Anmeldelser af brud på persondatasikkerheden

Fjerde kvartal 2019

Februar 2020

DATATILSYNET

Indhold

1. Anmeldelser af brud på persondatasikkerheden i fjerde 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.

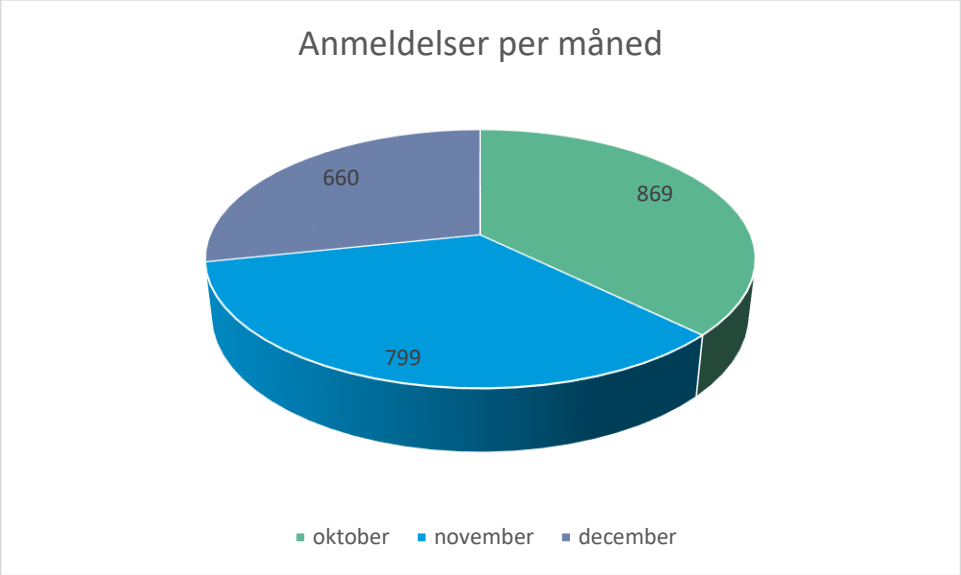
Udgangspunktet er, at brud på persondatasikkerheden altid skal anmeldes, med mindre det er usandsynligt, at det pågældende brud indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Datatilsynet udgiver kvartalsvist en oversigt over anmeldelser af brud på persondatasikkerheden, dog sådan at den første oversigt vedrørte perioden fra den 25. maj til 31. december 2018.

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

Datatilsynet har i perioden fra 1. oktober til 31. december 2019 modtaget 2.328 anmeldelser om persondatasikkerhedsbrud, og hertil skal lægges henvendelser om grænseoverskridende persondatasikkerhedsbrud, som er indberettet gennem Det Europæiske Databeskyttelsesråds samarbejdsportal.

Dette tal er en stigning på ca. 30 % sammenlignet med tallene fra de foregående kvartaler i 2019. Stigningen, der primært kan henføres til oktober og november måned, skyldes et mindre antal hændelser hos databehandlere, der løser opgaver for flere dataansvarlige. December måneds tal er på linje med det niveau og den trend, der var for det foregående kvartal, nemlig at antallet af indberetninger i den periode havde nået et mere ensartet niveau.



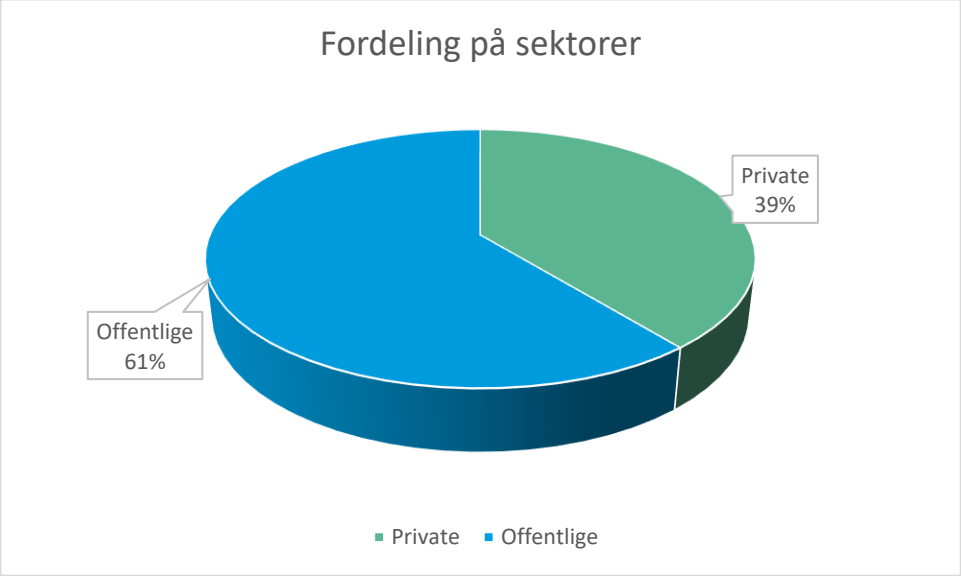
Det er stadigvæk sådan, at der ikke bliver indgivet flere anmeldelser, end der er pligt til.

Generelt ses der heller ikke væsentlige ændringer i de typer af brud, der bliver indberettet, og det er derfor tilsynets opfattelse, at der nu har etableret sig en fast rutine blandt de dataansvarlige, og reglernes anvendelse synes at være blevet alment kendt. Særligt vidner anmeldelserne om, at de dataansvarlige – generelt – har fået et godt overblik over interne procedurer og opsamlet erfaringer, sådan at de reelle brud, der sker, bliver opfanget og indberettet.

2. Fordelingen af anmeldelserne på de forskellige sektorer

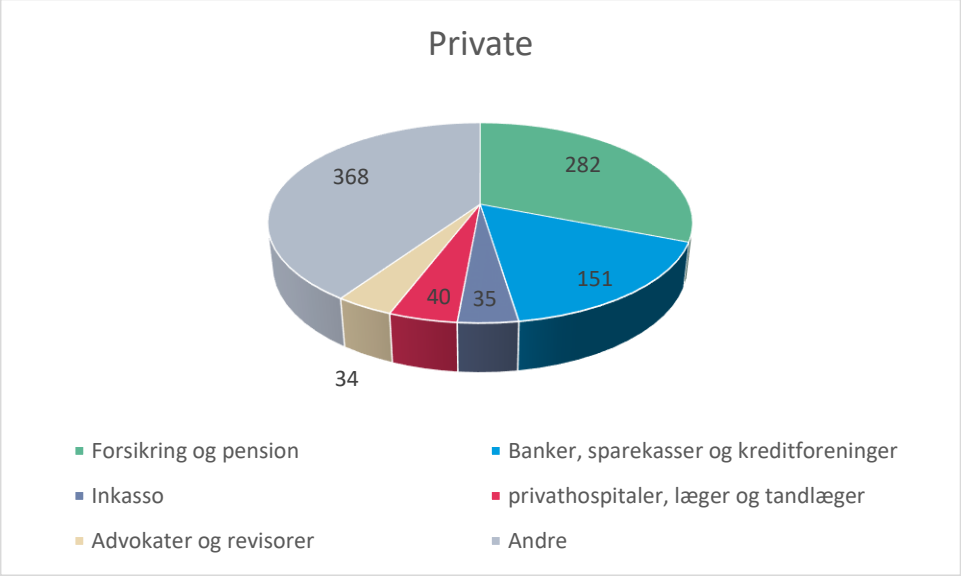
Anmeldelserne fordeler sig med 39 % fra private dataansvarlige, 61 % fra offentlige dataansvarlige.

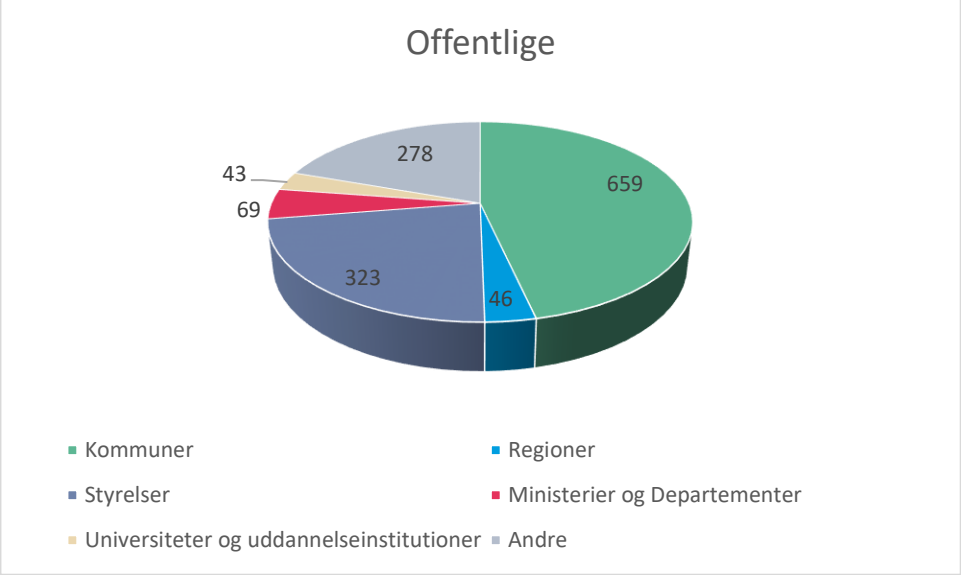
Denne fordeling er omtrent som i det forrige kvartal, men enkeltbrud hos databehandlere med services, der benyttes af mange dataansvarlige, kan periodisk ændre tallene i den ene eller anden retning. Som også anført i den foregående rapport er en del af forklaringen, at der nu også er flere af sikkerhedsbruddene hos de private dataansvarlige, der beror på enkelthændelser hos en databehandler, der så får effekt for en flerhed af private dataansvarlige.



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.

Langt den overvejende del 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.


Private
282
151
35
40
34
368
Forsikring og pension
Banker, sparekasser og kreditforeninger
Inkasso
privathospitaler, læger og tandlæger
Advokater og revisorer
Andre


Offentlige
659
46
323
69
43
278
Kommuner
Regioner
Styrelser
Ministerier og Departementer
Universiteter og uddannelseinstitutioner
Andre

3. Anmeldelsernes karakter

Generelt er billedet det samme, som er fremgået af de tidligere oversigter. Der er primært tale om enkeltstående fejl af typen, hvor oplysninger sendes til den forkerte modtager.

Det er stadigvæk over 70 % af de indkomne anmeldelser, der handler om oplysninger, der er sendt til den "forkerte" modtager, oftest ved en menneskelig fejl i afsendelsesøjeblikket. Den stigning i brud på persondatasikkerheden, der skyldes ekstern uretmæssig påvirkning såsom phishing, malware, hacking eller tilsvarende, som blev konstateret i første til tredje kvartal af 2019, er også tilstede i den nye periode. Disse hændelser udgør dog stadigvæk en mindre del af de samlede anmeldelser. Der er stadig en relativt høj intensitet af angrebsforsøg, der gør sig gældende vedrørende den generelle it-sikkerhed.

Der er i forhold til den forrige periode – igen – sket en stigning i antallet af uautoriserede adgangsforsøg inden for den såkaldte credential stuffing, altså tilfælde hvor uvedkommende forsøger at få adgang til forskellige tjenester og services (eller finde yderligere oplysninger om den registrerede) ved at forsøge logon med kendte kompromitterede kombinationer af brugernavne og kendeord.

Manglende tilgængelighed på grund af cryptolockers/ransomware forekommer stadig i et vist omfang, og der er stadigvæk flere tilfælde hvor reetablering fra backup – når dette var påkrævet – ikke har kunnet ske, og reetablering ikke har været forsøgt testet.

Der er generelt fokus på sikring af personoplysninger, når disse opbevares på fysiske enheder, der enten hyppigt er udsat for tyveri eller let mistes under transport (telefoner, tablets, transportable harddiske, usb-sticks, hukommelseskort og bærbare computere). Da der stadigvæk er flere af denne type af anmeldelser, hvor der ikke er sket reel kryptering af data på enheden, skal Datatilsynet igen indskærpe, 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. Brugernavn og kendeord på operativsystemniveau er **ikke** tilstrækkelig sikkerhed.

Blandt offentlige dataansvarlige har der kunnet konstateres, at især manglende anonymisering ved offentliggørelse af dagsordentekster og videregivelse ved aktindsigtsanmodninger forekommer som typetilfælde på brud på persondatasikkerheden. Datatilsynet opfordrer til, at der implementeres kvalitetskontrol eller anden foranstaltning, der – som yderligere et led – gennemgår disse ekspeditioner, da det ofte er følsomme oplysninger, der ved denne type hændelser kommer uvedkommende til kendskab.

Der er stadigvæk alt for mange tilfælde af den særlige form for "social engineering", hvor både nuværende og tidligere kærester/ægtefæller eller samlevende udnytter viden om den anden part i relationen til at få oplysninger fra kommunen, banken, telefonselskabet eller andre. Datatilsynet vil gerne indskærpe, at der etableres rutiner omkring de situationer, hvor oplysningerne gives til andre end den registrerede selv.

Datatilsynet skal indskærpe, at der **skal** tages stilling til om der skal ske underretning til de registrerede eller ej. Datatilsynet må stadigvæk jævnligt konstatere et betydeligt antal tilfælde svarende til ca. 15 % af anmeldelserne, hvor der ikke er foretaget en korrekt og fyldestgørende vurdering af, om der skal ske underretning til de registrerede. Den dataansvarlige skal kunne dokumentere, at de har vurderet risikoen for den registreredes rettigheder efter databeskyttelsesforordningens artikel 34, stk. 1, og det skal kunne godtgøres - såfremt en dataansvarlig ikke har informeret en registreret i de tilfælde, hvor der sandsynligvis er en høj risiko for den registreredes rettigheder. Datatilsynet har i perioden udstedt flere påbud til dataansvarlige om at foretage en sådan underretning.

Generelt er der mange tilfælde, hvor der under udviklingen af nye systemer og i testsituationer sker brud på persondatasikkerheden. Derfor skal det **indskærpes**, at alle produktionsdata,

kendeord, brugernavne, ip-adresser, certifikater og øvrige angrebsvektorer skal undergives en passende sikkerhed. En sådan sikkerhed skal som minimum være på niveau med det, der gælder for produktionsmiljøet, hvilket risikovurderingen skal afspejle. Det er Datatilsynets opfattelse, at brugen af produktionsdata til testformål ikke bør forekomme, andet end i helt enkeltstående tilfælde, og altid kun når niveauet af sikkerhed er minimum det samme som er vurderet passende for drifts-setuppet.

Der ses stadig for mange anmeldelser, hvor den dataansvarliges it-afdeling og/eller deres respektive databehandlere ikke har foretaget relevante løbende opdateringer af alle de system- og applikationskomponenter, der benyttes, og har beskyttet de netværk, de selv kontrollerer, mod trusler udefra ved en altid rigtigt konfigureret firewall.

4. Antallet af berørte

Billedet er her det samme, som fremgik af de tidligere oversigter.

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

Der er færre anmeldelser med udsendelse af e-mails til flere modtagere, hvor bcc-feltet ikke er brugt, men så tilsvarende flere med 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 der stadig tilfælde, 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.

5. 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.

Der er i perioden fra 25. maj 2018 til 31. december 2019 modtaget lidt over 10.000 anmeldelser. Af disse er de fleste brud på persondatasikkerheden, der fremstår som afgrænsede og enkeltstående hændelser med en ringe eller kun lille risiko for de registreredes rettigheder.

Af disse er ca. 9.500 allerede afsluttet over for den enkelte dataansvarlige. Et antal vedrører gentagelsestilfælde for godt 18 dataansvarlige med flere anmeldte brud. Herudover er der omkring 500 sager i forskellige stadier af afklaring af de faktiske omstændigheder med henblik på vurdering af eventuel sanktion og afgørelse.

Anmeldelser af brud på persondatasikkerheden

Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk