DIGITALISERINGSSTYRELSEN

Årsberetning 2022
Tilsyn med brud på persondatasikkerhed

December 2023

Indhold

Tilsyn med brud på persondatasikkerhed

1. Formålet med tilsynet

”…at styre risici for brud på persondatasikkerheden…”

Digitaliseringsstyrelsens tilsynsindsats har først og fremmest fokus på at sikre, at udbydere af elektroniske kommunikationstjenester træffer passende tekniske og organisatoriske foranstaltninger med henblik på at *styre risici for brud på persondata-sikkerheden* i forbindelse med udbuddet af elektroniske kommunikationstjenester.

Det overordnede formål med reglerne og tilsynet er at beskytte brugernes person-oplysninger. Det er en af de grundlæggende frihedsrettigheder i EU's Charter om grundlæggende rettigheder[1], at enhver har ret til beskyttelse af personoplysninger.

[1] Link: Den Europæiske Unions Charter om Grundlæggende Rettigheder (pdf)

2. Indberetning af brud på persondatasikkerheden

Udbydere af elektroniske kommunikationstjenester skal indberette brud på persondatasikkerheden i forbindelse med deres kommunikationstjenester til Digitaliseringsstyrelsen.

Udbydere af elektroniske kommunikationstjenester behandler en række personoplysninger i forbindelse med udbuddet af deres tjeneste. Det kan fx være abonnenters navne, adresser, telefonnumre (der evt. kan være hemmelige), e-mailadresser, kundenumre og betalingsoplysninger.

Brud på persondatasikkerheden kan fx vedrøre uautoriseret adgang til eller ændring af en eller flere af disse oplysninger eller uberettiget videregivelse af oplysninger til en tredjemand.

Udbydere er forpligtede til at underrette Digitaliseringsstyrelsen, når de konstaterer et brud på persondatasikkerheden i forbindelse med udbuddet af deres kommunikationstjeneste.[2]

Udbydere af elektroniske kommunikationstjenester, der oplever brud på persondatasikkerheden, som *ikke* er sket i forbindelse med udbuddet af en elektronisk kommunikationstjeneste, skal derimod indberette sådanne brud til Datatilsynet. Det kan fx være brud på oplysninger om udbyderens ansatte (HR-oplysninger og lignende).

Indberetninger til Digitaliseringsstyrelsen kan enten foretages via den elektroniske blanket til indberetninger af sikkerhedshændelser på virk.dk[3] eller via mail til brud-persondatasikkerhed@digst.dk

Den elektroniske blanket indeholder en række på forhånd definerede oplysninger, som indberetter så vidt muligt skal udfylde. Blanketten kan også anvendes til indberetning om sikkerhedshændelser til andre myndigheder, herunder Datatilsynet.

[2] Jf. art. 2 i Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013
[3] Link: https://virk.dk/myndigheder/stat/ERST/selvbetjening/Indberetning_af_brud_paa_sikkerhed/

3. Et effektivt og fokuseret tilsyn

Digitaliseringsstyrelsens tilsyn er i høj grad baseret på indberetninger fra udbydere af elektroniske kommunikationstjenester.

Digitaliseringsstyrelsen har tilrettelagt sit tilsyn så det er effektivt og konsistent. Digitaliseringsstyrelsen arbejder herigennem på løbende at sikre, at udbyderne implementerer passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden i forbindelse med udbuddet af elektroniske kommunikationstjenester.

Vores tilsynsindsats tager udgangspunkt i en løbende screening og behandling af de indberetninger om brud på persondatasikkerheden, som vi modtager fra udbydere af elektroniske kommunikationstjenester.

Herudover modtager Digitaliseringsstyrelsen også ind imellem henvendelser fra borgere om mulige brud på persondatasikkerheden, der giver styrelsen anledning til at rette henvendelse til udbyderen med henblik på en nærmere redegørelse om forholdene og de sikkerhedsforanstaltninger, som udbyderen har implementeret – eller agter at implementere.

Det er vores erfaring igennem flere års tilsyn, at langt de fleste brud på persondatasikkerheden i forbindelse med udbuddet af elektroniske kommunikationstjenester sker som følge af menneskelige fejl på trods af, at tjenesteudbyderne ellers har implementeret foranstaltninger for at styre risici for persondatasikkerheden. Uagtet at passende foranstaltninger er implementeret kan menneskellige fejl ikke fuldstændig undgås.

I de tilfælde, hvor bruddet skyldes en menneskelig fejl, men hvor bruddet er stoppet, og der allerede er implementeret passende foranstaltninger, vil Digitaliseringsstyrelsen som udgangspunkt lukke sagen uden yderligere påtale. Det forudsætter dog, at der ikke er andre forhold, der taler imod det.

Det er desuden vores erfaring, at udbydere ved konstatering af bruddet oftest allerede har implementeret eller – på baggrund af bruddet – har iværksat en proces for at implementere passende foranstaltninger med henblik på at styre risici for yderligere sikkerhedsbrud.

I de få tilfælde, hvor det er uklart, om der er – eller vil blive – implementeret passende foranstaltninger, retter vi henvendelse til udbyderen og anmoder om yderligere oplysninger herom.

3.1 Dialogbaseret tilsyn

Digitaliseringsstyrelsen lægger vægt på at føre et dialogbaseret tilsyn med henblik på at understøtte, at der hos udbydere af elektroniske kommunikationstjenester i videst muligt omfang bliver implementeret passende foranstaltninger med henblik på at styre risici for persondatasikkerheden.

I praksis betyder det dialogbaserede tilsyn, at vi på baggrund af udbyderes indberetninger eller henvendelser fra borgere retter henvendelse til udbydere og anmoder om nærmere redegørelse om de forhold og foranstaltninger, der ikke er tilstrækkeligt belyst, er uklare eller udeladt.

Vi tager på baggrund af udbyderes uddybende redegørelse stilling til videre processkridt, som kan være en af følgende:

- Sagen lukkes på baggrund af indberetningen og den opfølgende redegørelse.
- Der er behov for yderligere redegørelser om sagens forhold.
- Vi meddeler påbud om at gennemføre tiltag for bl.a. at sikre mod brud[4].
- Vi meddeler påbud om at underrette brugeren om bruddet[5].
- Vi anmelder sagen til politiet med et bødeforlæg[6].

Udover at føre tilsyn med, at udbyderne lever op til reglerne om at have passende tekniske og organisatoriske foranstaltninger, bistår vi også udbyderne med generel vejledning og besvarelse af konkrete spørgsmål, fx om

- håndtering af indberetninger om brud, som skyldes at brugernavne og passwords er blevet lækket efter et hackerangreb på en tredjeparts hjemmeside, og som ikke egentlig skyldes manglende foranstaltninger hos udbyderen, eller
- hvornår der i konkrete tilfælde er tale om brud på persondatasikkerheden der ikke er sket i forbindelse med udbuddet af en elektronisk kommunikationstjeneste, men som derimod er et brud på persondatasikkerheden, der skal indberettes til Datatilsynet.

3.2 Tilsyn på eget initiativ

Digitaliseringsstyrelsen foretager også tilsyn på eget initiativ.

---

[4] Jf. bekendtgørelse nr. 1882 af 4. december 2020, § 12, stk. 2
[5] Jf. bekendtgørelse nr. 1882 af 4. december 2020, § 13, stk. 2
[6] Jf. bekendtgørelse nr. 1882 af 4. december 2020, § 15

Tilsyn på eget initiativ kan fx tage udgangspunkt i tendenser, som vi har observeret i vores løbende tilsyn. Tilsyn på eget initiativ kan fx have fokus på ofte forekommende fejltyper eller en nærmere afgrænset kreds af udbydere. Digitaliseringsstyrelsen har ikke fundet anledning til at iværksætte tilsyn på eget initiativ i 2022.

3.3 Samarbejde med Datatilsynet

Digitaliseringsstyrelsens tilsyn med reglerne om persondatasikkerhed i den elektroniske kommunikationssektor er sektorspecifikke regler, der træder i stedet for den generelle databeskyttelsesforordning (GDPR), når det handler om beskyttelse af personoplysninger inden for den elektronisk kommunikationssektor.

Digitaliseringsstyrelsens tilsyn har derfor naturligt en snitflade til Datatilsynets tilsyn med de generelle regler om beskyttelse af personoplysninger, der baserer sig på GDPR-lovgivningen.

Digitaliseringsstyrelsen er løbende i dialog med Datatilsynet om udviklingen på retsområdet for databeskyttelse og om problemstillinger, der ligger i grænselandet mellem de to lovgivningsområder. Det kan fx være tilfældet i sager, hvor der sker et brud på perondatasikkerheden hos en tjenesteudbyder, men hvor det ikke umiddelbart er klart, om bruddet er sket i forbindelse med udbuddet af en elektronisk kommunikationstjeneste (Digitaliseringsstyrelsens tilsyn) eller ej (Datatilsynets tilsyn).

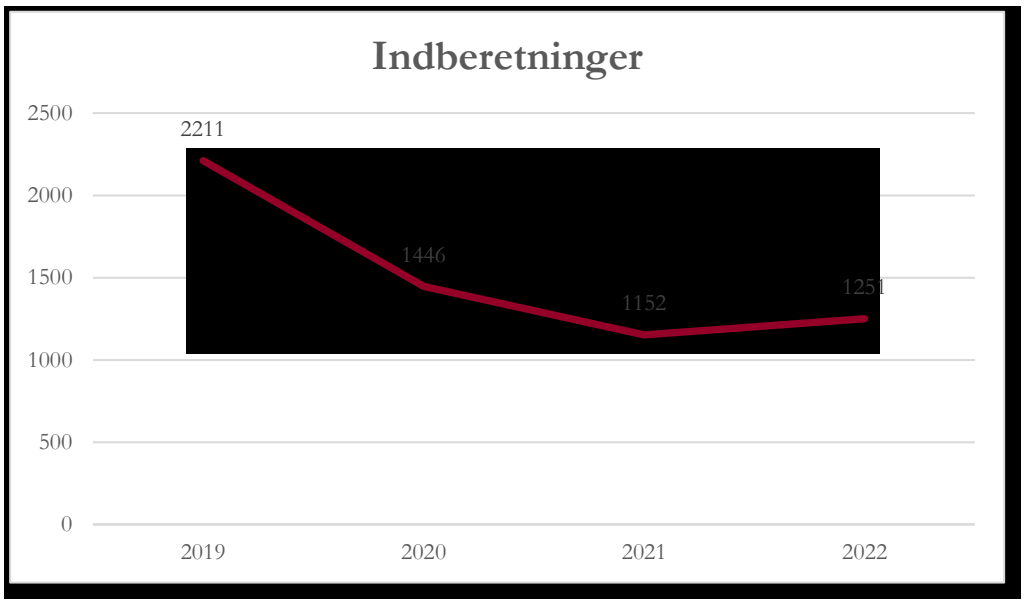
4. Fakta og nøgletal

Nøgletal for Digitaliseringsstyrelsens tilsyn med brud på persondatasikkerheden 2022.

I 2022 har Digitaliseringsstyrelsen modtaget 1.251 indberetninger om brud på persondatasikkerheden fra udbydere af elektroniske kommunikationstjenester.

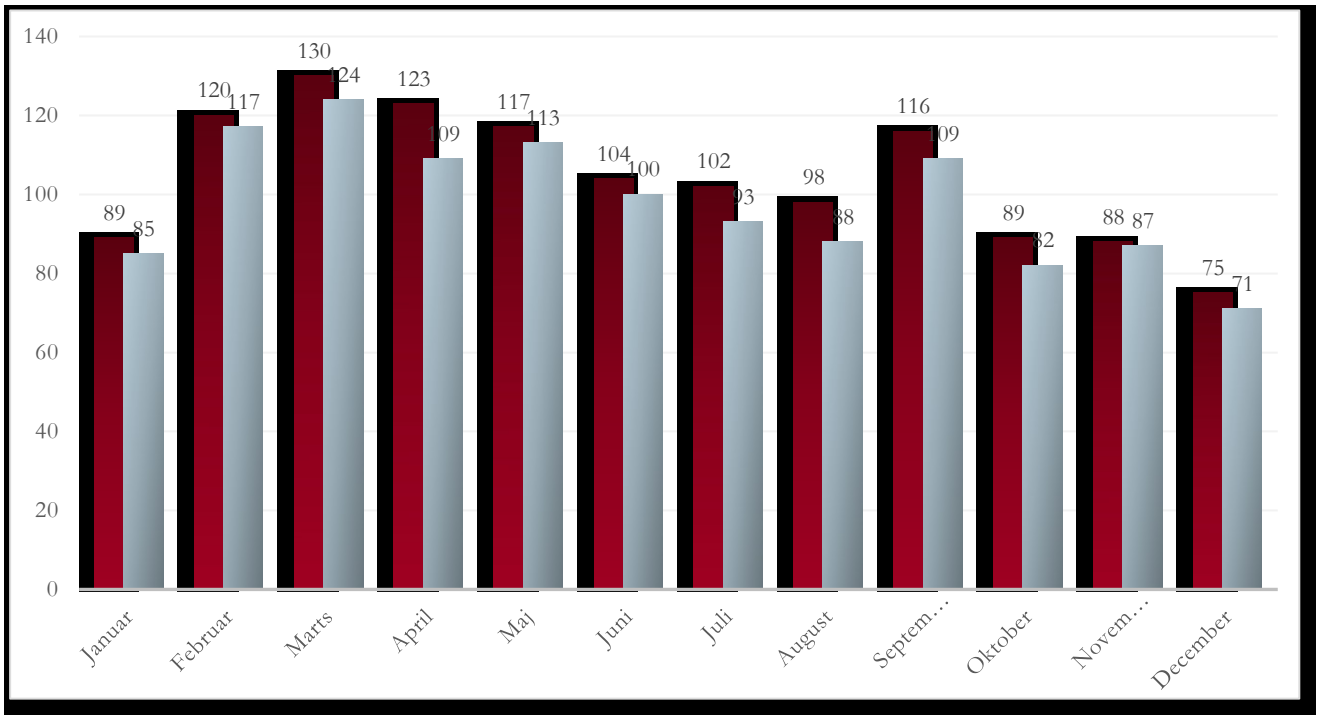
Antallet af indberetninger er faldet markant siden 2019, mens der i 2022 dog har været en lille stigning i forhold til året før.

Antal indberetninger pr. år de seneste fire år



Det er på baggrund af de seneste to år umiddelbart Digitaliseringsstyrelsens forventning, at antallet af indberetninger om brud på persondatasikkerheden i forbindelse med udbuddet af elektroniske kommunikationstjenester vil ligge på nogenlunde samme niveau i de kommende år. Dette baseres på, at udbyderne på den ene side fortsat vil have fokus på at styre risici for persondatasikkerhed, mens menneskelige fejl – der udgør ca. 95 pct. af sagerne – på den anden side ikke kan undgås fuldstændigt, uagtet at udbyderne har implementeret passende foranstaltninger.

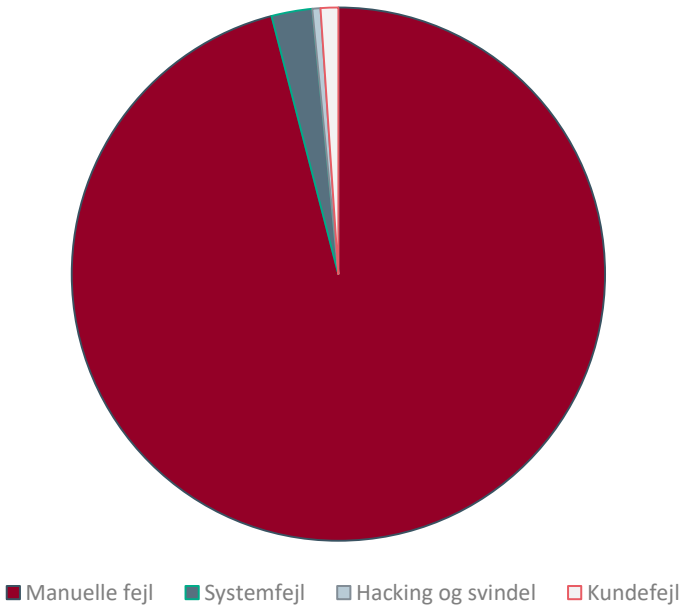
Antal sager pr. måned samt antallet af sager, der lukkes uden yderligere sagsbehandling



Figuren viser antal indberetninger samt sager der lukkes der lukkes uden yderligere sagsbehandling pr. måned i 2022

Diagrammet viser antallet af sager, der ikke giver anledning til yderligere sagsbehandling i sammenligning med det totale antal sager for hver måned i 2022. Af figuren fremgår det, at sagerne på baggrund af ovenstående kriterier i ca. 95 pct. af tilfældene ikke har givet anledning til yderligere sagsbehandling. Dette billede gør sig gældende på tværs af alle de udbydere, der har indberettet sager i 2022.

Fordelingen af fejltyper



Figuren viser et diagram fordelt på manuelle fejl, systemfejl, hacking eller svindel samt kundefejl.

Figuren viser, at langt de fleste indberetninger (ca. 95 pct.) vedrører brud, der er forårsaget af "manuelle fejl".

Manuelle fejl skyldes ofte simple fejlindtastninger af kundeservicemedarbejdere fx i forbindelse med oprettelse eller ændring af abonnementer eller ved overførsel af (forkerte) numre til abonnenter. Det er i disse sager oftest kun én persons oplysninger, der er omfattet af bruddet, og de omhandlede personoplysninger begrænser sig ofte til navn, kontaktoplysninger og/eller kunde-ID – altså personoplysninger, der som udgangspunkt ikke er fortrolige eller følsomme.

Den store andel af sådanne manuelle fejl betyder, at størstedelen af alle de indberettede persondatasikkerhedsbrud kun berører en person. Brud med flere berørte ses oftere i forbindelse med systemfejl eller hacking.

På baggrund af de indberetninger Digitaliseringsstyrelsen har modtaget fra udbydere af elektroniske kommunikationstjenester om brud på persondatasikkerheden i 2022, synes der at være en overordnet trend i retning af, at beskyttelsen af personoplysninger i den elektroniske kommunikationssektor i Danmark er blevet bedre over den periode, hvor Digitaliseringsstyrelsen har tal fra (2019-2022). Dette kan ses både i det markante fald i antallet af indberetninger siden 2019, og den store del af bruddene, som udgøres af manuelle fejl med begrænsede konsekvenser for de berørte.

Digitaliseringsstyrelsen iværksatte tilbage i 2021 en indsats for at informere danske nummeruafhængige interpersonelle kommunikationstjenester (NUIK-tjenester) om reglerne om persondatasikkerhed i den elektroniske kommunikationssektor og Digitaliseringsstyrelsens tilsyn hermed. Digitaliseringsstyrelsen modtog i 2021 tre indberetninger fra NUIK-tjenester, men har ingen indberetninger modtaget fra NUIK-tjenester i 2022.

5. Datakvalitet og dataanvendelse

Et godt datagrundlag er vigtigt for en kvalificeret tilsynsindsats.

Det er Digitaliseringsstyrelsens vurdering, at et godt datagrundlag er vigtigt for en kvalificeret tilsynsindsats. Vi arbejder derfor løbende med at forbedre den måde, vi anvender de data, vi indsamler, så vi kan kvalificere vores tilsyn.

For at kunne føre en mere datadrevet tilsynsindsats, er det vigtigt, at Digitaliseringsstyrelsen har et struktureret overblik over de indsamlede data. Ved at samle og organisere flere datapunkter – både om den enkelte sag og om større sagsmængder – kan vi gå fra formodninger om behov for indsatser til at foretage vurderinger baseret på fakta.

For at sikre datakvaliteten i Digitaliseringsstyrelsens tilsynsindsats har styrelsen over tid udviklet en screeningsproces, der understøtter løbende, struktureret registrering af data om indberetninger.

Ved at samle relevante data om indberetninger i ét overblik opnås en ensartet og standardiseret datastruktur. Dermed sikres det, at data kan anvendes i nye sammenhænge, fx til at identificere specifikke fejltyper på tværs af udbydere, eller til at identificere fejltyper, der går igen hos den enkelte udbyder eller på tværs af udbyderne. Denne information kan kvalificere Digitaliseringsstyrelsens tilsynsindsats med henblik på at identificere konkrete risici for persondatasikkerheden, så udbyderne kan træffe passende tekniske og organisatoriske foranstaltninger for at minimere disse risici.

Digitaliseringsstyrelsen anvender også de strukturerede data til en visualisering af sagerne bl.a. i forhold til udbyder, fejltype og sikkerhedsbrudenes generelle karakter. Visualiseringen anvendes i den interne rapportering, men det er Digitaliseringsstyrelsens ambition, at visualiseringen af data i højere grad også skal kunne anvendes i dialogen med selskaberne, bl.a. ved at kunne illustrere udviklingen i sikkerhedsbrud og typiske fejltyper.

digst.dk