ERHVERVSSTYRELSEN

# Indberetninger i 2019 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 persondata inden for elektronisk kommunikation.

Reglerne findes i bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og 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). Det vil i praksis sige teleselskaber på det danske marked.

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 o.lign.). 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 fald oplysninger udestod eller skal ajourføres.

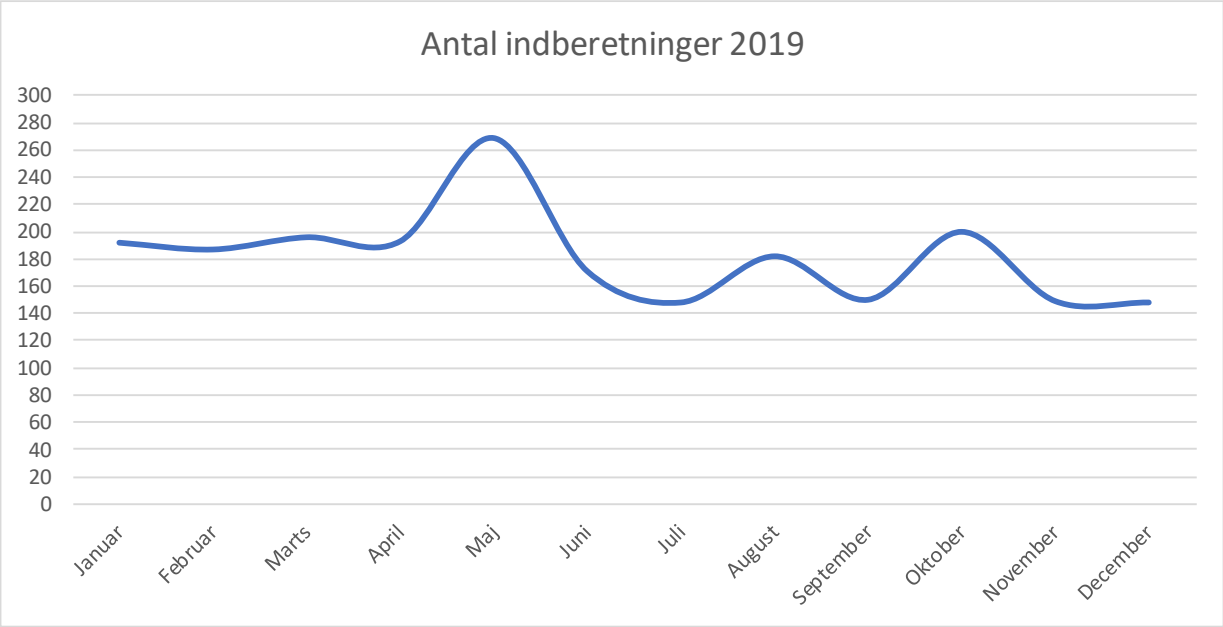
Indberetning af brud sker via den fælles offentlige indberetningsplatform, der kan findes på virk.dk.

Erhvervsstyrelsen behandler løbende de indberetninger om brud på persondatasikkerheden, som styrelsen modtager fra udbydere af offentlige elektroniske kommunikationstjenester. Erhvervsstyrelsen har bl.a. fokus på udbydernes identifikation, håndtering og løsning af hændelserne samt læring heraf, herunder eventuel iværksættelse af foranstaltninger for fremadrettet af undgå tilsvarende hændelser. Endvidere fokuseres på overholdelse af kravene om underretning af tilsynsmyndigheden og af de berørte personer.

# Indberetninger 2019

Erhvervsstyrelsen har, som det fremgår af figur 1, i 2019 modtaget 2.185 indberetninger fra udbydere af offentlige elektroniske kommunikationstjenester om brud på persondatasikkerheden.

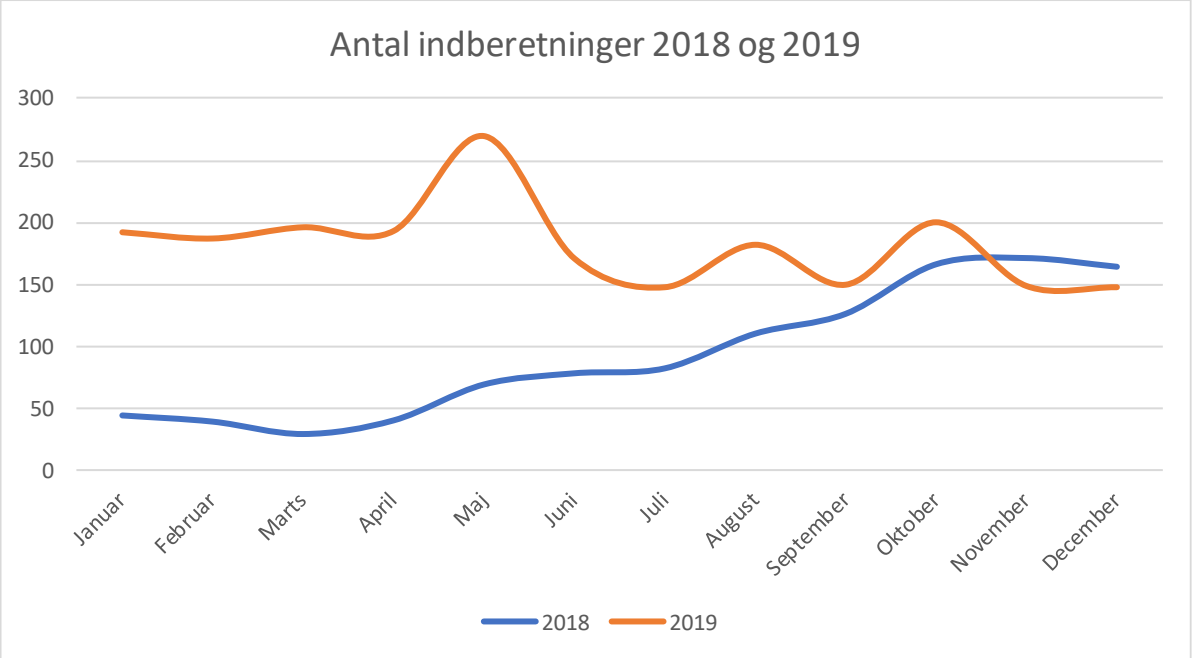
Figur 1: Antal indberetninger pr. måned 2019




Figur 1 viser, at antallet af indberetninger fluktuerer fra måned til måned. Gennemsnitligt modtog Erhvervsstyrelsen ca. 182 indberetninger pr. måned i 2019. I 96 pct. af de indberetninger styrelsen har modtaget, er 1-2 berørte af hændelsen.

Til sammenligning modtog styrelsen 1.131 indberetninger i 2018. Antallet af indberetninger modtaget i 2019 svarer således til en stigning på 92,5 pct. Figur 2 viser en sammenstilling af antallet af indberetninger om brud på persondatasikkerheden indberettet til Erhvervsstyrelsen for 2018 hhv. 2019.

Figur 2: sammenstilling af antal indberetninger for 2018 hhv. 2019.




Figur 2 viser en sammenstilling af indberetningerne fra 2018 og 2019. Grafen viser, at indberetningerne i 2018 steg betydeligt omkring maj måned, hvor GDPR fik virkning. Mod slutningen af 2018 stagnerede antallet dog. Antallet af indberetninger modtaget i 2019 er fortsat gennemsnitligt i på samme niveau som i 4. kvartal 2018.

## Typer af persondata, der er berørt at brud på persondatasikkerheden

Udbydere af elektroniske kommunikationstjenester håndterer persondata 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.

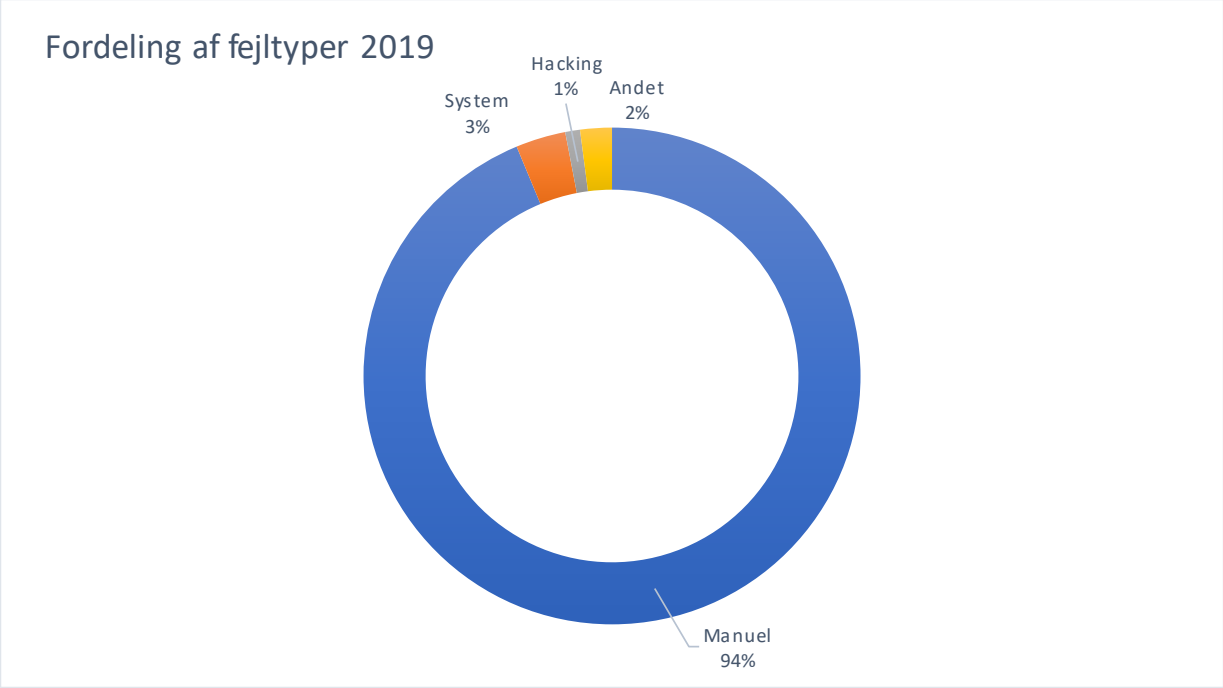
Typisk berører de enkelte brud på persondatasikkerheden ganske få personer. I forbindelse med fx større systemmigreringer ses der dog brud, hvor en større gruppe er berørt af hændelsen - dette uddybes nærmere nedenfor.

## Fordeling af fejltyper

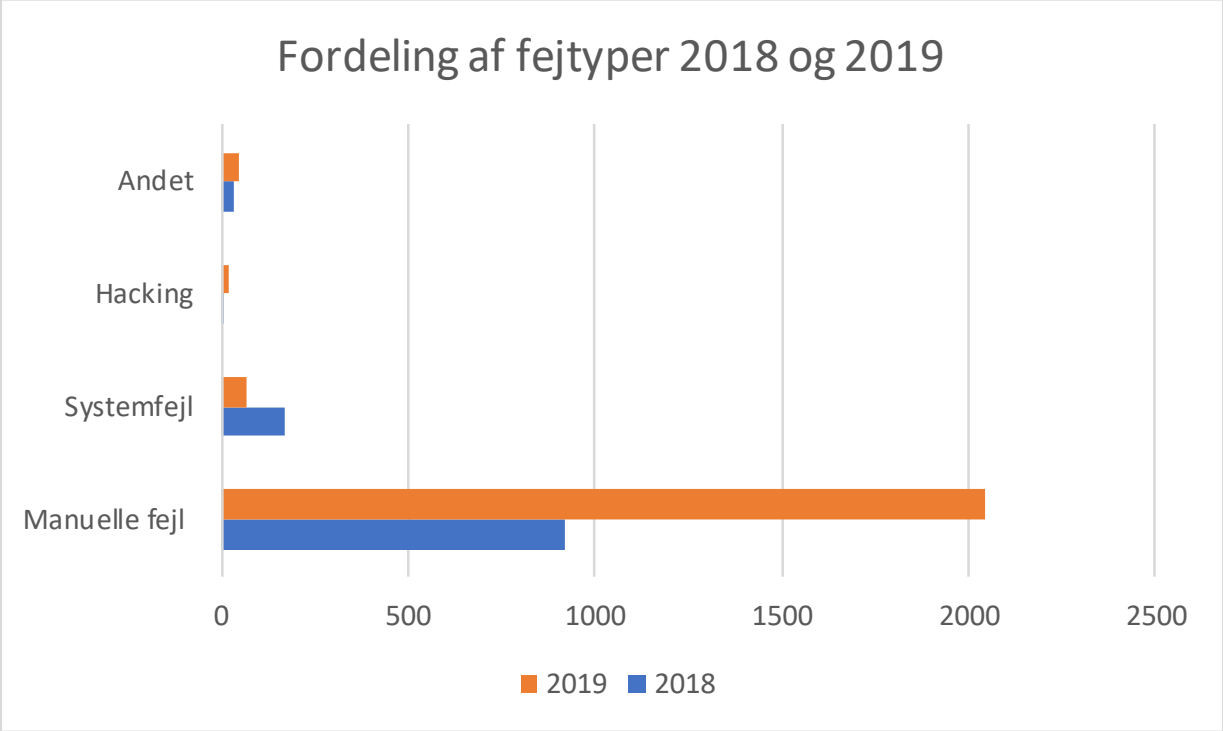
Indberetningerne fordeler sig i en række hovedgrupper. Manuelle fejl er den primære fejltype og udgør ca. 94 pct. af indberetningerne. Det drejer sig om menneskelige fejl, hvor fx en medarbejder taster data forkert. Ca. 3 pct. af indberetningerne skyldes systemfejl og er relateret til it-løsninger. En ganske lille del af indberetningerne vedrørte sikkerhedsbrud som følge af hacking. Endeligt vedrører 2 pct. af indberetningerne andre fejltyper, hvilket bl.a. dækker over svindel, tyveri samt tilfælde, hvor det på tidspunktet for indberetningen endnu var uklart, hvad fejlen skyldtes. Figur 3 illustrerer fordelingen af

fejltyper i 2019, og figur 4 sammenstiller fordelingen af fejltyper i 2018 hhv. 2019, og viser at manuelle fejl i både 2018 og 2019 var den kategori med flest indberetninger efterfulgt af indberetninger vedrørende hhv. systemfejl, andet og hacking.

Figur 2: Fordeling af fejltyper 2019




Figur 4: Fordeling af fejltyper i 2018 hhv. 2019



## Manuelle fejl

Udbydere af offentlige elektroniske kommunikationstjenester har i sagens natur megen kundekontakt (bl.a. gennem kundeservicecentre og butikker), og stort set samtlige personer og virksomheder i Danmark har enten ét eller flere abonnementer hos et teleselskab. Det er som oftest i kundeservice, at manuelle fejl sker. Af de manuelle fejl udgør tastefejl ca. 65 pct. Tastefejl vedrører oftest fejltastning af nummer, e-mail eller CPR-nummer. Fejltastning kan medføre, at en e-mail eller sms, der indeholder persondata, sendes til en forkert modtager. CPR-numre, der tastes forkert ved oprettelse af et kundeforhold, kan medføre, at en kontrakt indeholder forkert navn og adresse, uden at selve CPR-nummeret dog eksponeres.

Ca. 5 pct. af de indberettede brud skyldes tastefejl fra *kundens* side.

Andre manuelle fejl handler om, at data vedrørende en kunde indtastes i en andens kundes kundeprofil. Det kan fx ske, hvis et "systemvindue" i forbindelse med kundeekspedition ikke er blevet lukket ned efter afsluttet ekspedition (fx ved ændring og tilpasning af abonnement, eller lignende), eller fx hvis der sker et fejlopslag i udbyderens kundedatabase i forbindelse med en kundeekspedition. En anden fejl er forkerte vedhæftninger ved afsendelse af e-mail, eller fejl der opstår i forbindelse med brevflet. Som i 2018 har styrelsen i 2019 modtaget indberetninger, hvor fejlen beror på brug af fiktive e-mails ved oprettelse af kundeforhold. Hvis en kunde ikke ønsker at oplyse sin mail eller ikke har en sådan, sker det, at en kundeservicemedarbejder i stedet anvender en fiktiv mailadresse – fx "mangler@mail.dk". Hvis denne adresse viser sig faktisk at tilhøre en person og dermed ikke er fiktiv, vil ejeren af den "fiktive" mailadresse således modtage ordrebekræftelser o.l. med fx andre personers navn og kontaktoplysninger.

For at nedbringe manuelle fejl, er det i særdeleshed vigtigt, at teleselskaberne har fokus på at udbrede kendskab og viden om persondata i hele organisationen. Det kan ligeledes være en fordel at bygge systemer op, så det ikke er muligt at have flere "systemvinduer" åbne på samme tid. Dette vil minimere risikoen for, at en medarbejder får blandet kunder sammen i forbindelse med kundeekspedition. I forbindelse med kundeekspeditioner kan det yderligere være relevant at overveje, hvorvidt det er muligt at guide kunder til selv at taste ændringer via fx selvbetjeningsløsninger. På denne måde reduceres risikoen for, at kundeservicemedarbejderen taster data forkert.

Når der er tale om manuelle fejl, er det oftest 1-2 personer, der er berørt af det enkelte brud på persondatasikkerheden. Der kan dog også ske manuelle fejl, der bevirker, at et stort antal personer bliver berørt. Således er der set hændelser, hvor en menneskelig fejl i forbindelse med en migrering af kundedata fra et it-system til et andet it-system medførte, at et stort antal 'hemmelige' navne og adresser blev gjort offentligt tilgængelige.

## Systemfejl

Systemfejl udgjorde i 2019 ca. 3 pct. af indberetningerne til Erhvervsstyrelsen, mens tallet i 2018 var 15 pct. Der er således sket en drastisk nedgang i antallet af indberetninger, der har ophæng i systemfejl.

I 2019 modtog Erhvervsstyrelsen en række indberetninger om brud på persondatasikkerheden, der specifikt relaterede sig til migrering af persondata til andre it-systemer. Bruddet skyldes i disse sager, at kunders data er blandet sammen, hvilket fx resulterer i forkerte oplysninger på regninger, eller at

forkerte data fremgår af kunders selvbetjening. Migreringsfejl kan imidlertid også føre til større og mere alvorlige brud på persondatasikkerheden, hvor flere er berørte af samme fejl.

For at minimere risici for systemfejl i forbindelse med migreringer er det vigtigt, at der ved udvikling af nye systemer eller planlægning af migreringer er fokus på behandling og konsekvens for persondata tidligt i forløbet. Det er ligeledes vigtigt, at der foretages grundige tests af systemerne, for at identificere mulige fejl. Sådanne tests bør naturligvis ikke udføres med reelle persondata.

Omtrent 14 pct. af de indberettede systemfejl, relaterer sig til selskabernes selvbetjeningssystemer, hvor kunderne opretter og ændrer abonnementer, tv-pakker osv. Sådanne fejl opstår ofte ved systemopdateringer eller -migreringer, hvor persondata ikke overføres korrekt fx på grund af fejl i indstillinger, design, kode eller kompatibilitet. Dette kan blandt andet medføre, at kunder ”blandes sammen”, så én kunde kan se en anden kundes data på sin egen selvbetjeningsløsning.

Der er også eksempler, hvor en kunde har fået adgang til en anden kundes e-mailkonto via selvbetjeningsløsningen. Dette kan igen skyldes sammenblanding af kunders data, men det kan ligeledes opstå, hvis tidligere konti ikke er blevet lukket korrekt i systemet, og nye kunder får tildelt samme kontonumre som de tidligere kunder, og derved får adgang til deres selvbetjening.

Der er også eksempler, hvor en kunde, der har glemt sit brugernavn/adgangskode til selvbetjenings-løsningen, via en funktion til nulstilling af kodeord får adgang til en anden kundes selvbetjening. Dette kan fx ske ved, at et opsagt nummer ved en fejl stadig er lagret i systemet, så en ny kunde, der overtager det tidligere opsagte telefonnummer, får genoprettet brugernavn/adgangskode til den tidligere ejeres selvbetjening i stedet for sin egen.

## Hacking

Der har været et mindre antal indberetninger vedrørende hacking af selvbetjeningssystemer. Der er typisk tale om hacking af login-oplysninger, som fx giver adgang til informationer omkring kunders tv-pakker og online streamingtjenester. Uautoriseret adgang opnås fx ved brug af lister med brugernavne/e-mailadresser og passwords, der hidrører hacking af andre større platforme (fx Facebook og LinkedIn). Hackere tester disse lister af på selvbetjeningssystemerne, og hvis en bruger har anvendt samme brugernavn og adgangskode flere steder, kan det lykkes hackere at skaffe sig uautoriseret adgang. Antal berørte varierer, men der er – med enkelte undtagelser – oftest tale om ganske få personer.

## Andre

Denne kategori udgør (som vist i figur 2) ca. 2 pct. af de indberettede hændelser, og vedrører bl.a. svindel, tyveri samt tilfælde, hvor det på tidspunktet for indberetningen endnu var uklart, hvad fejlen skyldtes. 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.

# Erhvervsstyrelsens tilsyn

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

Ud over teleselskabernes indberetninger om brud på persondatasikkerheden modtager vi også henvendelser fra borgere om persondatasikkerheden hos teleselskaberne. Mange af disse henvendelser oversendes fra Datatilsynet, da borgere ikke nødvendigvis er bekendt med teleselskabernes særregulering, og derfor antager området falder under GDPR-reglerne. Borgerhenvendelser behandles ligeledes individuelt af Erhvervsstyrelsen.

Styrelsen analyserer i øvrigt løbende de indberetninger og borgerhenvendelser om brud på persondatasikkerheden, som styrelsen modtager. På baggrund af problemstillinger, som er principielle, generelle og/eller gentagende, kan styrelsen føre bredere tilsyn med teleselskaberne. Et bredt tilsyn kan vedrøre et enkelt selskab eller gå på tværs af branchen. 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.

Nedenfor er angivet en række eksempler på udvalgte brudsager, som Erhvervsstyrelsen behandlede i 2019.

## Fælles tilsyn med Rigspolitiet vedrørende indgreb i meddelelseshemmeligheden

Den 18. juli 2019 indledte Erhvervsstyrelsen i samarbejde med Rigspolitiet et fælles tilsyn med ni selskaber på tværs af branchen, vedrørende teleselskabernes risikostyring for persondatasikkerhed i forbindelse med indgreb i meddelelseshemmeligheden. På baggrund af selskabernes redegørelser i sagen blev der afholdt møder med selskaberne hos Rigspolitiet den 7. – 9. oktober 2019. Som følge af selskabernes redegørelser og de efterfølgende møder med de respektive selskaber, fulgte Erhvervsstyrelsen op med en række spørgsmål vedrørende selskabernes tekniske og organisatoriske foranstaltninger, herunder adgangspolitik, passwordhåndtering, systemudvikling, opdatering af systemer, slettepolitikker og fysisk adgangskontrol.

Tilsynet viste, at selskaberne umiddelbart har truffet passende tekniske og organisatoriske foranstaltninger vedrørende behandlingen af persondata i forbindelse med den praktiske bistand til politiet. Teleselskaberne revurderer løbende deres sikkerhedsforanstaltninger, herunder i forbindelse med indgreb i meddelelseshemmeligheden.

I december måned afsluttede Erhvervsstyrelsen således tilsynet med hovedparten af selskaberne og har fulgt individuelt op med enkelte selskaber, hvor der var behov for yderligere dialog vedrørende sikkerhedspolitikker.

## Spoofing

I december 2019 blev styrelsen via medierne bekendt med, at uvedkommende har kunnet foretage en hacking af teleselskabers voice-mail, så uvedkommende i visse tilfælde kunne tilgå beskeder m.m. uden brug af pinkode (spoofing).

Styrelsen modtog ligeledes i december 2019 indberetninger vedrørende denne problematik. På baggrund af indberetningerne bad styrelsen selskaberne fremsende supplerende oplysninger om bruddet. Styrelsen var ligeledes i dialog med andre myndigheder om denne problematik.

I styrelsens dialog med teleselskaberne bekræftede selskaberne overfor styrelsen, at problemstillingen er håndteret, og at selskaberne har implementeret en række tiltag til at imødegå lignende brud på persondatasikkerheden.

Erhvervsstyrelsen afsluttede sagerne, idet den konkrete problemstilling var håndteret af selskaberne, samt at det blev vurderet, at selskaberne havde iværksat passende tekniske og organisatoriske foranstaltninger til at imødegå lignende brud på persondatasikkerheden.

### Brudsager vedrørende eksponering af nummeroplysningsdata

Erhvervsstyrelsen førte ligeledes i 2019 tilsyn med et selskab vedrørende deres håndtering af nummeroplysningsdata.

Styrelsen havde i løbet af 2018 og januar 2019 modtaget en række indberetninger fra selskabet, som alle var kendetegnet ved, at et stort antal nummeroplysningsdata, der skulle have været registreret som "hemmelige" eller "udeladt", var blevet eksponeret.

På baggrund af indberetningerne har selskabet svaret på en række uddybende spørgsmål.

Selskabet har løbende redegjort for deres håndtering af nummeroplysningsdata i forhold til reglerne om persondatasikkerhed på området for elektronisk kommunikation. Erhvervsstyrelsen konkluderede, at styrelsen fandt det meget uheldigt, at selskabet ikke har haft processer, herunder reviewprocesser og quality assurance-processer, der har kunne hindre brud af denne karakter

På baggrund af selskabets redegørelser og supplerende oplysninger i sagen, herunder om de foranstaltninger selskabet har implementeret på baggrund af hændelserne, afsluttede styrelsen sagen ultimo 2019.

## Læringspunkter

På baggrund af de indberetninger, Erhvervsstyrelsen har modtaget i 2019, og de tendenser, som styrelsen ser på baggrund heraf, kan der bl.a. peges på følgende læringspunkter, som teleselskaberne kan lade sig inspirere af i deres daglige arbejde med persondatasikkerhed.

- Skab løbende opmærksomhed om persondatasikkerhed i hele organisationen - fra ledelsen til kundeservice og hos eventuelle eksterne databehandlere – således at evt. brud på persondatasikkerheden bliver identificeret og indberettet til Erhvervsstyrelsen.
- Gennemfør i forbindelse med ændringer i it-systemer og migrering af persondata grundige tests af systemændringerne forud for lancering.
- 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.
- Overvej, om der kan implementeres løsninger, der sikrer, at kundeservicemedarbejdere kun kan have ét "systemvindue" åbent ad gangen. På denne måde minimeres risikoen for, at persondata tastes forkert og kunder blandes sammen.
- Minimer brugen af post-its – både virtuelle og fysiske. Post-its fører ofte til, at data noteres på forkerte kundeforhold.

- Ved telefonopkald anbefales det, at kundeservicemedarbejdere guider kunden til i videst muligt omfang at bruge selvbetjening, så kunden selv indtaster sine data, fremfor at kundeservicemedarbejderen skal taste kundens oplysninger med de risici for fejl, det medfører.
- Overvej hvilke persondata, der behøver at indgå i beskeder til kunder. Sendes en sms om opdateringer eller lignende, kan dette gøres med et "Hej" i stedet for navn i sms'en.
- Skab en positiv indberetningskultur i organisationen.
- Sørg for et hurtigt beredskab i organisationen, så brud på persondatasikkerheden bliver indberettet til Erhvervsstyrelsen inden for 24 timer.