Anmeldelser af brud på persondatasikkerheden

Andet kvartal 2019

August 2019

DATATILSYNET

Indhold

1. Anmeldelser af brud på persondatasikkerheden i andet 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.

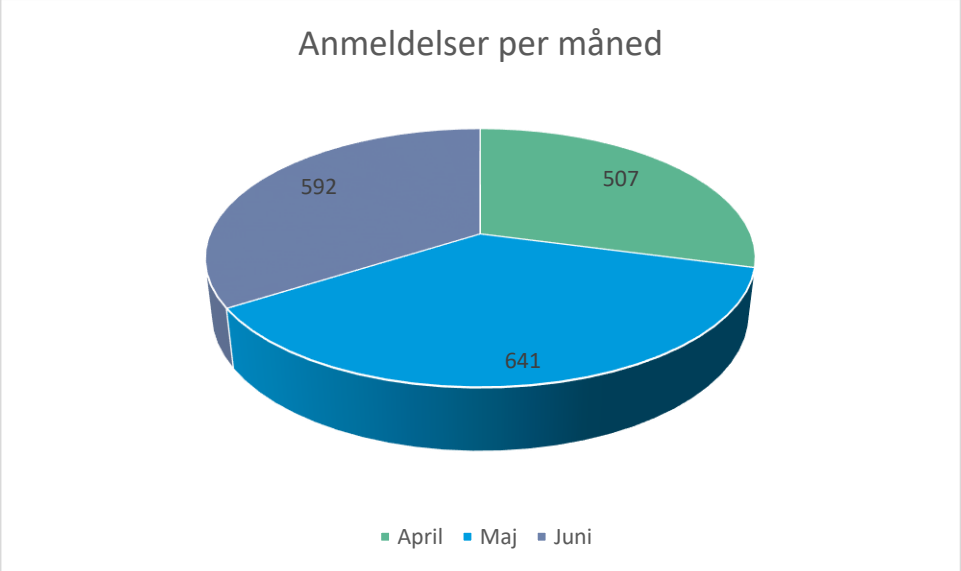
Udgangspunktet er, at brud på persondatasikkerheden altid skal anmeldes, med mindre det er usandsynligt, at det pågældende brud indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

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 andet kvartal 2019.

Datatilsynet har i perioden fra 1. april til 30. juni 2019 modtaget 1.740 anmeldelser om persondatasikkerhedsbrud, og hertil skal lægges henvendelser om grænseoverskridende persondatasikkerhedsbrud, som er indberettet gennem Det Europæiske Databeskyttelsesråds samarbejdsportal.

Der er i forhold til det første kvartal 2019 sket en yderligere stigning i antallet af anmeldelser på ca. 14 %. Når det gælder tallet for gennemsnitlige månedlige anmeldelser er det gået fra ca. 507 til 580 anmeldelser om måneden. Dette skal dog ses i sammenhæng med, at der siden den 25. maj 2018 har været en stigning på mere end 50 % over tid. Det tyder dog på, at det for sidste del af det andet kvartal i 2019 er ved at findes et mere stabilt niveau.



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

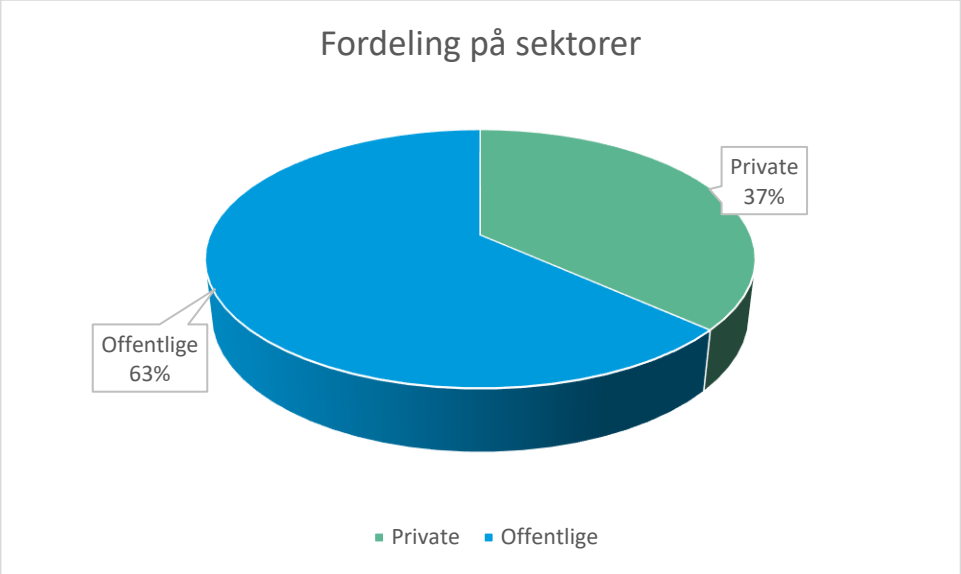
Der ses heller ikke væsentlige ændringer i de typer af brud, der bliver indberettet, og det er derfor tilsynets opfattelse, at den større rutine, de dataansvarlige har fået i de nye reglers

anvendelse, synes at være blevet alment udbredt. Særligt vidner anmeldelserne om, at de dataansvarlige – generelt – har fået et godt overblik over interne procedurer og opsamlet erfaringer, sådan at de skete reelle brud bliver opfanget og indberettet.

2. Fordelingen af anmeldelserne på de forskellige sektorer

Anmeldelserne fordeler sig med 37 % fra private dataansvarlige og 63 % fra offentlige dataansvarlige.

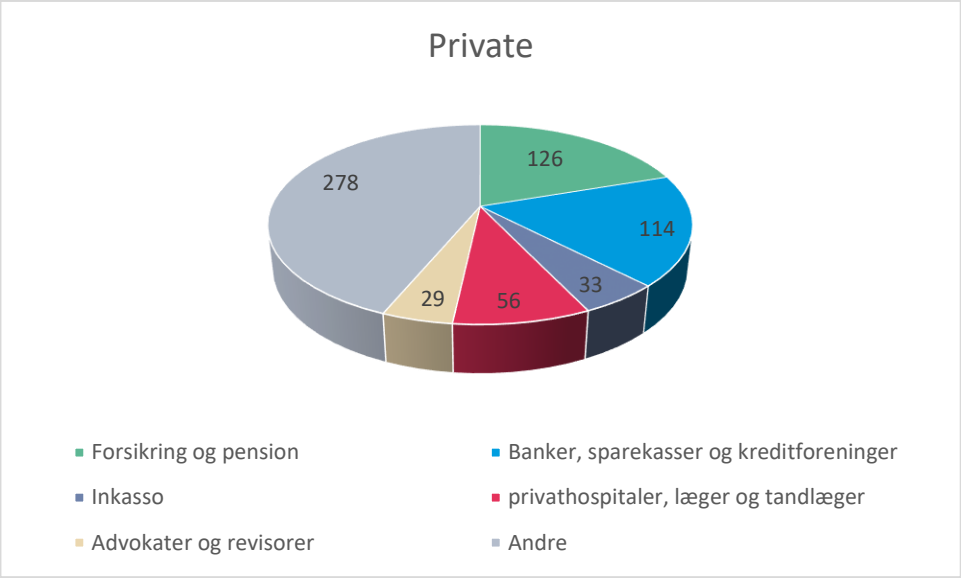
Denne fordeling er i det væsentlige identisk med den, der også blev belyst i oversigten fra første kvartal 2019. En del af forklaringen skal ses på den baggrund, at flere af sikkerhedsbruddene hos kommuner beror på enkelthændelser hos en databehandler, der så får effekt for en flerhed af dataansvarlige kommuner.

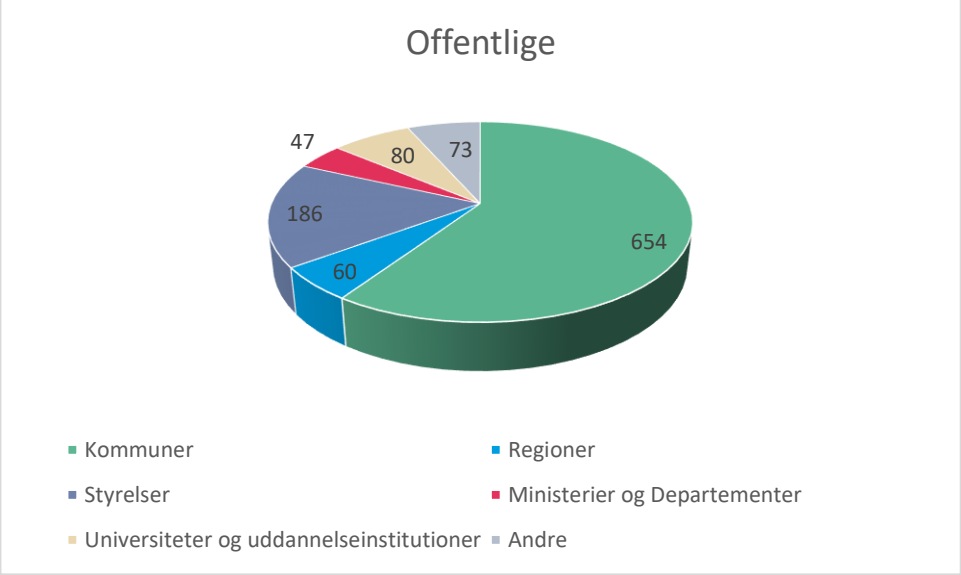


Da en del af anmeldelserne i den offentlige sektor beror på disse enkelthændelser, der berører flere dataansvarlige, er der tale om en generel stigning i antallet af enkelthændelser i den private sektor.

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
126
114
33
56
29
278
Forsikring og pension
Banker, sparekasser og kreditforeninger
Inkasso
privathospitaler, læger og tandlæger
Advokater og revisorer
Andre


Offentlige
47
80
73
186
654
60
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.

Omtrent 2/3 af de indkomne anmeldelser handler om oplysninger, der er sendt til den "forkerte" modtager, oftest ved en menneskelig fejl i afsendelsesøjeblikket. Der har dog i perioden været en stigning i brud på persondatasikkerheden, der skyldes ekstern uretmæssig påvirkning såsom phishing, malware, hacking eller tilsvarende, men disse udgør stadigvæk en mindre del af de samlede anmeldelser. Denne stigning falder altovervejende sammen med de udsving i intensiteten af angrebsforsøg, der gør sig gældende vedrørende den generelle it-sikkerhed.

Herudover er det for de private dataansvarlige særligt 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. Datatilsynet skal i denne henseende opfordre til, at der fastholdes agtpågivenhed på, at de mest oplagte af disse angreb stoppes ved at have fornødne mekanismer, for i realtid, at kunne vurdere uretmæssige brugsmønstre. Lige så vigtigt er det, at de enkelte registrerede – såfremt en kombination af ens brugernavn og kendeord er kompromitteret – husker at skifte disse i enhver sammenhæng de er benyttet.

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 kunne ske, og reetablering ikke har været forsøgt testet nogensinde.

Der er generelt fokus på sikring af personoplysninger, der 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). Der er dog stadigvæk en hel del anmeldelser hvor disse enheder mistes. 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.

Blandt offentlige dataansvarlige har der kunne 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.

Funktionaliteten hvor scanningsfunktionen i en multifunktionsprinter afsender en e-mail er også et typetilfælde blandt anmeldelserne. Især tilfælde hvor der også er mulighed for at scanne til e-mailadresser uden for egen organisation volder problemer, dels med "forkerte" modtagere dels med manglende kryptering af fortrolige og følsomme personoplysninger.

En særlig form for "social engineering" der også hyppigt ses, er situationer 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. Generelt bør opmærksomheden skærpes omkring de situationer hvor oplysningerne gives til andre end den registrerede selv.

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 funktionalitets-understøttelse 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.

Til de lidt mere kuriøse og antageligt årstidsbestemte brud på persondatasikkerheden, kan det i sommervarmen, når man arbejder for åbne vinduer, overvejes – som en passende sikkerhedsforanstaltning – at placere noget tungt på sine papirer sådan at disse ikke pludselig bliver trukket ud af vinduet i gennemtrækket. Herudover skal det såfremt det efter en risikovurdering heraf, tillades medarbejderne at arbejde udendørs i det gode vejr, indgå i vurderingen at såvel papirer og diverse mobile enheder, hyppigere kan glemmes, ses af uvedkommende eller slet og ret "forsvinde" i nydelsen af det dejlige vejr.

Datatilsynet ser stadig flere brud hvor der i den agile udvikling bruges repositorier, program- og datalagre der tilgås via internettet. 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, har som nævnt været i stigning og dette 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 den 25. maj 2018 til 30. juni 2019 modtaget lidt over 6000 anmeldelser. Af disse er 5/6 brud på persondatasikkerheden, der fremstår som afgrænsede og enkeltstående hændelser med en ringe eller kun lille risiko for de registreredes rettigheder.

Disse er enten allerede afsluttet eller ved at blive det over for den enkelte dataansvarlige. ca. 550 sager vedrører gentagelsestilfælde for godt 30 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 sanktion og afgørelse. Datatilsynet forventer at offentliggøre både afgørelser og indstillinger til politianmeldelser på tilsynets hjemmeside.

Anmeldelser af brud på persondatasikkerheden

Udgivet af:
Datatilsynet
Borgergade 28, 5.
1300 København K
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Datatilsynet
Borgergade 28, 5.
1300 København K
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk