Anmeldelser af brud på persondatasikkerheden i første kvartal 2019

Med databeskyttelsesforordningen blev der indført en generel forpligtelse for alle dataansvarlige til at anmelde brud på persondatasikkerheden til Datatilsynet. Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet.

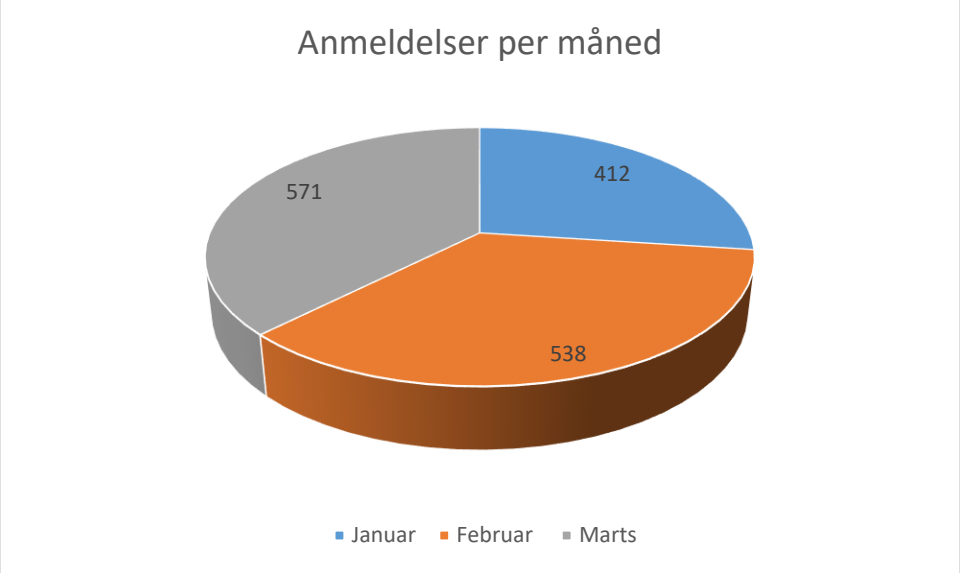
Udgangspunktet er, at brud på persondatasikkerheden altid skal anmeldes, med mindre det er usandsynligt, at det pågældende brud indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Den 6. februar 2019 offentliggjorde Datatilsynet første gang en oversigt over anmeldelser af brud på persondatasikkerheden for perioden fra den 25. maj til 31. december 2018.

Dette er en tilsvarende gennemgang af brud på persondatasikkerheden for første kvartal 2019.

Datatilsynet har i perioden fra 1. januar til 31. marts 2019 modtaget 1.521 anmeldelser om persondatasikkerhedsbrud, og hertil skal lægges henvendelser om grænseoverskridende persondatasikkerhedsbrud, som er indberettet gennem Det Europæiske Databeskyttelsesråds samarbejdsportal.

Der er i forhold til den første periode sket en stigning i antallet af anmeldelser på ca. 53 %. Når det gælder tallet for gennemsnitlige månedlige anmeldelser er det gået fra ca. 397 til 507 anmeldelser om måneden. Dette skal dog ses i sammenhæng med, at den første periode i sig selv indeholdt en stigning over tid, og at denne stigende tendens er fortsat hen over første kvartal 2019.



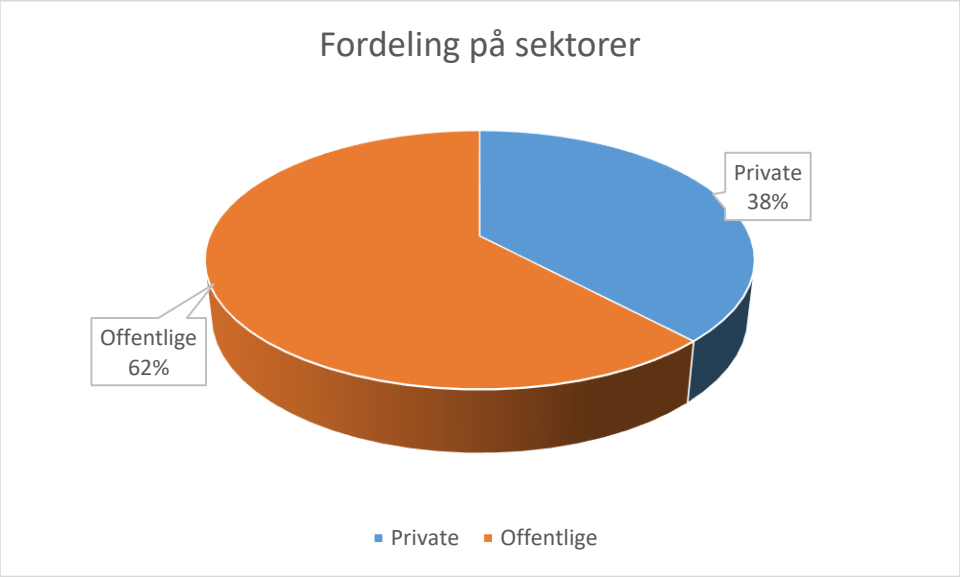
Der er stadigvæk sådan, at der generelt ikke bliver indgivet flere anmeldelser, end der er pligt til.

Der ses heller ikke væsentlige ændringer i de typer af brud, der bliver indberettet, og det er derfor tilsynets opfattelse, at det stigende antal anmeldelser primært skyldes, at de dataansvarlige har fået større rutine i de nye reglers anvendelse. Særligt er interne procedurer blevet opdateret i forhold til erfaringerne, sådan at flere reelle brud bliver opfanget og indberettet.

Fordelingen af anmeldelserne på de forskellige sektorer

Anmeldelserne fordeler sig med 38 % fra private dataansvarlige, 62 % fra offentlige dataansvarlige.

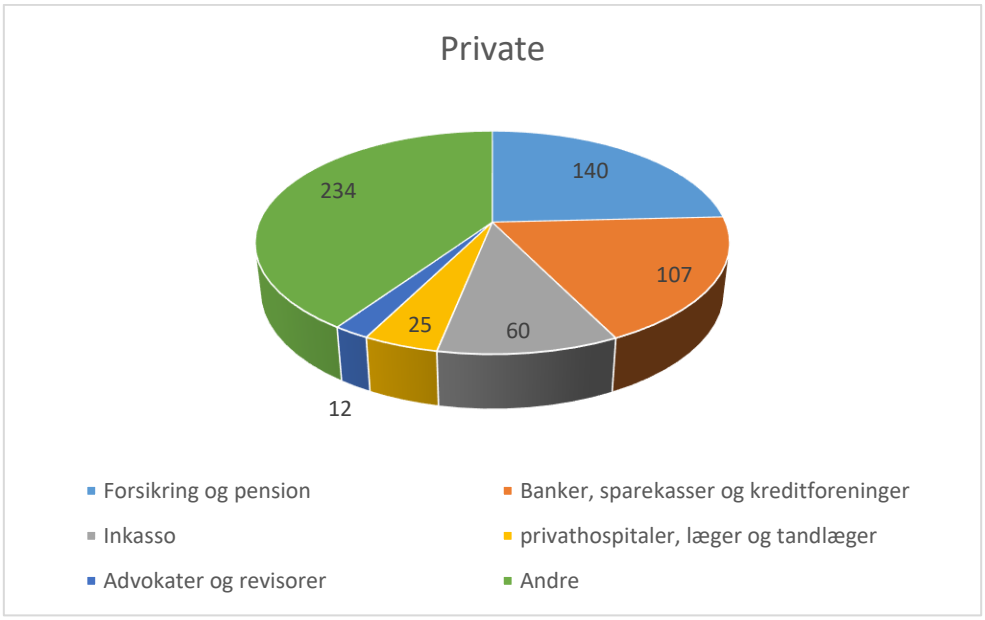
Den ændring, der er sket i forholdet mellem de to sektorer, skal ses i lyset af, at et stort antal brud fra private dataansvarlige på området for behandlinger af personoplysninger, der er foregået som led i udbud af offentligt tilgængelige elektroniske kommunikationstjenester, særligt telesektoren, nu ikke længere tilgår Datatilsynet. Herudover er indberetninger om grænseoverskridende brud nu flyttet fuldstændigt til Det Europæiske Databeskyttelsesråds samarbejdsportal.

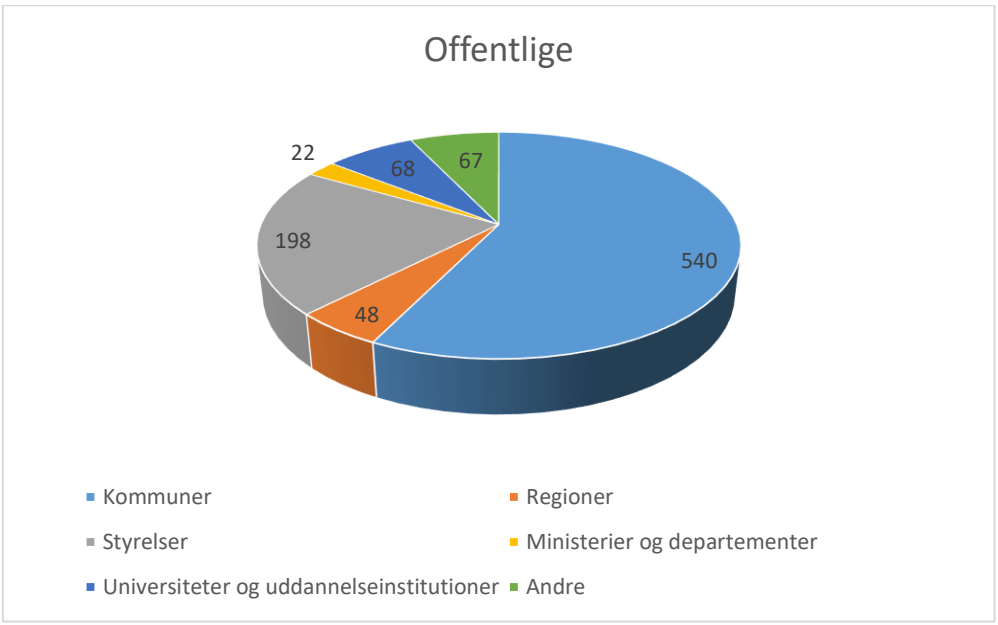


Dog er den generelle stigning i antallet af anmeldelser højere for den offentlige sektor, end det er i den private.

Det gælder – stadigvæk – for både de private og de offentlige anmeldelser, at de grupper af dataansvarlige, der har meget udadvendt kontakt med de registrerede, også er de dataansvarlige, der har flest anmeldelser.

Rigtig mange af anmeldelserne vedrører forhold, hvor oplysninger om en eller få registrerede er sendt på en sikker måde f.eks. via e-Boks, krypteret eller på en lukket kundeportal, men til en forkert modtager.





Anmeldelsernes karakter

Generelt er billedet det samme, som fremgik af oversigten for perioden fra 25. maj til 31. december 2018. Der er dog i den større mængde sager, der nu indkommer, primært tale om enkeltstående fejl af typen, hvor oplysninger sendes til den forkerte modtager.

Langt de fleste anmeldelser – nu mere end 2/3 – handler om oplysninger, der er sendt til den ”forkerte” modtager, oftest ved en menneskelig fejl i afsendelsesøjeblikket. Der er stadig en stor gruppe af brud, hvor

brevpost er sendt til den rette modtagers sidste folkeregisteradresse, men ved en fejl åbnes af en anden person, typisk fordi den registrerede er fraflyttet, eller fordi brevet bliver fejlafleveret af postbefordreren. Der er også en del anmeldelser af brud, hvor en fejl medfører, at oplysningerne ikke er undergivet den fortrolighed, som den dataansvarlige selv har vurderet nødvendig for behandlingen, f.eks. hvor e-mails, der efter intern instruks skulle sendes krypteret, bliver sendt uden at være det. Brud på persondatasikkerheden, der skyldes ekstern uretmæssig påvirkning såsom phishing, malware, hacking eller tilsvarende, er stadigvæk en mindre del af de samlede anmeldelser.

Den læring, der ses af de anmeldte brud på persondatasikkerheden er, at der – stadigvæk med fordel – kan arbejdes på de mere grundlæggende organisatoriske tiltag. Særligt der, hvor der benyttes funktionalitetsunderstøttelse såsom autoudførelse af e-mailadresser, standardbreve, der flettes til mange modtagere, og udsendelse af grafer, hvor de underliggende data ikke er fjernet, idet der stadig er mange anmeldelser af disse typer. Det skal som minimum overvejes at indføre tekniske og/eller organisatoriske foranstaltninger, der kan formindske risikoen ved brugen af de pågældende typer af behandlinger.

Der er generelt fokus på bedre sikring af personoplysninger, der opbevares på fysiske enheder og især de enheder, der enten hyppigt er udsat for tyveri eller let mistes under transport (telefoner, tablets, transportable harddiske, usb-sticks, hukommelseskort og bærbare computere). Datatilsynet vil gerne – igen – slå fast, at disse enheder – som udgangspunkt – slet ikke skal indeholde personoplysninger. I det omfang det er vurderet af den dataansvarlige, at de kan indeholde sådanne oplysninger, skal kryptering af indholdet være foretaget på en sådan måde, at ingen uvedkommende kan læse de pågældende oplysninger, hvis enheden mistes. Denne kryptering skal ikke kunne omgås.

Herudover kan de dataansvarlige med fordel instruere deres egne it-afdelinger og/eller deres respektive databehandlere om at foretage relevante løbende opdateringer af alle de system- og applikationskomponenter, der benyttes, og samtidig beskytte de netværk, de selv kontrollerer, mod trusler udefra ved en altid rigtigt konfigureret firewall.

Antallet af berørte

Også her er billedet det samme, som fremgik af oversigten for perioden fra 25. maj til 31. december 2018.

Generelt vedrører den altovervejende del af de indkomne anmeldelser brud, hvor antallet af berørte er én eller ganske få registrerede.

Undtagelserne er stadigvæk udsendelse af e-mails til flere modtagere, hvor bcc-feltet ikke er brugt, og flettebreve, hvor navn/adresse/andre personoplysninger er blevet "forskubbet", så alle på flettelisten har fået en andens oplysninger.

Uretmæssig påvirkning af informationssikkerheden begået af eksterne aktører er også en type af brud, der typisk også berører flere registrerede. Herudover er dette tilfældet, hvor en dataansvarlig har eksponeret hele eller store dele af datasæt indeholdende personoplysninger, på grund af fejl, manglende agtpågivenhed eller slet og ret fordi risikoen ved behandlingen enten ikke er vurderet eller er vurderet forkert.

Datatilsynets behandling af de indkomne brud

Datatilsynet er af den opfattelse, at sikkerhedsbrud, der udsætter fysiske personers rettigheder for risiko, generelt vil have karakter af forhold, som vil give anledning til - som minimum - kritik fra tilsynet.

Ved brud på persondatasikkerheden, der fremstår som en afgrænset og enkeltstående hændelse med en ringe risiko for de registreredes rettigheder, og hvor den dataansvarliges foranstaltninger i forlængelse af bruddet vurderes som umiddelbart tilstrækkelige i forhold til beskyttelsen af de registreredes rettigheder, vil Datatilsynet normalt afslutte sagen uden at udtale egentlig kritik.

Datatilsynet vil dog, hvis der fremkommer nye oplysninger i sagen, eller hvis der modtages nye anmeldelser om brud på persondatasikkerheden fra den pågældende dataansvarlige, kunne genoptage sagen og/eller lade denne indgå i vurderingen af eventuelle fremtidige brud.

Datatilsynet vil baseret på erfaringerne med sagsforløbet af de første afsluttede sager evaluere på, hvordan håndteringen af sagerne skal tilpasses sagsmængden.

Datatilsynet har for nuværende afsluttet 1.555 sager med et brev til de dataansvarlige.

De første sager med egentlige sanktioner er på vej ud til de dataansvarlige, og de første sager med indstilling om bødestraf vil blive overgivet til politi og domstole.

Datatilsynet forventer at offentliggøre både afgørelser og indstillinger til politianmeldelser på tilsynets hjemmeside.