**Det gør du, når der sker databrud**

**Som noget nyt skal virksomheder i visse situationer melde databrud til Datatilsynet senest 72 timer efter, at man er blevet bekendt med det.**

Et databrud defineres af Datatilsynet som et brud, der ”fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger der er transmitteret, opbevaret eller på anden måde behandlet.”

Som eksempler på brud på persondatasikkerheden kan nævnes:

* uautoriserede personer får adgang til personoplysninger. Det kan både være personer uden for eller inden for dataansvarliges organisation.
* Medarbejdere ændrer/sletter personoplysninger ved et uheld eller videregiver personoplysninger om en kunde til uvedkommende personer.
* Brud på den dataansvarliges server, hvor uvedkommende har fået indsigt i personoplysninger

”Er der sket et brud på persondatasikkerheden, risikerer virksomheden både at skulle underrette datatilsynet såvel som de berørte personer. Vurderingen er dog ikke helt den samme. Det er derfor en god idé, at virksomheden har en beskrevet proces for håndtering af disse situationer,” udtaler Tim Nielsen, advokat hos DAHL Advokatfirma, med speciale i bl.a. persondata.

**Det skal du vurdere ved et databrud**

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

**Hvem skal anmelde et brud og hvor henne**

Som udgangspunkt er det den dataansvarlige, som anmelder et brud på persondatasikkerheden til Datatilsynet.

En databehandler vil dog også kunne anmelde et brud på persondatasikkerheden til Datatilsynet på vegne af den dataansvarlige. Dette forudsætter imidlertid, at databehandleren har fået bemyndigelse hertil, og at dette fremgår af den databehandleraftale, der er indgået mellem parterne.

For at gøre det nemt og enkelt for virksomheder og myndigheder at indberette databrud, arbejdes der i øjeblikket på at etablere én fælles digital løsning, der vil blive placeret på Virk.dk. Løsningen vil være klar, når databeskyttelsesforordningen træder i kraft 25. maj 2018.

Danske virksomheder kan også behandle oplysninger om personer, der befinder sig i andre EU-medlemslande. I sådanne situationer kan det være nødvendigt, at kontakte myndighederne i de relevante lande.

**Berørte personer skal også have besked**

Når et brud på persondatasikkerheden indebærer en høj risiko for personers rettigheder og frihedsrettigheder, skal den dataansvarlige også underrette de berørte personer om bruddet.

Når man underretter de berørte personer, skal man 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 man har truffet for at håndtere bruddet på persondatasikkerheden. Herunder hvad man har gjort for at begrænse de mulige skadevirkninger.

Et eksempel kunne være, hvor en musikstreamingtjeneste er blevet hacket, og hvor brugerdatabasen (inkl. brugernes fulde navn, musikpræferencer samt brugernavn og adgangskode) efterfølgende er blevet offentliggjort på internettet.

De negative konsekvenser ved lækagen for de registrerede kan umiddelbart virke relativt harmløse. Men da adgangskoderne er blevet kompromitteret, skal de fornys.

Eftersom mange brugere anvender den samme adgangskode på forskellige konti, vil bruddet som en sekundær negativ virkning sandsynligvis også medføre et brud på fortroligheden i forbindelse med en anden konto.

Underretningen skal derfor også indeholde oplysninger om de sandsynlige negative virkninger i forbindelse med andre konti og bør derfor omfatte en anbefaling om at bruge forskellige adgangskoder på forskellige websteder og om at forny adgangskoderne til konti, hvor den kompromitterede adgangskode blev anvendt.

**Hvornår skal et brud ikke anmeldes**
Et brud på persondatasikkerheden skal ikke anmeldes til Datatilsynet, hvis det er usandsynligt, at bruddet indebærer en risiko for personernes rettigheder eller frihedsrettigheder.

Bruddet skal heller ikke anmeldes til de berørte kunder/personer, hvis den dataansvarlige efterfølgende har sikret, at den høje risiko for de registrerede ikke længere er reel.

Det kan f.eks. skyldes de sikkerhedsforanstaltninger, som er truffet af den dataansvarlige eller hurtig indgriben samt mulighed for at konstatere, om personoplysninger er kommet til uvedkommendes kendskab.

Den dataansvarlige vil endelig også kunne undlade at underrette de registrerede enkeltvis, hvis det i det konkrete tilfælde vil kræve en uforholdsmæssig indsats.

Som eksempel på et tilfælde, som umiddelbart må anses for at være omfattet af denne undtagelse, kan nævnes en situation, hvor en virksomhed har mistet adgang til alle kundeoplysninger i forbindelse med, at virksomheden er blevet ramt af ransomware.

Hvis virksomheden vurderer, at det vil kræve en uforholdsmæssig indsats at underrette til hver enkelt registrerede, vil der i stedet skulle foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

**Vil du vide mere?**

I forbindelse med [persondataforordningen har vi lavet et tema-univers om emnet](https://itb.dk/articles/databeskyttelse-og-sikkerhed/persondataforordningen), hvor du kan finde råd og vejledning om, hvordan du bliver klar til GDPR-direktivet.

Og så er du som medlem af IT-Branchen altid velkommen til at tage fat i [DAHL Advokatfirma](https://www.dahllaw.dk/) eller i Dansk Erhvervs jurister på 33 74 64 00, hvis du har spørgsmål om persondataforordningen.

**Eksempler fra Datatilsynet**Datatilsynet er kommet med et par eksempler på, hvornår man skal melde databrud til dem, og hvornår man ikke skal.

Man kan finde flere eksempler i Datatilsynets [Vejledning om håndtering af brud på persondatasikkerheden.](https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf)

|  |  |  |
| --- | --- | --- |
| **Eksempel** | **Skal der ske anmeldelse til Datatilsynet?** | **Skal den registrerede underrettes?**  |
| En klinik for fysioterapi bliver udsat for ransomware, da en medarbejder trykker på et link i en e-mail.Dette resulterer i, at al data, herunder helbredsoplysninger om 200 patienterne bliver krypteret og låst for klinikkens medarbejdere. Klinikken har foretaget backup af sine systemer, men det er også lykkes bagmændene at kryptere disse.  | Ja, klinikken bør anmelde hændelsen til Datatilsynet.  Dette skyldes bl.a., at uvedkommende potentielt kan have fået adgang til følsomme oplysninger vedrørende et stort antal personer, og at klinikken ikke vil have mulighed for at gendanne oplysningerne via deres backup kopi.  Klinikken bør underrette Datatilsynet uanset, om det lykkes klinikken af få frigivet oplysningerne.  | Ja, klinikken bør formentlig underrette de registrerede.  Udover karakteren af de oplysninger, som er blevet ramt af angrebet, kan det muligvis få negative konsekvenser for de berørte personer, at oplysninger om et behandlingsforløb eller lign. hos klinikken ikke kan gendannes.  |
| En HR-medarbejder sender ved en fejl lønsedler og ansættelseskontrakt til en forkert medarbejder i virksomheden.  Det aftales, at medarbejderen sletter dokumenterne med det samme efter at være blevet opmærksom på fejlen. | Ikke nødvendigvis.  Virksomheden kan vurdere, at bruddet ikke indebærer en risiko for den registrerede.  Dette kan skyldes, at der er tale om et ”internt” brud persondatasikkerheden og, at virksomheden har stor tillid til den pågældende medarbejder. | Hvis virksomheden vurderer, at der ikke er pligt til at underrette Datatilsynet, vil der heller ikke være pligt til at underrette den registrerede.  |
| Et lille flyttefirma har alle oplysninger om deres medarbejdere liggende på en computer, der ikke har backup. Computeren bliver ramt af vandskade, og oplysningerne kan ikke gendannes. På computeren lå bl.a. oplysninger om flere medarbejderes helbredsoplysninger.  | Hvis virksomheden kan sikre de registreredes rettigheder af anden vej end elektronisk, skal virksomheden ikke anmelde bruddet.  I modsat fald skal der ske anmeldelse til Datatilsynet.  | Idet den enkelte medarbejder skal kunne varetage sine interesser, skal der ske underretning af medarbejderne.  Det er den enkelte medarbejder der er nærmest til vurdere, om det, der er gået tabt, er blevet reetableret fyldestgørende. |
| En virksomhed har alle oplysninger om deres medarbejdere, inkl. personnumre og helbredsoplysninger, liggende på en computer. Computeren stjæles under et indbrud. Oplysningerne er ikke krypterede, men der skal almindeligt kodeord til for at låse computeren op.  | Ja, virksomheden skal anmelde bruddet til Datatilsynet.  Dette skyldes, at der er tale om følsomme og fortrolige personoplysninger om medarbejderne og, at der med de af virksomheden beskedne sikkerhedsforanstaltninger er en risiko for, at uvedkommende får adgang til personoplysningerne.  | Ja, virksomheden bør underrette hver medarbejder om bruddet, idet der er stor sandsynlighed for, at oplysningerne kan blive kompromitteret.  Den registrerede skal således have mulighed for at træffe de fornødne forholdsregler   |