Bech·Bruun

København. august 2019

Politik for notifikation af Datatilsynet

1. Indledning

Denne politik fastsætter de nærmere retningslinjer og interne procedurer for underretning af Datatilsynet ved sikkerhedsbrud.

Ved sikkerhedsbrud anmelder Fonden Climate Planet Foundation ("Fonden"), bruddet til Datatilsynet. Anmeldelsen skal ske uden unødig forsinkelse, og om muligt senest 72 timer efter at Fonden er blevet bekendt med bruddet. Forpligtelsen gælder ikke, hvis det er usandsynligt, at sikkerhedsbruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Formålet med pligten til at anmelde er at sikre transparens, og at Fonden reagerer, når der opstår et sikkerhedsbrud. En forudsætning for at overholde pligten er, at Fonden har procedurer på plads, så der kan ske anmeldelse, og så det er klart, hvad der skal anmeldes.

2. Hvornår gælder politikken

Ved konstatering af et sikkerhedsbrud skal pligten til at anmelde bruddet til Datatilsynet håndteres i overensstemmelse med denne politik.

3. Ansvarsfordeling

Det er besluttet, at Søren Poulsen, direktør, er overordnet ansvarlig for at håndtere sikkerhedsbrud, herunder anmeldelser til Datatilsynet. Hvis fx en medarbejder bliver opmærksom på et sikkerhedsbrud, eller hvis Fonden modtager oplysninger fra udefrakommende, der indikerer et sikkerhedsbrud, skal Søren Poulsen orienteres straks.

Da der er behov for at håndtere sikkerhedsbrud meget hurtigt, skal en underretning af Søren Poulsen ledsages af et telefonopkald eller en anmodning om at modtage bekræftelse på, at Søren Poulsen har set underretningen.

De skridt, der skal foretages i forbindelse med et muligt sikkerhedsbrud, er beskrevet i denne politik. Det er Søren Poulsen, der har det overordnede ansvar for, at de nødvendige oplysninger indhentes, og at vurderinger foretages i den forbindelse.

4. Hvornår er der tale om et sikkerhedsbrud

Det er tale om et sikkerhedsbrud, hvis en begivenhed 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 sikkerhedsbrud kan nævnes:

- Andre end den eller de personer hos Fonden, der er autoriseret til det, får adgang til personoplysninger
- Brud på en server eller manglende kryptering af en server, hvorved uvedkommende har fået adgang til personoplysninger
- Fondens bestyrelsesmedlemmer eller medarbejdere videregiver ubevidst eller bevidst personoplysninger til uvedkommende
- Personoplysninger er utilgængelige, fx på grund af en mistet krypteringsnøgle, strømsvigt eller denial of service-attack, og det indebærer en risiko for registreredes rettigheder eller frihedsrettigheder
- Fondens bestyrelsesmedlemmer eller medarbejdere ændrer eller sletter personoplysninger ved et uheld

5. Hvornår er Fonden "bekendt" med et sikkerhedsbrud

Pligten til at anmelde et sikkerhedsbrud til Datatilsynet indtræder, når Fonden er blevet bekendt med, at der er sket et sikkerhedsbrud.

Det kan fx være på baggrund af:

- Henvendelse fra en udefrakommende om, at vedkommende har modtaget oplysninger om en medarbejder eller borger/indskreven
- At en IT-leverandør opdager en mulig indtrængen, og en undersøgelse bekræfter dette
- At en hacker anmoder om løsesum for at frigive oplysninger fra IT-systemet

En simpel formodning om, at et sikkerhedsbrud har fundet sted, eller en simpel påvisning af en hændelse vil normalt ikke være tilstrækkeligt. En sådan simpel formodning kan dog føre til, at Fonden skal overveje behandlingssikkerheden.

6. Hvor hurtigt skal anmeldelsen til Datatilsynet ske

Fonden skal anmelde sikkerhedsbrud uden unødig forsinkelse. Det indebærer, at Fonden er forpligtet til at underrette Datatilsynet om sikkerhedsbruddet, så snart det er muligt – også, hvis dette tidspunkt indtræder før udløbet af de 72 timer.

Tidsgrænsen på de 72 timer for anmeldelsen af sikkerhedsbrud til Datatilsynet er ikke ubetinget, men foretages anmeldelsen ikke inden for de 72 timer, skal anmeldelsen ledsages af en begrundelse for forsinkelsen. Overskrides de 72 timer, skal det således være, fordi det ikke var muligt for Fonden at foretage anmeldelsen inden fristens udløb af særlige grunde, og Fonden skal nærmere redegøre for disse særlige grunde.

Der er mulighed for at komme med en trinvis anmeldelse til Datatilsynet, hvis der ikke inden for 72 timer er tilstrækkeligt overblik til at foretage en fuld anmeldelse.

Der kan også være behov for at opdatere anmeldelsen, hvis nærmere undersøgelser fx viser, at der alligevel ikke har været et sikkerhedsbrud, eller at sikkerhedsbruddet ikke har medført risiko for fysiske personers rettigheder eller frihedsrettigheder – eller hvis sikkerhedsbruddet viser sig at have haft større konsekvenser end først antaget.

7. Hvad skal anmeldelsen indeholde

Anmeldelsen skal beskrive karakteren af sikkerhedsbruddet i forhold til:

- Kategorierne af og det omtrentlige antal berørte registrerede
- Kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

Anmeldelsen skal beskrive de sandsynlige konsekvenser af sikkerhedsbruddet.

Anmeldelsen skal beskrive de foranstaltninger, som Fonden har truffet eller foreslår truffet for at håndtere sikkerhedsbruddet, herunder begrænsning af mulige skadevirkninger.

Andre relevante oplysninger kan fx være identiteten på en databehandler, hvis bruddet er sket hos databehandleren.

De ovenfor anførte oplysninger skal bidrage til, at Datatilsynet får mulighed for at følge og vurdere, om Fondens håndtering af sikkerhedsbruddet sker på en tilstrækkelig måde.

Datatilsynet kan også anvende oplysningerne ved vurderingen af, om der er behov for, at tilsynet intervenerer eller gør brug af sine korrigerende beføjelser til midlertidigt eller definitivt at begrænse eller forbyde videre behandling.

8. Hvornår behøver der ikke ske anmeldelse til Datatilsynet

Fonden kan efter en nærmere vurdering af sikkerhedsbruddet helt undlade at foretage anmeldelse, hvis det er usandsynligt, at sikkerhedsbruddet indebærer risiko for fysiske personers rettigheder eller frihedsrettigheder.

En undladelse kræver en høj grad af sikkerhed for, at denne betingelse er opfyldt. Det er Fonden, der har bevisbyrden for, at personoplysninger virkelig var beskyttet tilstrækkeligt.

Der kan fx være tale om, at uvedkommende har haft adgang til personoplysninger, som er lagret i krypteret form. Hvis det kan lægges til grund, at der er tale om en stærk

kryptering, som ikke kan brydes eller omgås inden for en tilstrækkelig lang årrække, kan det ud fra en konkret vurdering være usandsynligt, at der er risiko for fysiske personers rettigheder eller frihedsrettigheder.

9. Hvad gælder i forhold til databehandlere

Hvis en databehandler under Fonden bliver opmærksom på, at der er sket et sikkerhedsbrud, skal den pågældende uden unødig forsinkelse underrette Fonden herom.

Der er tale om en absolut regel, som databehandleren skal efterleve i alle tilfælde. Bestemmelsen giver ikke mulighed for, at databehandleren undlader at underrette om sikkerhedsbruddet med henvisning til, at databehandleren selv har vurderet, at det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.