Indberetninger i 2020 af brud på persondatasikkerhed på området for elektronisk kommunikation

Reglerne om persondatasikkerhed på området for elektronisk kommunikation

Erhvervsstyrelsen er tilsynsmyndighed for de særlige regler om persondatasikkerhed inden for elektronisk kommunikation.

Der er tale om sektorspecifikke regler, der træder i stedet for den generelle databeskyttelsesforordning (GDPR), når det handler om beskyttelse af personoplysninger inden for elektronisk kommunikation.

Reglerne findes i bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester samt i Kommissionens forordning nr. 611/2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden.

I medfør af disse regler skal udbydere af offentlige elektroniske kommunikationstjenester overholde forskellige krav for at sikre persondatasikkerheden i forbindelse med deres udbud af elektroniske kommunikationstjenester (fx telefoni- og internettjenester).

Udbyderne skal løbende træffe passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden. Foranstaltningerne skal sikre et sikkerhedsniveau, der, under hensyn til teknologiens aktuelle stade og omkostningerne ved at gennemføre foranstaltningerne, står i forhold til risici.

Hvis der sker et brud på persondatasikkerheden, skal udbyderne underrette Erhvervsstyrelsen herom, ligesom de personer, der er berørt af bruddet, som hovedregel skal underrettes.

Udbydere af offentlige elektroniske kommunikationstjenester skal underrette Erhvervsstyrelsen om alle brud på persondatasikkerheden. Efter GDPR skal et brud på persondatasikkerheden ikke indberettes til Datatilsynet, hvis det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. En sådan undtagelse findes ikke i telelovgivningen.

En udbyder skal alene underrette Erhvervsstyrelsen, og ikke (også) Datatilsynet, når der er tale om et brud på persondatasikkerheden, der relaterer sig til udbuddet af en offentligt tilgængelig elektronisk kommunikationstjeneste. Det omfatter fx uautoriseret adgang eller utilsigtet videregivelse af oplysninger om abonnenter, men eksempelvis ikke brud på oplysninger om

udbyderens egne ansatte (HR-data og lignende). I sidstnævnte tilfælde er det de almindelige regler efter GDPR, der gælder.

Udbydere af offentlige elektroniske kommunikationstjenester skal indberette et brud på persondatasikkerheden senest 24 timer efter påvisning af bruddet. Også på dette punkt adskiller reglerne om indberetning sig fra reglerne efter GDPR, hvor fristen er 72 timer. Der kan efterfølgende foretages en uddybende underretning senest tre dage efter den indledende underretning, i tilfælde af, at oplysninger udestod eller skal ajourføres.

Indberetning af brud sker via den fælles offentlige indberetningsplatform, der kan findes på virk.dk.

Udvidelsen af reglerne til også at omfatte andre tjenestetyper

Med bekendtgørelse nr. 1833 af 8. december 2020 blev nummeruafhængige interpersonelle kommunikationstjenester omfattet af særreglerne om persondatasikkerhed i teleloven. Ændringen skete som følge af udvidelsen af definitionen af begrebet "elektronisk kommunikationstjeneste" jf. direktiv (EU) nr. 2018/1972 om oprettelse af en europæisk kodeks for elektronisk kommunikation (teledirektivet) til også at omfatte "nummeruafhængige interpersonelle kommunikationstjenester".

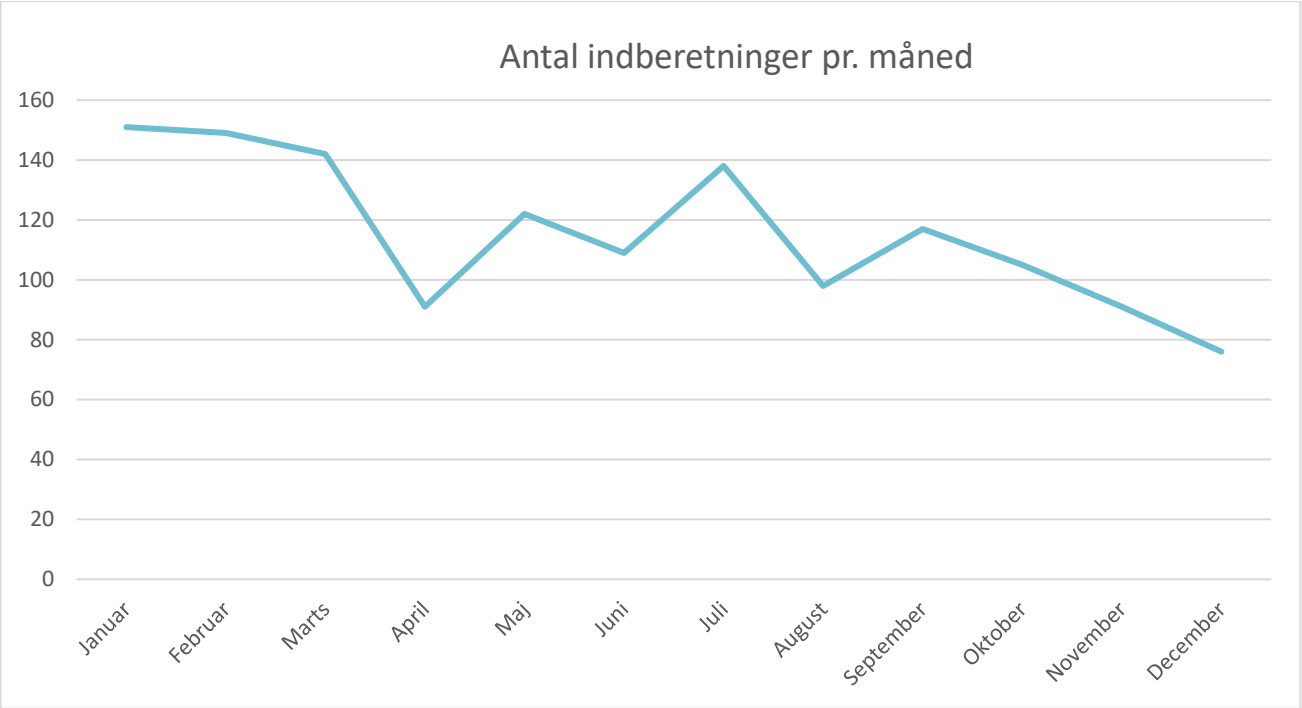
Ændringen har medført, at Erhvervsstyrelsens tilsyn med persondatasikkerhed på teleområdet fra 21. december 2020 har omfattet tilsyn med disse tjenester. Tjenesterne har tidligere været underlagt de generelle regler om databeskyttelse, som Datatilsynet fører tilsyn med.

Indberetninger 2020

Erhvervsstyrelsen har, som det fremgår af figur 1, i 2020 modtaget i alt 1.389 indberetninger fra udbydere af offentlige elektroniske kommunikationstjenester om brud på persondatasikkerheden.[1]

Figur 1: Antal indberetninger pr. måned 2020

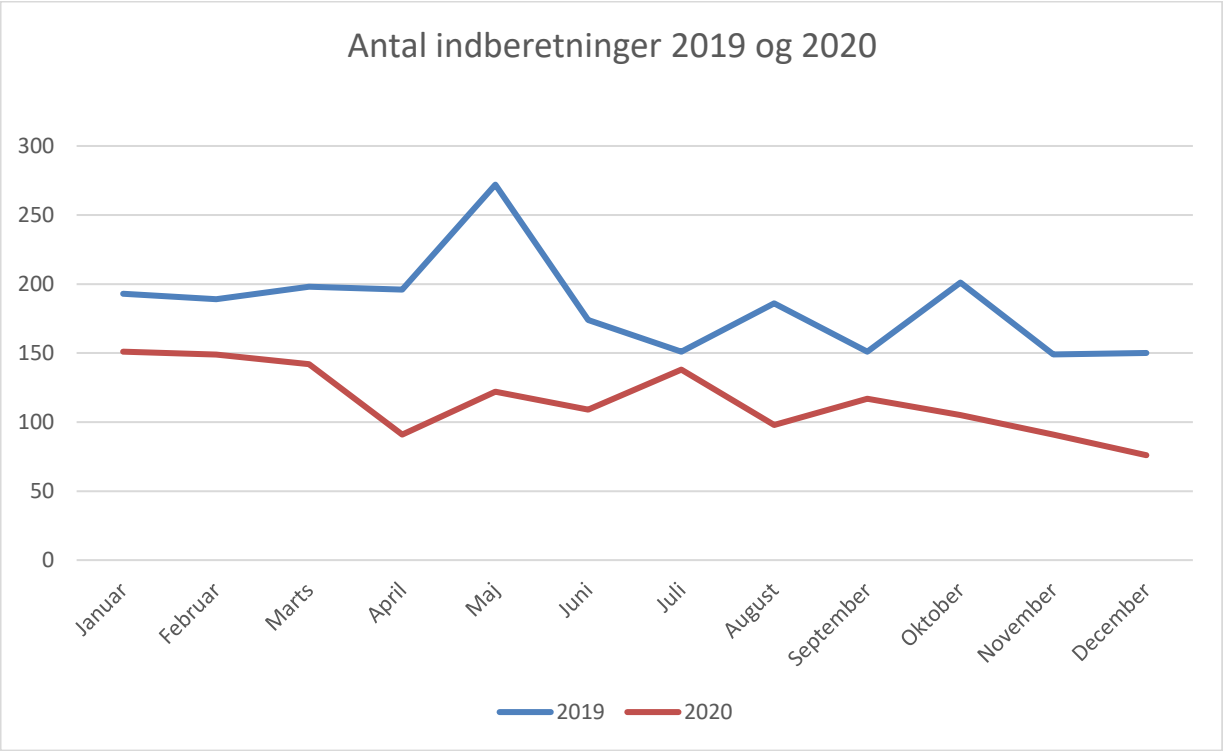
[1] *Offentlige elektroniske kommunikationstjenester* omfatter med ændringen af reglerne pr. 21. december 2020 også *nummeruafhængige interpersonelle kommunikationstjenester*. Erhvervsstyrelsen har dog ved udarbejdelsen af denne årsberetning endnu ikke modtaget indberetninger fra udbydere af disse tjenestetyper.



Figur 1 viser, at antallet af indberetninger fluktuerer fra måned til måned. Gennemsnitligt modtog Erhvervsstyrelsen ca. 116 indberetninger pr. måned i 2020. I 96 pct. af de indberetninger styrelsen har modtaget, er 1-2 berørte af hændelsen.

Til sammenligning modtog styrelsen 2.185 indberetninger i 2019. Antallet af indberetninger modtaget i 2020 svarer således til en nedgang på ca. 43 pct. Figur 2 viser en sammenstilling af antallet af indberetninger om brud på persondatasikkerheden indberettet til Erhvervsstyrelsen for 2019 hhv. 2020.

Figur 2: Sammenstilling af antal indberetninger for 2019 hhv. 2020.



Grafen viser, at Erhvervsstyrelsen generelt har modtaget færre indberetninger i 2020, hvilket er en modsat tendens i forhold til forrige år, hvor Erhvervsstyrelsens i 2019 modtog 92,5 pct. flere indberetninger set i sammenligning med 2018.

Typer af personoplysninger, der er berørt af brud på persondatasikkerheden

Udbydere af elektroniske kommunikationstjenester håndterer personoplysninger såsom navn, adresse, telefonnummer (som evt. kan være hemmeligt eller udeladt), e-mailadresse, abonnementsoplysninger, betalingsoplysninger, kundenummer eller kontonummer hos udbyderen.

Brud på persondatasikkerheden, der sker hos udbydere af offentlige elektroniske kommunikationstjenester, omfatter oftest eksponering af en eller flere af ovenstående typer data. Det gælder, uanset om der er tale om manuelle fejl, systemfejl eller andet.

Ved manuelle fejl såvel som systemfejl ses eksempler på hændelser, der fører til eksponering af 'hemmelige' og 'udeladte' nummeroplysningsdata (navn, adresse og telefonnummer), som må anses for at være særligt alvorligt i forbindelse med teleselskabers håndtering af kundedata.

Typisk berører de enkelte brud på persondatasikkerheden ganske få personer. I forbindelse med fx større systemmigreringer ses der dog brud, hvor en større gruppe er berørt af hændelsen - dette uddybes nærmere nedenfor.

Fordeling af fejltyper

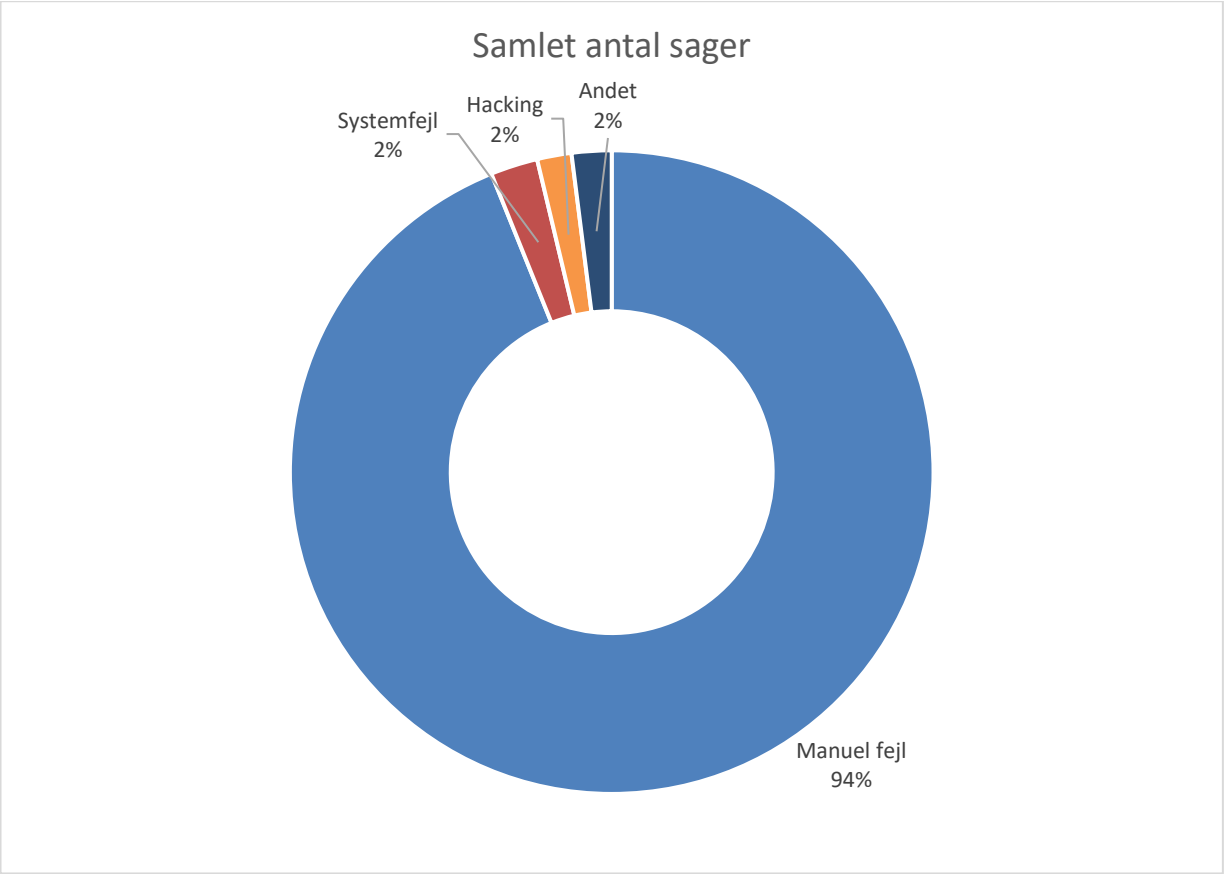
Som det ses af figur 3, fordeler indberetningerne sig i en række hovedgrupper.

Manuelle fejl er den primære fejltype og udgør ca. 94 pct. af indberetningerne. Det drejer sig om menneskelige fejl, hvor fx en medarbejder taster data forkert. Ca. 2 pct. af indberetningerne skyldes **systemfejl** og er relateret til it-løsninger. Ca. 2 pct. af indberetningerne vedrørte sikkerhedsbrud som følge af **hacking**.

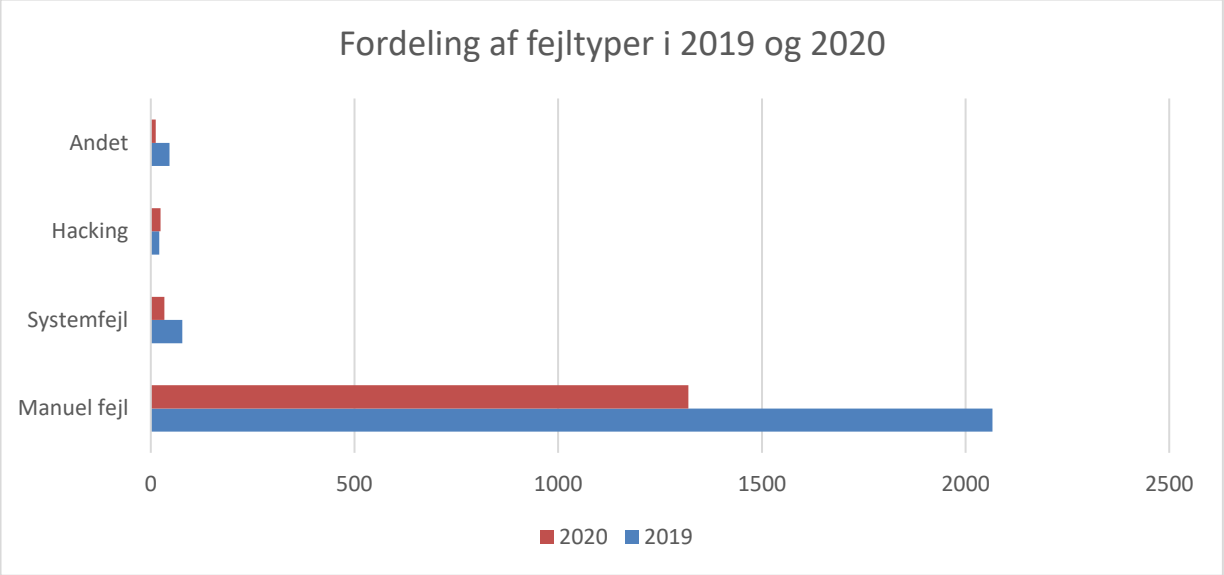
Endeligt vedrører 2 pct. af indberetningerne **andre fejltyper**, hvilket bl.a. vedrører svindel, tyveri samt tilfælde, hvor det på tidspunktet for indberetningen endnu var uklart, hvad fejlen skyldtes.[2]

Figur 3: Fordeling af fejltyper 2020

[2] Indberetning til Erhvervsstyrelsen skal ske senest 24 timer efter påvisning af bruddet på persondatasikkerheden, hvorfor hændelsesforløb i større eller mindre grad kan være uafklaret på tidspunktet for indberetningen. Hændelsesforløbet kan blive korrigeret efterfølgende, men dette vil ikke blive afspejlet i Erhvervsstyrelsens statistik.



Figur 4: Fordeling af fejltyper i 2019 og 2020



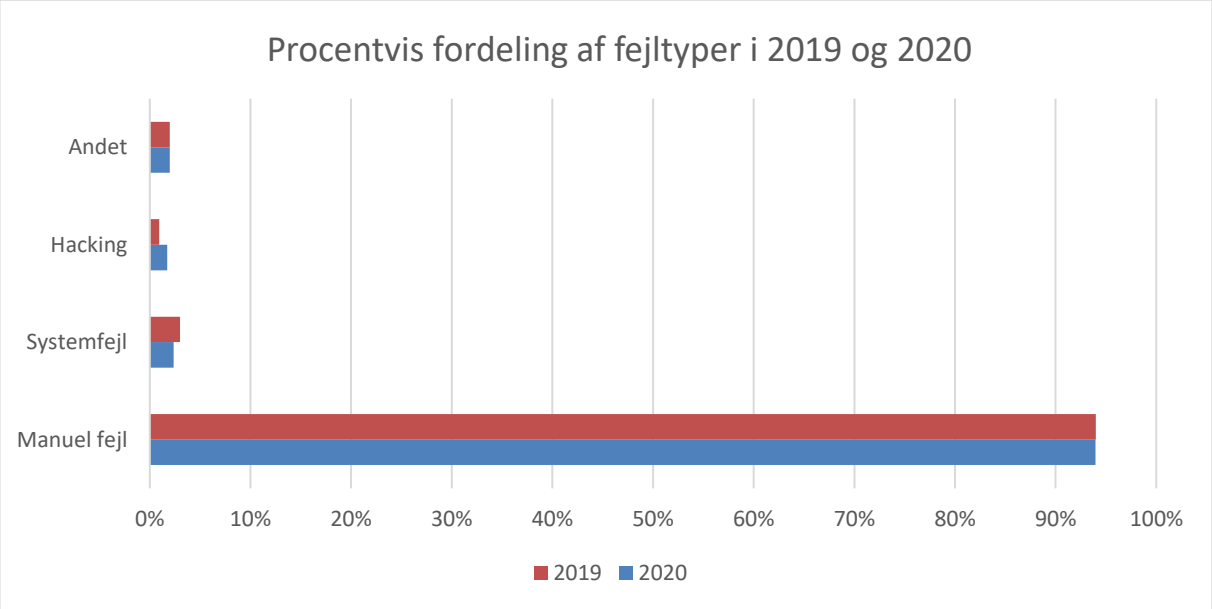
Figur 4 illustrerer fordelingen fejltyper i 2019, mens figur 5 nedenfor sammenstiller den procentvise fordeling af fejltyper i hhv. 2019 og 2020.

Det fremgår af figur 4, at **manuelle fejl** i både 2019 og 2020 var den kategori med flest indberetninger efterfulgt af en forholdsvis ligelig fordeling mellem indberetninger vedrørende hhv. systemfejl, hacking og andet.

Figur 4 viser herudover, at der i 2020 var indberettet 33 **systemfejl**, mens der i 2019 var indberettet 77 systemfejl. Der har således været indberettet langt færre systemfejl i 2020 sammenlignet med 2019, hvilket skal ses i en naturlig sammenhæng med, at der generelt forekommer en nedgang af det samlede antal indberetninger, ligesom det kan være et positivt tegn på, at teleselskaberne i løbet af 2019 har truffet fornødne tekniske sikkerhedsforanstaltninger, som har minimeret systemfejl. Systemfejl kan bl.a. bestå i systemopdateringer eller migreringsfejl af personoplysninger til andre it-systemer, som fx kan resultere i, at kunders data blandes sammen, herunder forkerte oplysninger på regninger, eller at forkerte data fremgår af kunders selvbetjening.

Der har været et mindre antal indberetninger vedrørende **hacking** af selvbetjeningssystemer. Der er typisk tale om hacking af login-oplysninger, som fx hidrører fra hacking af andre online platforme (fx sociale medier), hvor lister med brugernavne, e-mailadresser og passwords indsamles. Hvis en bruger har anvendt samme brugernavn og adgangskode flere steder, kan det lykkes hackere at skaffe sig uautoriseret adgang gennem såkaldt *brute force*-angreb ved brug af disse lister på selvbetjeningssystemerne.

Figur 5: Procentvise fordeling af fejltyper i 2019 og 2020



Det fremgår af figur 5, at fejltyperne i 2019 og 2020 ikke har de store forholdsmæssige udsving, samt at 94 pct. af det samlede antal indberetninger om brud på persondatasikkerheden i både 2020 og 2019 omhandlede manuelle fejl.

Videre kan det fremhæves, at 2 pct. af indberetningerne i 2020 vedrørte systemfejl og relaterede sig til it-løsninger, mens 4 pct. af alle indberetninger i 2019 omhandlede systemfejl. Der er således en marginal forholdsmæssig nedgang i antallet af systemfejl.

Endelig viser grafen, at der forekommer forholdsmæssigt flere hacking-sager i 2020 i sammenligning med 2019 – om end den forholdsmæssige andel stadig er beskeden.

Erhvervsstyrelsens tilsyn

Erhvervsstyrelsen behandler alle indberetninger individuelt, og er løbende i tæt dialog med selskaberne om deres håndtering af brud på persondatasikkerheden samt selskabernes tekniske og organisatoriske foranstaltninger for at hindre sådanne brud.

Erhvervsstyrelsen screener og vurderer løbende de indberetninger og borgerhenvendelser om brud på persondatasikkerheden, som styrelsen modtager. På baggrund af principielle, generelle og tilbagevendende eller nye problemstillinger, kan styrelsen føre et bredere tilsyn med selskaberne. Et bredt tilsyn kan vedrøre et enkelt selskab (selskabsbaseret tilsyn) eller gå på tværs af flere selskaber (emnebaseret tilsyn). Et sådan tilsyn er således ikke knyttet til den enkelte indberetning eller borgerhenvendelse, idet der er en flerhed af indberetninger m.v., der danner grundlag for tilsynet.

Erhvervsstyrelsen tager løbende stilling til, hvornår der er grundlag for at rejse en tilsynssag. Et tilsyn kan fx baseres på følgende forhold:

- Antallet af samme type hændelse, der hver for sig ikke er alvorlige, men hvor antallet giver anledning til se nærmere på, om selskabet (eller selskaberne) har truffet de fornødne foranstaltninger.
- Hændelsestyper, der går på tværs af selskaberne: Fx brug af passwords, håndtering af udeladte/hemmelige numre (118), adgang til andre kunders mailkonto.
- Den teknologiske udvikling giver anledning til at opdatere risikostyringen og evt. træffe andre foranstaltninger end tidligere.
- Mediedebat. Vi følger løbende debat- og nyhedsmedier for at identificere problemstillinger og konkrete sager, som det kan være relevant at tage op som tilsynssag.

Tilsynssagerne behandles efter sædvanlige forvaltningsretlige principper med partshøring, sagsoplysning osv.

Egen drift-undersøgelser

I foråret 2020 iværksatte Erhvervsstyrelsen et emnebaseret tilsyn med en række teleselskabers proces for udlevering af personoplysninger til politiet på baggrund af retskendelser. Erhvervsstyrelsen fik ved dette tilsyn indblik i teleselskabernes tekniske og organisatoriske foranstaltninger i relation til udlevering af sådanne oplysninger, herunder forløbet for udleveringen af personoplysninger til politiet.

Erhvervsstyrelsen vurderede, at teleselskaberne havde de fornødne tekniske og organisatoriske foranstaltninger, som bl.a. indebærer løbende kontrol med det udleverede data i form af stikprøvekontroller.

Udvalgte afgørelser

Erhvervsstyrelsen har i maj 2020 truffet afgørelse i to sager om brud på persondatasikkerheden. I begge sager traf Erhvervsstyrelsen afgørelse om, at selskabet havde oversendt for mange oplysninger til politiet som en del af de signaleringsdata, der oversendes efter politiets anmodning, og at denne oversendelse dermed udgør et brud på persondatasikkerheden.

Det fremgår også, at Erhvervsstyrelsen – på baggrund af selskabernes redegørelser og idet det er Erhvervsstyrelsens forståelse, at ordlyden af kendelser sidenhen er ændret, og selskaberne derfor ikke udleverer de pågældende oplysninger, medmindre dette fremgår eksplicit af kendelsen – ikke foretager sig yderligere i de konkrete sager.

Begge afgørelser kan læses på Erhvervsstyrelsens hjemmeside: https://erhvervsstyrelsen.dk/tilsyn-med-persondatasikkerheden-paa-teleomraadet

Borgerhenvendelser

Ud over selskabernes indberetninger om brud på persondatasikkerheden modtager Erhvervsstyrelsen også henvendelser fra borgere om persondatasikkerheden hos selskaberne. Erhvervsstyrelsen har i 2020 behandlet 26 borgerhenvendelser om persondatasikkerheden på området. Flere af disse henvendelser har tilknytning til indberetninger fra udbyderne om brud på persondatasikkerheden.

Hvis behandlingen af en borgerhenvendelse tydeliggør, at der foreligger et alvorligt sikkerhedsproblem, bliver der ført et tilsyn på området, jf. ovenfor.

Den enkelte borger er ikke part i tilsynet med selskaberne, men borgerens henvendelse kan danne grundlag for, at der rejses en tilsynssag – enten i det konkrete tilfælde, eller ved at borgerhenvendelsen sammen med indberetningerne kan danne grundlag for Erhvervsstyrelsens vurdering af, om der skal rejses et overordnet tilsyn.

Borgerhenvendelser besvares enten ved en generel henvisning til reglerne på området og Erhvervsstyrelsens tilsyn med selskaberne eller med en mere konkret orientering om den hændelse, borgeren henviser til.

Læringspunkter for selskaberne ift. risikostyring og håndtering af brud på persondatasikkerheden

- Øget fokus på gennemførelse af awareness-kampagner om persondatasikkerhed i hele organisationen – fra ledelsen til kundeservice og hos eventuelle eksterne databehandlere – så evt. brud på persondatasikkerheden bliver identificeret og indberettet til Erhvervsstyrelsen.
- Opfølgning af tidligere sikkerhedsbrud mhp. læring og at undgå lignende brud opstår i fremtiden.
- Løbende risikovurdering af de risici jeres virksomhed står overfor herunder løbende vurderinger af jeres foranstaltninger, så det sikres, at de er effektive, tidssvarende og de imødekommer det aktuelle tekniske niveau.
- Større fokus på at nedbringe manuelle fejl. Dette kan fx gøres ved:
    - Indførelse af eventuelle verificerings-mekanismer (både manuelle og tekniske mekanismer) ved indtastning af kundeoplysninger fx e-mail, kundenr., telefonnr. m.v.

    - Indførelse af tjenester, hvor kunden selv indtaster sine data, fremfor at kundeservicemedarbejderen taster kundens oplysninger med de risici for fejl, det medfører.
    - Gør overvejelser om dataminimering, så det kun er absolut nødvendige personoplysninger, der fremgår af mails afsendt fra selskabet.
- Øget fokus på at implementere foranstaltninger til at afhjælpe systemfejl, herunder implementer processer, der har fokus på databeskyttelse hele vejen i udviklings- og testforløb i forbindelse med migreringer af systemer og/eller udvikling af nye systemer.
- Fokus på at vejlede kunder/brugere om vigtigheden af at anvende stærke password på selvbetjeningsløsninger og lignende.
- Større fokus på foranstaltninger som skal sikre, at kontaktoplysninger ikke offentliggøres på fx 118.dk imod kunders ønske, særligt for så vidt angår kunder med hemmeligt eller udeladt nummer.