktiva åtgärder man vidtar.

- Personer i åldern 30–39 och högskole- och universitetsutbildade känner i högre grad till dataskyddsförordningen, vad de har för rättigheter och hur deras personuppgifter används.
- Äldre, och personer med låg utbildning upplever sig i större omfattning ha lägre kunskap om hur deras personuppgifter används, och upplever även större oro.

Tidigare undersökningar visar liknande mönster när det gäller svenskarnas internetanvändning. Den del av befolkningen som använder internet sällan eller inte alls utgörs i högre grad av äldre, personer med lägre hushållsinkomst och utbildning, kvinnor samt boende på landsbygden.[4]

Datainspektionens undersökning visar att olika demografiska grupper också har olika strategier för att skydda sin integritet.

- Män och personer i åldern 18–29 år är överrepresenterade bland dem som ibland eller alltid gör aktiva val för att undvika att surfvanor samlas in.
- Kvinnor och personer i åldern 65–79 är överrepresenterade bland dem som uppger att de ofta eller ibland avstår från att använda en digital tjänst om de känner osäkerhet kring hur deras personuppgifter kommer att hanteras.

90-talister har i andra undersökningar beskrivits som helt vana vid nätet och smarta mobiler och snabba med att hoppa på nya tjänster på internet. Personer födda på 00-talet har ibland getts epitetet digitala medborgare.[5] Datainspektionens undersökning visar att yngre personer också varit snabbast med att anamma de nya rättigheter som dataskyddsförordningen medfört.

- Bland personer i åldern 18–29 år har 22 procent utnyttjat någon av rättigheterna i dataskyddsförordningen.
- I den totala befolkningen har 16 procent utnyttjat någon av rättigheterna i dataskyddsförordningen. Ytterligare 18 procent har funderat på att använda någon av rättigheterna.

4 Internetstiftelsen: Svenskarna och Internet 2018, sid 4.
5 Internetstiftelsen: Svenskarna och Internet 2018, sid 98 och 108.

Medborgare som vänder sig till Datainspektionen ifrågasätter ofta om en viss personuppgiftsbehandling är laglig

Datainspektionen svarar varje dag på ett stort antal frågor från engagerade och ibland upprörda medborgare. Knappt ett år efter att dataskyddsförordningen började gälla har myndigheten besvarat cirka 9 000 frågor från medborgare via e-post och telefon.

- Omkring en fjärdedel av de frågor som medborgare ställer till Datainspektionen handlar om att lagligheten i en specifik personuppgiftsbehandling ifrågasätts. Återkommande områden där lagligheten ifrågasätts rör till exempel direktmarknadsföring och arbetsgivares hantering av anställdas personuppgifter.
- Ytterligare en fjärdedel av de frågor som medborgare ställer till Datainspektionen handlar om rätten till radering. Vanliga frågor gäller till exempel att företag har kvar personuppgifter trots att kundrelationen är avslutad sen länge, eller att verksamheter vägrar radera personuppgifter som medborgare inte anser att de har rätt att behålla.
- Drygt en av tio frågor till Datainspektionen handlar om att medborgare ifrågasätter säkerheten som omgärdar personuppgifter.
- Nästan en av tio frågor från medborgare rör kamerabevakning och en av tio frågor handlar om rätten till registerutdrag.

Utöver att ställa frågor till Datainspektionen kan medborgare lämna in klagomål till myndigheten. Det är inte alltid uppenbart vad som skiljer en fråga från ett klagomål – gemensamt för båda kategorierna är ofta att medborgaren är upprörd över det sätt som personuppgifter hanterats på. En viktig distinktion är dock att klagomål alltid handlar om att medborgarens egna personuppgifter behandlats felaktigt. Genom dataskyddsförordningen har handläggningen av klagomål också fått skarpa tidsfrister. Normalt ska ett klagomålsärende avgöras av Datainspektionen inom tre månader.

Innehållet i klagomålen följer i stort samma mönster som medborgarnas frågor.

- Nästan en tredjedel av klagomålen till Datainspektionen rör sajter som Eniro, Hitta, Lexbase, Mr Koll, Ratsit och Merinfo som publicerar stora mängder personuppgifter om enskilda på nätet. Dessa sajter har ett så kallat frivilligt utgivningsbevis. Datainspektionen har mycket begränsade möjligheter att medverka till att få dessa personuppgifter borttagna, eftersom det i svensk lag finns ett undantag från dataskyddsförordningen när det finns ett utgivningsbevis.
- Cirka vart femte klagomål till Datainspektionen handlar om lagligheten i en viss personuppgiftsbehandling. Återkommande är

till exempel klagomål som handlar om att verksamheter samlar in personnummer, när medborgaren anser att det borde räcka med kontaktuppgifter.

- Klagomål som rör rätten till radering, direktmarknadsföring, kamerabevakning och otillräckliga säkerhetsåtgärder står för omkring 10 procent vardera av det totala antalet klagomål.

Integritet och dataskydd ur medborgarnas perspektiv – sammanfattande bedömning

För att på ett översiktligt sätt sammanfatta resultaten från Datainspektionens undersökning om medborgarnas perspektiv på integritet och dataskydd kan en ”integritetsskyddstrappa” användas. De olika trappstegen beskriver olika nivåer för medvetenhet, kunskap och aktiva åtgärder avseende integritetsrisker och integritetsskydd.

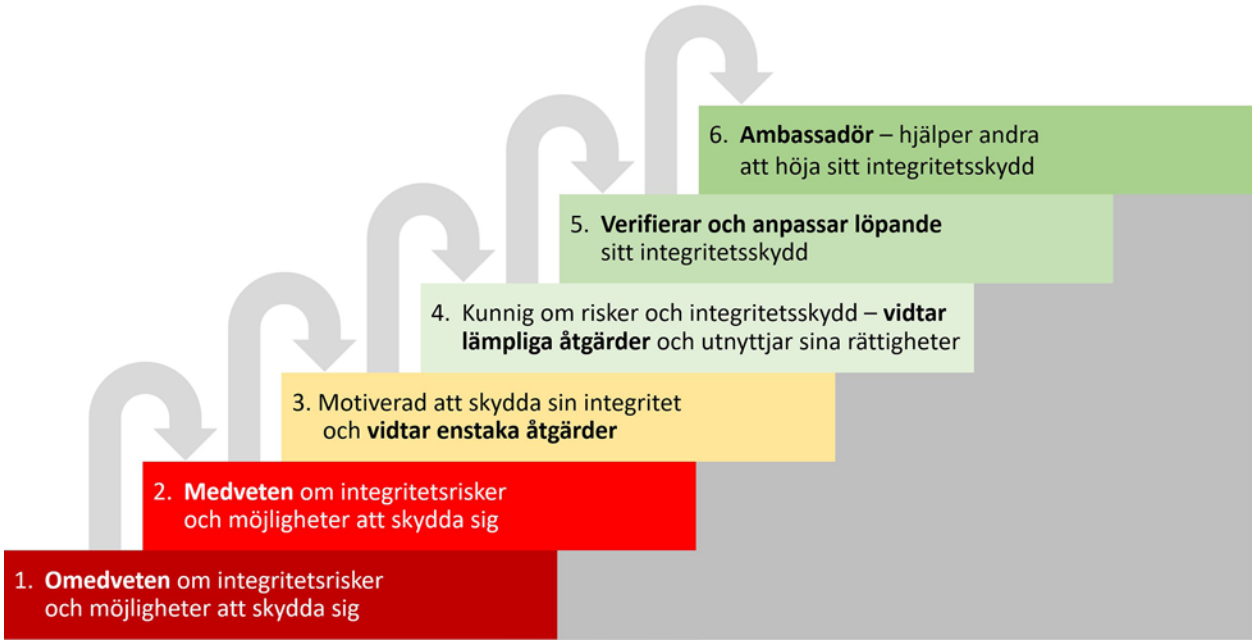

Bild 1. Integritetsskyddstrappan – medborgares medvetenhet om integritetsrisker och kunskap om att skydda personuppgifter.

Det nedersta steget i trappan kännetecknas av en omedvetenhet om såväl integritetsrisker som möjligheter att skydda sig. Datainspektionens undersökning omfattar medborgare mellan 18-79 år, och av dessa bedöms endast en liten del tillhöra denna grupp. Äldre och personer med endast grundskoleutbildning är troligen något överrepresenterade på steg ett. Även om Datainspektionens undersökning inte omfattar barn är det sannolikt att många, särskilt yngre barn, också är omedvetna om integritetsrisker och möjligheter att skydda sig.

En stor majoritet av den vuxna befolkningen bedöms ha nått, eller passerat, steg två – som kan beskrivas som en grundläggande medvetenhet om integritetsrisker och möjligheter att skydda sig. Trots att den snabba tekniska utvecklingen kan göra att det upplevs som svårt att hålla sig a jour, visar Datainspektionens undersökning till exempel att en majoritet av befolkningen känner till att appar i vissa fall kan innebära att företag kan följa en persons fysiska förflyttningar.

Trappans tredje steg beskriver personer som är motiverade att skydda sin integritet och vidtar vissa enstaka åtgärder. Omkring hälften av befolkningen bedöms ha passerat de två första stegen och nått åtminstone nivån där de vidtar någon typ av integritetsskyddande åtgärder. Som exempel visar Datainspektionens undersökning att hälften av medborgarna uppger att de gör aktiva val för att hindra att surfvanor och surfbeteende samlas in när de använder internet. Ungefär lika många uppger att de ibland eller ofta avstår från att använda en digital tjänst för att de känner osäkerhet på hur personuppgifterna kommer att användas, vilket också kan sägas vara en form av integritetsskyddande åtgärd.

På ett fjärde steg i integritetsskyddstrappan är individen kunnig om risker. Även om det är svårt för den enskilde att fullt ut påverka sitt integritetsskydd vidtar individen här en kombination av olika integritetsskyddande åtgärder, både generella och mer situationsanpassade. Här ingår också att aktivt använda sina rättigheter. Att 16 % procent av befolkningen uppger att de använt någon av sina rättigheter ger en indikation om hur många som kommit till denna nivå i sitt integritetsskydd. Som nämnts tidigare är yngre personer överrepresenterade i denna grupp.

Det femte steget kännetecknas av att den enskilde, så långt det är möjligt, löpande verifierar och anpassar sitt integritetsskydd. Endast en liten del av den svenska befolkningen bedöms ha nått steg fem.

Givet att det är första gången Datainspektionen genomför en undersökning riktad till allmänheten är det svårt att värdera resultaten. Det faktum att var sjätte medborgare utnyttjat någon av sina rättigheter vittnar om vilja och engagemang hos medborgare att värna sina personuppgifter. Att stärka enskildas rättigheter är ett viktigt syfte med dataskyddsförordningen. Det är därför positivt att så pass många utnyttjat sina rättigheter redan under det första året.

Det är viktigt att ha i åtanke att dataskyddsförordningen ger individer en rad förstärkta rättigheter, men inga skyldigheter. Ytterst står det var och en fritt att avgöra i vilken utsträckning vi vill sätta oss in i risker och möjliga åtgärder som rör integritet och dataskydd. Samtidigt är kunniga medborgare som ställer krav på säker och transparent personuppgiftshantering betydelsefulla, eftersom de driver på utvecklingen mot digital trygghet.

Regeringens digitaliseringsstrategi framhåller digital kompetens som ett viktigt delmål för att nå visionen om ett hållbart digitaliserat Sverige. Digital kompetens handlar bland annat om tekniska färdigheter att använda digitala verktyg och tjänster. Datainspektionens undersökning visar att medborgare med mer kunskap om hur personuppgifter används är mindre oroliga för hur deras personuppgifter hanteras. För att öka den digitala tryggheten är en viktig aspekt av digital kompetens att också känna till olika integritetsrisker och åtgärder som kan vidtas för att minska riskerna.

Integritet och dataskydd ur verksamheternas perspektiv – företag, myndigheter och andra organisationer som hanterar personuppgifter

Lika välkänd som dataskyddsförordningen hunnit bli hos medborgare är den också hos företag, myndigheter och andra organisationer som hanterar personuppgifter.

De flesta uppger att implementeringen av dataskyddsförordningen fungerat bra

Myndigheter och andra offentliga organ är enligt dataskyddsförordningen skyldiga att utse ett dataskyddsombud, det vill säga en person som har till uppgift att informera, ge råd och övervaka efterlevnaden av dataskyddsförordningen inom organisationen. Även vissa företag är skyldiga att utse ett dataskyddsombud, till exempel om de behandlar känsliga personuppgifter i stor utsträckning. En del företag har valt att utse ett dataskyddsombud även om de inte omfattas av lagkraven. De flesta verksamheter med dataskyddsombud har kommit långt i sitt arbete med integritet och dataskydd.

- Tre av fyra dataskyddsombud anser att implementering av dataskyddsförordningen fungerat bra.
- Tre av fyra dataskyddsombud uppger att deras organisation har tagit fram riktlinjer för hur personuppgifter ska hanteras och att de har nya grundläggande skyldigheter och rutiner på plats, som till exempel en förteckning över verksamhetens personuppgiftsbehandlingar, relevanta personuppgiftsbiträdesavtal samt rutiner för att lämna ut registerutdrag och rapportera personuppgiftsincidenter till Datainspektionen.

Även företag som inte utsett ett dataskyddsombud har i flera avseenden kommit långt i implementeringen av dataskyddsförordningen.

- Fyra av fem företag utan dataskyddsombud uppger att de känner till dataskyddsförordningen bra och att arbetet med dataskydd och integritet är prioriterat.
- Tre av fyra företag har utsett en ansvarig för arbetet med integritet och dataskydd.
- Ungefär sju av tio uppger att de har riktlinjer för hur personuppgifter ska hanteras, har en förteckning över vilka personuppgiftsbehandlingar som finns i verksamheten och rutiner för att lagra och gallra personuppgifter.

Olika branscher har kommit olika långt

Olika branscher har kommit olika långt i implementeringen av dataskyddsförordningen. Bland verksamheterna som har dataskyddsombud utmärker sig ett antal branscher och sektorer.

- Bank- och finansbranschen samt it- och telekombranschen har i många avseenden kommit längre än andra i sitt arbete med integritet och dataskydd. Även privata vård- och omsorgsföretag har i flera avseenden kommit längre än genomsnittet.
- Kommuner och landsting[6] är överrepresenterade bland dem som tycks ha större utmaningar och i mindre omfattning arbetar kontinuerligt och systematiskt med integritet och dataskydd.

Även bland företag som inte anmält något dataskyddsombud finns skillnader mellan olika branscher. Företagsstorlek har också betydelse för i vilken omfattning verksamheterna arbetar med dataskyddsfrågor. Företag med fler än 50 anställda har generellt sett kommit längre i arbetet med dataskydd.

- Privata vård- och omsorgsföretag och utbildningsföretag uppger i högre grad än andra att de har ett kontinuerligt och systematiskt arbete med integritet och dataskydd.
- Företag inom hotell- och restaurangbranschen samt transportbranschen uppger i mindre grad än andra att de har ett kontinuerligt och systematiskt arbete med integritet och dataskydd.
- Det framgår även att småföretag med färre än tio anställda i mindre utsträckning både arbetar med frågorna och har grundläggande rutiner på plats.

6 Begreppet landsting är på väg att fasas ut, den 1 januari 2019 bytte de sista landstingen namn till regioner. Under 2019 uppdateras ett stort antal författningar som en följd av namnbytet. Eftersom Datainspektionens frågeformulär togs fram 2018 används genomgående i rapporten begreppet landsting.

Stort behov av vägledning och stöd från Datainspektionen

De största utmaningarna i dataskyddsarbetet uppges vara att få till fungerande rutiner och processer och att tolka regelverket. Behovet av stöd och vägledning i att tolka regelverket är påtagligt i de frågor som företag, myndigheter och andra organisationer ställer till Datainspektionen.

- En tredjedel av de frågor som företag, myndigheter och andra organisationer ställer till Datainspektionen handlar om avvägningar kring den rättsliga grunden för en specifik personuppgiftsbehandling. Särskilt vanliga är frågor om samtycke, som innebär att den enskilde godkänt personuppgiftsbehandlingen, och intresseavvägning mellan verksamhetens behov av att behandla personuppgifterna och den enskildes intresse av skydd för sina personuppgifter.
- En av tio frågor handlar om vad som är lämpliga säkerhetsåtgärder.
- En av tio frågor rör vilka regler som gäller för kamerabevakning.
- En av tio frågor handlar om gränsdragningar mellan olika personuppgiftsansvariga och personuppgiftsbiträden.

Bank- och finansbranschen anmäler flest personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Såväl privata som offentliga verksamheter måste anmäla personuppgiftsincidenter till Datainspektionen.

Bank- och finansbranschen anmäler flest personuppgiftsincidenter och står för en femtedel av samtliga anmälda incidenter, vilket förstärker intrycket av att branschen har kommit långt när det gäller att ha rutiner för arbetet med integritet och dataskydd.

Knappt hälften av samtliga anmälda personuppgiftsincidenter handlar om vad som i dataskyddsreglerna kallas för obehörigt röjande och obehörig åtkomst.

- Vanliga personuppgiftsincidenter är till exempel att brev som innehåller personuppgifter skickats till fel mottagare.
- Även att någon olovligen berett sig tillgång till personuppgifter, till exempel genom att behörigheter har tilldelats felaktigt förekommer förhållandevis ofta.

Sammantaget bekräftar de anmälda personuppgiftsincidenterna resultatet från undersökningarna att det är en utmaning att få till fungerande rutiner och processer i arbetet med integritet och dataskydd.

Den mänskliga faktorn är den i särklass vanligaste anledningen till att personuppgiftsincidenter inträffar. Totalt förklaras sex av tio incidenter med den mänskliga faktorn.

Integritet och dataskydd ur verksamheternas perspektiv – sammanfattande bedömning

Precis som medborgarnas perspektiv på integritet och dataskydd ovan beskrivits i en ”integritetsskyddstrappa”, kan en ”regelefterlevnadstrappa” användas för att ge en övergripande bild av hur långt privata och offentliga verksamheter i Sverige kommit i arbetet med att anpassa verksamheten till dataskyddsförordningen.

De olika trappstegen beskriver hur långt företag, myndigheter och organisationer kommit avseende medvetenhet, kunskap och efterlevnad av dataskyddsförordningen.

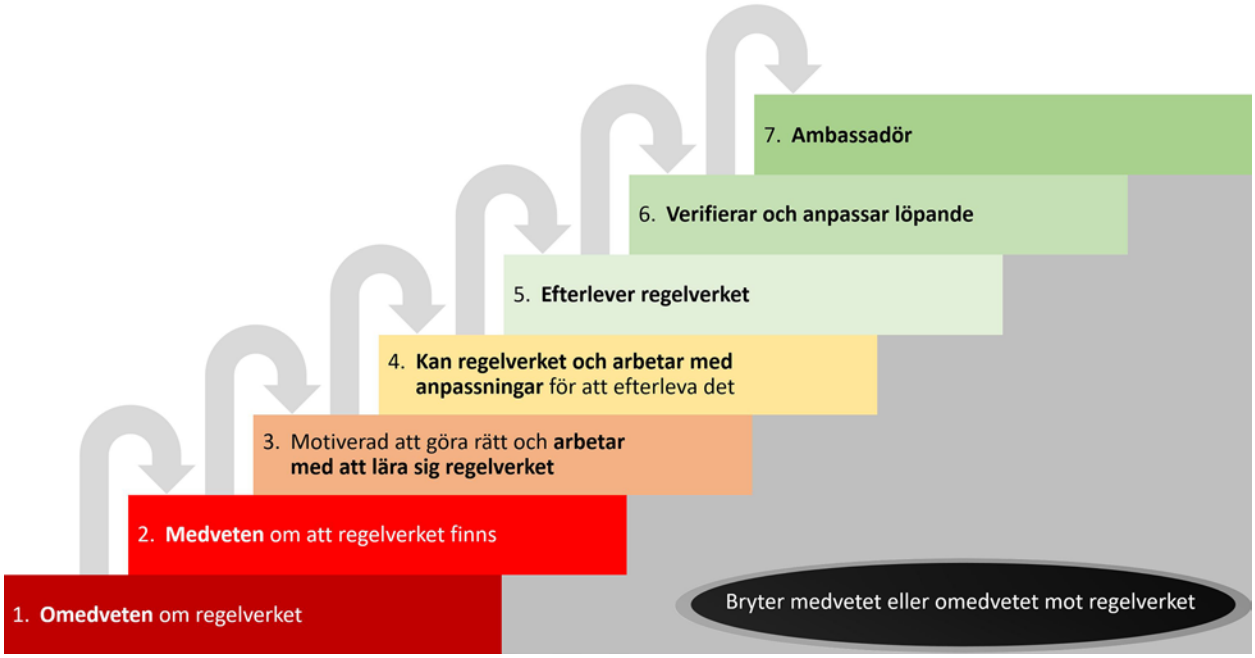

Bild 2. Regelefterlevnadstrappan – verksamheternas mognad avseende efterlevnad av dataskyddsförordningen.

På regelefterlevnadstrappans första steg är verksamheten omedveten om att dataskyddsreglerna finns. Datainspektionens undersökningar ger bilden att väldigt få svenska företag, myndigheter och andra organisationer befinner sig här.

En mindre andel privata företag bedöms finnas på det andra steget, som innebär att de är medvetna om att dataskyddsförordningen finns men har låg kunskap om regelverket och hur det påverkar deras egen verksamhet. Småföretag med färre än 10 anställda är överrepresenterade

i denna grupp. Nästan en fjärdedel av småföretagen uppger i undersökningen att de bara känner till dataskyddsförordningen lite eller inte alls har hört talas om den. Datainspektionens undersökning visar också att vissa företag inom transport-, samt hotell- och restaurangbranschen finns här. En knapp tredjedel av transportföretagen känner bara till dataskyddsförordningen lite eller har inte hört talas om den.

Majoriteten av svenska privata och offentliga verksamheter bedöms ha nått åtminstone regelefterlevnadstrappans tredje steg. De flesta är motiverade att göra rätt och arbetar med att lära sig regelverken. Att både dataskyddsombuden och privata företag som inte anmält dataskyddsombud uppger att ledningen är engagerad i frågor som rör integritet och dataskydd bidrar till att skapa goda förutsättningar för det fortsatta arbetet. Samtidigt är det tydligt att vissa sektorer har större utmaningar. Dataskyddsombud inom kommun och landsting upplever genomgående att de har större utmaningar i arbetet med integritet och dataskydd än andra.

Vissa branscher utmärker sig positivt i undersökningen till dataskyddsombud och har nått åtminstone nivå fyra i trappan – de kan regelverket och arbetar med anpassningar för att efterleva det. Undersökningen visar att företag inom bank och finansbranschen samt it- och telekombolag generellt sett kommit längre än andra i arbetet med integritet och dataskydd.

Dataskyddsförordningen har bara gällt ett år och i många delar saknas fortfarande praxis. Det är därför för tidigt att bedöma om några verksamheter nått nivå fem eller sex i regelefterlevnadstrappan, där regelverket efterlevs, men integritetsskyddet också löpande verifieras och anpassas.

Såväl privata som offentliga verksamheter har mycket att vinna på ett aktivt arbete med integritet och dataskydd. En rättssäker och transparent personuppgiftshantering bygger förtroende. Datainspektionens undersökning har visat att hälften av medborgarna någon gång avstått från att använda en digital tjänst för att de känt en osäkerhet kring hur deras personuppgifter hanteras. En nyligen genomförd global undersökning har också visat att företag med en hög regelefterlevnad när det gäller dataskyddsförordningen bland annat drabbades av mindre negativa konsekvenser i samband med IT-angrepp eller andra typer av personuppgiftsincidenter.[7]

7 Cisco Cybersecuity Series 2019: Maximizing the value of your data privacy investments – Data Privacy Benchmark Study.

Slutsatser

Mycket har hänt på bara ett år med den nya dataskyddsförordningen. Samtidigt ger Datainspektionens undersökningar ett antal insikter som kan utgöra avstamp för Sveriges fortsatta arbete med integritet och dataskydd.

Grundläggande strukturer finns på plats – nu är nästa steg att skapa ett kontinuerligt och systematiskt arbete

De allra flesta företag, myndigheter och organisationer har under dataskyddsförordningens första år tagit fram grundläggande riktlinjer och rutiner för personuppgiftshantering. Samtidigt uppger bara hälften av dataskyddsombuden att medarbetarna i deras organisation efterlever dataskyddsförordningen. Både bland verksamheter med dataskyddsombud och privata företag utan dataskyddsombud uppger ungefär hälften att deras organisation i hög utsträckning arbetar kontinuerligt och systematiskt med integritets- och dataskyddsfrågor.

Den största utmaningen kopplat till dataskyddsförordningen upplevs vara att få till fungerande rutiner och processer. När dataskyddsförordningen nu går in på sitt andra år är det angeläget att privata och offentliga verksamheter tar nästa steg. För att framtagna riktlinjer och rutiner ska fungera fullt ut i praktiken behöver de löpande anpassas och utvecklas, både i takt med att de prövas i den praktiska verkligheten och att praxis utarbetas.

Hälften av dataskyddsombuden uppger att integritet och dataskydd är en prioriterad fråga för ledningen, vilket kan uppfattas som en liten andel. Bara ett av tio dataskyddsombud upplever dock att en av de största utmaningarna med dataskyddsförordningen är att få gehör hos ledningen, vilket indikerar goda förutsättningar för det fortsatta arbetet.

Kommuner, landsting och småföretag riskerar att halka efter

Kommuner, landsting och företag med färre än tio anställda utmärker sig i en rad frågor i Datainspektionens undersökning. Genomgående har de färre grundläggande skyldigheter och rutiner på plats och svaren i undersökningen ger bilden att de i lägre omfattning än andra sektorer implementerat dataskyddsförordningen.

Flera omständigheter hos kommuner och landsting skulle kunna förklara varför utmaningarna i dataskyddsarbetet är större där än i andra sektorer. På frågan om vad som är de största utmaningarna i arbetet svarar dataskyddsombud inom kommun och landsting i högre grad än andra att det är en utmaning att få till fungerande rutiner och processer, att dataskyddsreglerna upplevs hindra eller försvåra verksamheten och att de har gamla IT-system som försvårar dataskyddsarbetet. Sju av tio

dataskyddsombud inom kommun och landsting uppger att de aldrig, sällan eller bara ibland blir involverade i projekt eller andra sammanhang där beslut fattas som får följder för dataskyddet. Endast tre av tio dataskyddsombud inom kommun och landsting uppger att ledningen är kunniga och insatta i dataskyddsfrågor.

Att ta tillvara digitaliseringens potential är en nyckel i den fortsatta utvecklingen av de offentliga välfärdstjänsterna i Sverige. I den nationella digitaliseringsstrategin konstateras att det behövs en ökad digital kompetens på alla nivåer i offentlig sektor. För att innovation och verksamhetsutveckling ska åstadkomma en hållbar nytta för medborgarna behöver teknikens möjligheter balanseras med ett fokus på digital trygghet. I det fortsatta arbetet med att öka den digitala kompetensen hos beslutsfattare och andra nyckelpersoner inom kommuner och landsting är det därför angeläget att dataskydd är en integrerad del.

Det finns också ett behov av särskilda satsningar för att fortsätta stärka förmågan hos småföretag i deras arbete med dataskydd. Sverige har en omkring en miljon företag med färre än tio anställda, som av förklarliga skäl kan ha svårt att säkerställa resurser och kompetens för dataskyddsarbetet. Särskilt småföretag som hanterar känsliga personuppgifter eller stora mängder personuppgifter behöver få stöd i att komma till nästa nivå i dataskyddsarbetet.

Medarbetare behöver fortsatt utbildning i dataskydd

För att Sverige ska nå målet om digital trygghet behöver regelefterlevnaden fortsätta öka hos såväl medarbetare i privata och offentliga verksamheter. Dataskyddsförordningen är ett förhållandevis komplicerat regelverk. Att kontinuerligt vidta kompetenshöjande åtgärder på olika nivåer i organisationer är därför en nödvändig del av det fortsatta arbetet. I undersökningen uppger ungefär hälften av dataskyddsombuden att dataskydd och informationssäkerhet ingår i introduktionsutbildningen av nya medarbetare. Bara i en tredjedel av verksamheterna får medarbetarna löpande utbildning i dataskydd och informationssäkerhet.

Behovet av fortsatt utbildning understryks också i inflödet av personuppgiftsincidenter till Datainspektionen. Den vanligaste orsaken till inrapporterade personuppgiftsincidenter är den mänskliga faktorn, vilket i många fall kan bero på att medarbetarna inte känner till fastställda rutiner tillräckligt bra.

Dataskyddsombuden behöver få avsätta tillräckligt med tid

Dataskyddsombuden har en nyckelroll när det gäller det arbetet med dataskydd. En framgångsfaktor är att de kan avsätta tillräckligt med tid

för arbetet. Över hälften av dataskyddsombuden uppger i Datainspektionens undersökning att de har för lite tid för att effektivt kunna arbeta med frågorna. Majoriteten arbetar deltid som dataskyddsombud och ungefär hälften av dessa saknar en överenskommelse om hur stor andel av arbetstiden som ska ägnas åt uppdraget.

Verksamheter vars dataskyddsombud uppger att de inte har tillräckligt med tid avsatt saknar oftare grundläggande dataskyddsrutiner. De har med andra ord ett större arbete framför sig innan de kan börja bygga upp ett kontinuerligt och systematiskt arbete.

Stort behov av fortsatt stöd och kompensutveckling för dataskyddsombud

Nästan hälften av dataskyddsombuden uppger att en av de största utmaningarna i dataskyddsarbetet är att det är oklart hur regelverket ska tolkas. Här har Datainspektionen en viktig uppgift att kontinuerligt fortsätta utvecklingen av stödet till dataskyddsombuden.

Förutsättningarna för dataskyddsombuden kan också förbättras på en rad andra områden. Bara en tredjedel uppger att de som regel blir involverade i god tid i projekt som har betydelse för dataskyddet. Ungefär hälften anser att deras uppdrag kan bli tydligare, och att de inte fullt ut får den utbildning och kompetensutveckling som krävs för att arbeta med dataskyddsfrågor i organisationen.

Att skapa goda förutsättningar för dataskyddsombudet är ett viktigt ansvar för ledningen i alla personuppgiftsansvariga verksamheter.

Integritet och dataskydd ur medborgarnas perspektiv

För att få en bild av hur medborgarna ser på integritet och dataskydd ett år efter att dataskyddsförordningen började gälla har Datainspektionen genomfört en undersökning riktad mot allmänheten. I undersökningen har totalt 1 003 webbintervjuer genomförts.[8]

Resultatet från undersökningen redovisas nedan i tre olika avsnitt, där det första ger en övergripande bild av hur medvetna medborgarna är om integritetsrisker. Frågorna i avsnittet beskriver bland annat kännedom, kunskap, oro och förtroende ur olika aspekter som berör integritet och hantering av personuppgifter.

Det andra avsnittet beskriver medborgarnas kännedom om dataskyddsförordningen och de olika rättigheter som förordningen reglerar.

I det tredje avsnittet ligger fokus på olika typer av aktiva åtgärder som medborgare vidtar för att skydda sin integritet. Det kan handla om att till exempel göra aktiva val för att hindra att surfvanor kartläggs, eller att avstå från att använda en digital tjänst på grund av osäkerhet kring hur personuppgifterna kommer att användas. Ytterligare ett sätt att aktivt värna sin integritet är att använda de nya rättigheter som dataskyddsförordningen ger. Undersökningsresultatet beskriver därför också hur stor andel av medborgarna som uppger att de använt någon av rättigheterna.

Undersökningen ger en viktig bild av hur medborgarna ser på frågor som rör integritet och dataskydd. Varje dag hör ett antal medborgare av sig till Datainspektionen med frågor eller klagomål kring hur deras personuppgifter hanteras. För att ytterligare fördjupa bilden av medborgarnas perspektiv på integritet och dataskydd ges avslutningsvis en beskrivning av de frågor och klagomål som kommer till Datainspektionen.

8 Undersökningen är genomförd av företaget Novus på uppdrag av Datainspektionen. Undersökningen är genomförd via webbintervjuer i Novus slumpmässigt rekryterade och representativa Sverigepanel. Resultaten är riksrepresentativa. Intervjuerna genomfördes under perioden 21 – 27 februari 2019 och svarsfrekvensen uppgår till 53 procent. Metoden beskrivs mer utförligt i en bilaga till denna rapport. Undersökningen i sin helhet finns på www.datainspektionen.se

Medvetenhet om integritetsrisker

- **De flesta är medvetna om att personuppgifter samlas in, men få har kunskap om hur de används.** En stor majoritet av medborgarna känner till att personuppgifter samlas in, men bara en tredjedel uppger att de har kunskap om hur personuppgifterna används.
- **Tre av fyra känner i någon mån oro för hur personuppgifter används.** Finansiella uppgifter och hälsouppgifter anses särskilt känsliga. Det finns en återkommande oro kring att använda sitt bankkort på nätet. Samtidigt finns också en mer diffus oro kopplat till att förlora kontrollen över sina personuppgifter. Även riktad reklam skapar oro.
- **Högst förtroende har medborgarna för vård, banker och myndigheter när det gäller hanteringen av personuppgifter.** Lägst förtroende har medborgarna för personuppgiftshanteringen i appar, sociala medier och på sökmotorer.

En stor majoritet av medborgarna är medvetna om att personuppgifter samlas in

Det finns en förhållandevis stor medvetenhet bland medborgarna om att personuppgifter samlas in och kan användas för olika syften. Nio av tio känner till att internetvanor och surfbeteende registreras och i vissa fall kan säljas vidare till andra företag i syfte att anpassa reklam. Även kännedomen om att appar i vissa fall kan innebära att företag kan följa hur individer förflyttar sig är utbredd. Åtta av tio uppger att de känner till att nedladdade appar innebär att företag kan följa deras fysiska förflyttning.

För att få en uppfattning om den generella medvetenheten har frågor ställts om några specifika exempel på hur personuppgifter kan användas. Frågorna beskriver situationer där det förekommer att personuppgifter delas, vilket inte ska tolkas som att det alltid sker eller alltid är lagligt. Kännedomen är hög om att samverkande myndigheter i vissa fall kan dela personuppgifter med varandra. Omkring sju av tio uppger att de är medvetna om att personuppgifter kan delas mellan myndigheter. Betydligt färre, ungefär fyra av tio, känner till att personuppgifter inom vården i vissa fall kan användas till forskning.

Svaren visar på vissa demografiska skillnader. Såväl ålder, kön, utbildning som var man bor i landet spelar roll för graden av medvetenhet. Att internetvanor och surfbeteende registreras och kan

användas för anpassad reklam är mest känt bland yngre personer, 18-29 år, universitets- och högskoleutbildade och boende i Stockholm. Minst känt är det bland äldre, 65–79 år, personer med grundskoleutbildning, och personer boende i Småland och Västsverige.

Att appar i mobilen kan innebära att företag kan följa dig fysiskt är mest känt bland män och personer i åldrarna 18–29 år. Lägst kännedom har äldre personer mellan 65–79 år och kvinnor.

Att myndigheter som samverkar i vissa fall delar dina personuppgifter och att hälsouppgifter som lämnas till vården i vissa fall kan användas för forskning är mest känt bland universitets- och högskoleutbildade.

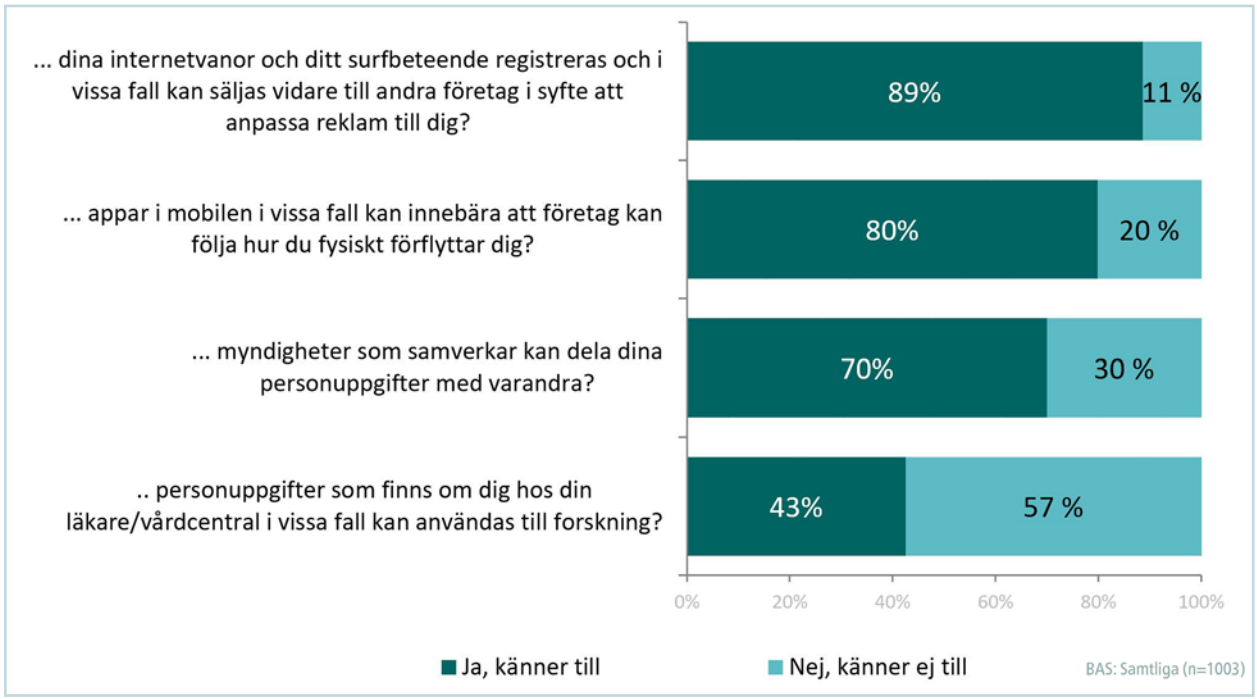

Bild 3. Fråga: Känner du till att… ?

Nästan sju av tio har låg kunskap om hur personuppgifterna används

Samtidigt som medvetenheten är förhållandevis hög om att personuppgifter samlas in, är kunskapen om hur de används betydligt lägre. Nästan sju av tio har låg kunskap om hur deras personuppgifter används. Bara en knapp tredjedel uppger att de har mycket eller ganska hög kunskap om hur deras personuppgifter kommer att användas när de lämnas till företag, myndigheter och organisationer.

Även här finns vissa demografiska skillnader. Personer i åldrarna 30–49 samt universitets- och högskoleutbildade är överrepresenterade bland dem som anser att de har hög kunskap.

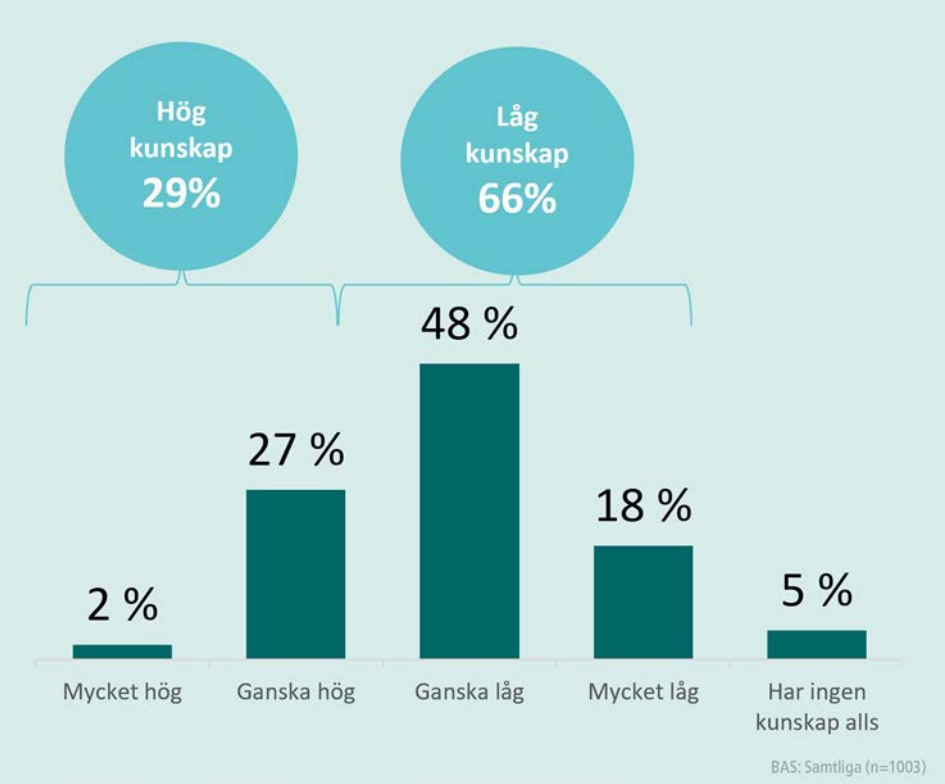

Bild 4. Fråga: Hur ser du på din allmänna kunskap om hur dina personuppgifter kommer att användas när du lämnar dem till företag, myndigheter och organisationer?

Tre av fyra känner i någon mån oro för hur deras personuppgifter används

Mot bakgrund av att kunskapen om hur personuppgifter används är förhållandevis låg, följer att många känner viss oro för hur uppgifterna används. Tre av fyra uppger att de i någon utsträckning känner oro för hur deras personuppgifter används. Samtidigt är det bara en mindre del som uppger att de känner mycket eller ganska stor oro – det vanligaste svaret är istället att man känner ”viss” oro.

De som upplever sig ha kunskap om hur personuppgifter används tenderar också att vara mindre oroliga. Personer som anser sig ha bra kunskap om hur personuppgifter kommer att användas är överrepresenterade bland dem som inte känner någon oro.

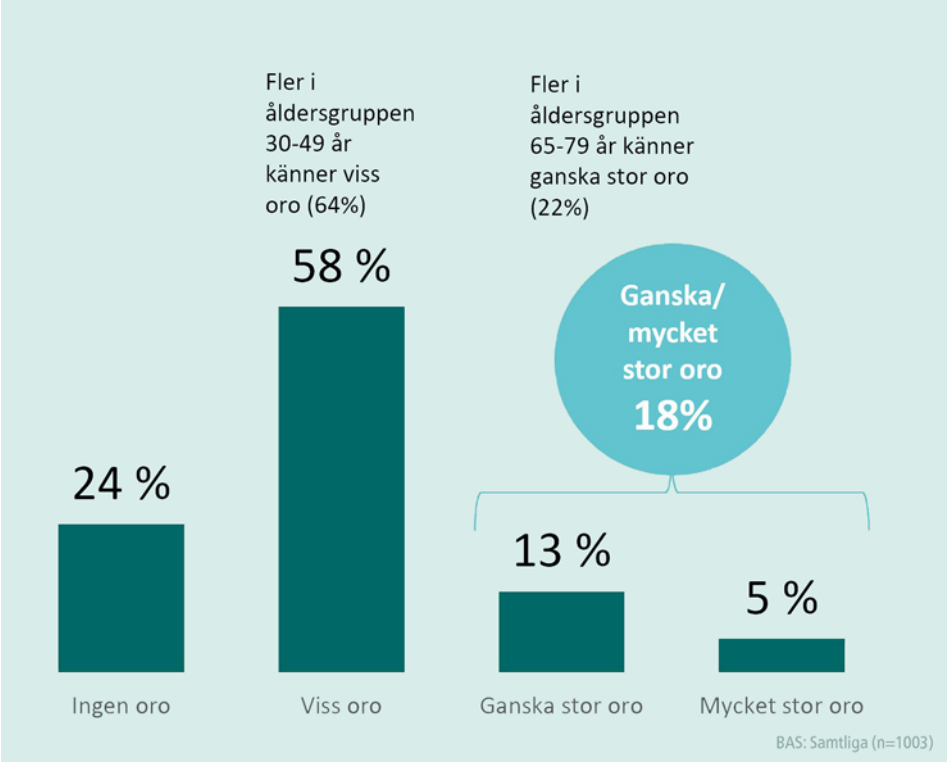

Bild 5. Fråga: I vilken utsträckning känner du oro för hur dina personuppgifter används av företag, myndigheter och organisationer?

Finansiell information och hälsouppgifter anses känsligast

För att fördjupa förståelsen av den oro som finns hos medborgarna har en öppen fråga ställts i undersökningen om i vilka situationer intervjupersonerna är oroliga för hur deras personuppgifter används. Vanliga situationer där människor uppger att de känner oro för hur deras personuppgifter används är till exempel vid bankärenden eller inköp på nätet.

”Att mina personuppgifter ska användas när det gäller bedrägerier”.

”När det gäller känsliga uppgifter eller bankortinformation”.

”Bankärenden på nätet”.

Oron för att finansiella uppgifter ska hamna i orätta händer återspeglas när intervjupersonerna fått rangordna vilken typ av personuppgifter de anser är känsligast att olika verksamheter samlar in. Finansiell information som till exempel kontokortsuppgifter anses allra känsligast av flest.

Även hälsouppgifter kommer högt i rangordningen av vilken typ av personuppgifter som anses särskilt känsliga. Något färre tycker att identifiering via digital teknik som till exempel ansiktsigenkänning är särskilt

känslig, likaså personliga fotografier och filmer samt surfdata som beskriver vilka sajter en person besökt.

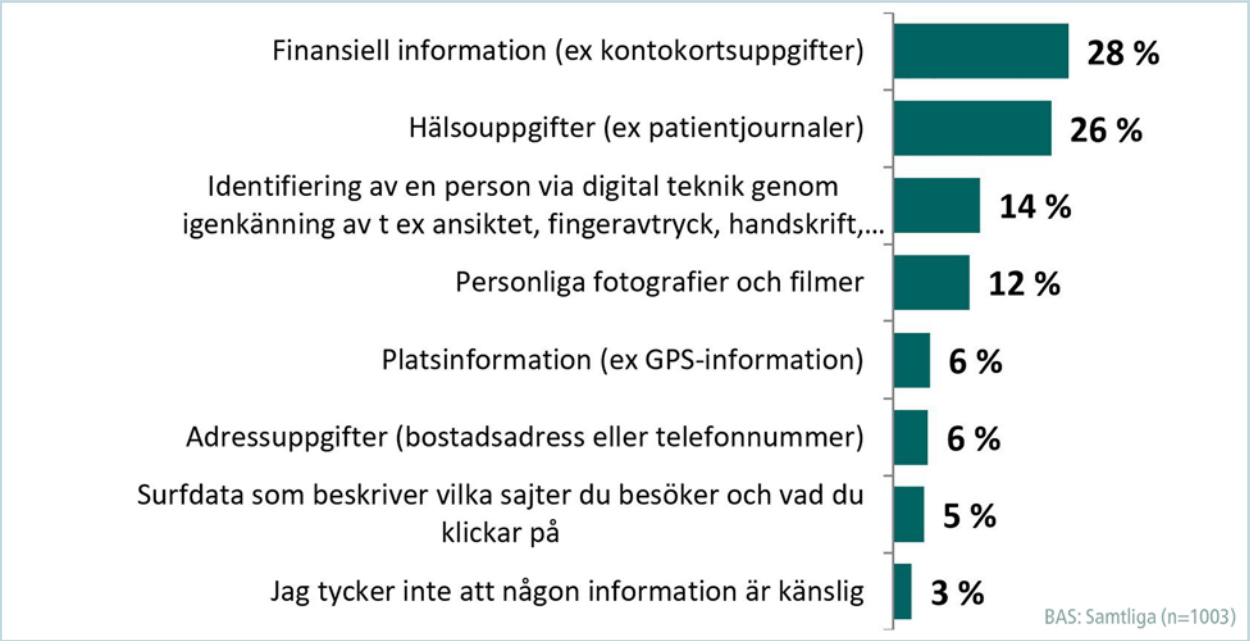

Bild 6. Fråga: Vilken typ av personuppgifter tycker du är särskilt känsliga att företag, myndigheter och organisationer samlar in och använder?

Ett antal frågor har också ställts om specifika situationer, där de medverkande i undersökningen fått uppge om de känner oro. Störst är oron för att drabbas av olagligt intrång där till exempel ”hackare”, kriminella eller andra obehöriga kan komma åt personuppgifter. Drygt hälften, 52 procent, uppger att de känner mycket eller ganska stor oro över detta.

Andra situationer där medborgarna känner mycket eller ganska stor oro handlar om

- att inte ha kontroll över hur personuppgifterna används (40 procent känner mycket eller ganska stor oro)
- att internetvanor och surfbeteende registreras och säljs vidare till andra företag i syfte att anpassa reklam (39 procent känner mycket eller ganska stor oro)
- att appar i mobilen kan innebära att företag kan följa hur individer fysiskt förflyttar sig (37 procent känner mycket eller ganska stor oro)
- att en anställd inom en myndighet eller ett företag tar del av personuppgifter i annat syfte än att utföra sitt arbete (32 procent känner mycket eller ganska stor oro)
- att personuppgifter delas eller förs vidare till andra företag eller myndigheter (31 procent känner mycket eller ganska stor oro).

Intrycket att relativt många upplever det som olustigt att inte ha kontroll över hur personuppgifterna används förstärks i de öppna svarsalternativen. Flera kommenterar att de känner oro för att deras personuppgifter ska säljas vidare och hamna i orätta händer. Återkommande i de öppna svarsalternativen är också kommentarer om riktad reklam, så kallad direktmarknadsföring.

”Dålig säkerhet som gör att uppgifter läcker ut”.

”Att de används i framtiden på ett sätt som jag inte tänkt på”

”För att kartlägga mig och då kunna manipulera vissa saker om mig”

”I marknadsföringssyfte, typ riktad reklam, när det profiteras på uppgifterna”.

Högst förtroende för vården, myndigheter och banker – lägst för sökmotorer, sociala medier och appar

Skillnaderna är stora mellan de verksamheter som har störst respektive lägst förtroende när det gäller hantering av personuppgifter. Störst förtroende har medborgarna för vård, myndigheter och banker, som cirka sex av tio uppger att de har mycket stort eller ganska stort förtroende för.

Lägst förtroende har sökmotorer, sociala medier och appar, där endast ett fåtal uppger att de har stort förtroende för verksamheternas personuppgiftshantering.

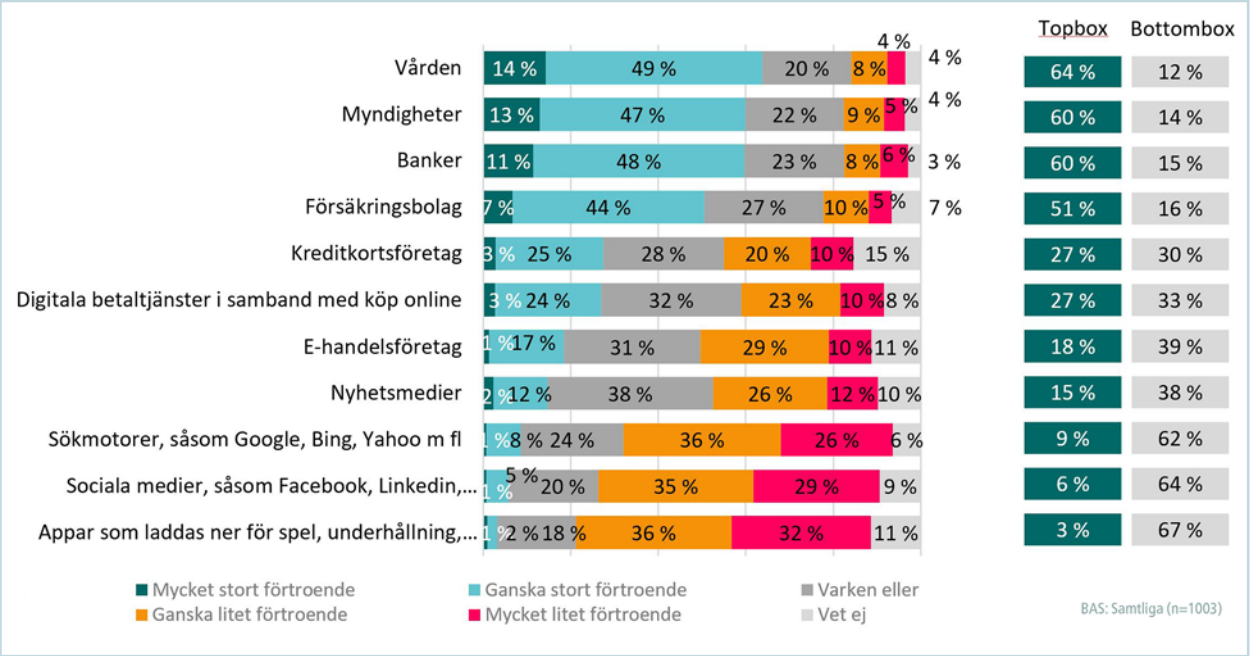

Bild 7. Fråga: Hur stort är ditt förtroende för följande aktörer när det gäller deras hantering av dina personuppgifter? (Topbox innebär mycket

eller ganska stort förtroende. Bottombox innebär ganska litet eller mycket litet förtroende).

Samtidigt som medborgarna har störst förtroende för personuppgiftshanteringen inom vården, myndigheter och banker är det bara ungefär hälften som anser att dessa verksamheter är bra på att informera om hur de använder personuppgifter.

Sämst på att informera anses nyhetsmedier, sökmotorer och appar, där endast cirka tio procent anser att de är bra på att informera om hur de använder personuppgifter.

Medborgarnas kännedom om dataskyddsförordningen och vad regelverket innebär

- **En stor majoritet av medborgarna känner på en övergripande nivå till dataskyddsförordningen** och att regelverket innehåller förstärkta rättigheter
- **Mest välkänd är rätten till information, som tre av fyra uppger att de känner till.** Kännedomen om vilka rättigheter som finns varierar dock kraftigt. Minst känd är rätten att få personuppgifter återlämnade eller överförda till ett annat företag, så kallad dataportabilitet. Endast en av fyra uppger att de känner till rättigheten.
- **Kännedomen om rättigheterna är ojämnt fördelad i befolkningen.** Störst kännedom om rättigheterna i förordningen har personer mellan 30 och 49 år med universitets- eller högskoleutbildning.

Åtta av tio känner till både dataskyddsförordningen och rättigheterna

Ett viktigt syfte med dataskyddsförordningen är att stärka individens rättigheter när det gäller hur personuppgifter hanteras. Regelverket kan hjälpa den enskilde att ta kontrollen över hur personuppgifterna får användas.

En grundläggande förutsättning för att kunna utöva sina rättigheter är att känna till att de finns. Dataskyddsförordningen fick under 2018 stor massmedial uppmärksamhet. Floden av e-postbrev där människor ombads samtycka till fortsatt personuppgiftsbehandling bidrog också till att sätta det nya regelverket på kartan.

Knappt ett år efter att förordningen började gälla visar Datainspektionens undersökning att medborgarna i stor utsträckning känner till den nya förordningen och vad den innebär. Drygt åtta av tio intervjupersoner känner till dataskyddsförordningen, och knappt hälften svarar att de känner till förordningen ganska eller mycket bra. Endast två procent har inte hört talas om förordningen.

Det finns signifikanta skillnader mellan olika grupper när det gäller kännedom om förordningen. Personer i åldrarna 30–49 år och universitets- och högskoleutbildade känner i högre utsträckning till förordningen.

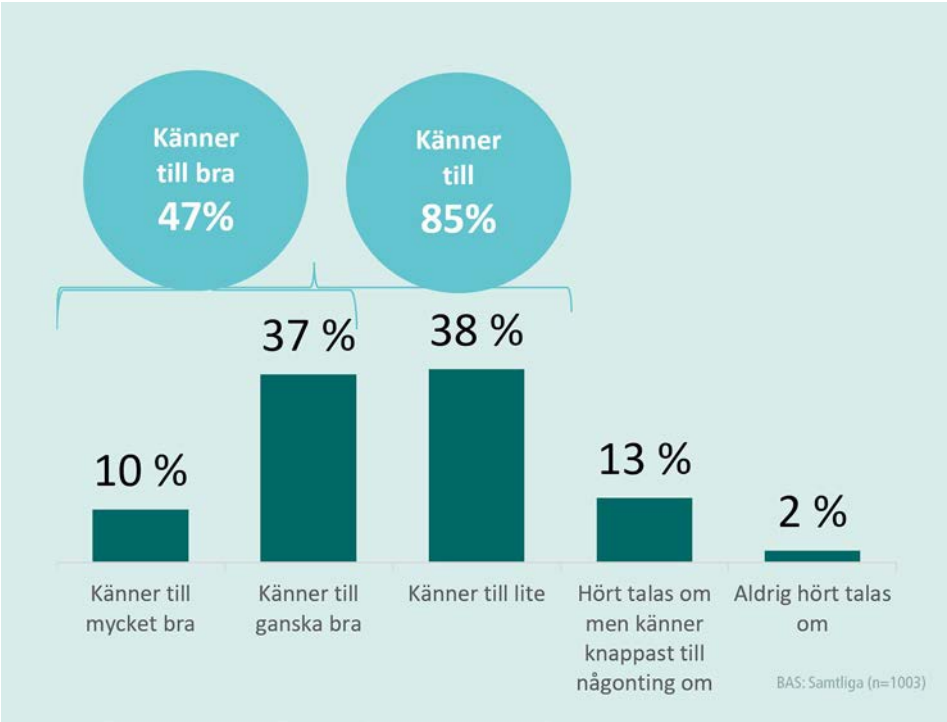

Bild 8. Fråga: Hur väl känner du till den nya dataskyddsförordningen och vad den innebär?

Medborgarna känner också i stor utsträckning till att förordningen ger individerna specifika rättigheter när det gäller att skydda sina personuppgifter. Drygt åtta av tio känner till att rättigheterna finns, och fyra av tio uppger att de känner till dem ganska eller mycket bra.

Även när det gäller kännedomen om rättigheterna syns skillnader mellan olika demografiska grupper. Personer i åldrarna, 30–49 år, och universitets- och högskoleutbildade känner i högre grad till bra eller mycket bra att rättigheterna finns.

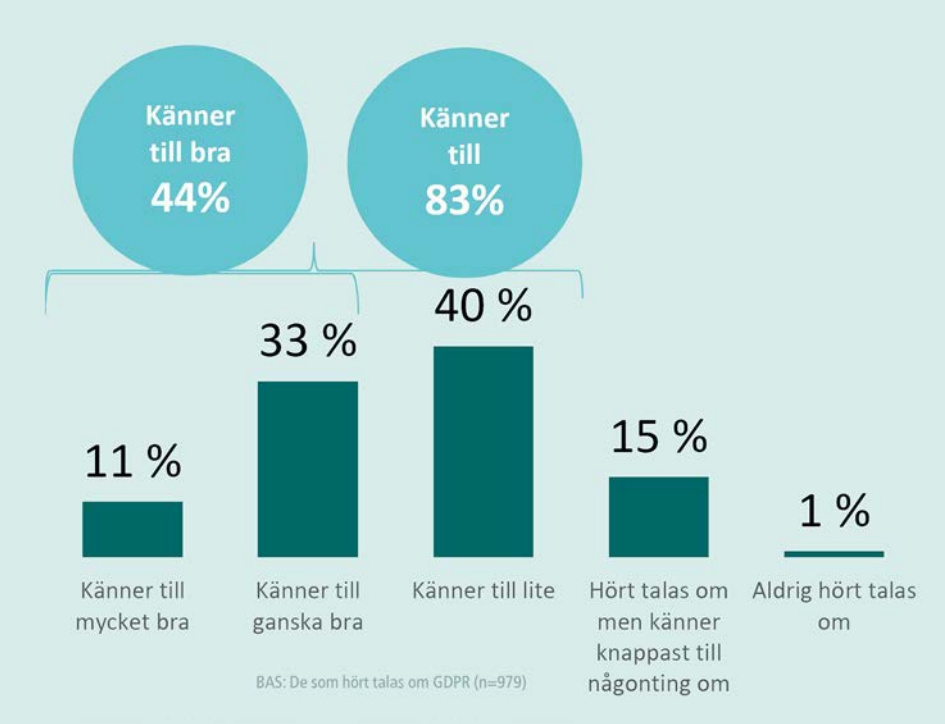

Bild 9. Fråga: I vilken utsträckning känner du till att GDPR ger dig specifika rättigheter när det gäller att skydda dina personuppgifter?

Rätten till information är den mest kända rättigheten

På en övergripande nivå finns alltså en hög kännedom om att dataskyddsförordningen finns och att den omfattar ett antal förstärkta rättigheter. Medborgarnas kunskap om vilka rättigheterna är varierar dock.

Rätten till information tycks ha fått störst genomslag. Ungefär tre av fyra uppger att de känner till rätten att få veta vilka personuppgifter en verksamhet har om en individ och hur uppgifterna används. Sannolikt har det stora antalet e-postmeddelanden där medborgare ombetts samtycka till fortsatt personuppgiftshantering eller informerats om en personuppgiftspolicy bidragit till att sätta rätten till information på kartan.

Något mindre kända är rättigheterna som rör rättelse, radering och begränsning. Ungefär hälften av medborgarna uppger att de känner till rättigheterna att i vissa fall be en organisation radera personuppgifter, invända mot eller under vissa omständigheter begränsa hur personuppgifter används.

De minst kända rättigheterna är rätten till rättelse och rätten till dataportabilitet. Lite mer än en tredjedel känner till rätten att utan onödigt dröjsmål få felaktiga personuppgifter rättade. När det gäller rätten att få personuppgifter återlämnade eller överförda till ett annat

företag, så kallad dataportabilitet, uppger endast en fjärdedel att de känner till det.

Kunskapen om vilka rättigheter som finns är även här större i åldrarna 30–49 år, samt bland universitets- och högskoleutbildade.

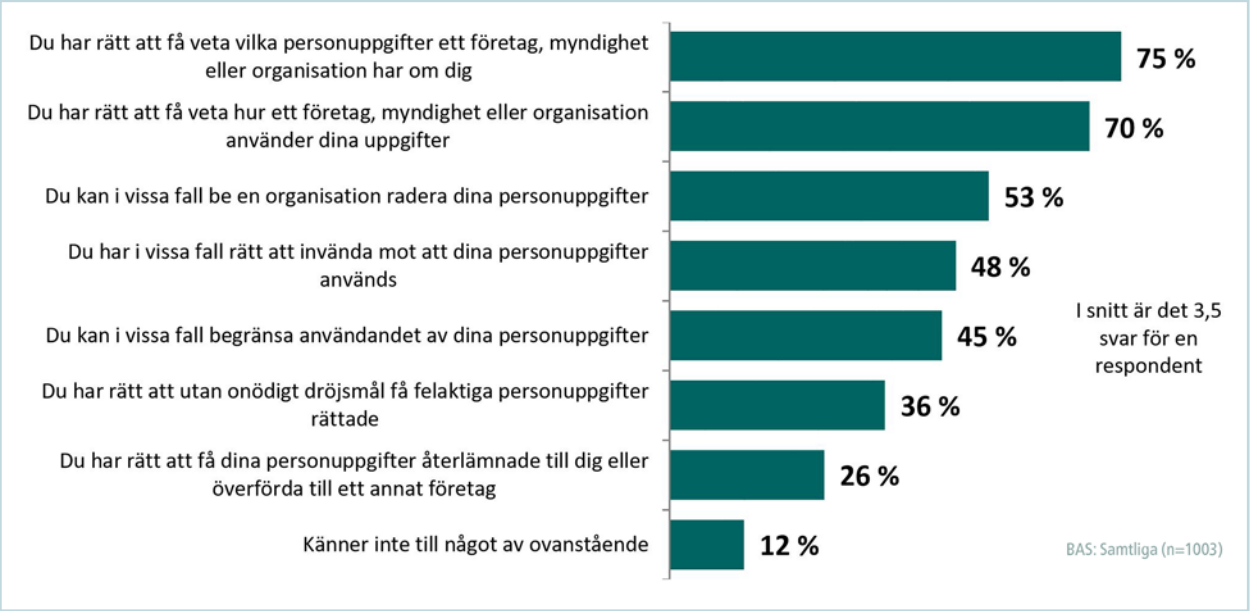

Bild 10. Fråga: Markera vilka av följande rättigheter du känner till när det gäller hur företag, myndigheter och organisationer använder dina personuppgifter?

Aktiva åtgärder för att skydda sin integritet

- **Nästan sex av tio läser sällan eller aldrig användarvillkoren** när de registrerar sig på en sajt eller laddar ned en app. En något mindre andel, två av fem, läser alltid eller ibland villkoren.
- **Det finns en medvetenhet om att skydda sina personuppgifter. Drygt hälften uppger att de gör aktiva val** för att hindra att surfvanor och surfbeteende samlas in när de använder internet. Ungefär lika stor andel uppger att de ibland eller ofta avstår från att använda en digital tjänst för att de känner osäkerhet om hur personuppgifterna kommer att användas.
- **Olika demografiska grupper har olika strategier för att skydda sin integritet.** Yngre personer och män är överrepresenterade bland dem som i större utsträckning gör aktiva val för att undvika att surfvanor samlas in. Kvinnor och äldre personer väljer i större utsträckning att avstå från att använda en tjänst om de känner osäkerhet kring hur deras personuppgifter kommer att hanteras.
- **Var sjätte medborgare har använt någon av de rättigheter som regleras i dataskyddsförordningen.** Ytterligare en sjättedel har funderat på att använda någon av rättigheterna. Yngre medborgare har i större utsträckning använt sina rättigheter. Bland personer mellan 18 och 29 år uppger drygt en femtedel att de använt någon av sina rättigheter.

Över hälften läser väldigt sällan eller aldrig användarvillkor

Som framkommit tidigare är det förhållandevis få medborgare som upplever att verksamheter är bra på att informera om hur de använder personuppgifter. Samtidigt är medborgarna generellt sett inte särskilt bra på att läsa användarvillkoren när de registrerar sig på en sajt eller laddar ned en app.

Nästan en av fyra läser aldrig användarvillkoren vid registrering på en sajt. Ytterligare en dryg tredjedel uppger att det förekommer att de läser användarvillkor, men väldigt sällan.

Kvinnor och äldre personer i åldrarna 50–64 år och 65–79, är överrepresenterade bland dem som i större utsträckning läser användarvillkor. Även personer som känner oro för hur deras personuppgifter används läser oftare användarvillkor.

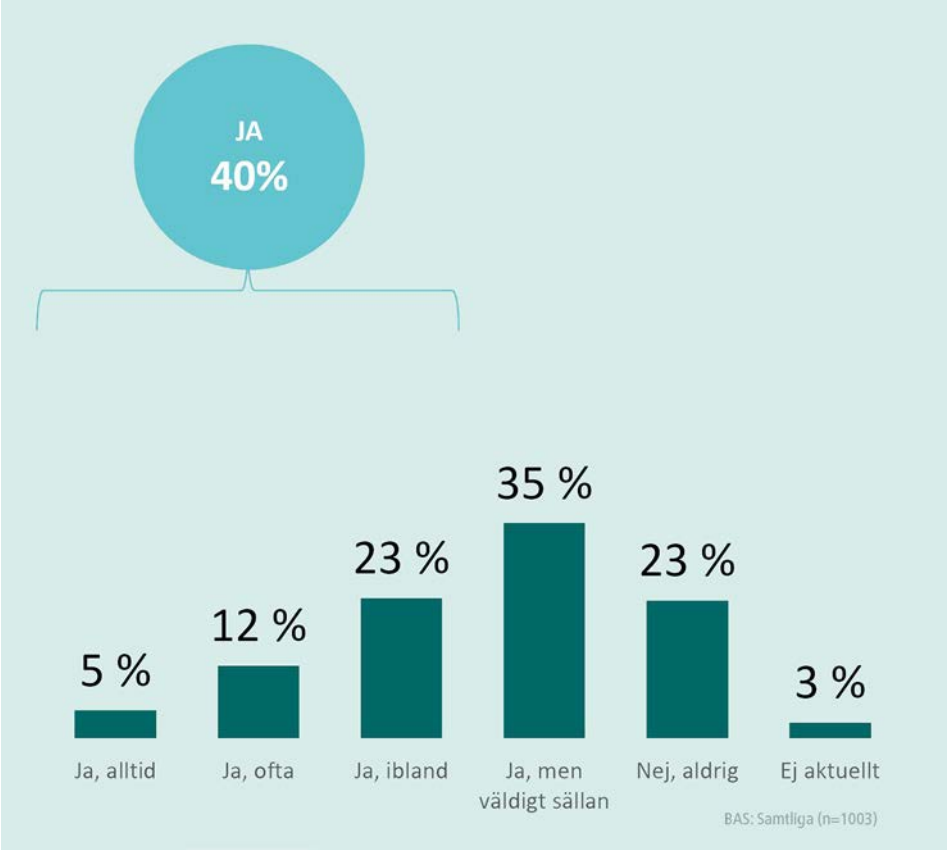

Bild 11. Fråga: Läser du användarvillkoren när du registrerar dig på en sajt eller laddar ner en app?

Drygt hälften gör aktiva val för att hindra att deras internetvanor ska samlas in

Drygt hälften gör ibland eller alltid aktiva val för att förhindra att deras surfvanor och surfbeteende samlas in och används.

Män och yngre personer i åldern 18–29 gör i högre utsträckning aktiva val för att hindra att surfvanor och surfbeteende samlas in. Även personer som känner oro för hur deras personuppgifter används gör i större utsträckning aktiva val.

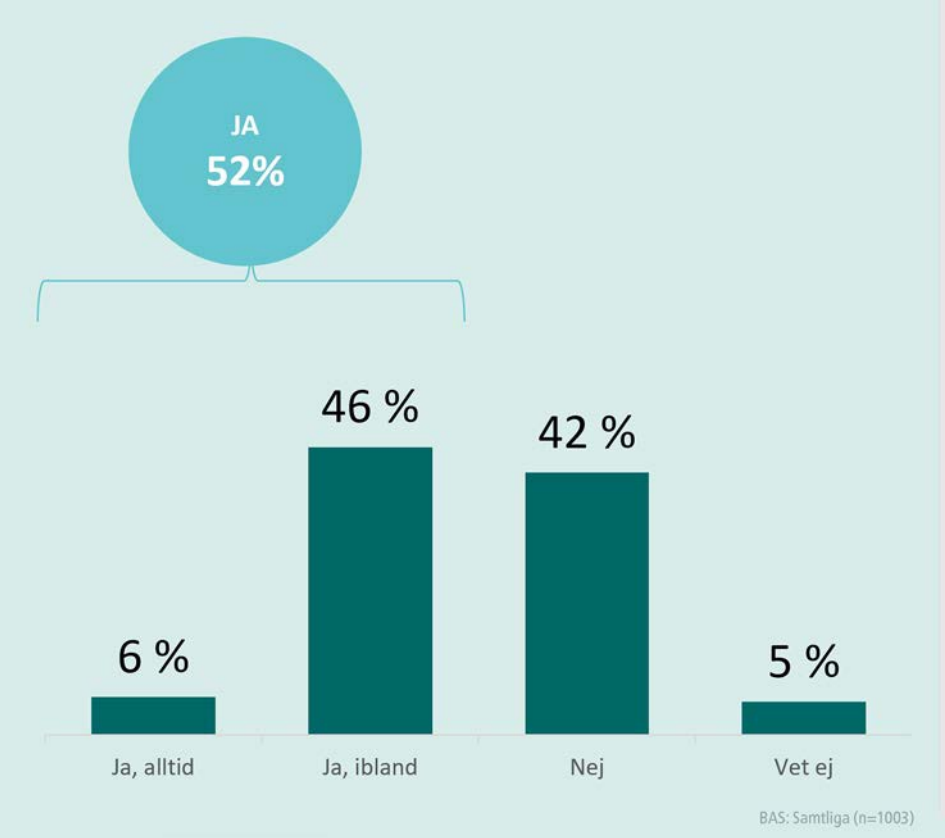

Bild 12. Fråga: Gör du aktiva val för att hindra att dina surfvanor och ditt surfbeteende samlas in när du använder internet?

Bland de som inte gör några aktiva val för att förhindra att deras surfvanor och surfbeteende samlas in finns en stor okunskap. Sju av tio uppger att de inte vet vilka aktiva val de kan göra för att begränsa insamlingen av surfvanor.

Åldersgruppen 65–79 år, liksom personer som känner oro, känner i högre grad inte till vilka aktiva val de kan göra.

Hälften avstår ofta eller ibland från att använda en digital tjänst på grund av osäkerhet kring hur personuppgifterna kommer att användas

Om medborgare känner osäkerhet avseende hur ens personuppgifter kommer att användas är ett av de yttersta sätten att skydda sin integritet att faktiskt avstå från att använda en tjänst. Nästan hälften av medborgarna uppger att de ofta eller ibland avstår från att använda digitala tjänster på grund av osäkerhet kring hur personuppgifterna används.

Mindre vanligt är att avstå från att använda en tjänst efter en personlig kontakt med ett företag, en myndighet eller en organisation.

Omkring en tredjedel av medborgarna har dock ofta eller ibland avstått från att använda en tjänst vid personlig kontakt med en verksamhet för att de är osäkra på användning av personuppgifterna.

Personer som känner oro är för hur deras personuppgifter används är mer benägna att avstå från att använda digitala tjänster om de känner osäkerhet kring hur deras personuppgifter kommer att användas. Detta mönster följer svaren hos dem som vidtar aktiva åtgärder för att förhindra att deras surfvanor och surfbeteende samlas in – även där är personer som känner oro överrepresenterade.

Undersökningen visar att olika demografiska grupper i befolkningen har olika strategier för att skydda sin integritet. Medan yngre personer och män är överrepresenterade bland dem som i större utsträckning vidtar aktiva åtgärder för att undvika att surfvanor samlas in, är det fler kvinnor och äldre personer som väljer att avstå från att använda en tjänst om de känner osäkerhet kring hur deras personuppgifter kommer att användas.

Grupper som i högre grad avstår från att använda en digital tjänst utgörs av personer i åldrarna 65–79 år, samt kvinnor.

Grupper som i högre grad avstår att använda en tjänst vid personlig kontakt med verksamheter utgörs av personer i åldrarna 65–79 och 50–64 år.

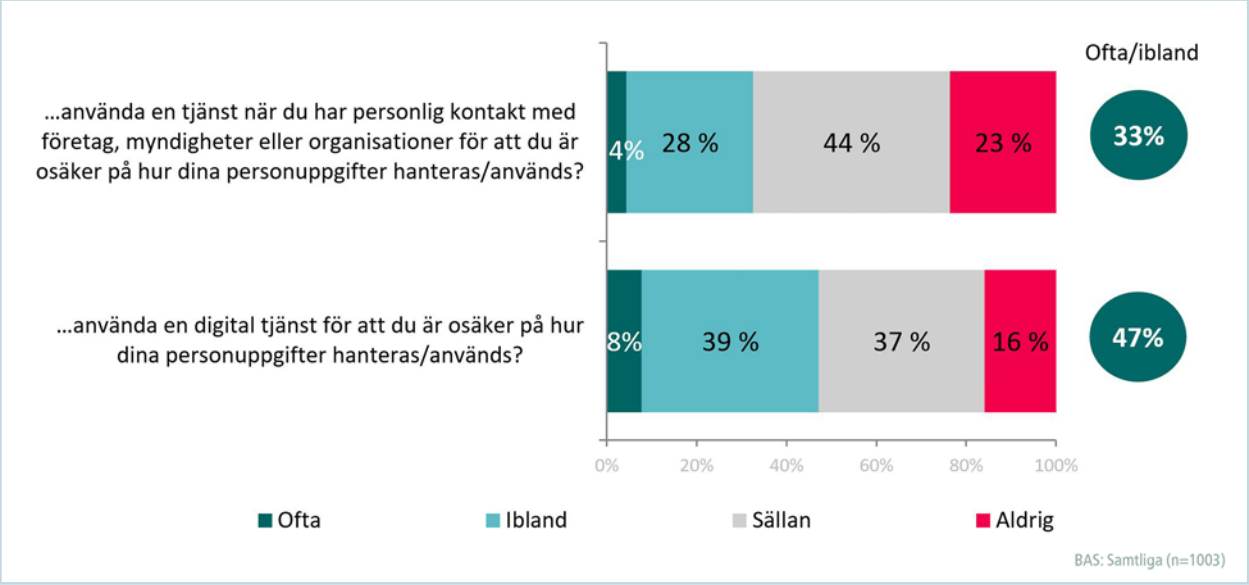

Bild 13. Fråga: Hur ofta händer det att du avstår från något av följande?

Osäkerhet kring användning av personuppgifter styr när en tjänst väljs bort

Eftersom hälften av medborgarna ofta eller ibland avstår från att använda en digital tjänst på grund av osäkerhet kring hur personuppgifterna

används är det intressant att fördjupa analysen av vad som gör att en tjänst väljs bort. Datainspektionen har därför ställt en öppen fråga om vad som krävs för att personer ska avstå från att använda en tjänst för att de är osäkra på hur personuppgifterna kommer att användas.

Bland de vanligaste anledningarna till att avstå från att använda en tjänst är att aktören upplevs som oseriös och att informationen är bristfällig, vilket skapar misstänksamhet. Återkommande bland svaren är också att det inte känns bra att lämna ut hela sitt personnummer eller att för mycket personlig information efterfrågas. För många räcker det med en känsla av osäkerhet för att avstå från att använda tjänsten. Magkänslan styr således i hög grad när en tjänst väljs bort.

”Dålig information från första början, eller luddig, oseriös sida med dåligt språk”.

”När det inte känns relevant med efterfrågad information”.

”Det räcker med att jag är osäker, för att jag ska avstå”.

”Att de frågar efter mitt kontonummer”.

”Intuition och magkänsla”.

Var sjätte medborgare har utnyttjat någon av rättigheterna i dataskyddsförordningen

Ett aktivt sätt för medborgare att skydda sin integritet är att utöva de rättigheter som finns i dataskyddsförordningen. Det kan handla om till exempel att begära ett registerutdrag för att få veta vilka personuppgifter ett företag, myndighet eller organisation har och hur de används.

Ungefär var sjätte medborgare, 16 procent, har utnyttjat någon av de rättigheter som regleras i dataskyddsförordningen. Ytterligare drygt en sjättedel, 18 procent, har funderat på att använda någon av rättigheterna. När medborgare använt en rättighet eller funderat på att använda den, handlar det oftast om invändningar mot hur personuppgifter används eller begäran om att en organisation ska radera personuppgifter.

Bland de som har använt någon av rättigheterna är yngre personer i åldern 18–29 år överrepresenterade. Drygt två av tio, 22 procent, i åldern 18–29 uppger att de använt minst en av rättigheterna.

Personer i åldern 30 till 49 år är överrepresenterade bland dem som uppger att de funderat på att begära information om hur ett företag, myndighet eller organisation använder personuppgifter.

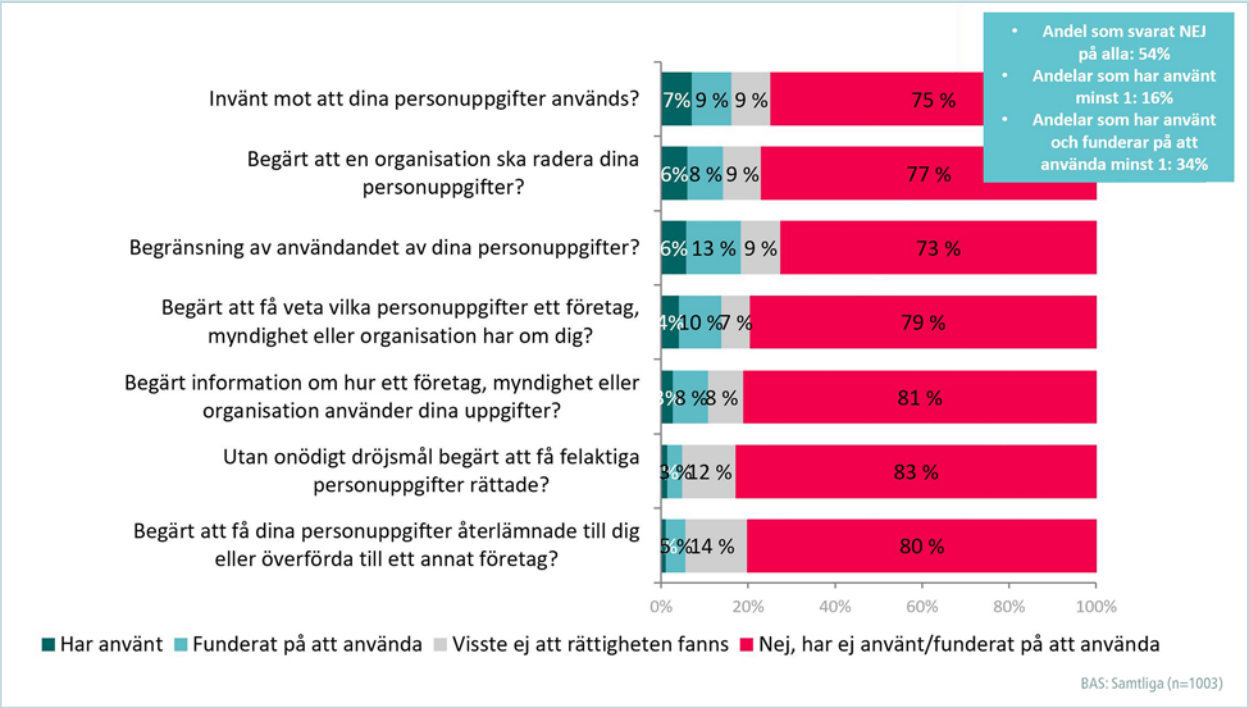

Bild 14. Fråga: Har du använt, eller funderat på att använda, någon av dina rättigheter i dataskyddsförordningen GDPR när det gäller att skydda dina personuppgifter under de senaste 12 månaderna?

Vilka frågor ställer medborgare till Datainspektionen?

- **Omkring en fjärdedel av frågorna till Datainspektionen handlar om att medborgare ifrågasätter om en specifik personuppgiftsbehandling är laglig.** Återkommande områden är till exempel direktmarknadsföring och arbetsgivares hantering av anställdas personuppgifter.
- **Cirka en fjärdedel av alla frågor som medborgare ställer till Datainspektionen handlar om rätten till radering.** Den enskilt vanligaste frågan rör hur man som privatperson gör för att få bort personuppgifter från sajter med utgivningsbevis, till exempel Eniro, Hitta, Lexbase, Mr Koll, Ratsit och Merinfo.
- **Ungefär en tiondel av alla frågor från medborgare handlar om kamerabevakning.**
- **Andra vanliga frågor rör rätten till information via registerutdrag**, rätten till rättelse och vilka säkerhetsåtgärder som är nödvändiga vid en viss typ av personuppgiftsbehandling.

De medborgare som hör av sig med frågor till Datainspektionen kan antas ha en större medvetenhet om integritetsrisker och rättigheter än genomsnittet av befolkningen. För att ge en bild av vilka frågor som kan aktualiseras hos dem som mer aktivt arbetar med att skydda sin integritet ges i detta avsnitt en beskrivning av de frågor som medborgare ställer till Datainspektionen.

Datainspektionen hanterar årligen en stor mängd frågor från privatpersoner och verksamheter via myndighetens upplysningstjänst. Under perioden 25 maj 2018 till 23 april 2019 har cirka 8 200 frågor kommit in och besvarats via e-post, och ungefär samma antal, 8 100, har besvarats via telefonsamtal. I storleksordningen hälften av det totala antalet frågor, såväl via telefon som via e-post, bedöms komma från privatpersoner. Övriga frågor kommer från företag, myndigheter och andra organisationer som hanterar personuppgifter.

Nedan ges en översikt av de vanligaste skriftliga frågorna från privatpersoner som kommit in till Datainspektionen under perioden 25 maj 2018–10 april 2019. Datainspektionen har i nuläget ingen heltäckande statistik av vilka frågeområden som är mest frekvent förekommande i inflödet till myndigheten. För att kvantifiera hur vanliga olika typer av frågor är har därför ett slumpmässigt urval av 200 frågor från privat-

personer som kommit in via e-post analyserats.[9] Sammanställningen har sedan diskuterats i intervjuer och workshops med medarbetare inom Datainspektionen som har stor erfarenhet av att dagligen besvara frågor från medborgare.

Ungefär 70 procent av det totala antalet frågor som medborgare ställer till Datainspektionen bedöms röra privata företag. I den resterande delen gäller ungefär fem procent vardera hälso- och sjukvården, statliga myndigheter och ideella organisationer.

Ungefär var fjärde fråga till Datainspektionen handlar om rätten till radering

Rätten till radering är en av de mest frekventa frågeställningar som privatpersoner hör av sig till Datainspektionen om. Vanliga frågor gäller till exempel att ett företag har kvar personer i sina register trots att kundrelationen är avslutad sedan länge. Det framförs även frågor kring möjligheterna att bestämma vilka verksamheter som ska få spara personuppgifter.

Ytterligare vanliga frågor är hur träffar vid sökning på eget personnamn i sökmotorer kan tas bort och om verksamheter kan vägra att radera uppgifter som medborgaren inte anser att de har rätt att spara. Medborgarna känner inte alltid till att företag kan ha andra lagstadgade skyldigheter att spara personuppgifter, till exempel genom bokföringslagen.

Den enskilt vanligaste frågan till Datainspektionen från medborgare handlar om hur man gör för att få sina personuppgifter raderade från sajter som har så kallade frivilliga utgivningsbevis, till exempel Eniro, Hitta, Lexbase, Mr Koll, Ratsit och Merinfo. Omkring en av tio frågor till myndigheten från privatpersoner handlar om sajter med utgivningsbevis. Många upprörda medborgare känner sig kränkta av publiceringen av omfattande uppgifter om dem. Totalt har Datainspektionen hanterat över 1500 frågor som rör utgivningsbevis under året.

Cirka var fjärde fråga ifrågasätter lagligheten i en viss personuppgiftsbehandling

Ytterligare omkring en fjärdedel av frågorna från medborgare till Datainspektionen handlar om att lagligheten i en specifik personuppgiftsbehandling ifrågasätts. Ofta beskriver frågeställaren en konkret situation där dennes personuppgifter behandlats och undrar om hanteringen är tillåten.

9 100 av frågorna har besvarats i upplysningstjänsten. 100 av frågorna i urvalet har rört mer komplicerade frågor som besvarats av sakenheterna på Datainspektionen.

Om en specifik personuppgiftsbehandling är laglig eller inte beror bland annat på vilken rättslig grund verksamheten stödjer sig på för behandlingen. Hos en del medborgare finns missuppfattningen att personuppgiftshantering alltid kräver samtycke, de övriga rättsliga grunder som en personuppgiftsbehandling kan stödjas på är, av förklarliga skäl, mindre kända hos medborgare.

Frågor om direktmarknadsföring är återkommande. En vanlig fråga är om det är lagligt att företag och organisationer använder personuppgifter utan individens samtycke, till exempel för reklamutskick via mejl.

Andra återkommande frågor handlar om arbetsgivares behandling av anställdas personuppgifter. Exempel på frågor kan vara att en anställd undrar om arbetsgivaren har rätt att kontrollera den anställdes in- och utloggningstider avseende arbetspass för att säkerhetsställa att arbetstiderna hålls.

Cirka en av tio frågar om vilka säkerhetsåtgärder som krävs vid personuppgiftshantering

Genom dataskyddsförordningen har kraven skärpts på olika typer av säkerhetsåtgärder i samband med personuppgiftshantering. Frågor om vilken typ av säkerhetsåtgärder som krävs är återkommande från medborgare. Det kan både handla om att medborgare upplever att säkerheten är tillfredsställande, men också att till exempel krav på kryptering och tvåfaktorsautentisering leder till att medborgare upplever att det är komplicerat att få tillgång till sina uppgifter till exempel hos myndigheter.

Ungefär en av tio frågor handlar om kamerabevakning

Kamerabevakning är ytterligare ett av de områden som genererar flest frågor från medborgare till Datainspektionen. Ungefär var tionde fråga handlar om kamerabevakning. Det finns ett tydligt behov bland medborgare att förstå förutsättningarna på området.

En stor del av frågorna handlar om privatpersoners kamerabevakning, till exempel vad som får bevakas i det egna hemmet och om det är lagligt att ha kameror uppsatta på en privat bostad som även täcker en del av grannens tomt. Exempel på andra typer av frågor om kamerabevakning är om hyresvärden får kamerabevaka trappuppgången eller tvättstugan, om en restaurang får filma gatan utanför restaurangen och i vilka situationer tillstånd behövs.

Vanligt med frågor om rätten att få information genom registerutdrag

Inflödet av frågor från medborgare till Datainspektionen bekräftar bilden att rättigheten att få information är en förhållandevis välkänd rättighet. I storleksordningen en av femton frågor som privatpersoner ställer till Datainspektionen handlar om rätten att via ett registerutdrag få ut information om vilka personuppgifter en verksamhet har om en och hur de används.

Vanliga frågor är till exempel vilka uppgifter privatpersoner har rätt att ta del av, om det finns några begränsningar avseende uppgifter som lämnas ut samt leveranstid för registerutdraget.

Återkommande är också att privatpersoner kontaktat ett företag och begärt registerutdrag, varpå företaget begärt att frågeställaren legitimerar sig. Det är inte ovanligt att den enskilde ifrågasätter kravet på identifiering och hör av sig till Datainspektionen för att få vägledning.

…men också många övriga frågor

Slutligen finns en relativt stor grupp av frågor från medborgare som är svåra att kategorisera. Det kan röra sig om frågor om till exempel rätten till rättelse eller personuppgiftsincidenter.

Andra frågor rör endast delvis eller inte alls dataskyddsförordningen, till exempel identitetskapning. Ytterligare exempel kan handla om dataskyddsombudens roll och funktion, vem inom ett företag som är personuppgiftsansvarig, och vad som gäller för ostrukturerade personuppgifter i förhållande till förordningen.

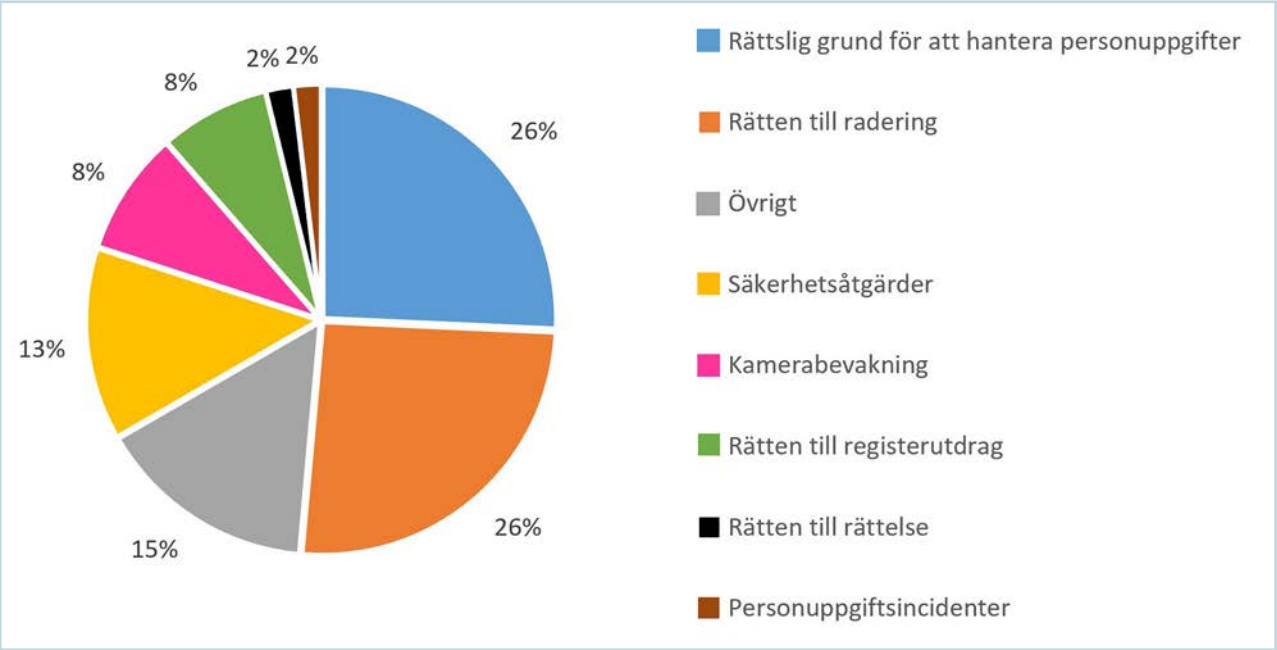

Bild 15. Frågeområden – privatpersoner.

Vad rör klagomålen som kommer in till Datainspektionen?

- **Vanligaste klagomålet till Datainspektionen handlar om sajter med utgivningsbevis.** Nästan en tredjedel av klagomålen rör webbplatser som till exempel Eniro, Hitta, Lexbase, Mr Koll, Ratsit och Merinfo som publicerar en stor mängd personuppgifter om enskilda medborgare på nätet.
- **Cirka var femte klagomål handlar om lagligheten i en viss personuppgiftsbehandling.** Återkommande är till exempel klagomål som handlar om att verksamheter samlar in personnummer, medan medborgaren anser att det borde räcka med kontaktuppgifter.
- **Andra vanliga klagomål rör rätten till radering, direktmarknadsföring, kamerabevakning och otillräckliga säkerhetsåtgärder.** Dessa kategorier står för omkring 10 procent vardera av det totala antalet klagomål.

Medborgare som anser att någon behandlat personuppgifter på ett sätt som strider mot dataskyddsförordningen kan klaga till Datainspek-

tionen. Under perioden 25 maj 2018 till 23 april 2019 har Datainspektionen tagit emot cirka 3 100 klagomål som rör dataskydd.[10] Omkring 80 procent av klagomålen rör privata aktörer. Statliga myndigheter och kommuner står för omkring fem procent vardera av klagomålen.

Det är inte alltid uppenbart vad som skiljer en fråga från ett klagomål – gemensamt för båda kategorierna är ofta att medborgaren är upprörd över det sätt som personuppgifter hanterats. En viktig distinktion är dock att klagomål alltid handlar om att medborgarens egna personuppgifter behandlats felaktigt. Dataskyddsförordningen reglerar också att den som anmäler ett klagomål till Datainspektionen har rätt att inom rimlig tid få besked om hur undersökningen fortskrider och resultatet av undersökningen.

Nedan ges en översikt av de vanligaste klagomålen som kommit in till Datainspektionen under perioden 25 maj 2018–10 april 2019[11].

Vanligaste klagomålet handlar om sajter med utgivningsbevis

Nästan en tredjedel av de klagomål som inkommit till Datainspektionen under dataskyddsförordningens första år rör sajter med så kallat frivilligt utgivningsbevis. Det handlar om webbplatser som till exempel Eniro, Hitta, Lexbase, Mr Koll, Ratsit och Merinfo som publicerar en stor mängd personuppgifter om enskilda medborgare på nätet.

Dessa sajter har ett så kallat frivilligt utgivningsbevis vilket gör att de i princip är undantagna från dataskyddsförordningens regler. Sedan 2003 kan en innehavare av en databas få grundlagsskydd för databasen genom att ansöka om utgivningsbevis. Utgivningsbevis utfärdas av Myndigheten för press, radio och tv och gäller i tio år. För att ett utgivningsbevis ska utfärdas krävs bland annat att en utgivare har utsetts, att besökaren själv måste uppsöka databasen och att den är tillgänglig för allmänheten. Det ställs däremot inte upp några krav på att verksamheten ska ha ett visst innehåll eller syfte.

Svaret är med andra ord att medborgare kan begära att få sina personuppgifter raderade, men att sajterna inte har någon skyldighet att ta bort dem. Eftersom sajter med utgivningsbevis genom den avgränsning som gjorts i svensk lag i princip är undantagna från dataskyddsförordningens bestämmelser har Datainspektionen mycket begränsade möjligheter att bidra till att få personuppgifterna borttagna.

10 I denna sammanställning ingår klagomål som rör dataskyddsförordningen, brottsdatalagen, kamerabevakningslagen och den tidigare kameraövervakningslagen.

11 Kvantifiering av de vanligaste klagomålen har skett genom ett slumpmässigt urval av 100 klagomål under perioden. Sammanställningen har därefter kvalitetssäkrats i intervjuer och workshops med medarbetare som har stor erfarenhet av att hantera klagomål.

Cirka var femte klagomål handlar om lagligheten i en viss personuppgiftsbehandling

Ett stort antal klagomål handlar om att lagligheten i en specifik personuppgiftsbehandling ifrågasätts. Om en specifik personuppgiftsbehandling är laglig beror bland annat på vilken rättslig grund som verksamheten stödjer sig på för personuppgiftsbehandlingen.

Återkommande är till exempel klagomål som handlar om att verksamheter sparar och använder privatpersoners personnummer, vilket den berörda medborgaren inte anser befogat. Att verksamheterna sparar namn och adress anses tillräckligt.

Var tionde klagomål handlar om direktmarknadsföring

Drygt var tionde klagomål till Datainspektionen rör direktmarknadsföring. Det kan till exempel handla om att företag fortsätter att via sms eller e-post skicka reklam, trots att den enskilde meddelat att den inte önskar någon marknadsföring. Vissa medborgare klagar också på att de får sms och e-postmeddelanden med reklam, trots att det inte lämnat något samtycke.

Var tionde klagomål rör rätten till radering

Ett vanligt scenario i de klagomål som anmäls till Datainspektionen är att företag har kvar, eller endast delvis har tagit bort personuppgifter i sina register, trots att den enskilde medborgaren begärt att uppgifterna ska raderas. Ungefär ett av tio klagomål rör rätten till radering.

I vissa fall har företagen överhuvudtaget inte svarat på begäran om att personuppgifter ska tas bort. Klagomålen kan också komma från medborgare som har begärt att sökmotorer på Internet ska ta bort specifika sökträffar på medborgarens namn, men uppgifterna har inte tagits bort. Sökträffarna som ska tas bort kan till exempel innehålla länkar till sajter med utgivningsbevis, eller till tidningsartiklar med inaktuell information.

Var tionde klagomål rör otillräckliga säkerhetsåtgärder

Omkring var tionde klagomål handlar om att medborgare anser att ett företag, myndighet eller annan organisation inte skyddar personuppgifterna på ett tillfredsställande sätt. Ofta anser medborgaren att det är för lätt att komma åt personuppgifterna och önskar att Datainspektionen ska kräva ökad säkerhet genom till exempel kryptering eller tvåfaktorsautentisering.

Var tionde klagomål handlar om kamerabevakning

När det gäller klagomål angående kamerabevakning handlar det i regel om bevakning av offentliga platser, till exempel gallerior. Klagomålen rör också i vissa fall arbetsgivares bevakning av de anställda. Medborgaren som kontaktar Datainspektionen tycker ofta att det är olustigt att vara övervakad i offentliga miljöer eller på arbetsplatsen. Totalt är det nästan ett av tio klagomål till Datainspektionen som rör kamerabevakning.

Övriga klagomål

Andra återkommande klagomål till Datainspektionen kan till exempel handla om specifika personuppgiftsincidenter, rätten till registerutdrag eller rätten till rättelse. Det är dock värt att notera att endast ett par procent av det totala antalet klagomål handlar om rätten till register-utdrag, vilket kan ses i ljuset av att de flesta både privata och offentliga verksamheter i Datainspektionens undersökning uppger att de har rutiner på plats för att lämna ut registerutdrag.

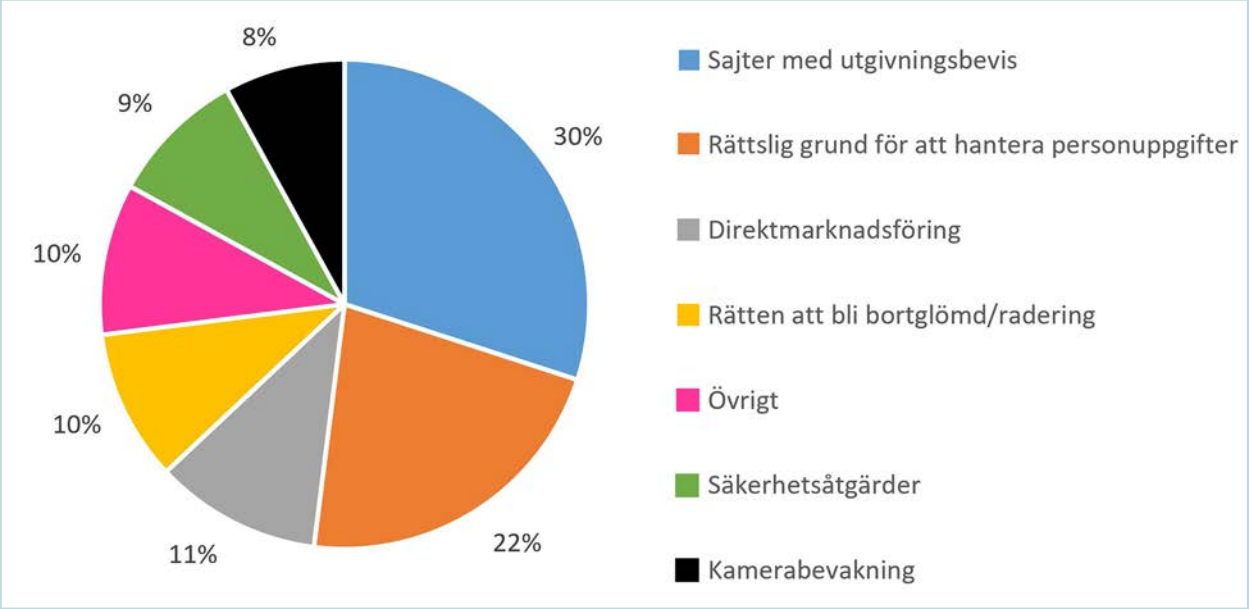

Bild 16. Klagomål – privatpersoner.

Integritet och dataskydd ur verksamheternas perspektiv

Företag, myndigheter och andra organisationer som hanterar personuppgifter

En röd tråd i GDPR är ett förstärkt skydd för individers grundläggande rättigheter i samband med att personuppgifter behandlas. Samtidigt som individens rättigheter förstärkts, har ansvaret för de företag, myndigheter och andra organisationer som hanterar personuppgifter skärpts. Verksamheter som hanterar personuppgifter måste sätta sig in i regelverken, följa dem och kunna visa vilka bedömningar som gjorts och åtgärder som vidtagits för att stärka skyddet av personuppgifter.

För att kartlägga hur långt verksamheterna kommit i sitt arbete med integritet och dataskydd har Datainspektionen genomfört två undersökningar som vänder sig till företag, myndigheter och andra organisationer som hanterar personuppgifter. Den ena undersökningen har riktats mot verksamheter som anmält till Datainspektionen att de utsett ett dataskyddsombud. Den andra undersökningen fokuserade på företag som inte utsett något dataskyddsombud.

Verksamheter som utsett ett dataskyddsombud

I och med att GDPR började gälla är alla myndigheter skyldiga att utse ett dataskyddsombud. Skyldigheten gäller även företag och andra verksamheter som har som kärnverksamhet att regelbundet, systematiskt och i stor omfattning övervaka enskilda personer eller behandla känsliga personuppgifter eller uppgifter om brott.

Vem som är dataskyddsombud ska meddelas till Datainspektionen. Det är svårt att säga hur stort det totala antalet verksamheter är som är skyldiga att utse ett dataskyddsombud, men totalt har Datainspektionen i maj 2019 fått in drygt 7 500 anmälningar om dataskyddsombud.

I undersökningen riktad mot verksamheter som utsett ett dataskyddsombud har totalt 1 687 webbintervjuer genomförts.[12] Merparten av frågorna syftade till att ge en bild av verksamheternas mognad inom integritet och dataskydd. Eftersom dataskyddsombuden

12 Undersökningen är genomförd via webbintervjuer av företaget Novus, på uppdrag av Datainspektionen. Urvalet består av registrerade dataskyddsombud hos Datainspektionen. Dataskyddsombud som är ansvariga för flera verksamheter har ombetts svara på enkäten två gånger – för två (slumpmässigt utvalda) verksamheter som de är dataskyddsombud för. Intervjuerna genomfördes under perioden 19 februari till 18 mars 2019. Svarsfrekvensen i undersökningen är 44 procent. Metoden beskrivs mer utförligt i en bilaga till denna rapport. Undersökningen i sin helhet finns på www.datainspektionen.se.

har en så viktig roll i att informera, ge råd och kontrollera organisationens dataskyddsarbete fokuserar en del av frågorna även på vilka förutsättningar dataskyddsombuden upplever att de har att arbeta med frågorna.

Av samtliga svar i undersökningen representerar ungefär hälften privata företag, cirka två av tio kommuner och ungefär en av tio vardera statliga myndigheter eller intresseorganisationer. Övriga svar kommer antingen från landstinget eller en annan typ av verksamhet. Av verksamheterna i undersökningen svarar 80 procent att de är skyldiga att ha ett dataskyddsombud, och knappt 20 procent har det frivilligt.

Diagrammen redovisar procentandelar. I de diagram där totala procentsatsen överstiger 100 procent har flera svarsalternativ varit möjliga.

Verksamheternas mognad i arbetet med integritet och dataskydd

- **Tre av fyra dataskyddsombud uppger att implementeringen av dataskyddsförordningen har fungerat bra.** Ungefär lika stora andelar uppger att de tagit fram riktlinjer för hur personuppgifter ska hanteras, har en förteckning över vilka personuppgiftsbehandlingar som finns i verksamheten, har tagit fram relevanta personuppgiftsbiträdesavtal samt har rutiner för att rapportera personuppgiftsincidenter till Datainspektionen och lämna ut registerutdrag.
- **Ungefär hälften av dataskyddsombuden uppger att deras organisation i hög utsträckning arbetar kontinuerligt och systematiskt med frågor som rör integritet och dataskydd.** Ungefär lika stora andelar uppger att dataskydd och informationssäkerhet ingår i introduktionsutbildningen för nya medarbetare och att de har rutiner för hantering av personuppgifter i e-post och lagring och rensning av personuppgifter.
- **Privata företag uppger i högre grad att de har ett kontinuerligt och systematiskt arbete med integritet och dataskydd.** Branscher som utmärker sig positivt i flera av undersökningens frågor är bank- och finansbranschen, it- och telekombranschen samt i viss mån även privata företag inom vård och omsorg. Dataskyddsombud inom kommun och landsting är överrepresenterade bland dem som uppger att organisationen i låg utsträckning arbetar kontinuerligt och systematiskt med integritet och dataskydd.
- **Hälften av dataskyddsombuden uppger att dataskydd och integritet är en prioriterad fråga för ledningen.** En motsvarande andel uppger att även organisationens medarbetare förstår varför regelverket införts, tycker att det är viktigt och efterlever det.
- **De största utmaningarna i dataskyddsarbetet** handlar om att få till fungerande rutiner och processer och att tolka regelverket.

Tre av fyra dataskyddsombud uppger att implementeringen av dataskyddsförordningen har fungerat bra

Nästan tre av fyra dataskyddsombud anser att implementeringen av dataskyddsförordningen har fungerat mycket eller ganska bra. Bara en av

tio uppger att implementeringen inte fungerat bra.

Privata företag svarar i högre utsträckning att implementeringen gått mycket eller ganska bra. I denna grupp finns också ett antal verksamheter som själva valt att inrätta ett dataskyddsombud även om de inte är skyldiga att göra det. Att det från ledningen funnits ett engagemang att självmant inrätta ett dataskyddsombud har sannolikt bidragit till att ge goda förutsättningar i implementeringsarbetet.

Vissa branscher utmärker sig i svaren. Dataskyddsombud inom bank- och finansbranschen och it- och telekombranschen, svarar i större utsträckning att implementeringen har fungerat bra, medan dataskyddsombud inom kommunal verksamhet är överrepresenterade bland dem som inte anser att implementeringen fungerat bra.

I svaren kan också urskiljas andra signifikanta skillnader som ger viss vägledning om varför implementeringen i vissa organisationer fungerat sämre. Bland de som uppgett att implementeringen inte fungerat bra finns en överrepresentation av dataskyddsombud som uppgett att de haft för lite tid avsatt.

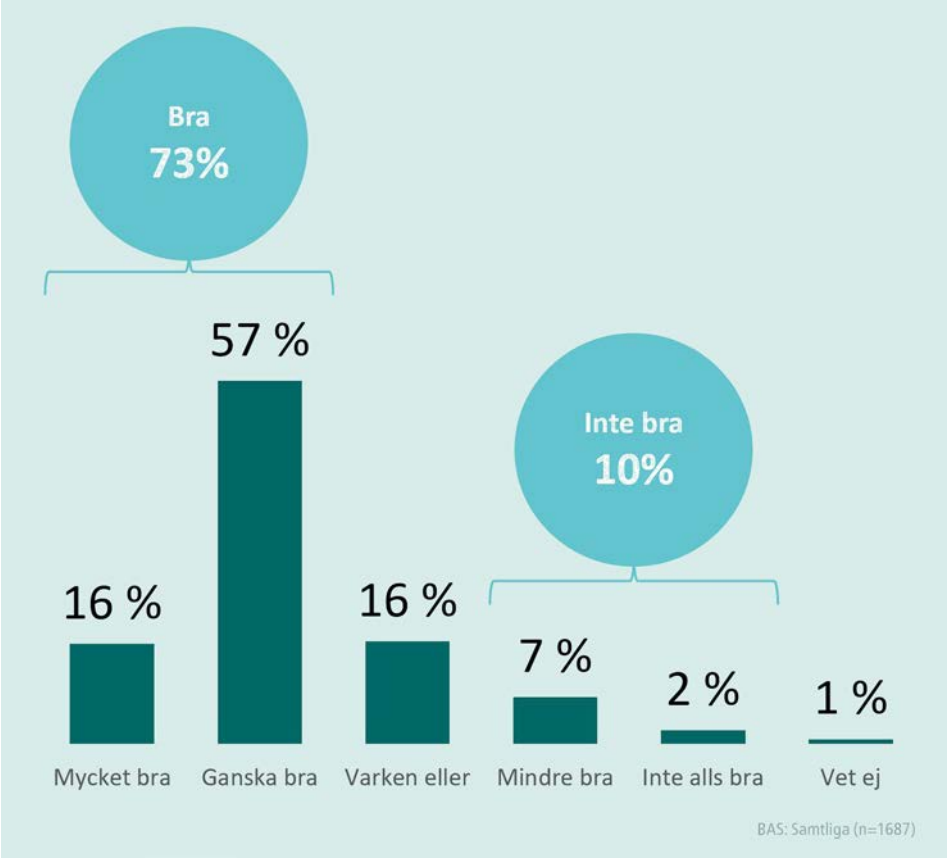

Bild 17. Fråga: Hur upplever du att implementeringen av GDPR och kompletterande lagstiftning har fungerat fram till idag i er organisation?

Tre av fyra har tagit fram riktlinjer för hur verksamheten ska hantera personuppgifter

En grundläggande del av arbetet med att förbereda och genomföra implementeringen av dataskyddsförordningen har för många verksamheter varit att ta fram riktlinjer för hur personuppgifter ska hanteras. Här överensstämmer svaren väl med hur dataskyddsombuden bedömer att implementeringen gått. Nästan tre av fyra dataskyddsombud uppger att organisationen som en följd av dataskyddsförordningen har tagit fram riktlinjer och rutiner för hur verksamheterna ska hantera personuppgifter. Knappt en fjärdedel har delvis tagit fram riktlinjer och rutiner. Endast två procent av respondenterna har inte tagit fram några riktlinjer och rutiner.

Dataskyddsombud inom bank- och finansbranschen samt privata bolag inom vård och omsorg svarar i högre grad att de tagit fram riktlinjer och rutiner, medan kommun och landsting är överrepresenterade bland dem som i högre utsträckning svarar att de delvis tagit fram riktlinjer och rutiner.

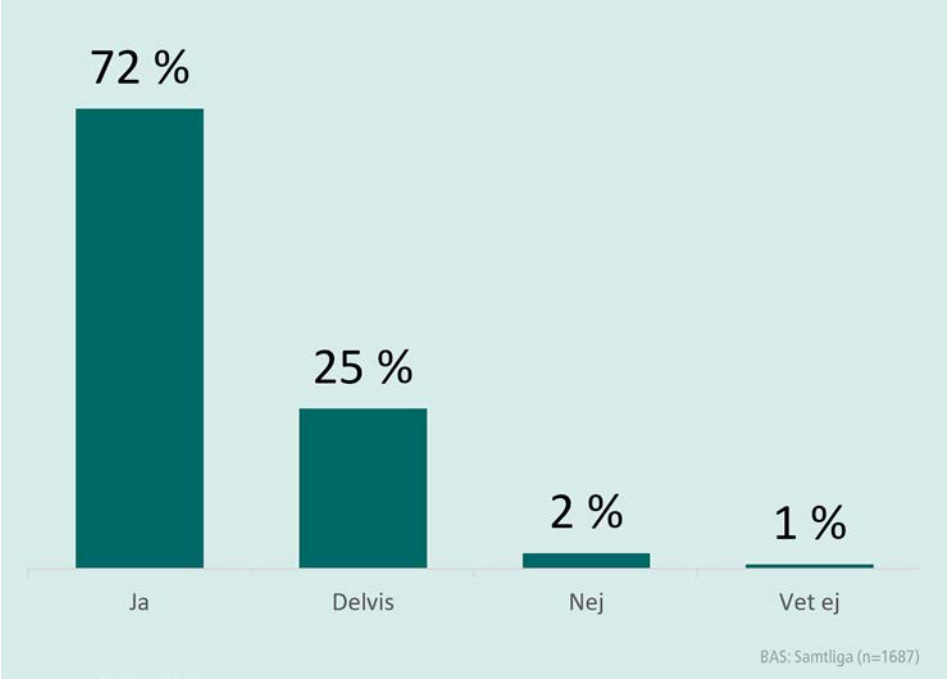

Bild 18. Fråga: Har ni som en följd av GDPR tagit fram riktlinjer och rutiner för hur er verksamhet ska hantera och använda personuppgifter?

En majoritet har förteckning över personuppgiftsbehandlingar och personuppgiftsbiträdesavtal

Enligt dataskyddsförordningen är verksamheter som hanterar personuppgifter skyldiga att föra ett register eller en förteckning över sina olika behandlingar av personuppgifter. Undantag från kravet finns i vissa fall för företag med färre än 250 anställda, men majoriteten av

verksamheterna i undersökningen bedöms vara skyldiga att ta fram en förteckning över personuppgiftsbehandlingar. Tre av fyra verksamheter uppger också att de har tagit fram en sådan förteckning. Merparten av de som inte svarar ja uppger att de delvis tagit fram en förteckning.

Dataskyddsförordningen kräver att det upprättas personuppgiftsbiträdesavtal när andra verksamheter ska behandla personuppgifter för den personuppgiftsansvariges räkning, till exempel vid outsourcing. Kravet syftar till att säkerställa att de som utför behandlingen följer kraven i förordningen. För att säkerställa att underleverantörer följer kraven i förordningen behövs ett personuppgiftsbiträdesavtal. Nästan tre av fyra uppger att de tagit fram relevanta personuppgiftsbiträdesavtal. Merparten av de som inte svarar ja uppger att de delvis tagit fram relevanta personuppgiftsbiträdesavtal.

När det gäller utbildning av medarbetarna i dataskydd och informationssäkerhet är bilden inte riktigt lika positiv. Knappt hälften av dataskyddsombuden uppger att dataskydd och informationssäkerhet ingår i introduktionsutbildningen för nya medarbetare, och mindre än en tredjedel uppger att medarbetarna löpande får utbildning i dataskydd och informationssäkerhet.

Bank- och finansbranschen är överrepresenterade bland de som genomfört samtliga åtgärder. Även verksamheter som frivilligt har ombud och där ombuden har tillräckligt med tid är överrepresenterade bland de som genomfört samtliga åtgärder.

It- och telekombranschen och privata företag utbildar i högre utsträckning både nya och gamla medarbetare i dataskydd och informationssäkerhet.

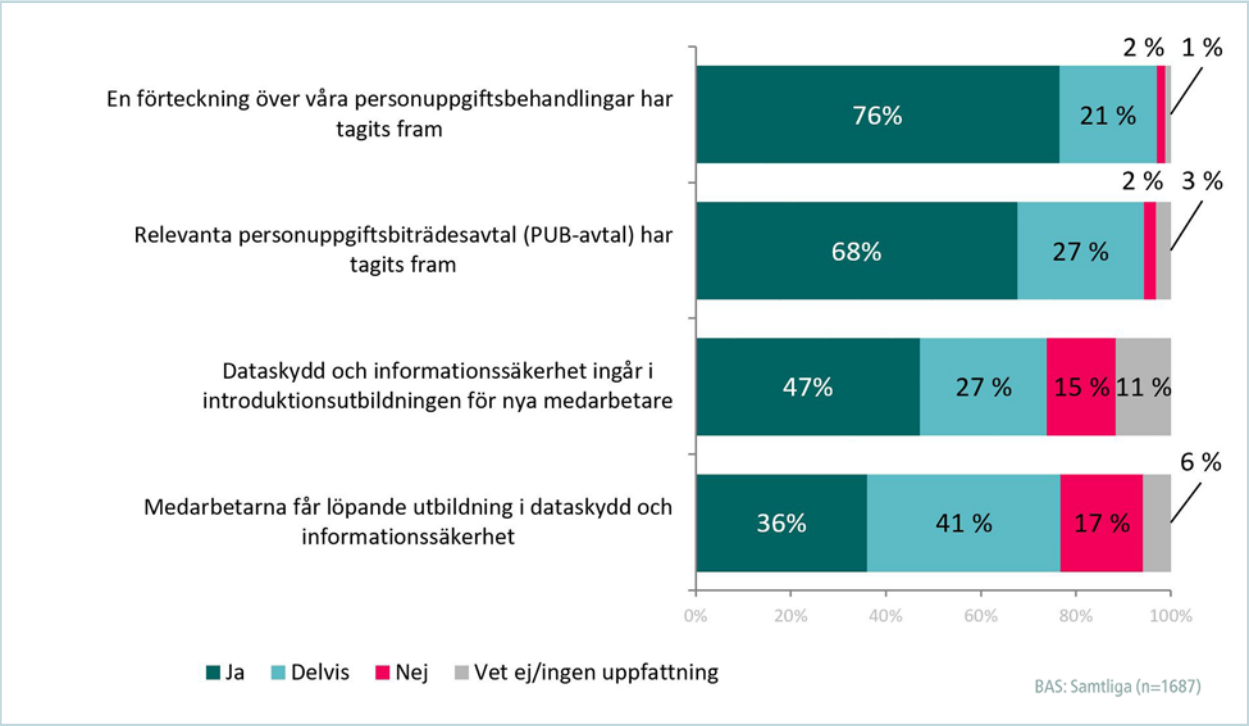

Bild 19. Fråga: Har ni vidtagit någon av följande åtgärder?

Ungefär tre av fyra har rutiner för att rapportera personuppgiftsincidenter och att lämna ut registerutdrag

Dataskyddsombuden har i undersökningen också fått svara på om de har fyra mer konkreta rutiner på plats; rutiner för att anmäla personuppgiftsincidenter till Datainspektionen, att lämna ut registerutdrag, att lagra och rensa personuppgifter samt att hantera personuppgifter i e-post.

Vanligast är att organisationerna har rutiner för att rapportera personuppgiftsincidenter och att lämna ut registerutdrag. Ungefär tre av fyra dataskyddsombud uppger att sådana rutiner finns.

Drygt hälften av organisationerna har även rutiner för att lagra och rensa personuppgifter och hantera personuppgifter i e-post. Bland dem som uppger att de har rutiner för hantering av personuppgifter i e-post är privata bolag inom vård och omsorg överrepresenterade.

Dataskyddsombud inom bank- och finansbranschen och it- och telekombranschen är överrepresenterade bland dem som uppger att de har samtliga fyra rutiner. Även dataskyddsombud med tillräckligt med avsatt tid har i högre grad svarat att de har samtliga fyra rutiner.

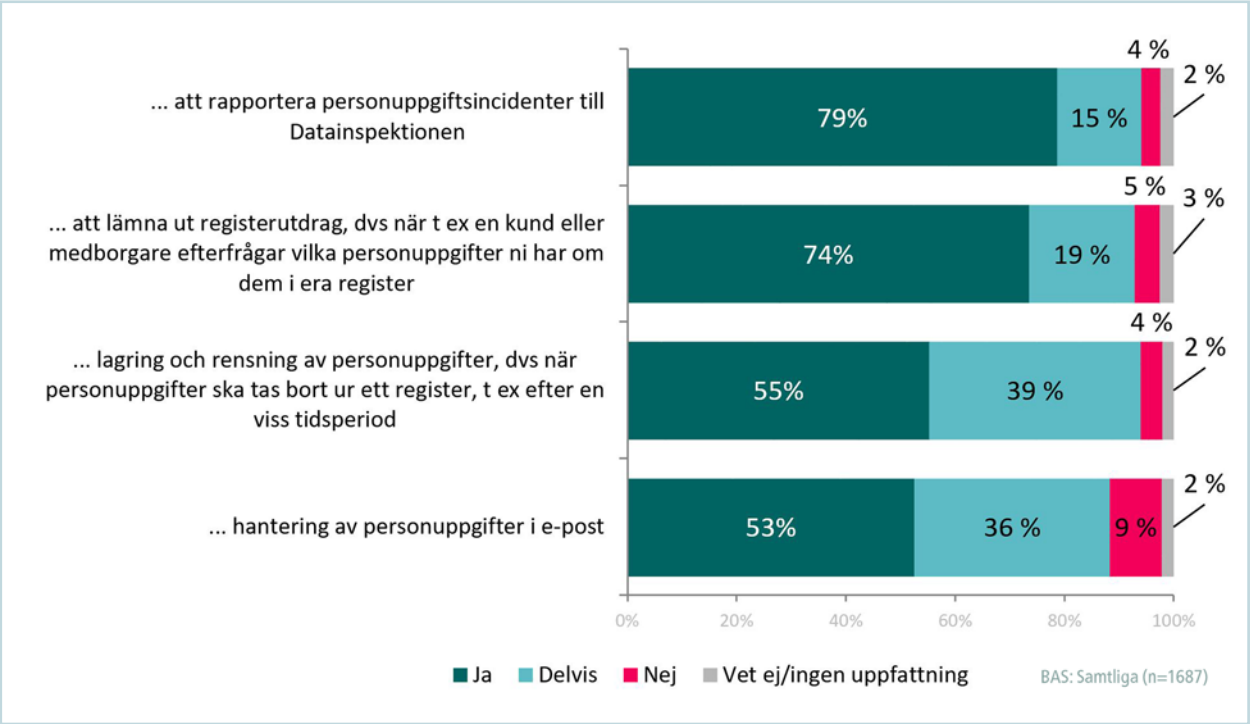

Bild 20. Fråga: Finns rutiner för... ?

Hälften av organisationerna arbetar i hög utsträckning kontinuerligt och systematiskt med integritets- och dataskyddsfrågor

En majoritet av organisationerna uppger alltså att implementeringen av dataskyddsförordningen fungerat bra och att de har grundläggande dokument och rutiner för att hantera personuppgifter. När det gäller att få till stånd ett kontinuerligt och systematiskt arbete med integritets- och dataskyddsfrågor sjunker andelen. Cirka hälften av de tillfrågade dataskyddsombuden anser att organisationen kontinuerligt och systematiskt arbetar med integritets- och dataskyddsfrågor. Ungefär ett av sju dataskyddsombud uppger att organisationen i låg utsträckning arbetar kontinuerligt och systematiskt med frågorna.

I princip samma skillnader mellan branscher återkommer som i bedömningen av implementeringen. Bank- och finansbranschen och it- och telekombranschen är överrepresenterade bland de som uppger att arbetet med frågorna sker kontinuerligt och systematiskt. Även dataskyddsombud inom privat vård och omsorg svarar i högre grad att de har ett kontinuerligt och systematiskt arbete. Bland dem som i högre utsträckning uppgett att organisationen i låg utsträckning arbetar kontinuerligt och systematiskt med frågorna är dataskyddsombud inom kommun och landsting överrepresenterade.

Även i bedömningen av graden av kontinuerligt och systematiskt arbete återkommer tiden som en framgångsfaktor. Dataskyddsombud

som bedömer att de har tillräckligt med tid avsatt är överrepresenterade bland de som uppgett att i de hög utsträckning arbetar kontinuerligt och systematiskt. De som inte tycker att de har tillräckligt med tid avsatt, uppger däremot i större omfattning att arbetet i låg utsträckning är kontinuerligt och systematiskt.

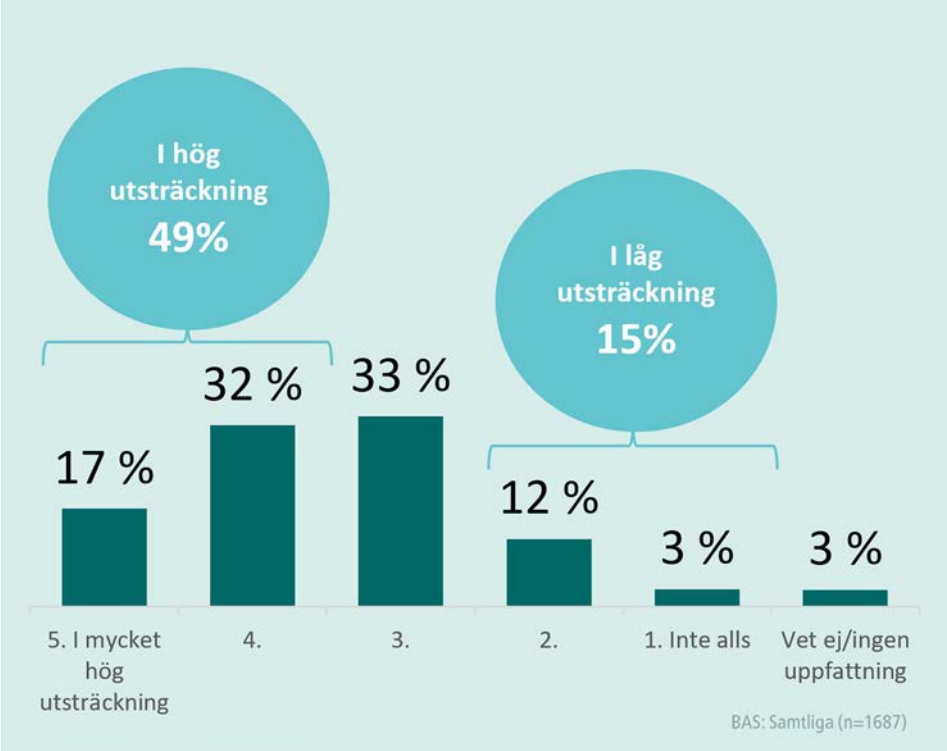

Bild 21. Fråga: I vilken utsträckning arbetar er organisation kontinuerligt och systematiskt med integritets- och dataskyddsfrågor?

Hälften anser att det är lätt att få gehör i ledningen och att frågorna är prioriterade

För att få till stånd ett systematiskt och kontinuerligt arbete med integritets- och dataskyddsfrågor är det avgörande att det finns ett engagemang i organisationens ledning. När dataskyddsombuden fått frågor som rör om de upplever att dataskydd är en prioriterad fråga för ledningen stämmer bilden väl med graden av kontinuerligt och systematiskt arbete.

Omkring hälften av dataskyddombuden upplever att det är lätt att få gehör för dataskyddsfrågor i ledningen och att integritet och dataskydd är prioriterade frågor för ledningen – det vill säga lika stor andel som uppger att de i hög utsträckning har ett kontinuerligt och systematiskt arbete med frågorna.

Även när det gäller ledningens engagemang utmärker sig bank- och finansbranschen, it- och telekombranschen samt vård och omsorgsföretag positivt. Dataskyddsombud i dessa branscher uppger i högre

utsträckning att de har lätt att få gehör hos ledningen och att data- och integritetsskydd är prioriterat i ledningen.

Bland de som uppger att det inte är lätt att få gehör och att data- och integritetsskydd inte är prioriterat är kommuner och landsting överrepresenterade.

En tredjedel av dataskyddsombuden uppger att ledningen är insatta och kunniga, medan hälften uppger att ledningen delvis är insatta och kunniga. Regelverket i dataskyddsförordningen är förhållandevis komplext och det är därför förklarligt att de flesta ledningar uppfattas som delvis insatta och kunniga. Resultatet understryker dock behovet av dataskyddsombudens centrala uppgift att ge information och rådgivning.

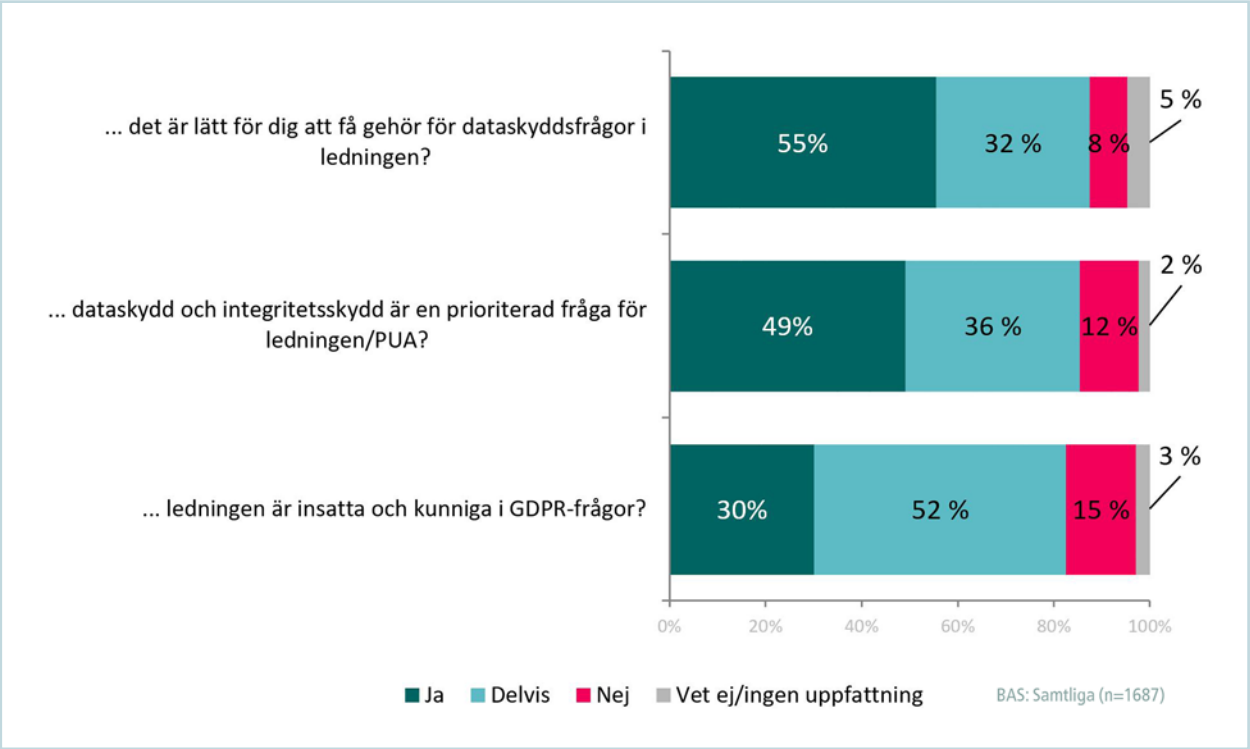

Bild 22. Fråga: Upplever du att...?

Ledningens och medarbetarnas engagemang och kunskap följs åt

Ledningens engagemang och kunskap om dataskyddsförordningen tycks återspegla sig i medarbetarnas. När dataskyddsombuden fått frågor som rör medarbetarna bedömer ungefär hälften att medarbetarna i hög eller mycket hög utsträckning förstår varför regelverket införts, tycker att regelverket att viktigt och efterlever det.

Även hos medarbetarna bedömer dataskyddsombuden kunskapen lägre än om regelverket upplevs som viktigt.

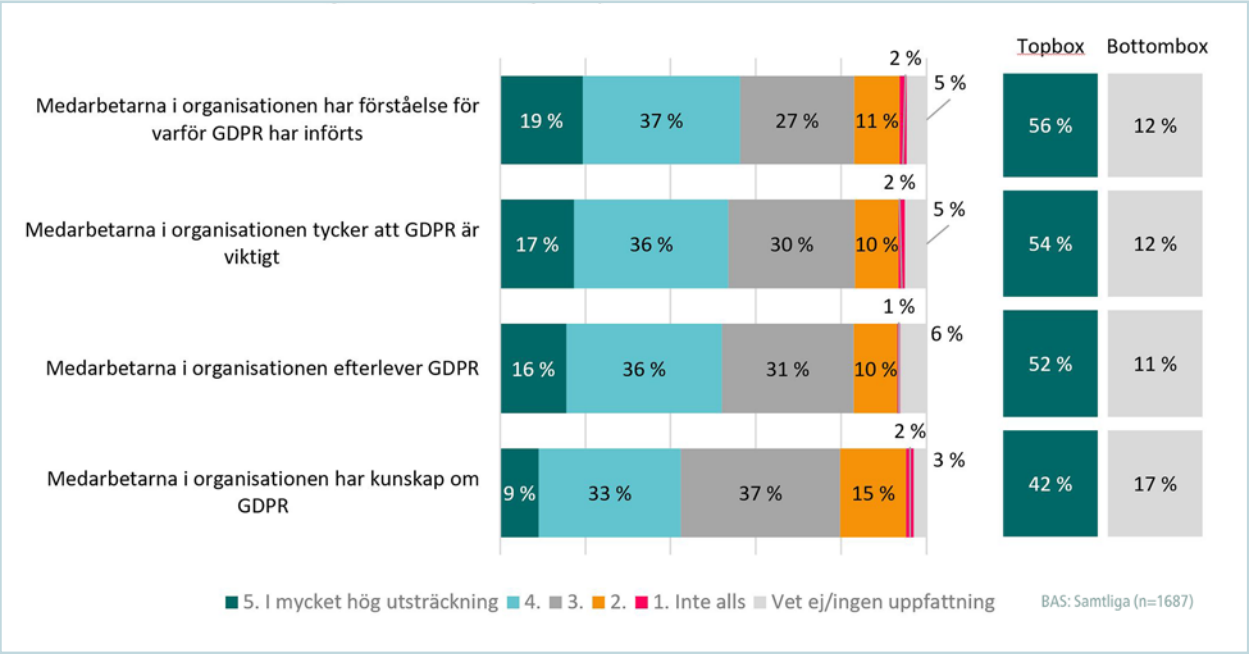

Bild 23. Fråga: I vilken utsträckning instämmer du i följande påståenden? (Topbox innebär mycket eller ganska hög utsträckning. Bottombox innebär liten utsträckning eller inte alls)

Största utmaningarna – att få till rutiner och processer samt att tolka regelverket

För att kunna fortsätta utveckla ett kontinuerligt och systematiskt dataskyddsarbete är det angeläget att förstå vad dataskyddsombuden upplever som de största utmaningarna. Kunskapen är viktig både för ledningen i verksamheter som hanterar personuppgifter – men också för Datainspektionens fortsatta arbete med att ge vägledning och stöd.

De främsta utmaningarna för dataskyddsombuden handlar om att få till fungerande rutiner och processer och att tolka regelverket. Ungefär en tredjedel uppger också att det är utmanande att regelverket upplevs hindra eller försvåra verksamheten, att organisationen är fast i gamla it-system eller att det är svårt att frigöra personella resurser till dataskyddsarbete.

En utmaning kopplad till rollen som dataskyddsombud återkommer också i svaren. Ungefär en tredjedel av dataskyddsombuden beskriver det som utmanande att balansera den delen av uppdraget som handlar om att ge intern rådgivning och information med att även kontrollera och följa upp regelefterlevnaden.

Endast en av sju upplever brist på engagemang och kunskap hos ledningen som utmanande.

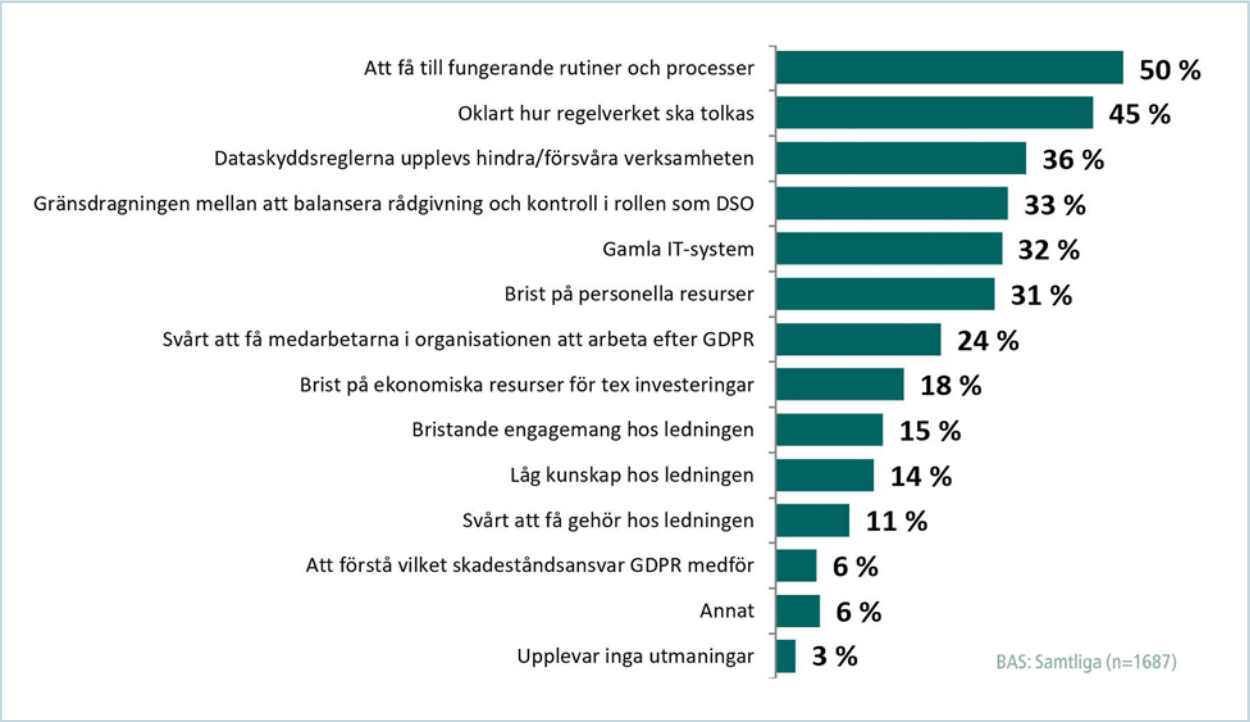

Bild 24. Fråga: Vilka anser du är de största utmaningarna med GDPR?

Dataskyddsombudens förutsättningar

- **Nio av tio dataskyddsombud rapporterar direkt till högsta ledningen, nämnden eller styrelsen.**
- **Flertalet, knappt åtta av tio, kan få hjälp och stöd av andra anställda eller andra dataskyddsombud.**
- **Majoriteten, sex av tio, arbetar deltid med dataskyddsfrågor.** Av de som arbetar deltid har hälften ingen fastställd avsatt tid; tiden avsätts efter behov. Samtidigt uppger mer än hälften av samtliga ombud att de inte har tillräckligt med tid avsatt för att frågorna.
- **Dataskyddsombuden blir oftast involverade i projekt som rör dataskyddet, men inte alltid i tid.** Sex av tio uppger att de oftast blir involverade i projekten, men endast en tredjedel blir inbjudna i tid. En förhållandevis stor andel, fyra av tio, uppger att de sällan eller aldrig blir involverade.
- **Drygt hälften anser att de får den utbildning och kompetensutveckling som krävs.**
- **Knappt hälften anser att uppdraget som dataskyddsombud är tydligt.**

Dataskyddsombuden har en nyckelroll i arbetet med att höja integritets- och dataskyddet i personuppgiftsansvariga verksamheter. För att få en bild av vilka förutsättningar dataskyddsombuden har i sitt uppdrag har ett antal frågor i undersökningen inriktats mot omständigheter kopplade till själva arbetet som dataskyddsombud.

På en övergripande nivå kan det sägas finnas två olika huvudtyper av dataskyddsombud. Dels de som är anställda i verksamheten, dels externa dataskyddsombud som ofta innehar rollen för flera verksamheter. Ungefär fyra av tio dataskyddsombud uppger att de ansvarar för endast en verksamhet. En lika stor andel att de ansvarar för fler än fem verksamheter. Värt att notera är att tre procent av dataskyddsombuden uppger att de ansvarar för 40 eller fler verksamheter. I Datainspektionens register över anmälda dataskyddsombud finns vissa som ansvarar för uppemot 80 verksamheter.

Utbildningsbakgrunden hos dataskyddsombuden varierar, men omkring en tredjedel är jurister. Näst vanligast är utbildning inom it eller ekonomi, vilket 12 procent vardera uppger att de har.

Majoriteten rapporterar till högsta ledningen

Som beskrivits ovan är det förhållandevis ovanligt att dataskydds-ombuden upplever bristande kunskap eller engagemang hos ledningen som en utmaning. En bidragande förklaring kan vara att majoriteten, ungefär sex av tio dataskyddsombud, rapporterar direkt till högsta ledningen. Bland dessa är dataskyddsombud inom bank- och finans-sektorn överrepresenterade.

Cirka en tredjedel rapporterar till närmaste chef, majoriteten av dessa rapporterar dock till sin närmaste chef och till högsta ledningen, styrelsen, nämnden eller annan. Endast en av tio har uppgett att de endast rapporterar till närmaste chef. Dataskyddsombud inom kommuner och landsting svarar i högre utsträckning att de rapporterar till närmsta chef.

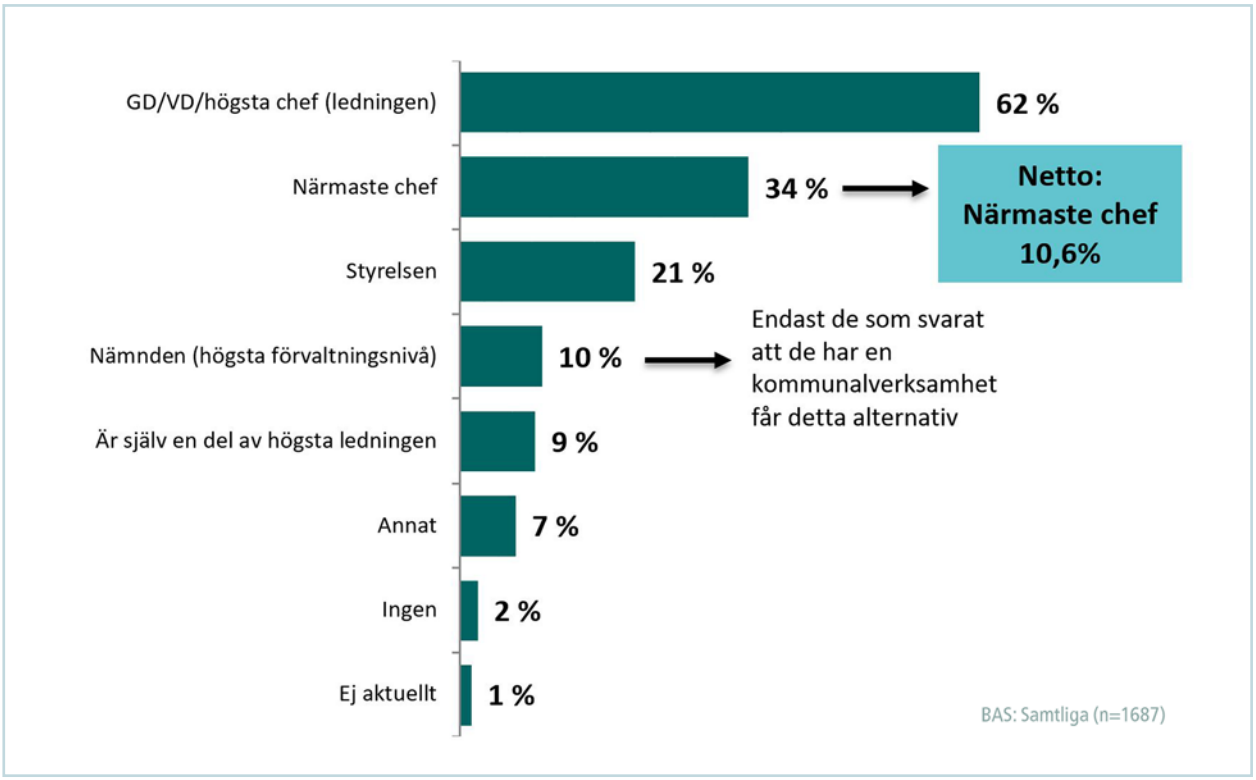

Bild 25. Fråga: Vilka rapporterar du till i frågor som rör dataskydd?

Majoriteten arbetar deltid som dataskyddsombud

Av de tillfrågade dataskyddsombuden svarar majoriteten, drygt sex av tio, att de arbetar deltid med dataskyddsfrågor. Drygt en femtedel av dataskyddsombuden i undersökningen arbetar heltid. I denna grupp är dataskyddsombud som ansvarar för tre eller fler verksamheter överrepre-senterade, medan ombud med ansvar för endast en verksamhet i större utsträckning arbetar deltid.

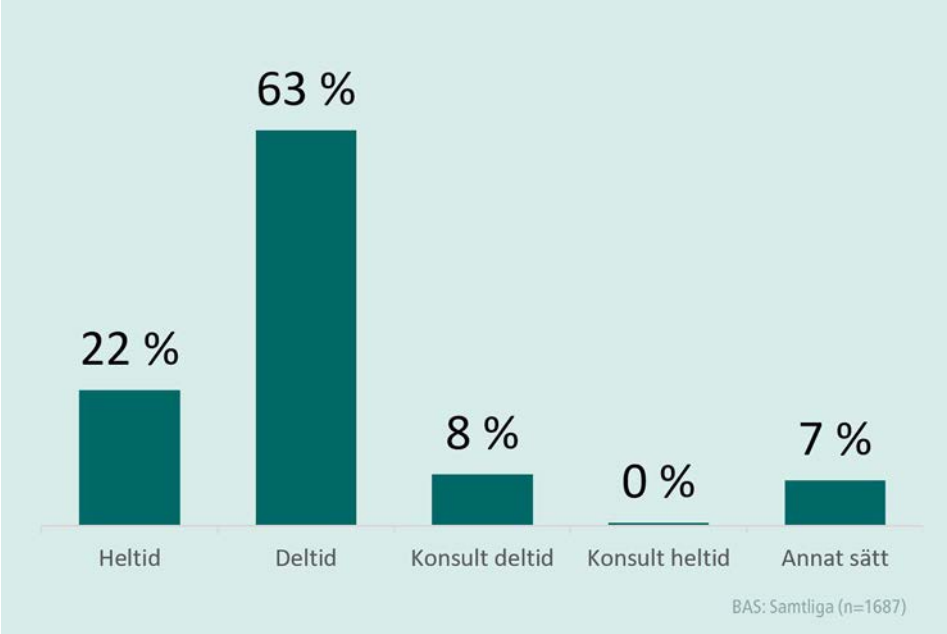

Bild 26. Fråga: Arbetar du som dataskyddsombud på heltid eller deltid?

Av de som arbetar deltid har knappt hälften ingen fastställd tid avsatt för dataskyddsfrågorna; arbetstiden avsätts efter behov. En något mindre andel, knappt fyra av tio, har en avsatt arbetstid för dataskyddsfrågor motsvarande mindre än 40 procent av en heltidstjänst.

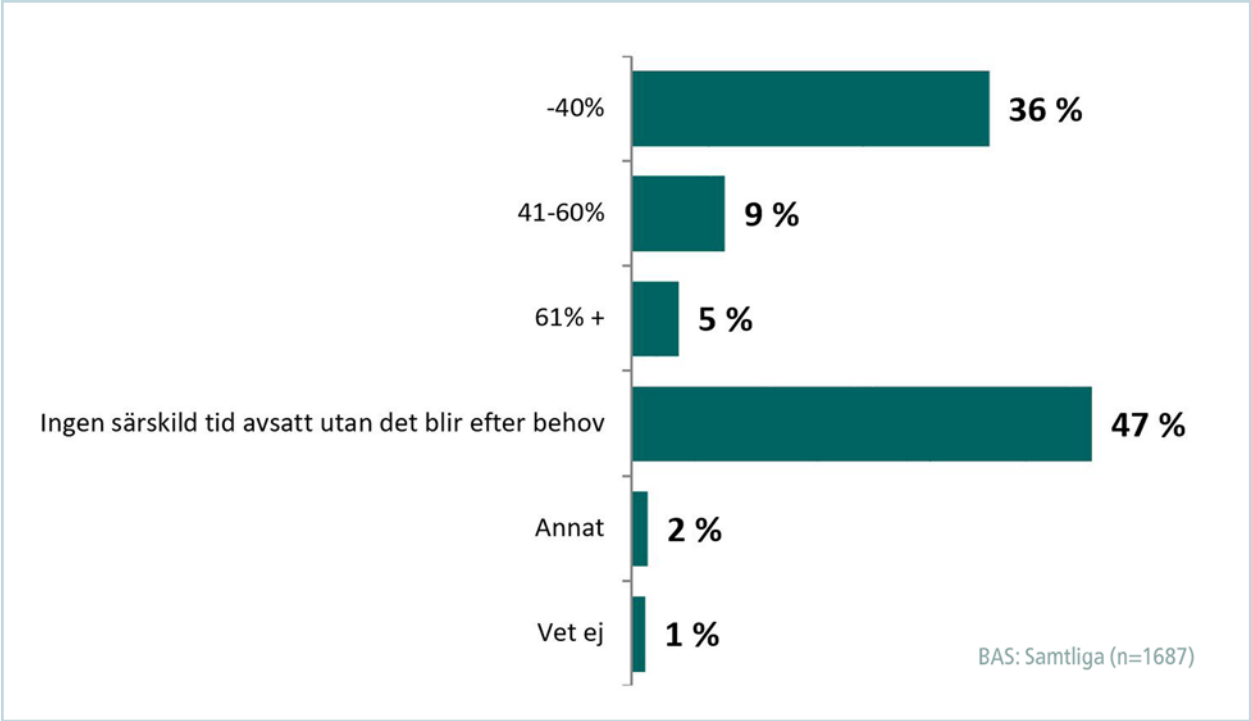

Bild 27. Fråga: Ungefär hur stor del av din totala tid är avsatt för att arbeta med dataskyddsfrågor?

Mer än hälften av dataskyddsombuden upplever att de inte har tillräckligt med tid avsatt

Knappt hälften av dataskyddsombuden anser att de har tillräckligt med tid avsatt. Övriga, det vill säga över hälften, upplever att de inte har tillräckligt med tid avsatt, eller bara delvis har tid att på ett tillfredsställande sätt hinna med arbetet.

Dataskyddsombud i privat sektor upplever sig i större utsträckning ha tillräckligt med tid. Bland de som upplever att de har tillräckligt med tid utmärker sig bland annat dataskyddsombud inom bank- och finansbranschen och it- och telekombranschen.

Av de som svarar att de delvis eller inte har tillräckligt med tid, är dataskyddsombud inom statliga myndigheter och kommuner överrepresenterade.

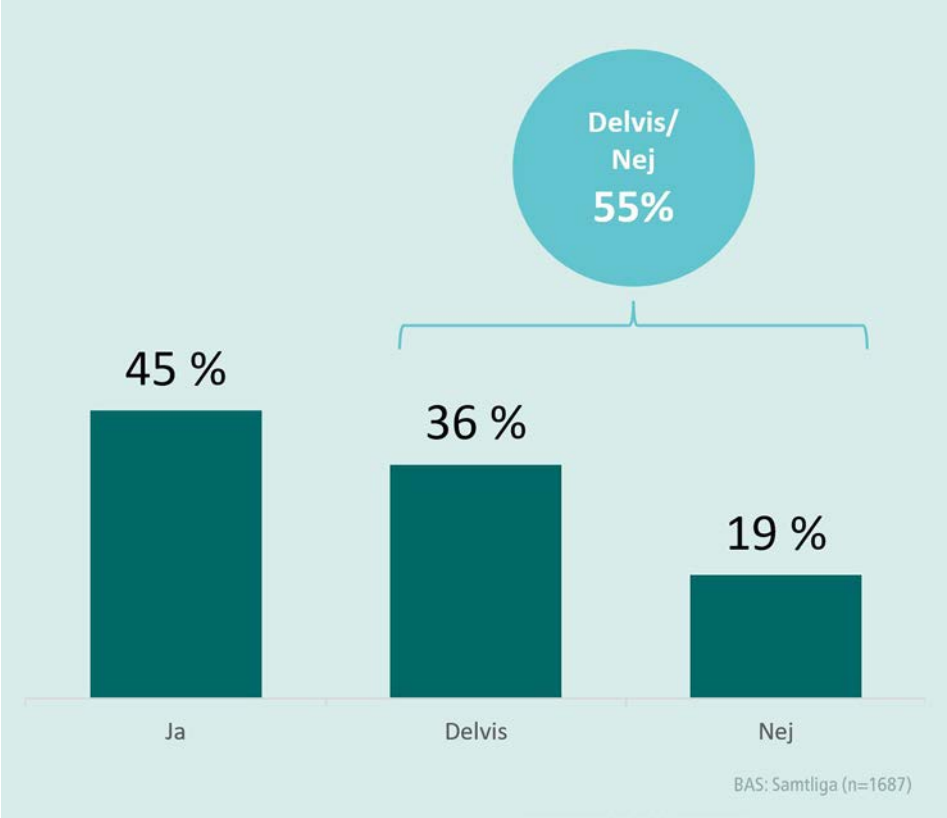

Bild 28. Fråga: Finns tillräckligt med tid avsatt för att du på ett tillfredsställande sätt ska hinna med att arbeta med dataskyddsfrågor?

Knappt hälften tycker att uppdraget som dataskyddsombud är tydligt

Rollen som dataskyddsombud är ny och infördes i de allra flesta verksamheter i maj 2018. Mot den bakgrunden är det inte så förvånande att en förhållandevis stor andel, nästan hälften av dataskyddsombuden, upplever att uppdraget endast delvis är tydligt och att en av tio tycker att uppdraget är otydligt. Mindre än hälften anser att uppdraget är tydligt.

Det finns ett samband mellan hur tydligt uppdraget upplevs och den tid dataskyddsombuden kan lägga på uppdraget. Heltidsarbetande dataskyddsombud och de som upplever att de har tillräckligt med tid avsatt för uppdraget svarar i högre utsträckning att uppdraget är tydligt.

Bland de dataskyddsombud som upplever uppdraget som tydligt är bank- och finansbranschen och it- och telekombranschen överrepresenterade. Bland dem som inte upplever uppdraget som tydligt är kommuner och landsting överrepresenterade.

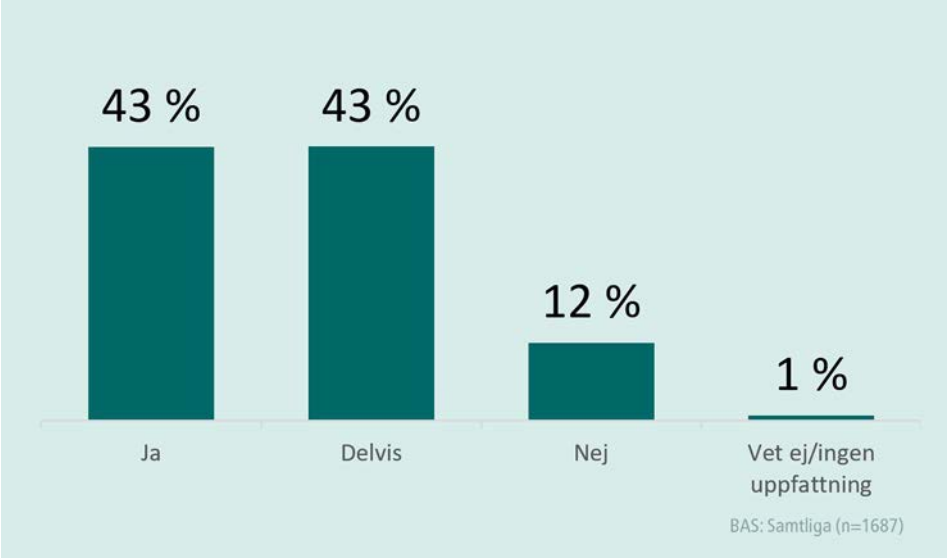

Bild 29. Fråga: Upplever du att ditt uppdrag som dataskyddsombud är tydligt när det gäller vad du ska åstadkomma och leverera?

Dataskyddsombuden blir oftast involverade i projekt som rör dataskyddet, men inte alltid i rätt tid

En förutsättning för att kunna utföra uppdraget som dataskyddsombud på ett bra sätt är att bli involverad i utvecklingsprojekt eller andra aktiviteter som får konsekvenser för skyddet av personuppgifter. Det är också centralt att dataskyddsombudet blir involverad tidigt i arbetet.

Knappt sex av tio dataskyddsombud uppger att de alltid eller oftast blir involverade i projekt eller andra sammanhang där beslut fattas som får följder för dataskyddet. Endast tre av tio uppger att de som regel blir involverade i god tid.

Samtidigt är andelen som uppger att de bara blir involverade ibland, sällan eller aldrig förhållandevis stor – här finns drygt fyra av tio dataskyddsombud. För ett av sju dataskyddsombud har arbetet mest karaktär av att ”släcka bränder”, när de blir involverade i olika projekt eller aktiviteter upplever de inte att det är i rätt tid.

Dataskyddsombud som uppger att de ibland, sällan eller aldrig blir involverade i projekt med följder för dataskyddet är kraftigt överrepresenterade bland kommuner och landsting.

Bland de som uppger att de alltid blir involverade är bank- och finansbranschen, it- och telekombranschen samt övriga privata företag överrepresenterade. Även de verksamheter som inte är skyldiga att utse ett dataskyddsombud utan gjort det på eget initiativ utmärker sig positivt – där uppger dataskyddsombuden i större utsträckning än genomsnittet att de alltid blir involverade.

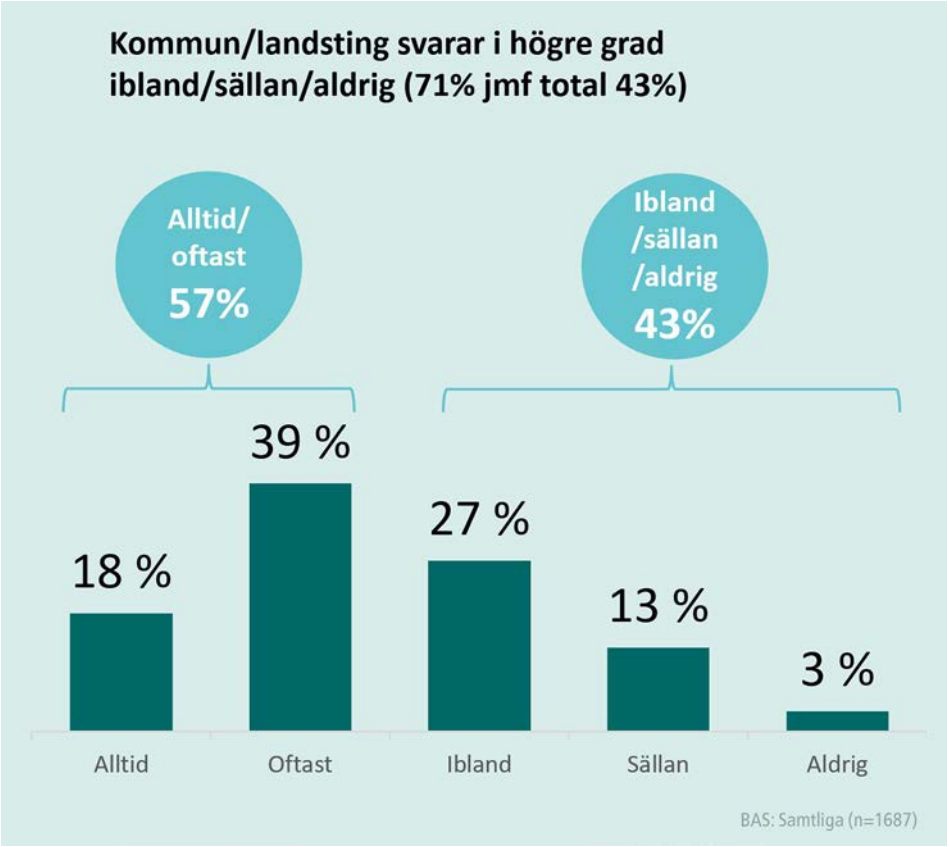

Bild 30. Fråga: I vilken utsträckning blir du involverad i projekt eller andra sammanhang där beslut fattas som får följder för dataskyddet?

Nedan redovisas andelen som blir involverade i projekten i tid.

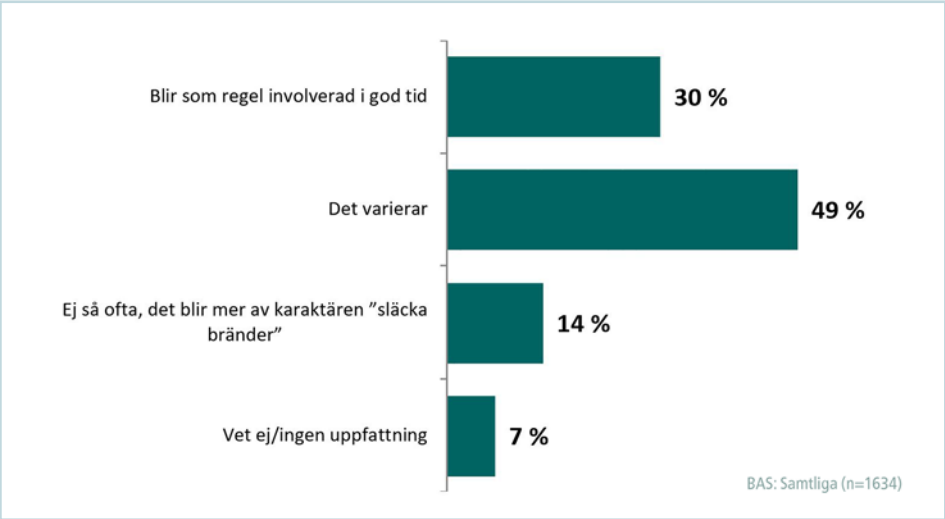

Bild 31. Fråga: När du deltar i projekt eller andra sammanhang som handlar om dataskydd, blir du normalt sett involverad i god tid, eller handlar ditt arbete mer om att ”släcka bränder”?

Drygt hälften av dataskyddsombuden anser att de får den utbildning och kompetensutveckling som krävs

Drygt hälften av dataskyddsombuden i undersökningen anser att de får den utbildning och kompetensutveckling som krävs för att kunna arbeta med dataskyddsfrågor. Bland dessa finns en överrepresentation inom bank- och finansbranschen, it- och telekombranschen samt privata företag i övrigt. Även i de verksamheter som inte är skyldiga att utse ett dataskyddsombud, utan gjort det på eget initiativ, är det vanligare att dataskyddsombuden tycker sig få tillräcklig kompetensutveckling.

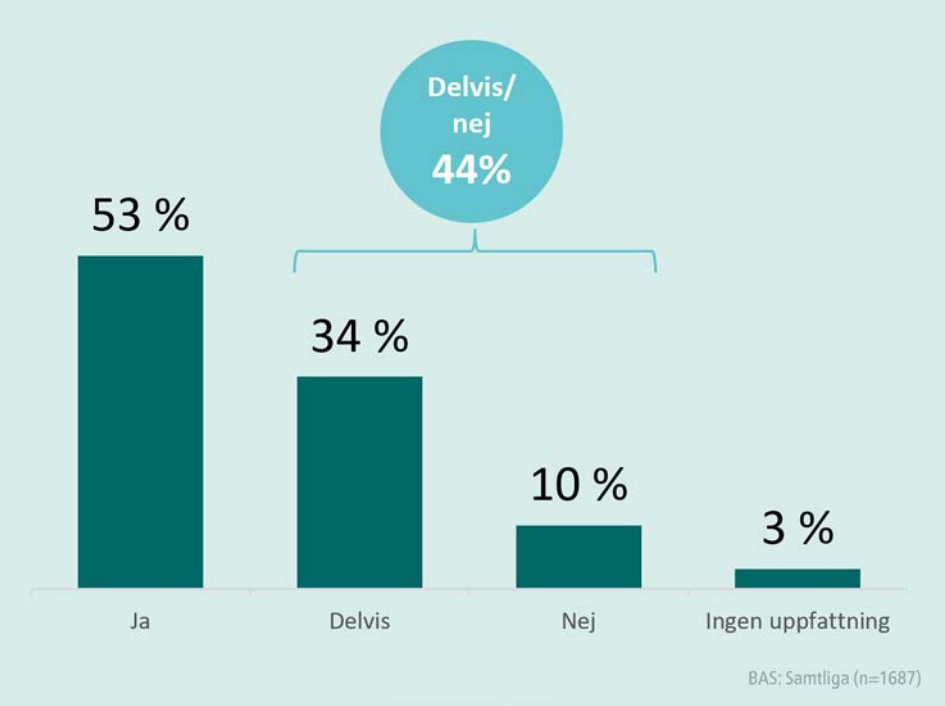

Bild 32. Fråga: Anser du att du får den utbildning och kompetensutveckling som krävs för att kunna arbeta med dataskyddsfrågor i organisationen?

Flertalet kan få stöd och hjälp av andra anställda eller dataskyddsombud

Dataskydd är ett komplext arbetsfält som spänner genom såväl juridik som teknik. Ofta krävs avvägningar och bedömningar av risker och konsekvenser både ur verksamhetens perspektiv och för den enskilde vars personuppgifter som finns registrerade. Dessutom är regelverket nytt och det saknas i stora delar praxis att luta sig mot. Att dataskyddsombuden inte arbetar isolerat, utan har möjlighet att få stöd av såväl andra medarbetare i organisationen som andra dataskyddsombud kan därför underlätta arbetet väsentligt.

Av samtliga dataskyddsombud uppger tre av fyra att de vid behov kan få stöd och hjälp. Vanligast är att dataskyddsombuden uppger att de kan få stöd och hjälp av andra anställda. Ungefär en av sju uppger att de arbetar i en fast grupp med flera medarbetare.

Samtidigt uppger knappt fyra av tio dataskyddsombud att de i huvudsak arbetar ensamma.

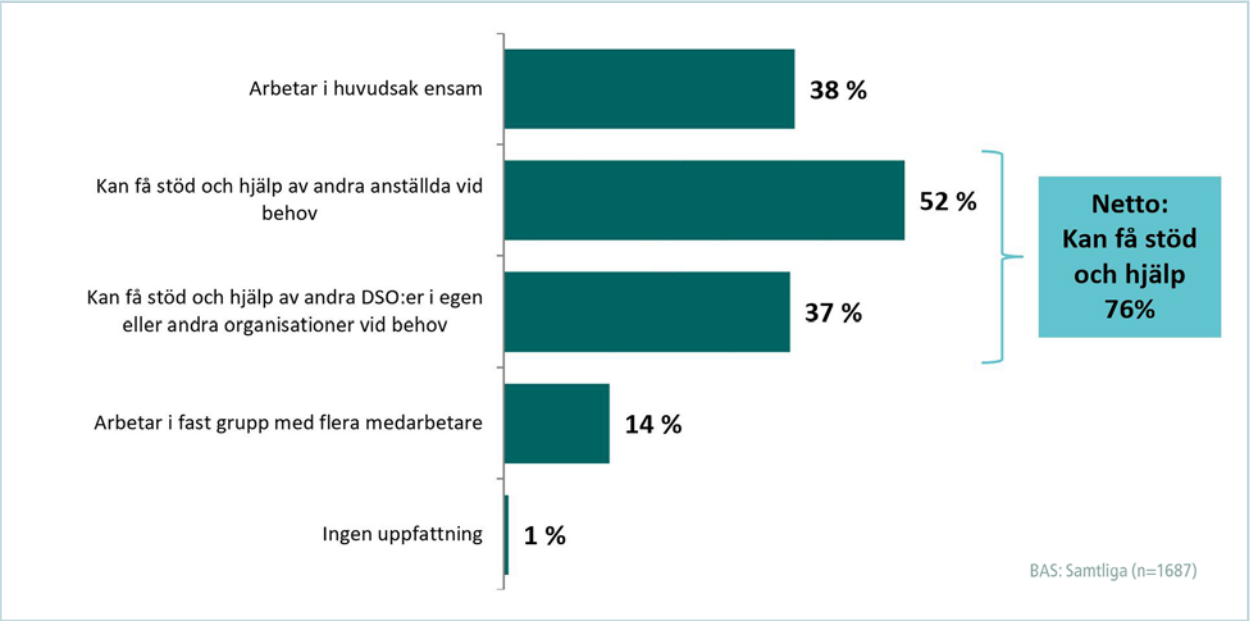

Bild 33. Fråga: Arbetar du i huvudsak ensam eller kan du få stöd och hjälp av andra anställda eller andra dataskyddsombud med dataskyddsfrågor?

Företag som inte anmält ett dataskyddsombud

- **Drygt fyra av fem företag uppger att de känner till dataskyddsförordningen bra och att arbetet med dataskydd och integritet är prioriterat.** Tre av fyra har också utsett en ansvarig för arbetet med integritet och dataskydd.
- **Ungefär sju av tio uppger att de har riktlinjer för hur personuppgifter ska hanteras**, har en förteckning över vilka personuppgiftsbehandlingar som finns i verksamheten och har rutiner för att lagra och gallra personuppgifter.
- **Sex av tio företag uppger att de i hög utsträckning arbetar kontinuerligt och systematiskt med frågor som rör integritet och dataskydd.** Drygt hälften, sex av tio, har även rutiner för att hantera personuppgifter i e-post och lämna ut registerutdrag, något färre har rutiner för att rapportera personuppgiftsincidenter till Datainspektionen.
- **Olika branscher har kommit olika långt.** Företag inom vård, omsorg och utbildning uppger i högre grad att de har ett kontinuerligt och systematiskt arbete med dataskydd, medan företag inom hotell- och restaurangbranschen och transport är överrepresenterade bland de som i låg utsträckning arbetar kontinuerligt och systematiskt med integritet och dataskydd.
- **Småbolag efterlever i mindre omfattning dataskyddsförordningen.** Bolag med 1–9 anställda utmärker sig genom att de generellt svarar att de mindre omfattning arbetar med frågorna.
- **Företagens medarbetare anses i stor utsträckning ha fått information om förordningen, och anses även efterleva regelverket.**
- **De största utmaningarna i dataskyddsarbetet** handlar om att få till fungerande rutiner och processer, att tolka regelverket och att arbetet innebär ökad administration.

För att få en bild av hur långt arbetet med integritet och dataskydd kommit i företag som inte utsett ett dataskyddsombud har Datainspektionen genomfört en undersökning även mot denna grupp. Eftersom det

här inte funnits tillgängliga kontaktuppgifter som underlättat utskick av webbintervjuer, har istället totalt 800 telefonintervjuer genomförts.[13]

Företagen i undersökningen finns inom branscherna drift (el, vatten och avlopp), handel, transport, hotell och restaurang, tjänsteföretag, utbildning samt vård och omsorg. 90 procent av företagen har ett kundregister, varav hälften har både privat- och företagskunder. Ungefär en tredjedel av företagen är små bolag med färre än tio anställda. Dock ingår inga enmansföretag i undersökningen.

Ungefär hälften av dem som svarat i undersökningen har varit VD inom företaget. De flesta övriga har haft en annan typ av ledningsposition som till exempel ägare, ekonomichef, it-chef eller personalchef.

En stor majoritet av företagen känner till dataskyddsförordningen

Att dataskyddsförordningen är välkänd framgår av att en stor majoritet av företagen uppger att de känner till regelverket bra och vad den innebär för verksamheten. Endast omkring ett av sju företag uppger att de bara känner till regelverket lite, eller har hört talas om det men knappt känner till något om vad det innebär för företaget.

Kännedomen om dataskyddsförordningen och vad den innebär för företaget är högre i större företag. Av de som känner till förordningen bra är företag med fler än 50 anställda överrepresenterade, medan det finns en överrepresentation av företag med en till nio anställda bland de som i mindre omfattning känner till förordningen eller har bara hört talas om den.

Det går också att se vissa skillnader i kännedom mellan olika branscher. Företag inom utbildningsbranschen svarar i större utsträckning att de känner till dataskyddsförordningen bra, medan transportbranschen samt hotell och restaurang är överrepresenterade bland de som endast lite känner till förordningen eller har bara hört talas om den.

13 Undersökningen genomfördes av undersökningsföretaget Novus på uppdrag av Datainspektionen. Intervjuerna har genomförts via telefon under perioden 19 februari till 19 mars 2019. Svarsfrekvensen i undersökningen uppgår till 42 procent. Urvalet har levererats av Statistiska centralbyrå, SCB. Metoden i undersökningen beskrivs mer utförligt i en bilaga till denna rapport. Undersökningen i sin helhet finns på www.datainspektionen.se.

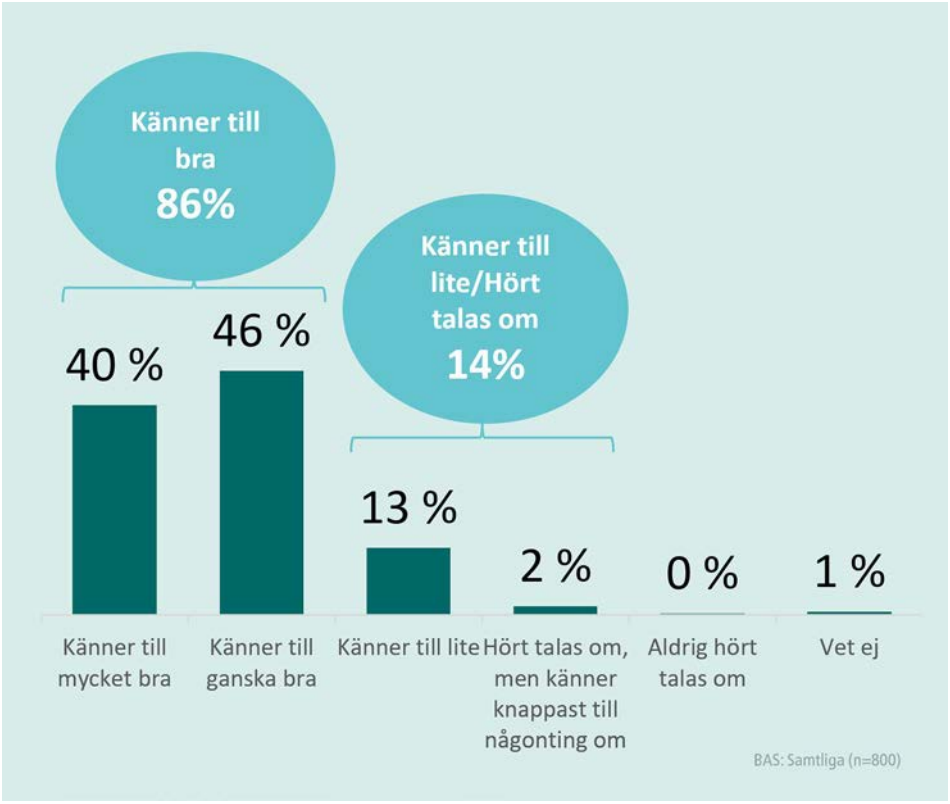

Bild 34. Fråga: I vilken utsträckning arbetar er organisation kontinuerligt och systematiskt med integritetsfrågor och dataskydd avseende person-uppgiftshantering?

Fyra av fem uppger att arbetet med integritet och dataskydd är prioriterat

Fyra av fem intervjupersoner uppgav att arbetet med integritet och dataskydd är mycket eller ganska högt prioriterat inom företaget. Bland företag inom utbildning samt vård och omsorg svarade nästan samtliga att arbetet är prioriterat. Av de som uppgav att det är mindre prioriterat var verksamheter inom hotell och restaurang överrepresenterade.

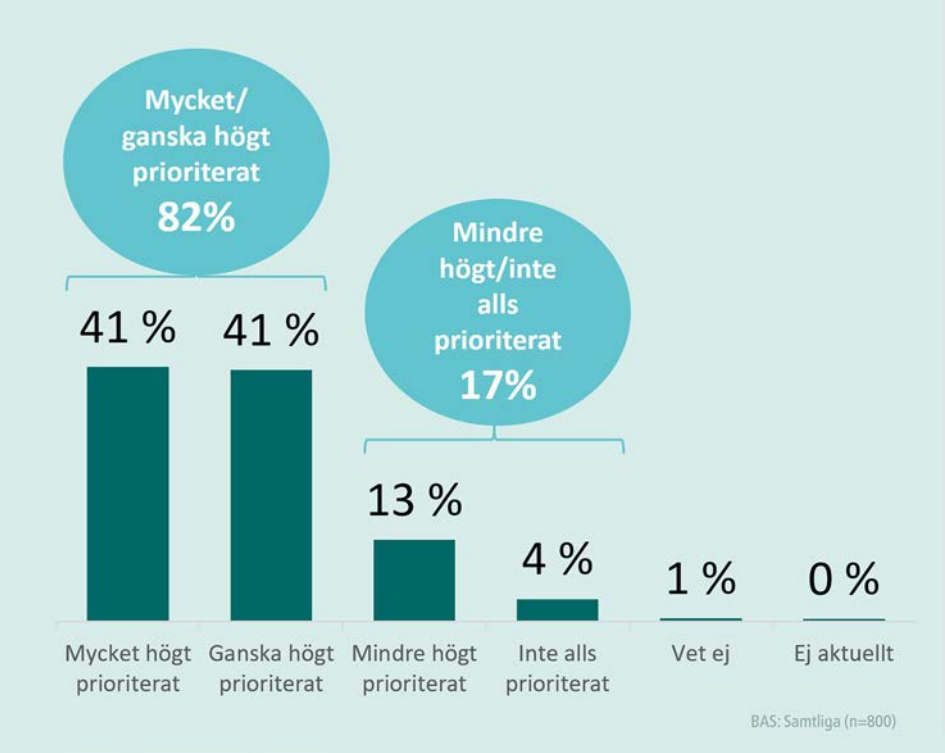

Bild 35. Fråga: Hur prioriterat skulle du säga att ert arbete med integritetsfrågor och dataskydd är avseende personuppgiftshantering?

En majoritet av företagen har en utpekad ansvarig för integritets- och dataskyddsfrågor

Ett led i att ge arbetet med integritet och dataskydd prioritet kan vara att utse en särskild person med ansvar för frågorna. Andelen företag som uppger att de har en utpekad ansvarig överensstämmer också i hög grad med andelen som uppger att arbetet är prioriterat. Tre av fyra företag uppger att de utsett en ansvarig person för integritets- och dataskyddsfrågor, som dock inte är dataskyddsombud.

Drygt ett av tio företag uppger att de utsett ett dataskyddsombud som dock inte anmälts till Datainspektionen. Skäl till att dataskyddsombudet inte registrerats hos Datainspektionen är till exempel att företaget inte är skyldiga att göra det, inte sett något behov eller inte kände till att möjligheten fanns.

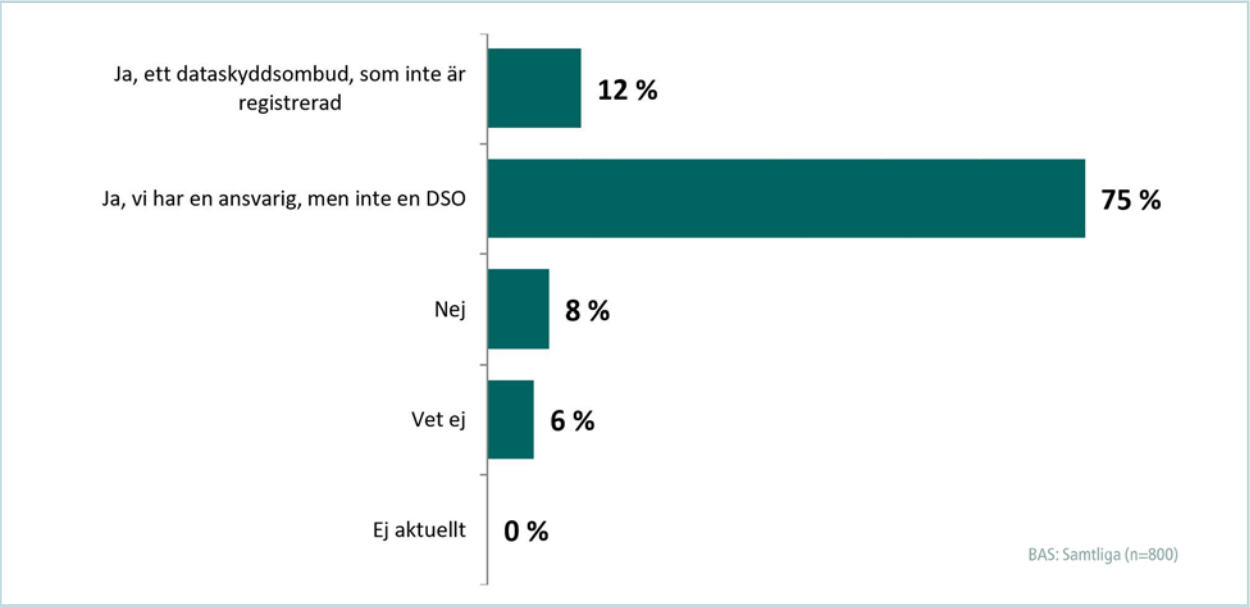

Bild 36. Fråga: Har er verksamhet utsett en person som ansvarar för integritets- och dataskyddsfrågor?

Drygt sju av tio har tagit fram riktlinjer för hur företaget ska hantera personuppgifter

Som en följd av dataskyddsförordningen har flertalet, drygt sju av tio företag, tagit fram riktlinjer och rutiner för hur verksamheten ska hantera och använda personuppgifter. En mindre andel, 17 procent har delvis tagit fram riktlinjer, och sju procent har inte tagit fram riktlinjer och rutiner för hantering av personuppgifter.

Även här finns ett samband mellan storlek på företaget och mognadsgrad i dataskyddsarbetet. Företag med fler än 50 anställda har i högre grad tagit fram rutiner och riktlinjer för personuppgiftshantering, medan företag med mellan en och nio anställda oftare uppger att de inte eller bara delvis tagit fram riktlinjer och rutiner.

Vissa skillnader finns också mellan olika branscher. Bland företag inom vård och omsorg uppger en majoritet att de tagit fram riktlinjer och rutiner, medan det är betydligt ovanligare inom transportbranschen.

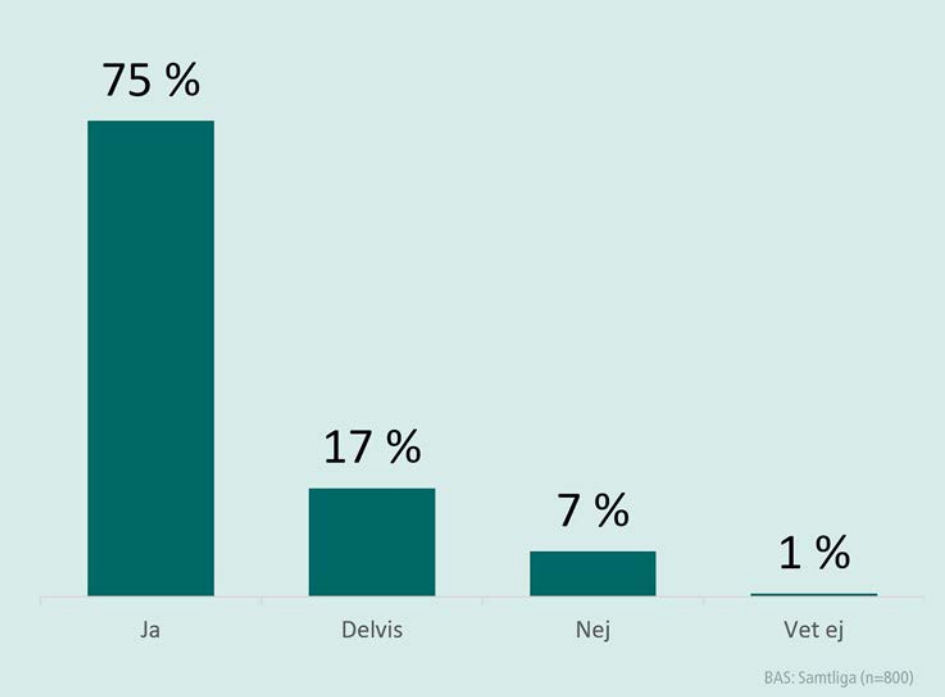

Bild 37. Fråga: Har ni som en följd av GDPR tagit fram riktlinjer och rutiner för hur er verksamhet ska hantera och använda personuppgifter?

Knappt sju av tio har tagit fram en förteckning över personuppgiftshantering

Företagen har i undersökningen också fått svara på om de vidtagit ett antal mer konkreta åtgärder i sitt dataskyddsarbete. Personuppgiftsansvariga och personuppgiftsbiträden är enligt dataskyddsförordningen skyldiga att föra en förteckning över behandlingar av personuppgifter, vilket knappt sju av tio företag uppger att de har. I detta sammanhang är det värt att påtala att den absoluta merparten av företagen som ingått i undersökningen har färre än 250 anställda, och därmed i vissa fall kan vara undantagna från skyldigheten att föra en förteckning.

Utbildningsbranschen är överrepresenterade bland de som tagit fram förteckningar. Småföretag med en till nio anställda samt transportbranschen har i högre grad delvis eller inte alls tagit fram förteckningar.

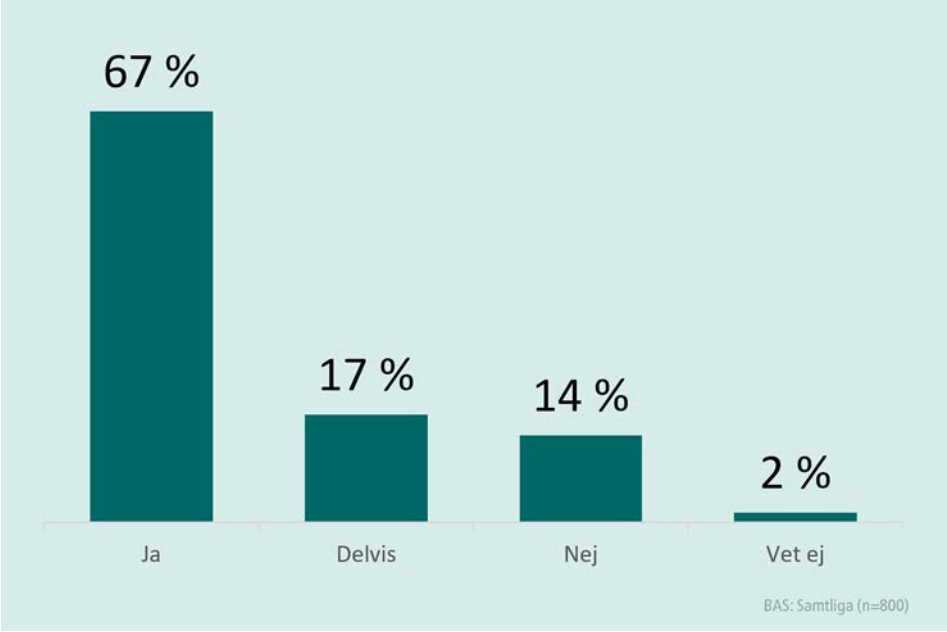

Bild 38. Har ni som en följd av GDPR tagit fram en förteckning över vilka personuppgifter ni använder i olika syften och sammanhang?

Många företag har rutiner för rensning av personuppgifter, men färre för rapportering av incidenter

Företagen har i undersökningen också fått svara på om de har fyra mer konkreta rutiner på plats; rutiner för att anmäla personuppgiftsincidenter till Datainspektionen, att lämna ut registerutdrag, att lagra och rensa personuppgifter samt att hantera personuppgifter i e-post.

Här kan noteras en viss skillnad i svaren gentemot undersökningen riktad mot dataskyddsombud. Bland dataskyddsombuden uppger flest att de har rutiner för att anmäla personuppgiftsincidenter till Datainspektionen och att lämna ut registerutdrag. Bland företagarna är det vanligaste svaret istället att de har rutiner för att lagra och rensa personuppgifter. Ungefär tre av fyra företag uppger att sådana rutiner finns.

Ungefär sex av tio företag i undersökningen har också tagit fram rutiner för att lämna ut registerutdrag samt hantering av personuppgifter i e-post. Endast fyra av tio företag uppger att de har rutiner för att rapportera personuppgifter till Datainspektionen.

Företag med fler än 50 anställda instämmer i högre grad i samtliga påståenden, medan små bolag med en till nio anställda är överrepresenterade bland dem som i högre omfattning inte instämmer i samtliga påståenden. Småbolagen är dessutom kraftigt överrepresenterade bland företag som saknar rutiner för att rapportera personuppgiftsincidenter.

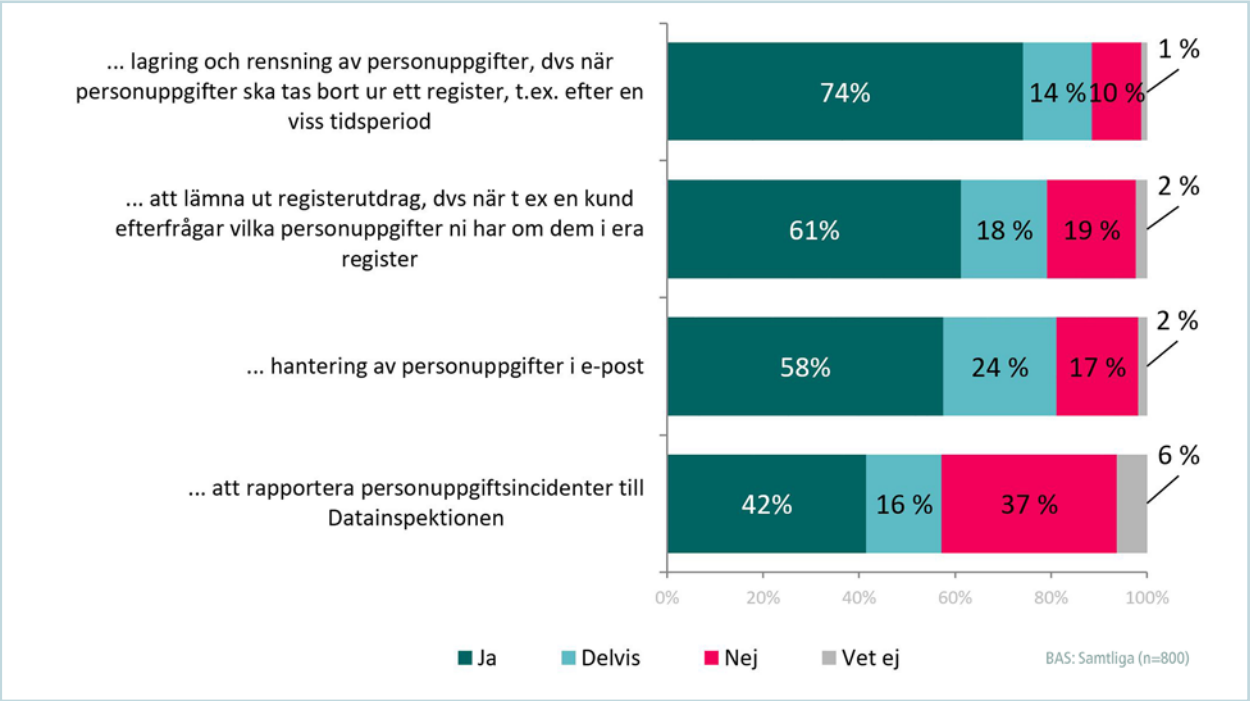

Bild 39. Fråga: Har ni rutiner för… ?

Drygt hälften av företagen arbetar i hög utsträckning kontinuerligt och systematiskt med integritets- och dataskyddsfrågor

Nästan sex av tio företag uppger att de i hög eller mycket hög utsträckning arbetar kontinuerligt och systematiskt med integritetsfrågor och dataskydd. Bland dessa är företag inom vård och omsorg samt utbildning överrepresenterade. Det finns också en överrepresentation av företag med fler än 50 anställda.

Omvänt är mindre företag, med mellan en och nio anställda, överrepresenterade bland dem som inte arbetar kontinuerligt och systematiskt med dataskydd. Totalt uppgav omkring ett av sju företag att de arbetar i mindre utsträckning eller inte alls har ett kontinuerligt och systematiskt arbete. I denna grupp finns en överrepresentation inom branscherna transport samt hotell och restaurang.

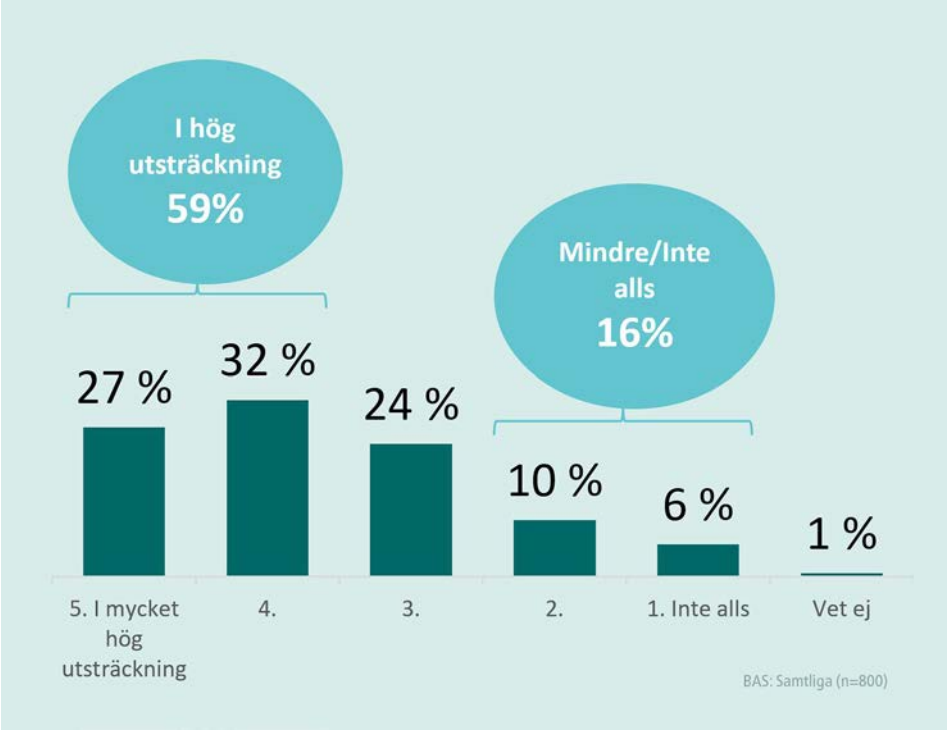

Bild 40. Fråga: I vilken utsträckning arbetar er organisation kontinuerligt och systematiskt med integritetsfrågor och dataskydd avseende personuppgiftshantering?

Medarbetarna anses i stor utsträckning ha fått information om dataskyddsförordningen och även efterleva det

Intervjupersonerna har tagit ställning till ett antal påståenden som bland annat rör medarbetarnas kunskap och inställning till dataskyddsförordningen. Tre av fyra företag i undersökningen anser att medarbetarna har fått information om hur personuppgifter ska hanteras enligt dataskyddsförordningen och att de också efterlever förordningen.

Två tredjedelar av företagen anser också att medarbetarna har förståelse för varför dataskyddsförordningen införts. Omkring hälften uppger att medarbetarna har kunskap om regelverket och tycker att det är viktigt.

Utbildningsföretag är överrepresenterade bland de som i högre grad instämmer i samtliga påståenden, medan företag inom transportbranschen är överrepresenterad bland de som i lägre grad instämmer i påståendena.

Här kan noteras en viss skillnad gentemot resultatet i undersökningen riktad mot dataskyddsombud. Bland dataskyddsombuden är det till exempel bara drygt hälften som anser att medarbetarna i organisationen efterlever dataskyddsförordningen. En del av skillnaden kan sannolikt förklaras med storlek på organisation. Majoriteten av dataskyddsom-

budens svar rör organisationer som är betydligt större än företagen i denna undersökning, vilket ökar komplexiteten i arbetet med att anpassa organisationen till nya regelverk. Det är också tänkbart att dataskydds-ombuden i större utsträckning inser hur mycket som krävs för att fullt ut efterleva dataskyddsförordningen, och därför skattar medarbetarnas regelefterlevnad lägre.

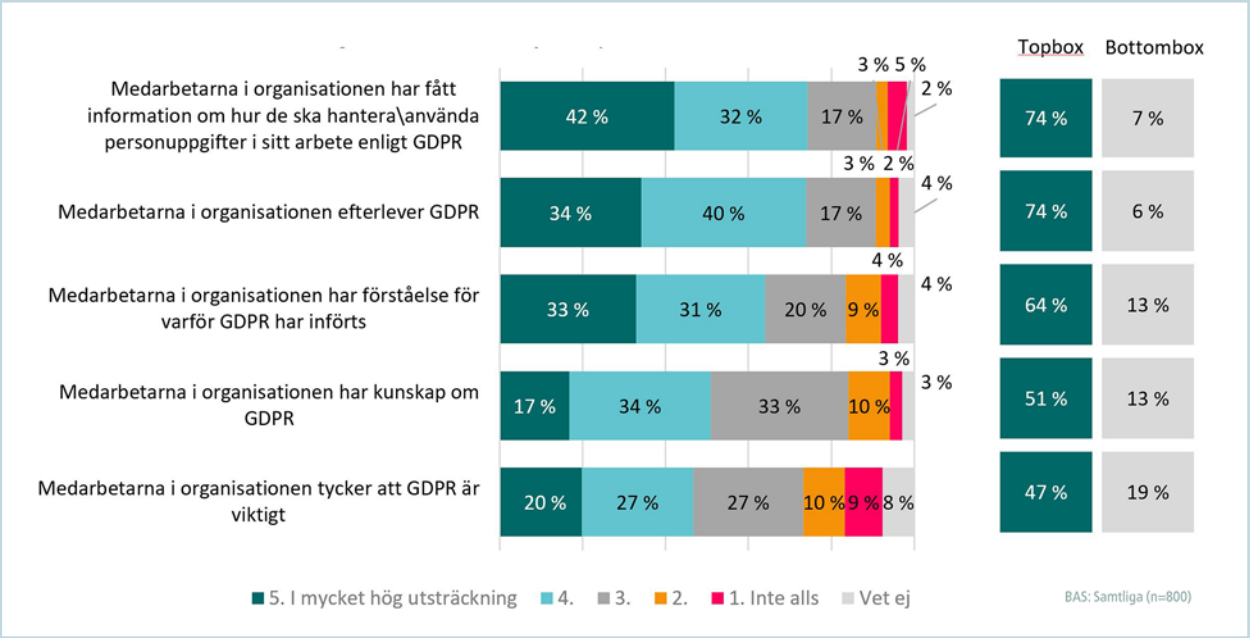

Bild 41. Fråga: I vilken utsträckning instämmer du i följande påståenden?

Största utmaningarna – tolkning av regelverket, att få till rutiner och processer samt ökad administration

De största utmaningarna som företagen upplever i dataskyddsarbetet handlar om att det är oklart hur regelverket ska tolkas och att få till fungerande rutiner och processer. Dessa är också de utmaningar som dataskyddsombuden upplever som svårast. För företagen tillkommer även utmaningen att dataskyddsförordningen upplevs som tidskrävande och innebär ökad administration. En något mindre andel uppger att det är svårt med alla regler, och att få alla medarbetarna att arbeta efter dataskyddsförordningen.

Bolag med fler än 50 anställda är överrepresenterade bland de som anser att största utmaningen är att få medarbetarna att arbeta efter dataskyddsförordningen.

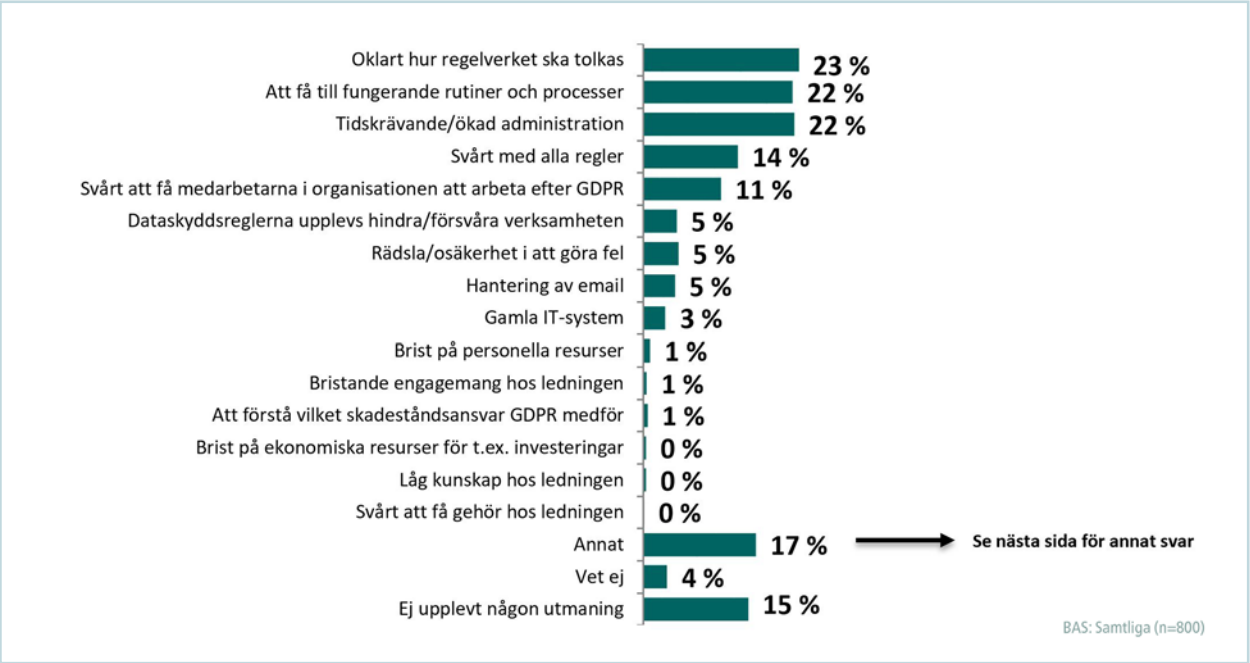

Bild 42. Fråga: Vad upplever du som den största utmaningen när det gäller att anpassa hanteringen av personuppgifter enligt GDPR?

Vilka frågor ställer företag, myndigheter och andra organisationer till Datainspektionen?

- **Avvägningar kring rättsliga grunder är den vanligaste frågan.** Omkring en tredjedel av de frågor som företag, myndigheter och andra organisationer ställer till Datainspektionen handlar om att verksamheten behöver stöd i avvägningar kring rättsliga grunder för personuppgiftsbehandling. Särskilt vanligt är frågor om samtycke och intresseavvägning.
- **Vad som är lämpliga säkerhetsåtgärder och vilka regler som gäller för kamerabevakning** står för ungefär en tiondel vardera av frågorna från verksamheter.
- **Gränsdragningar mellan olika personuppgiftsansvariga och personuppgiftsbiträden** står också för ungefär en tiondel av frågorna.

I båda undersökningarna framkommer att en av de största utmaningarna med dataskyddsförordningen är att tolka regelverket. Att många organisationer behöver stöd och vägledning i sitt dataskyddsarbete är också

påtagligt i inflödet av frågor till Datainspektionen. Myndigheten svarar varje dag på ett stort antal frågor via e-post och i telefonsamtal. En analys av de skriftliga frågor som företag, myndigheter och andra organisationer vänder sig med till Datainspektionen bidrar till att fördjupa bilden av vilka utmaningar verksamheterna har i arbetet med integritet och dataskydd.[14]

Under perioden 25 maj 2018 till 23 april 2018 kom det in cirka 8 200 skriftliga frågor Datainspektionen, varav ungefär hälften kom från företag, myndigheter och andra organisationer. Den andra hälften av frågorna kom från medborgare som till exempel vill ha stöd i att utöva sina rättigheter.

Privata företag är överrepresenterade bland de verksamheter som ställer frågor till Datainspektionen, ungefär sex av tio frågor kommer från den privata sektorn medan en av tio frågor kommer från kommuner. Bara några få procent av det totala antalet frågor till Datainspektionen kommer från statliga myndigheter. Ser man enbart till mer komplexa förfrågningar, som ofta kräver en rättslig utredning från Datainspektionen, ökar andelen frågor från statliga myndigheter, kommuner och aktörer inom hälso- och sjukvård.

Även hos ideella organisationer och ekonomiska föreningar finns ett stort behov av vägledning, de står för ungefär en femtedel av alla frågor som ställs till Datainspektionen. Ofta rör det sig om mindre organisationer som bostads- och hyresrättsföreningar eller idrottsföreningar som av förklarliga skäl ofta har mindre kunskap och resurser om dataskydd än större verksamheter.

14 Sammanställningen bygger på ett slumpmässigt urval av 200 frågor från verksamheter under perioden 25 maj 2018-10 april 2019. 100 av frågorna har besvarats i upplysningstjänsten och 100 av frågorna har rört mer komplicerade frågor som besvarats av Datainspektionens sakenheter. De vanligaste frågorna har kategoriserats och resultatet har därefter kvalitetssäkrats i intervjuer och workshops med medarbetare med stor erfarenhet av att besvara frågor från verksamheter.

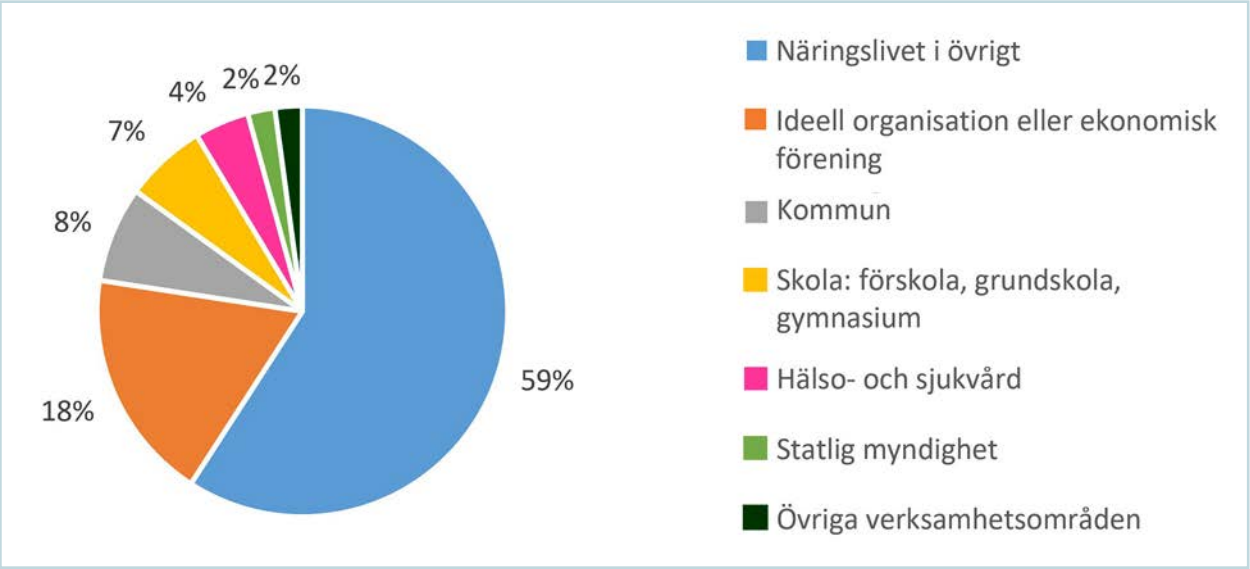

Bild 43. Branscher som ställer frågor till Datainspektionen.

Drygt en tredjedel av verksamheternas frågor till Datainspektionen handlar om stöd i avvägningar om den rättsliga grunden

För att en personuppgiftsbehandling ska vara laglig måste den stödja sig på någon av de sex olika rättsliga grunder som anges i dataskyddsförordningen. Avvägningar kring rättslig grund för att hantera personuppgifter är det område som genererar flest frågor till Datainspektionen. Ungefär en tredjedel av de frågor som verksamheter ställer till Datainspektionen rör ärenden där verksamheter på olika sätt behöver stöd kring de rättsliga grunderna.

Ofta efterfrågas vägledning kring giltigt samtycke och den intresseavvägning som behöver ske mellan verksamhetens behov av personuppgifter, och den enskildes rätt till skydd av uppgifterna.

Kombinationen av olika regelverk är också en utmaning för många som vänder sig till Datainspektionen. Vanliga frågor handlar till exempel om vad som gäller när en privatkund vill att bolaget raderar dennes personuppgifter, men bokföringslagen anger att samma personuppgifter ska sparas i sju år.

En av tio frågor handlar om gränsdragningar kopplat till personuppgiftsansvaret

Många verksamheter undrar vilket ansvar en personuppgiftsansvarig respektive ett personuppgiftsbiträde har. I vissa situationer kan två verksamheter vara separat eller gemensamt personuppgiftsansvariga, till exempel om de behandlar samma personuppgifter, vilket ytterligare kan komplicera gränsdragningen.

En av tio frågor rör säkerhetsåtgärder

I dataskyddsförordningen anges att verksamheter som hanterar personuppgifter måste vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå. Många verksamheter ställer frågor till Datainspektionen om säkerhetsåtgärder. En vanlig fråga är till exempel vilka tekniska säkerhetsåtgärder som är lämpliga för att skydda uppgifter i e-post. Vidare kan frågorna gälla organisatoriska åtgärder som till exempel behörighetsstyrning, det vill säga strukturen som styr vilka personer inom en organisation som får ta del av personuppgifter i olika system och register.

En av tio frågor rör kamerabevakning

Kamerabevakning utgör också ett vanligt frågeområde bland verksamheterna, omkring en tiondel av alla frågor rör kamerabevakning. Kamerafrågorna är överrepresenterade bland de mer komplexa förfrågningar som ofta kräver en rättslig utredning från Datainspektionen.

Den vanligaste frågan om kamerabevakning är om tillstånd behövs. Verksamheterna efterfrågar även vägledning kring vilka utrymmen och områden, både inom- och utomhus, som är lagliga att bevaka.

Återkommande frågor är även om det är tillåtet att bevaka avgränsade områden i anslutning till arbetsplatsen, till exempel en parkering, om arbetsgivare kan kamerabevaka butikspersonalen under arbetstid eller om skolor har rätt att bevaka eleverna under skoltid för att skapa lugn.

Stor variation i frågorna

Cirka en tredjedel av frågorna rör inte något av områdena ovan utan handlar om andra delar i dataskyddsarbetet. Det är en stor spridning på innehållet, men frågor som förekommer frekvent handlar till exempel om

- personuppgiftsbiträdesavtal
- dataskyddsombudens roll
- vad som ska redovisas i en personuppgiftspolicy
- vilka skyldigheter verksamheterna har när det gäller att lämna ut registerutdrag

- vad som är tillåtet när det gäller att behandla anställdas personuppgifter
- direktmarknadsföring
- under vilka omständigheter en personuppgiftsincident ska anmälas till Datainspektionen
- molntjänster och
- tredjelandsöverföring.

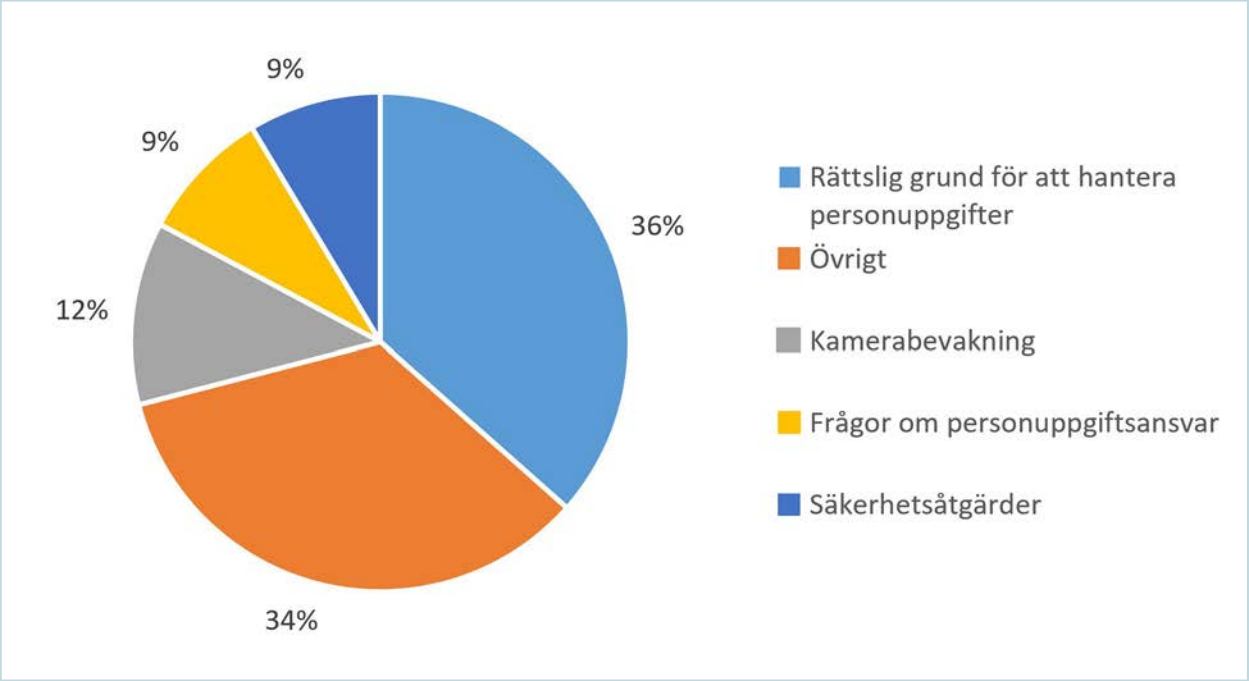

Bild 44. Frågeområden – verksamheter.

Vilken typ av personuppgiftsincidenter anmäls till Datainspektionen?

- **Bank- och finansbranschen är den bransch som anmäler flest personuppgiftsincidenter, de står för en femtedel av samtliga anmälda incidenter.** Majoriteten av de anmälda incidenterna från bank- och finansbranschen utgörs av mindre allvarliga incidenter, vilket förstärker intrycket från undersökningarna att bank- och finansbranschen har kommit långt när det gäller rutiner för arbetet med integritet och dataskydd.
- **Knappt hälften av de anmälda personuppgiftsincidenterna handlar om obehörigt röjande och obehörig åtkomst.** De anmälda incidenterna bekräftar resultatet från undersökningarna att det är en utmaning att få till fungerande rutiner och processer i arbetet med integritet och dataskydd.
- **Den mänskliga faktorn är den i särklass vanligaste anledningen till att incidenter inträffar.** Totalt förklaras sex av tio incidenter med den mänskliga faktorn, viket ger skäl att understryka vikten av att verksamheter som hanterar personuppgifter fortsätter att utbilda medarbetare och kontinuerligt följa upp riktlinjer och rutiner.

Genom dataskyddsförordningen infördes en skyldighet för alla verksamheter som behandlar personuppgifter att anmäla personuppgiftsincidenter till Datainspektionen. Ytterst syftar skyldigheten att anmäla personuppgiftsincidenter till att stärka integritetsskyddet. Genom anmälningsskyldigheten har kraven höjts på alla verksamheter som hanterar personuppgifter att ha rutiner på plats för att kunna upptäcka, rapportera och utreda incidenter.

Under perioden 25 maj 2018–1 maj 2019 fick Datainspektionen in drygt 3 500 anmälningar om personuppgiftsincidenter. I detta avsnitt sammanfattas några iakttagelser från inflödet av incidentanmälningar. [15] Några reflektioner kring inflödet av anmälda personuppgiftsincidenter görs också kopplat till resultatet från undersökningarna om hur långt företag,

15 Siffrorna i sammanställningen bygger på uppgifter från samtliga personuppgiftsincidentsanmälningar som anmälts under perioden 25 maj – 31 mars 2019. Datainspektionen har tidigare publicerat rapporten *Anmälda personuppgiftsincidenter 2018 (2019:1)*. I rapporten finns en mer utförligt beskrivning av de personuppgiftsincidenter som anmäldes under de första sju månaderna med GDPR. Fördelningen mellan branscher, typer av incident och vad incidenterna beror på är i princip oförändrade när ytterligare tre månader gått.

myndigheter och andra organisationer kommit i sitt arbete med integritet och dataskydd.

Flest personuppgiftsincidenter rapporteras från bank- och finansbranschen

Bank- och finansbranschen är den enskilda bransch som anmäler flest personuppgiftsincidenter. I undersökningen till verksamheter med dataskyddsombud är bank- och finansbranschen också överrepresenterade bland de som svarar att de har rutiner för att anmäla personuppgiftsincidenter.

Att en organisation eller bransch anmäler många personuppgiftsincidenter behöver inte vara en indikation på bristande säkerhet. I vissa fall kan det tvärtom tyda på att verksamheten har strukturer och rutiner som ger en god förmåga att upptäcka och rapportera personuppgiftsincidenter. Denna bild förstärks av resultatet i undersökningen riktad mot dataskyddsombud, där svaren från bank/finans genomgående indikerar att de kommit längre i arbetet med integritet och dataskydd än andra branscher.

Över 70 procent av anmälningarna från bank- och finansbranschen beror på felaktiga brevutskick, det vill säga att brev eller e-post som innehåller personuppgifter oavsiktligt hamnat hos fel mottagare. Att banker och övriga aktörer inom finansbranschen typiskt sett anmäler även mindre allvarliga incidenter tyder på stabila rutiner för att upptäcka och anmäla incidenter.

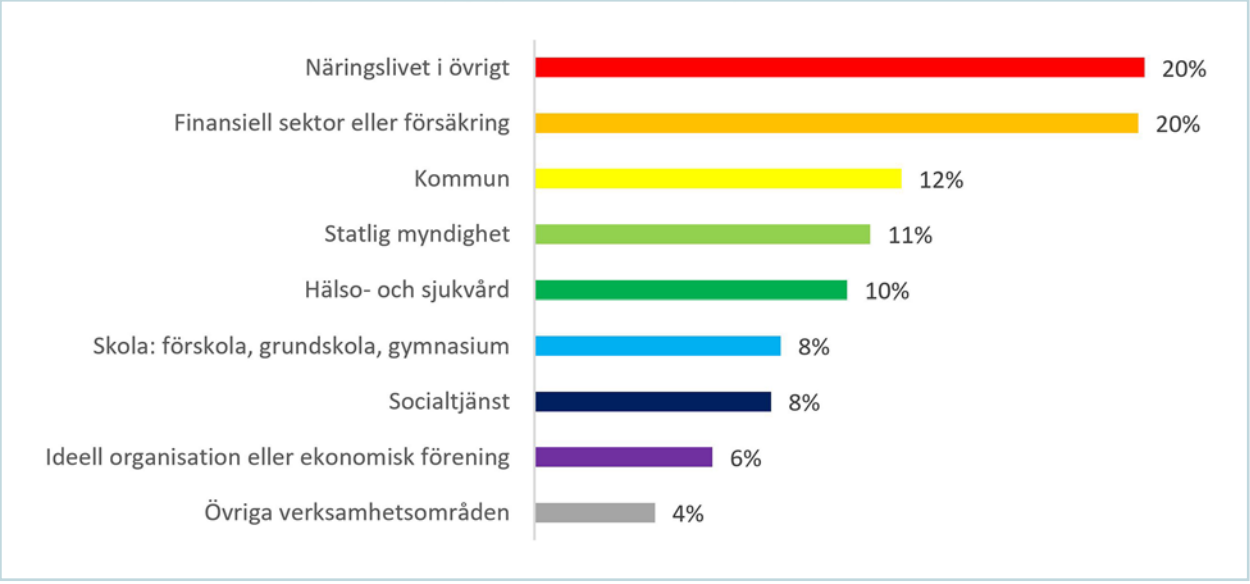

Bild 45: Andel personuppgiftsincidenter per verksamhetsområde.

Mänskliga faktorn vanligaste orsaken till personuppgiftsincidenter

Den mänskliga faktorn uppges vara den vanligaste orsaken till de anmälda personuppgiftsincidenterna. Nästan sex av tio incidenter berodde på den mänskliga faktorn. Typiskt sett handlar det om att individer begått ett misstag vid hantering av personuppgifter i sina verksamheter. Majoriteten av de personuppgiftsincidenter som beror på den mänskliga faktorn handlar om felskickade brev och e-postmeddelanden, men där finns också en rad andra typer av incidenter.

Att en så stor andel av incidenterna uppges bero på den mänskliga faktorn ger skäl att understryka vikten av att verksamheter som hanterar personuppgifter fortsätter att utbilda medarbetare och kontinuerligt följa upp riktlinjer och rutiner. Som undersökningen riktad till dataskyddsombud visar är det bara omkring en tredjedel av verksamheterna som svarar på ja på frågan om medarbetarna löpande får utbildning i frågor som rör integritet och dataskydd. Knappt hälften av dataskyddsombuden uppger att dataskydd och informationssäkerhet ingår i introduktionsutbildningen för nya medarbetare.

Antagonistiska angrepp är den näst vanligaste förklaringen till personuppgiftsincidenter. De utgör 15 procent av samtliga anmälningar. Totalt rör det sig om ungefär 500 incidenter, där stöld, förlust och olika former av it-angrepp är vanligast. De anmälda incidenterna kan handla till exempel om att tjänstedatorer glömts i kollektivtrafiken, att organisationen haft inbrott eller varit utsatta för ett it-angrepp genom till exempel phishing, malware eller hacking. Även om dessa incidenter är förhållandevis få till antalet är det typiskt sett större grupper av registrerade som berörs.

Värt att notera är att kategorin ”näringslivet i övrigt”, som totalt står för en femtedel av samtliga incidentanmälningar, anmäler betydligt fler antagonistiska angrepp än övriga sektorer. Det är den enda sektor där mänsklig faktor inte är den vanligaste orsaken till varför incidenter inträffar. Den vanligaste orsaken till varför incidenter inträffar är istället antagonistiska angrepp. Totalt har ”näringslivet i övrigt” anmält över 300 incidenter som uppges bero på antagonistiska angrepp.

Bild 46. Orsaker till incidenterna.

Stort antal incidenter handlar om obehörigt röjande och obehörig åtkomst

Som beskrivits ovan är felskickade brev den vanligaste typen av incident. Näst vanligast är obehörig åtkomst och obehörigt röjande.

Obehörig åtkomst står för en fjärdedel av alla anmälda personuppgiftsincidenter. Denna kategori handlar om att någon olovligen berett sig tillgång till personuppgifter, till exempel genom att behörigheter till ett it-system har tilldelats felaktigt eller för generellt. Ett annat återkommande exempel är att det upptäcks att personuppgifter har funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning.

Obehörigt röjande innebär att den personuppgiftsansvarige eller någon under den personuppgiftsansvariges ledning hanterat personuppgifter på ett sätt så att de kommit till obehörigas kännedom. Det kan handla till exempel om att en stor mängd mottagare av ett e-postmeddelande med känslig information kunnat se vilka andra som fått samma e-postmeddelande.

Att få till fungerande rutiner och processer beskrivs som den främsta utmaningen med dataskyddsförordningen i såväl undersökningen till dataskyddsombud som undersökningen till företag som inte anmält ett dataskyddsombud. Inflödet av personuppgiftsincidenter till Datainspektionen bekräftar bilden. Svårigheten att få till fungerande rutiner och processer är sannolikt också en bidragande förklaring till att så många incidenter orsakas av den mänskliga faktorn. Som framgår av diagrammet ovan uppges också att nästan en av tio incidentanmälningar direkt ha orsakats av brister i organisatoriska rutiner och processer.

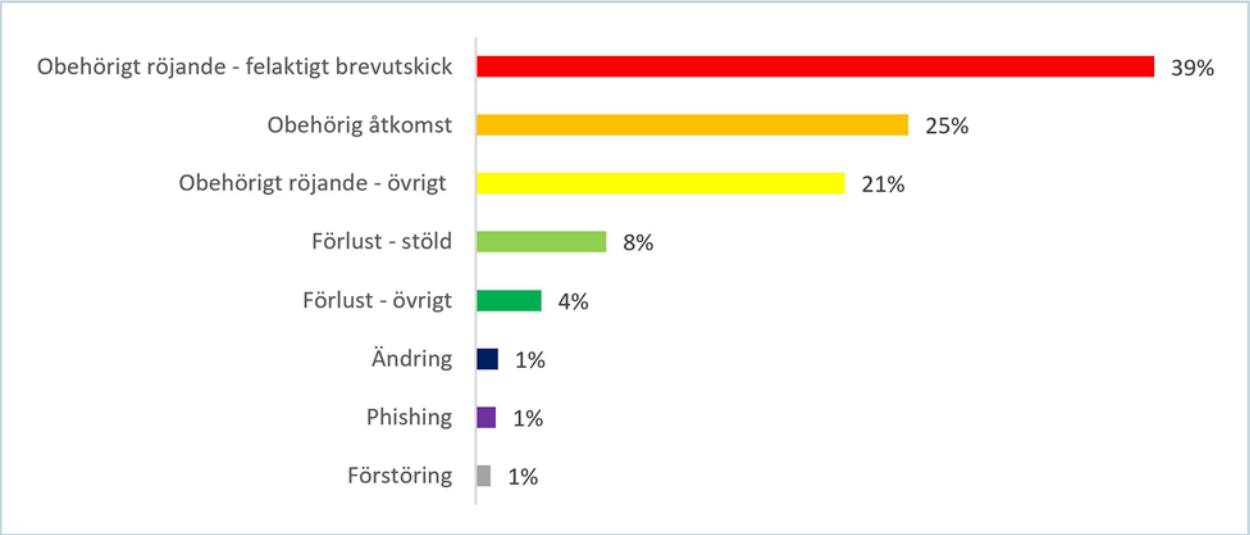

Bild 47: Typ av inrapporterade personuppgiftsincidenter.

Bilaga: Metodbeskrivning

Undersökningarna har genomförts av undersökningsföretaget Novus på uppdrag av Datainspektionen.

Undersökning: Integritet och dataskydd ur medborgarnas perspektiv

Syfte

Undersökningens syfte är att ge en bild av allmänhetens inställning, attityder och beteende avseende insamling och användning av person-uppgifter i främst digitala kanaler.

Metod

Målgrupp: Svenska allmänheten i åldrarna 18-79 år

Antal intervjuer: 1 003

Fältperiod: 21–27 februari 2019

Deltagarfrekvens: 53%

Urval: Undersökningen är genomförd via webbintervjuer i Novus slumpmässigt rekryterade och representativa Sverigepanel.

Det finns inget som tyder på att bortfallet skulle snedvrida resultatet, utan undersökningen är åsiktsmässigt representativ för den grupp som skulle undersökas, och de slutsatser som presenteras i undersökningen gäller hela populationen.

Redovisning av resultat

Resultaten för allmänheten levereras i en diagramrapport. Markerade signifikanta skillnader i rapporten är jämfört mot totalen (kön, ålder, utbildning och region). Resultatet har viktats mot verklig profil.

Felmarginal

Vid 1 000 intervjuer:
Vid utfall 20/80: +/- 2,5%
Vid utfall 50/50: +/- 3,2%

Undersökning: Integritet och dataskydd i verksamheter som utsett ett dataskyddsombud

Syfte

Undersökningens syfte är att öka förståelsen för dataskyddsombudens förutsättningar att arbeta med dataskyddsfrågor. Undersökningen ska även ge ökad kunskap om verksamheternas mognad avseende integritets- och dataskyddsfrågor, samt ge Datainspektionen bättre underlag för att stötta och vägleda dataskyddsombuden i deras arbete.

Metod

Målgrupp: Registrerade dataskyddsombud hos Datainspektionen

Antal intervjuer: 1 687

Fältperiod: 19 februari – 18 mars 2019

Deltagarfrekvens: 44%

Urvalsgrupper och antal svar:
DSO med 1 verksamhet – utskick till 2392 varav 1039 svar
DSO med 2 verksamheter – utskick till 556 varav 210 svar
DSO med 3 eller fler verksamheter – utskick till 908 varav 440 svar

Undersökningen är genomförd via webbintervjuer med urval från Datainspektionen.

Val av intervjuperson

I urvalet har senast registrerade dataskyddsombud valts som kontaktperson. Dataskyddsombud som ansvarar för fler än två verksamheter har fått en enkät för respektive verksamhet, dvs två enkäter totalt. Dataskyddsombud som ansvarar för fler än två verksamheter har också fått två enkäter, där de två verksamheterna valts slumpmässigt. Anledningen till att dataskyddsombud med fler än två verksamheter endast besvarat enkäter för två av verksamheterna är att vi bedömt det som alltför belastande att besvara fler enkäter. Tillvägagångssättet ökar antalet verksamheter i undersökningen, vilket också ökar möjligheten att dra relevanta slutsatser av undersökningsresultaten. I resultaten redovisas ett dataskyddsombud per verksamhet, oavsett om ombudet har svarat för en eller två verksamheter.

Redovisning av resultat

Resultaten för undersökningen levereras i en diagramrapport. Diagrammen redovisar procentandelar. I de diagram där totala procentsatsen överstiger 100 procent har flera svarsalternativ varit möjliga. Signifikanta skillnader mot totalen redovisas för olika undergrupper.

Felmarginal

Vid 1 000 intervjuer:
Vid utfall 20/80: +/- 2,5%
Vid utfall 50/50: +/- 3,2%

Vid 1600 intervjuer:
Vid utfall 20/80: +/- 2,0%
Vid utfall 50/50: +/- 2,5%

Undersökning: Integritet och dataskydd hos företag som inte anmält ett dataskyddsombud

Syfte

Undersökningen avser att öka kunskap och förståelse för företagens förutsättningar att arbeta med dataskyddsfrågor. Undersökningen ska även öka kunskapen om verksamheternas mognad avseende integritets- och dataskyddsfrågor.

Metod

Målgrupp: verksamheter som hanterar personuppgifter i form av kund-, leverantörsregister eller medlemsregister samt de verksamheter som har ett dataskyddsombud som inte är registrerat hos Datainspektionen.

Antal intervjuer: 800 efter screening (1 173 före screening)

Fältperiod: 19 februari – 19 mars 2019

Urval, deltagarfrekvens, total penetration och bortfallsredovisning :
Urvalet har levererats av SCB baserat på utvalda branscher. Branscherna är valda för att omfatta större mängder privatkunder samt även företagskunder. För att få en spridning över branscher och storleksklasser sattes följande kvoter:

	1–9 anst	10–49 anst	50+ anst	Total
Drift (el, vatten, avlopp)	30	30	30	90
Handel	50	50	50	150
Transport	30	30	30	90
Hotell/restaurang	30	30	30	90
Tjänsteföretag	70	70	60	200
Utbildning	30	30	30	90
Vård/omsorg	30	30	30	90
Total	**270**	**270**	**260**	**800**

Totalresultaten har sedan viktats mot verklig profil.

Nettourvalet omfattade 2 809 företag, varav 1 637 utgör bortfall:

- Ej anträffbara/telefonsvarare/bortresta/sjuka: 1 235 företag
- Vägrare: 402 företag

Av de som nåtts svarade 74% på undersökningen

Totalt genomfördes 1 173 bruttointervjuer (exkl screening), vilket betyder att den totala deltagarfrekvensen uppgick till 42%.

Totalt screenades 372 personer bort, kvar återstår 800 intervjuer

- Total penetration 68% (800 av 1173), d v s 32% har screenats bort enligt följande:
- 19% har inga register
- 13% har redan ett dataskyddsombud, som dock inte anmälts till Datainspektionen

Val av intervjuperson:

De tillfrågade att medverka i undersökningen är i första hand VD. Om inte VD varit tillgänglig eller nåbar har sökningen skett i följande ordning: ägare, ekonomichef, it-chef, annan person i verksamhetens ledning, eller annan person i verksamheten som bedömts bäst lämpad att svara på frågor som rör dataskydd.

Redovisning av resultat

Resultaten för undersökningen levereras i en diagramrapport. Diagrammen redovisar procentandelar. I de diagram där totala procentsatsen överstiger 100 procent har flera svarsalternativ varit möjliga. Signifikanta skillnader mot totalen redovisas för olika undergrupper. Resultatet är viktat mot verklig profil.

Felmarginal

Vid 800 intervjuer:
Vid utfall 20/80: +/- 2,8%
Vid utfall 50/50: +/- 3,5%

Kontakta Datainspektionen

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

Datainspektionen