Anmeldelser af brud på persondatasikkerheden

Efter den 25. maj 2018 – hvorfra databeskyttelsesforordningen finder anvendelse – er der blevet 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 der er usandsynligt, at det pågældende brud indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

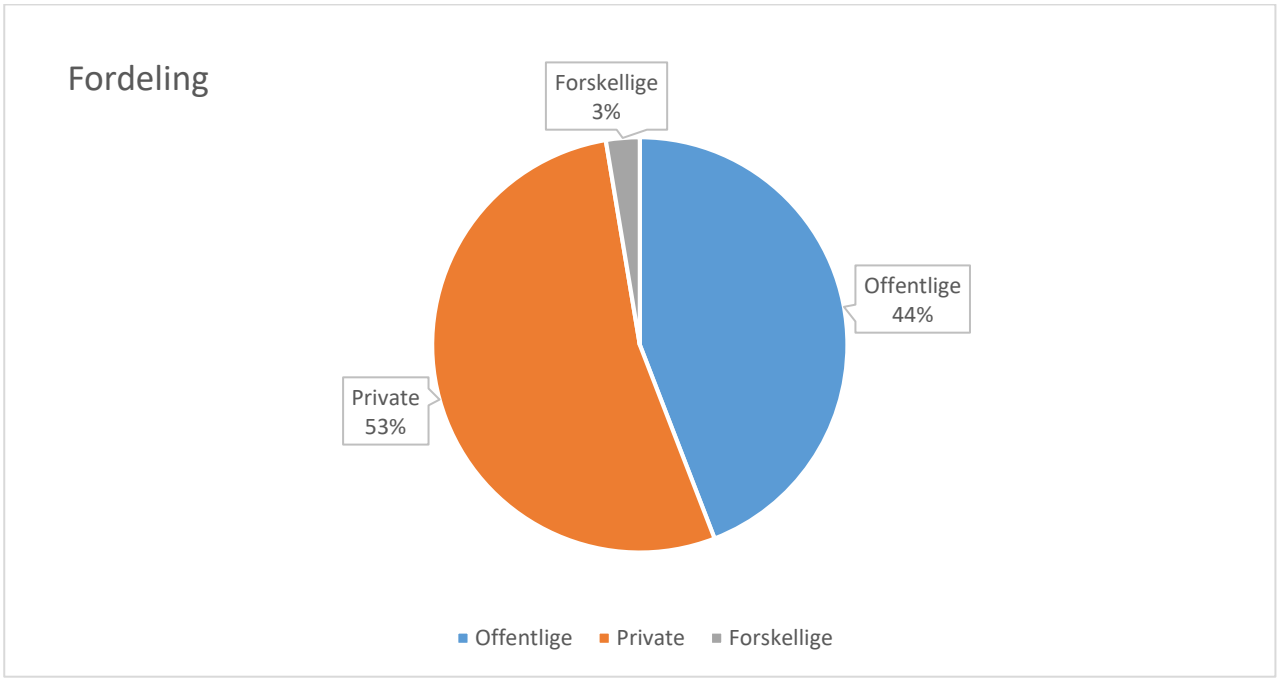
Denne tekst er en overordnet gennemgang af de anmeldelser om persondatasikkerhedsbrud, som Datatilsynet har modtaget i 2018 under databeskyttelsesforordningens anvendelse.

Datatilsynet har i perioden fra den 25. maj til 31. december 2018 modtaget 2.780 anmeldelser om persondatasikkerhedsbrud, ligesom tilsynet i samme periode har modtaget henvendelser om grænseoverskridende persondatasikkerhedsbrud gennem Det Europæiske Databeskyttelsesråds samarbejdsportal.

Der er kun ganske få af anmeldelserne, der ikke har indeholdt et brud på persondatasikkerheden, og det må derfor konstateres, at der generelt ikke bliver indgivet anmeldelser, der ikke er pligt til.

Fordelingen af anmeldelserne på de forskellige sektorer

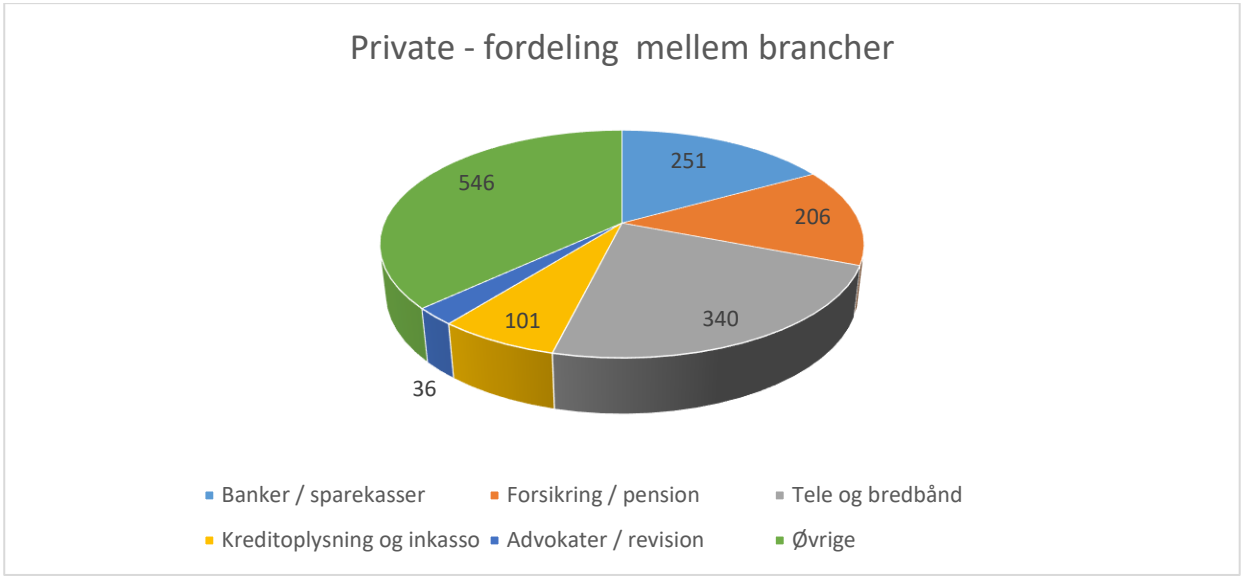
Anmeldelserne fordeler sig med 53 % fra private dataansvarlige, 44 % fra offentlige dataansvarlige og 3 % i gruppen forskellige. De forskellige er typisk grænseoverskridende brud for private dataansvarlige, anmeldt direkte til Datatilsynet her i Danmark.

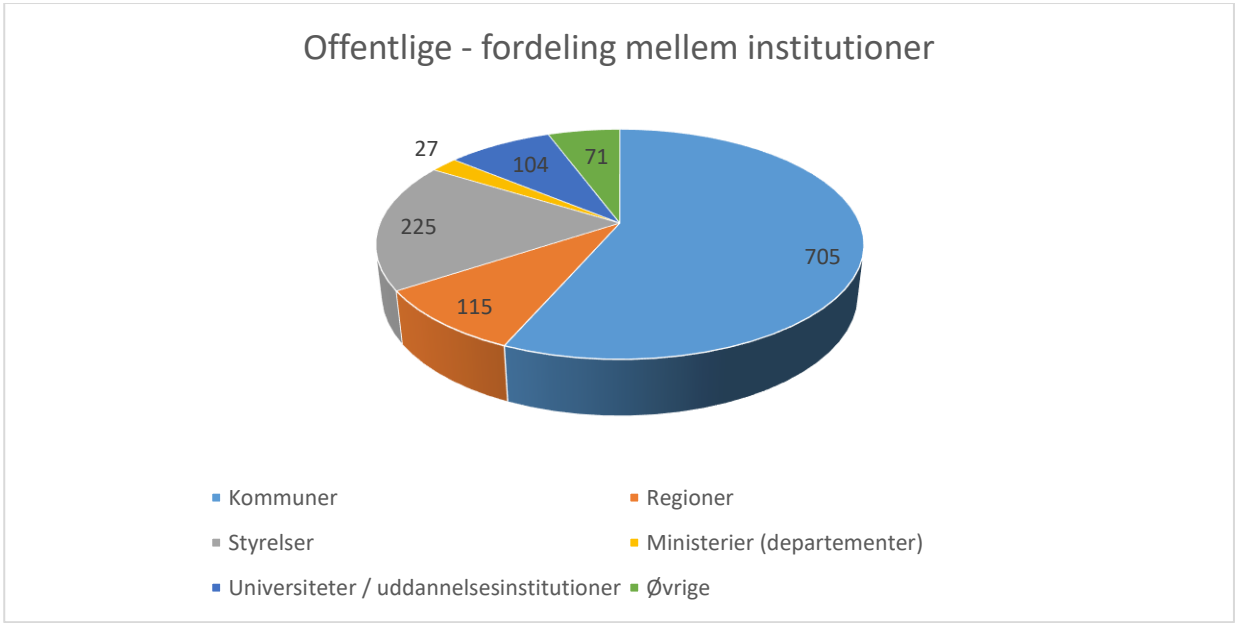


Det bemærkes, at hvor der i den første del af perioden var en overvægt af anmeldelser fra private dataansvarlige, har fordelingen mod slutningen af perioden bevæget sig mod en svag overvægt af offentlige anmel-

delser. Dette skyldes blandt andet, at anmeldelser fra dataansvarlige på området for behandlinger af personoplysninger, der er foregået som led i udbud af offentligt tilgængelige elektroniske kommunikationstjenester, særligt telesektoren, nu primært tilgår Erhvervsstyrelsen.

Generelt gælder det 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. 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

Datatilsynet har konstateret, at langt de fleste anmeldelser - ca. 2/3 - går på oplysninger, der er sendt til den "forkerte" modtager, oftest ved en menneskelig fejl i afsendelsesøjeblikket. I tillæg til denne gruppe er der en særlig variant heraf, der tegner sig for ca. 5 % af anmeldelserne. Det drejer sig om situationer, 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. En anden udbredt gruppe af anmeldelser er oplysninger, der ved en fejl 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. Tyveri af udstyr eller dokumenter fra aflåste lokaler, boliger og biler eller de tilfælde, hvor udskrifterne eller enheden bliver mistet i det offentlige rum, typisk i offentlige transportmidler, forekommer også relativt ofte. Brud på persondatasikkerheden, der skyldes ekstern uretmæssig påvirkning såsom phishing, malware, hacking eller tilsvarende udgør mindre end 5 % af de samlede anmeldelser. Typisk vil denne type hændelser dog berøre et højere antal registrerede.

Den umiddelbare læring af de anmeldte brud på persondatasikkerheden er, at visse typer af funktionalitetsunderstøttelse såsom autoudførelse af e-mailadresser, standardbreve, der flettes til mange modtagere, og udsendelse af grafer, hvor de underliggende data ikke er fjernet, skal revurderes hos de respektive dataansvarlige. I hvert fald skal det som minimum overvejes at indføre tekniske og/eller organisatoriske foranstaltninger, der kan formindske risikoen ved brugen af de pågældende typer af behandlinger. Herudover skal Datatilsynet erindre om at benytte bcc og ikke cc ved afsendelse af mail til flere modtagere.

Der er behov for 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). Disse enheder skal som udgangspunkt slet ikke indeholde personoplysninger, men 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.

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 applikations-komponenter der benyttes og samtidig beskytte de netværk, de selv kontrollerer, mod trusler udefra ved en altid rigtigt konfigureret firewall.

Antallet af berørte

Generelt vedrører den altovervejende del af de indkomne anmeldelser brud, hvor antallet af berørte er én eller ganske få registrerede. Således vedrører ca. 80 % af anmeldelserne mindre end fem berørte registrerede. Der findes typiske grupper af anmeldelser, hvor antallet af berørte er højere, nemlig 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. Som nævnt tidligere, berører de fleste typer af påvirkning af informationssikkerheden begået af eksterne aktører også 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

Når et brud bliver anmeldt til Datatilsynet, vil tilsynet, efter journalisering, foretage en vurdering af risikoen for de registreredes rettigheder, risikoprofilen af den hændelse, der ligger til grund for bruddet, omfanget af bruddet og forhold, der kan relateres til den dataansvarlige, herunder om der er sket en vurdering af, om de registrerede skal underrettes og i givet fald om underretning er sket.

Sikkerhedsbruddet vil herefter – på baggrund af vurderingen – blive sagsbehandlet.

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.

Halvdelen af de indkomne sager – ca. 1.400 – forventes afsluttet af Datatilsynet på den anførte måde, og af disse er ca. 900 allerede afsluttet med et brev til de dataansvarlige.

Omkring 700 sager er stadig under behandling, hvilket betyder, at de er ved at blive oplyst eller vurderet. De sidste ca. 600 sager er sager, hvori der, på grund af antallet af anmeldelser hos den enkelte dataansvarlige, pågår en genvurdering fra tilsynets side. Begge disse grupper af sager behandles med henblik på, at Datatilsynet træffer en afgørelse og fastsætter en sanktion, herunder f.eks. politianmeldelse.

55 af sagerne har været undergivet hastesagsbehandling grundet bruddets karakter. Dette kan f.eks. skyldes, at risikoen for de registreredes rettigheder har været høj, typisk på grund af at eksponering af data stadig skete efter anmeldelsen, eller at akut underretning af de registrerede har været vurderet nødvendig.