GDPR: Førstehjælp ved sikkerhedsbrud

GDPR kræver, at I følger en særlig procedure, når I oplever brud på persondatasikkerheden i virksomheden (og ja, alle oplever sikkerhedsbrud).

Følger I denne trin-for-trin-guide, begrænser I skaden, lever op til jeres forpligtelse – og står jer bedst med Datatilsynet.

VISMA | DataLøn

Genkend et sikkerhedsbrud, når du ser det

Både du selv og dine kolleger skal være i stand til at se, at der er sket et brud på persondata-sikkerheden. Det kræver, at I grundlæggende forstår, hvornår I har en personoplysning mellem hænderne (eller tasterne), og altså ved hvad en personoplysning er. Er du i tvivl, så kan du hente guiden:
Lær at spotte en personoplysning.

Typiske GDPR-sikkerhedsbrud

- En mail med persondata sendes til forkert modtager
- En pc bliver stjålet
- Virksomheden bliver hacket
- En computerskærm bliver ikke låst
- Der er indbrud i virksomheden
- Papirer med personoplysninger ryger i papirkurven frem for i makulatoren
- Persondata, der skulle krypteres, sendes ukrypteret

Omkring halvdelen af de anmeldelser, Datatilsynet får, handler om persondata, der er sendt til en forkert modtager.

Hjælp, der er sket et sikkerhedsbrud!

Råb straks op, hvis du opdager eller er ophavsmand til et sikkerhedsbrud, der involverer persondata. Det værste du kan gøre, er at stikke hovedet i busken. Ulykken skal stoppes, og så skal I bekende jeres synder. I første omgang betyder det, at sikkerhedsbruddet skal beskrives i den hændelseslog, som GDPR kræver, at I fører.

Alle medarbejdere, og i særdeleshed dem der kommer direkte i kontakt med persondata i deres arbejde, skal vide, hvem der fører loggen hos jer. De skal også vide, hvor hurtigt de skal reagere.

Hændelsesloggen er din ven

Hændelsesloggen er som en dagbog, I betror jer til. Her skal alle forkerte håndteringer af personoplysninger noteres, stort som småt. Og I skal til enhver tid kunne vise hændelsesloggen frem for Datatilsynet. Det giver ikke pluspoint at fejle, men hvis I har bekendt jeres synder i hændelsesloggen, vil tilgivelsen ofte være inden for rækkevidde.

Bekend og beskriv, hvad der er sket

I hændelsesloggen skal I beskrive sikkerhedsbruddet, gerne i korte men præcise træk: Hvornår skete det, hvad skete der (i hvilke systemer), hvem og hvis persondata var involveret i bruddet, hvad har I gjort for at stoppe ulykken og udbedre den skade, som bruddet har forvoldt?

Vurdér next step

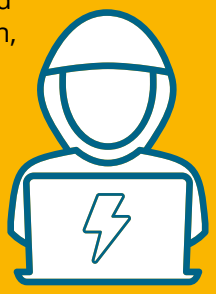
Når ulykken er stoppet, og I har overblik over situationen og skadens omfang, skal I vurdere tre ting:

1. Skal de, der har fået kompromitteret deres persondata, have besked?
2. Skal I anmelde sikkerhedsbruddet til Datatilsynet?
3. Bør I eventuelt ændre jeres forretningsgange, så I undgår et lignende uheld?

Next step afhænger af bruddets alvor og omfang. Og her skal I have flere parametre ind over i vurderingen: Hvilke persondata drejer det sig om? Hvor høj er risikoen for dem, der har fået deres persondata behandlet forkert? Er det så stort og graverende et brud, at Datatilsynet direkte skal orienteres, eller rækker det med hændelsesloggen?

Eksempel på risikovurdering:
Får I hacket persondata som for eksempel CPR-numre og kontonumre, er risikoen for at data vil blive misbrugt, høj. Hackere har sjældent reelle hensigter, og bruddet bør du anmelde til Datatilsynet.

Omvendt hvis du kommer til at sende en mail med CPR-numre til en forkert kollega. Så vil det typisk række med et notat i hændelsesloggen, da det ikke er sandsynligt, at en kollega har dårlige hensigter og for eksempel vil begive sig ud i identitetstyveri.



Husk, at det altid vil handle om at foretage en konkret vurdering.

Datatilsynets rolle

Som navnet antyder, skal Datatilsynet føre tilsyn. De kan både vælge at komme rigtig på besøg, og de kan vælge blot at udbede sig forskelligt materiale. Det vil altid inkludere hændelsesloggen, som I vil have 24 timer til at fremsende.

Når I oplever alvorlige brud på persondatasikkerheden og vurderer, at I skal anmelde det til Datatilsynet, skal I gøre det inden for 72 timer.

Vil du vide mere og have hjælp med virksomhedens GDPR-arbejde, kan du kontakte vores juridiske GDPR-specialister på 72 27 90 16.

Du kan finde aktuelle GDPR-webinarer på dataløn.dk/gdpr-webinar