Minivejledning til håndtering af brud på persondatasikkerheden

Denne vejledning er alene ment for at give klinikken/osteopaten som *dataansvarlig* et overblik over de pligter, som man har, hvis der konstateres et databrud/brud på persondatasikkerheden. Minivejledningen er således kun et uddrag af Datatilsynets vejledning fra februar 2018, som i sin helhed kan hentes på www.datatilsynet.dk. Det direkte link til tilsynets vejledning findes her.

Hvad er et brud på persondatasikkerheden

Et brud på persondatasikkerheden defineres som: "Et brud sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller anden måde behandlet."

Et brud på persondatasikkerheden kan f.eks. rent teknisk ske, når den dataansvarliges it-systemer med personoplysninger ikke er tilstrækkelig sikret, således at udefrakommende får adgang til oplysningerne (f.eks. hacking). Det kan imidlertid også være den dataansvarliges egen håndtering af personoplysningerne, der kan forårsage et brud, f.eks. hvis den dataansvarlige ubeføjet videregiver eller ændrer personoplysningerne. Et andet eksempel, når det gælder den dataansvarliges egen håndtering af personoplysningerne er, hvis den dataansvarlige ulovligt eller som følge af et hændeligt uheld (f.eks. brand eller oversvømmelse) i en periode ikke har adgang til eller ender med at tilintetgøre personoplysningerne.

Som eksempler på brud på persondatasikkerheden kan nævnes:

1) **Andre personer end den eller de personer hos dataansvarlige, der er autoriseret til det, får (uautoriseret) adgang til personoplysninger. Det kan både være personer uden for eller inden for dataansvarliges organisation.**

2) **Den dataansvarliges medarbejdere ændrer eller sletter personoplysninger ved et uheld.**

3) **Brud på den dataansvarliges server, hvor uvedkommende har fået indsigt i personoplysninger – f.eks. kundedatabasens CPR-oplysninger, kreditkortoplysninger el.lign.**

4) **Den dataansvarliges medarbejdere videregiver ubevidst eller bevidst personoplysninger om en borger/kunde til en anden borger/kunde – eller måske ligefrem flere andre uvedkommende personer.**

5) **Når manglede kryptering af den dataansvarliges hjemmeside indeholdende f.eks. et kundelogin resulterer i, at en eller flere uvedkommende får direkte adgang til kundens personoplysninger.**

Et brud på persondatasikkerheden er samtidig en "informationssikkerhedshændelse". Men det er kun "informationssikkerhedshændelser", der fører til *"hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger"*, der er omfattet af databeskyttelsesforordningens definition af et brud på persondatasikkerheden. En "informationssikkerhedshændelse" vil således ikke altid være et brud på persondatasikkerheden. Som et eksempel herpå kan nævnes flere forgæves forsøg på log-in, som vil være at betragte som en sikkerhedshændelse, men **uden** at der samtidig er tale om et brud på persondatasikkerheden. Dette vil derfor ikke kræve anmeldelse til Datatilsynet m.v.

Brud på persondatasikkerheden skal anmeldes til Datatilsynet.

Som udgangspunkt skal alle brud på persondatasikkerheden anmeldes til Datatilsynet. Det er således kun, hvis det er usandsynligt, at bruddet på persondatasikkerheden ikke har indebåret en risiko for fysiske personers rettigheder eller frihedsrettigheder, at man som dataansvarlig kan undlade at anmelde det.

Den dataansvarlige skal straks efter at være blevet bekendt med bruddet på persondatasikkerheden vurdere sandsynligheden for, om bruddet indebærer en risiko for de berørte fysiske personers rettigheder.

Følgende forhold bør altid indgå i den konkrete vurdering af risikoen for de registreredes rettigheder og frihedsrettigheder som følge af et brud på persondatasikkerheden:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse;
- Oplysningernes art og omfang;
- Risikoen for at registrerede kan identificeres;
- Konsekvenser bruddet kan have for de registrerede;
- Hvorvidt bruddet omfatter særlige registrerede (f.eks. hvis der er tale om børn eller særligt udsatte);
- Antallet af berørte fysiske personer;

For en uddybende beskrivelse, se Datatilsynets vejledning pkt. 3.3

Den dataansvarliges forpligtelser

Dataansvarlig og databehandler

Som det helt klare udgangspunkt er klinikken/ osteopaten den *dataansvarlige* i lovens forstand, mens en eventuel aftale med et (it-) firma om at benytte deres platform/it-system til opbevaring at persondata 'alene' indebærer , at (it-) firmaet er *databehandler*.

Datatilsynet har anført følgende eksempel der kan belyse forskellen mellem dataansvarlig og databehandler.

> "Fitness A bruger et system, der ejes og administreres af Web B
>
> En fitnesskæde (Fitness A) har brug for at behandle personoplysninger, herunder navne, person- numre, e-mailadresser og kontooplysninger, om sine medlemmer. Formålet med behandlingen er bl.a., at Fitness A skal kunne opkræve betaling for medlemskab.
>
> Fitness A ønsker at benytte et elektronisk system, hvori de nødvendige oplysninger kan registreres, opbevares og ajourføres mv. Fitness A indgår derfor en aftale med IT-virksomheden Web B, som har udviklet et system "FitnessCare", der kan det, som Fitness A ønsker. Oplysningerne, som Fitness A indtaster i systemet, opbevares på servere hos Web B, som ejer og administrerer "FitnessCare".
>
> I aftalen mellem Fitness A og Web B fremgår det klart, at Web B kun må behandle oplysninger om Fitness A's medlemmer på den måde, som er aftalt med og godkendt af Fitness A.
>
> Fitness A bestemmer således, med hvilke formål, der skal behandles personoplysninger (så Fitness A kan opkræve betaling fra deres medlemmer mv.) og hvordan oplysningerne skal behandles. Fitness A er derfor dataansvarlig.
>
> Aftalen mellem Web B og Fitness A går her ud på, at Web B skal levere en ydelse, der består i, at Web B skal behandle (opbevare mv.) personoplysninger. Ydelsen er altså behandling af personoplysninger. Når behandlingen samtidig alene sker på vegne af Fitness A, er Web B i denne situation databehandler.

Undtagelsesvis og i helt særlige tilfælde, vil der ikke være behov for, at datasikkerhedsbruddet anmeldes til Datatilsynet. Det kræver, at den dataansvarlige konkret vurderer, at ikke er en risiko for konsekvenser for de berørte personers rettigheder.

Det anbefales dog, at alle datasikkerhedsbrud anmeldes til Datatilsynet, idet undtagelsen for at anmelde fortolkes ret snævert. Det er den dataansvarlige, som har bevisbyrden for, at der foreligger omstændigheder, der gør, at det er usandsynligt, at et brud på persondatasikkerheden har eller kan få konsekvenser for de berørte personer.

Datatilsynet anfører, at du eksempelvis som dataansvarlig kan undlade anmeldelse til tilsynet, hvis " oplysningerne f.eks. er endt hos en forkert modtager, som du som dataansvarlig har stor tillid til og forventer vil tilbagelevere eller destruere oplysningerne". Det er den dataansvarlige, som har bevisbyrden for, at der foreligger omstændigheder, der gør, at det er usandsynligt, at et brud på persondatasikkerheden har eller kan få konsekvenser for de berørte personer.

Hvem skal anmelde bruddet til Datatilsynet

Den **dataansvarlige** har det juridiske ansvar for at anmelde et brud på persondatasikkerheden til Datatilsynet, og har også ansvaret for at det sker rettidigt. En databehandler vil også kunne anmelde et brud på persondatasikkerheden til Datatilsynet på vegne af den dataansvarlige, hvis databehandleren har fået fuldmagt til det, og at dette fremgår af den databehandleraftale, der er indgået mellem databehandleren og den dataansvarlige.

Som dataansvarlig er du forpligtet til at anmelde bruddet til Datatilsynet, så snart det er muligt – også selv om dette tidspunkt er inden 72 timer, fra du bliver bekendt med bruddet.

Tidspunktet for anmeldelse:

Du skal som dataansvarlig "uden unødig forsinkelse" og om muligt senest 72 timer, efter at du er blevet bekendt med bruddet, anmelde bruddet til Datatilsynet. Foretages anmeldelsen til Datatilsynet ikke inden for 72 timer, skal du i anmeldelsen også vedlægge en begrundelse for forsinkelsen.

Når det gælder tidsgrænsen på de 72 timer, tager Datatilsynet ikke hensyn til, at den dataansvarlige måske først bliver bekendt med bruddet uden for normal kontortid, herunder i weekender og på helligdage. Overskrides de 72 timer, skal du som dataansvarlig være i stand til at redegøre for de særlige grunde, der umuliggjorde anmeldelse til Datatilsynet inden for fristen.

Hvad skal indgå i anmeldelsen og hvilke oplysninger har Datatilsynet brug for?

Når en dataansvarlig anmelder et brud på persondatasikkerheden til Datatilsynet, skal anmeldelsen som minimum:

- **beskrive karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger**
- **angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes**
- **beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden**
- **beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.**

Du skal anmelde bruddet til Datatilsynet, selvom du ikke er i stand til at afgive alle de oplysninger, der som minimum skal med i anmeldelsen, inden for tidsfristen på de 72 timer. Du skal i givet fald i stedet for give oplysningerne trinvist til Datatilsynet uden yderligere forsinkelse.

Den digitale indberetning findes på www.virk.dk., med brug af virksomhedens NemID. https://virk.dk/myndigheder/stat/ERST/selvbetjening/Indberetning_af_brud_paa_sikkerhed/

Skemaet kan ses i pdf. format her

Databehandlerens forpligtelser

Bliver en *databehandler* opmærksom på, at der er sket et brud på persondatasikkerheden, har databehandleren pligt til uden unødig forsinkelse at underrette den dataansvarlige om bruddet. Der er tale om en absolut forpligtelse, dvs. en forpligtelse, som databehandleren skal efterleve i alle tilfælde. Databehandleren kan f.eks. ikke undlade at underrette den dataansvarlige om et brud på persondatasikkerheden med henvisning til, at databehandleren selv har vurderet, at det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Underretning af den registrerede

Hvis brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal den dataansvarlige **også** underrette den/de registrerede om bruddet. Formålet med underretningen er bl.a. at give den registrerede mulighed for at træffe de fornødne forholdsregler i tilfælde af, at der er sket kompromittering af vedkommendes personoplysninger.

Den dataansvarlige skal underrette den registrerede uden unødig forsinkelse efter, at bruddet på persondatasikkerheden er påvist.

Underretningen til den registrerede skal beskrive karakteren af bruddet på persondatasikkerheden og som minimum:

- angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
- beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
- beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Hvis det er relevant, bør den dataansvarlige også give den registrerede specifikke råd om, hvordan den registrerede kan beskytte sig mod mulige negative konsekvenser af bruddet, som f.eks. nulstilling eller ændring af adgangskoder, hvis den registreredes adgangsoplysninger er blevet kompromitteret.

Underretningen af den registrerede skal gives i et klart og forståeligt sprog.

Den dataansvarlige skal underrette den registrerede direkte, f.eks. via e-mail, brev, sms eller lignende. En underretning, der begrænser sig til en pressemeddelelse eller et opslag i en virksomheds blog vil typisk ikke være tilstrækkelig. Meddelelsen til den registrerede må heller ikke sendes til vedkommende sammen med anden information, så som generelle opdateringer, nyhedsbreve eller standardmeddelelser fra den dataansvarlige.

Det er den dataansvarlige, der har ansvaret for at underrette de berørte personer om et brud på persondatasikkerheden. Den dataansvarlige vil dog kunne uddelegere opgaven med at underrette de registrerede til eksempelvis en databehandler. Dette forudsætter imidlertid, at databehandleren har fået bemyndigelse hertil. Det er dog vigtigt i den forbindelse at understrege, at det overordnede juridiske ansvar for, at der er foretaget underretning af de registrerede, forbliver hos den dataansvarlige uanset, at den dataansvarlige har bemyndiget databehandleren til at forestå underretningen.

Hvis den dataansvarlige efter at have foretaget en vurdering af alle de mulige konsekvenser og negative virkninger for de registrerede af et brud på persondatasikkerheden når frem til, at bruddet er af en sådan karakter, at det sandsynligvis ikke vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder, er det dog ikke nødvendigt at underrette den registrerede.

Bevisbyrden for, at ovennævnte betingelse er opfyldt, påhviler den dataansvarlige. Den dataansvarlige skal således f.eks. i forbindelse med en sag hos Datatilsynet være i stand til at begrunde, hvorfor underretning af den registrerede blev fravalgt.

Intern dokumentation

Den dataansvarlige skal dokumentere alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved brud på persondatasikkerheden, dets virkninger og de afhjælpende foranstaltninger.

Kravet om intern dokumentation gælder uanset om, den dataansvarlige skal anmelde bruddet til datatilsynet, eller om det undtagelsesvis er vurderet, at der ikke skal ske en. Formålet med dokumentationspligten er at sætte tilsynet i stand til at kontrollere, om forpligtelsen om at anmelde visse brud på persondatasikkerheden er overholdt.

Dokumentationen skal indeholde en række informationer om bruddet, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne afhjælpende foranstaltninger.

Eksempel på internt dokumentationsregister:

Brud på persondatasikkerheden hos [navnet på virksomheden/myndigheden]:

Beskrivelse af bruddet:

1. Dato og tidspunkt for bruddet?
2. Hvad er der sket?
3. Årsagen til bruddet?
4. Hvilken type personoplysninger er berørt?
5. Hvilke konsekvenser har bruddet for de berørte personer?
6. Hvilke afhjælpende foranstaltninger er truffet?
7. Er der sket anmeldelse af bruddet til Datatilsynet (hvis ja, hvornår)?

7.1 Hvis nej, begrundelse for ikke at anmelde bruddet til Datatilsynet?

8. Er der sket underretning af de berøte personer (hvis ja, hvornår)?

8.1 Hvis nej, begrundelse for ikke at underrette de berøte personer?

November 2021 Danske Osteopater

Tjekliste og opsummering

1) Den dataansvarlige skal i tilfælde af et brud på persondatasikkerheden uden unødig forsinkelse og om muligt inden 72 timer foretage anmeldelse af bruddet til Datatilsynet via Virk.dk, (https://virk.dk/myndigheder/stat/ERST/selvbetjening/Indberetning_af_brud_paa_sikkerhed/) medmindre det er usandsynligt, at bruddet medfører en risiko for personers rettigheder eller frihedsrettigheder.

2) En række minimumskrav til indholdet af anmeldelsen (udfyldelse af blanket):

   - Karakteren af bruddet på persondatasikkerheden mv.
   - Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
   - De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
   - De foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

3) Anmeldelse til Datatilsynet kan ske trinvist.

4) Den dataansvarlige skal underrette den registrerede, når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

5) Den dataansvarlige skal underrette den enkelte registrerede uden unødig forsinkelse.

6) Underretningen, der skal gives i et klart og forståeligt sprog, skal beskrive karakteren af bruddet og mindst indeholde oplysninger om:

   - Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
   - De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
   - De foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

7) Det er ikke nødvendigt at underrette den registrerede, hvis en af følgende betingelser er opfyldt:

   A) Den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger.

   B) Den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registrerede ikke længere er reel.

   C) Det vil kræve en uforholdsmæssig indsats – i så fald skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

8) Den dataansvarlige skal dokumentere alle brud, herunder de faktiske omstændigheder, konsekvenser og trufne afhjælpende foranstaltninger.

Internt dokumentationsregister:

Brud på persondatasikkerheden hos [navnet på virksomheden/myndigheden]:

1. Dato og tidspunkt for bruddet?

2. Hvad er der sket?

3. Årsagen til bruddet?

4. Hvilken type personoplysninger er berørt?

5. Hvilke konsekvenser har bruddet for de berørte personer?

6. Hvilke afhjælpende foranstaltninger er truffet?

7. Er der sket anmeldelse af bruddet til Datatilsynet (hvis ja, hvornår)?

7.1 Hvis nej, begrundelse for ikke at anmelde bruddet til Datatilsynet?

8. Er der sket underretning af de berøte personer (hvis ja, hvornår)?

8.1 Hvis nej, begrundelse for ikke at underrette de berøte personer?

Beskrivelse af bruddet: