Håndtering af brud på persondatasikkerheden

– kort fortalt



Denne korte vejledning giver et overblik over de væsentligste databeskyttelsesregler for håndtering af brud på persondatasikkerheden. Den bygger på Datatilsynets vejledning "Håndtering af brud på persondatasikkerheden" og erstatter ikke den fulde vejledning, hvor du finder uddybende juridiske forklaringer, konkrete eksempler og en nærmere gennemgang af reglerne.

DATATILSYNET

1. Hvornår er der tale om et brud?

Et brud på persondatasikkerheden er et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Brud kan vedrøre fortrolighed (uvedkommende får adgang), integritet (oplysninger ændres) eller tilgængelighed (oplysninger går tabt eller bliver utilgængelige). Flere typer kan forekomme samtidig.

EKSEMPEL

En e-mail sendes til en forkert modtager, en medarbejder tilgår oplysninger uberettiget, eller et ransomwareangreb gør oplysninger utilgængelige. Et mislykket hackerangreb er derimod ikke nødvendigvis et brud. Det afgørende er, om personoplysninger er blevet kompromitteret. Uautoriseret adgang kan udgøre et brud, selvom ingen beviseligt har læst oplysningerne.

En bevidst videregivelse, som den dataansvarlige troede var lovlig, men som senere viser sig ulovlig, er som det klare udgangspunkt ikke et brud på persondatasikkerheden. Den kan dog stadig være i strid med databeskyttelsesreglerne.

2. Hvornår skal bruddet anmeldes til Datatilsynet?

Den dataansvarlige skal som udgangspunkt anmelde bruddet, medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Vurder både sandsynligheden for og alvoren af mulige konsekvenser.

Se b.la. på oplysningernes karakter og mængde, muligheden for at identificere personer, hvem der kan have fået adgang, bruddets varighed, antallet af berørte og om særligt sårbare personer er omfattet. Mulige konsekvenser kan være identitetstyveri, økonomisk tab eller krænkelse af privatlivet. Et brud kan være anmeldelsespligtigt, selvom kun én person er berørt.

EKSEMPEL

Hvis oplysninger er beskyttet med stærk kryptering, som uvedkommende ikke kan omgå, kan det efter en konkret vurdering være usandsynligt, at bruddet indebærer en risiko. Undersøg dog, om bruddet også har påvirket oplysningernes tilgængelighed eller integritet. Beslutter du ikke at anmelde, skal du kunne dokumentere din vurdering.

3. Hvornår og hvordan skal du anmelde?

Et anmeldelsespligtigt brud skal anmeldes uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet. De 72 timer er ikke en ventefrist. Fristen gælder også i weekender og på helligdage.

Den dataansvarlige anses som udgangspunkt for at være bekendt med et brud, når en medarbejder bliver bekendt med det. En mistanke er ikke i sig selv tilstrækkelig, men skal undersøges hurtigst muligt. Når de indledende undersøgelser med rimelig grad af sikkerhed viser, at personoplysninger er kompromitteret, er den dataansvarlige normalt bekendt med bruddet. Hvis du fortsat er i tvivl, men ikke kan afvise, at der er sket et brud, bør du som hovedregel anmelde hændelsen. Du kan ikke udskyde fristen ved at vente med undersøgelsen.

Anmeld som udgangspunkt inden for fristen, selvom du endnu ikke har alle oplysninger. Supplér anmeldelsen uden yderligere unødig forsinkelse, når du ved mere. Anmelder du efter 72 timer, skal forsinkelsen begrundes.

Anmeldelse sker som udgangspunkt via Virk.dk. Den skal som minimum indeholde:

- Bruddets karakter og, om muligt, kategorier og omtrentligt antal berørte personer og registreringer.
- Kontaktoplysninger på databeskyttelsesrådgiveren eller et andet kontaktpunkt.
- De sandsynlige konsekvenser af bruddet.
- De trufne eller planlagte foranstaltninger til at håndtere bruddet og begrænse skadevirkningerne.

Det er den dataansvarlige, der har ansvaret for anmeldelsen. En databehandler skal underrette den dataansvarlige uden unødig forsinkelse, når databehandleren bliver bekendt med et brud – uanset databehandlerens egen risikovurdering. Databehandleren kan anmelde på vegne af den dataansvarlige, men overtager ikke ansvaret.

4. Hvornår skal de berørte personer underrettes?

Hvis bruddet sandsynligvis indebærer en høj risiko for de berørte personers rettigheder og frihedsrettigheder, skal de som udgangspunkt underrettes. Tærsklen for underretning er altså højere end for anmeldelse til Datatilsynet. Hvis den høje risiko kun gælder nogle af de berørte, skal disse personer underrettes.

Underretningen skal ske uden unødig forsinkelse. Der gælder ikke en fast 72-timersfrist. Hurtig underretning kan være afgørende, f.eks. hvis adgangskoder eller oplysninger, der kan misbruges økonomisk, er kompromitteret.

Underretningen skal være klar og forståelig og mindst beskrive bruddets karakter, kontaktoplysninger, sandsynlige konsekvenser og trufne eller planlagte foranstaltninger. Forklar konkret, hvad bruddet kan betyde for personen, og giv relevante råd til at begrænse konsekvenserne.

Underret som det klare udgangspunkt direkte og skriftligt, f.eks. via Digital Post, brev, e-mail eller sms. En generel nyhed på hjemmesiden er normalt ikke tilstrækkelig.

5. Hvornår kan underretning undlades?

Selvom bruddet oprindeligt indebærer en høj risiko, kan underretning efter en konkret vurdering undlades, hvis:

- Oplysningerne allerede før bruddet var beskyttet af passende foranstaltninger, der gør dem uforståelige for uvedkommende, eksempelvis effektiv kryptering.
- Efterfølgende foranstaltninger sikrer, at den høje risiko sandsynligvis ikke længere vil indtræde.
- Direkte underretning kræver en uforholdsmæssig indsats. I så fald kan du undlade at underrette hver person direkte, men skal i stedet offentliggøre en meddelelse eller anvende en anden foranstaltning, som informerer de berørte på en tilsvarende effektiv måde. Du skal kunne begrunde, hvorfor direkte underretning er uforholdsmæssig.
- Underretning kan efter databeskyttelseslovens § 22 begrænses, hvis afgørende private eller offentlige hensyn vejer tungere end den berørtes interesse i at få oplysningerne. **Undtagelsen forudsætter en nærliggende fare for skade af væsentlig betydning for de pågældende interesser og skal som udgangspunkt vurderes for hver enkelt oplysning.** Kun de oplysninger, som undtagelsen omfatter, må undlades. Ved tvivl bør du som hovedregel underrette.

Du skal kunne begrunde undladelsen. Datatilsynet kan påbyde underretning, hvis betingelserne er opfyldt.

6. Dokumentér bruddet, og hav procedurer klar

Alle brud på persondatasikkerheden skal dokumenteres – også dem, der hverken anmeldes til Datatilsynet eller fører til underretning. Dokumentér de faktiske omstændigheder, bruddets virkninger og de afhjælpende foranstaltninger. Notér risikovurderingen og begrundelserne for evt. ikke at anmelde eller underrette.

Der er ingen særlige formkrav til dokumentationen. Datatilsynet anbefaler som udgangspunkt at opbevare den i fem år, men opbevaringen skal fortsat overholde de øvrige databeskyttelsesregler.

Hav procedurer, så medarbejderne ved, hvem de skal kontakte, hvordan brud standses, og hvordan anmeldelse og underretning sker rettidigt. Følg op på hændelsen for at forebygge nye brud. Undersøg, om der også gælder anmeldelsespligt til andre myndigheder.

Kort tjekliste ved et brud

- ✓ Undersøg hændelsen, og begræns skadevirkningerne.
- ✓ Afklar hvilke oplysninger og personer der er berørt, og vurder risikoen.
- ✓ Anmeld til Datatilsynet uden unødig forsinkelse, hvis bruddet er anmeldelsespligtigt.
- ✓ Underret de berørte uden unødig forsinkelse, hvis der sandsynligvis er høj risiko, og ingen undtagelse gælder.
- ✓ Dokumentér hændelsen, beslutningerne og opfølgningen.