

GDPR nyheder – grænseoverskridende databrud

Grænseoverskridende databrud - anmeld én gang, men oplys om brud i alle lande



Ved grænseoverskridende behandlinger af personoplysninger kan et brud på persondatasikkerheden indebære en risiko for personer i mere end ét EU-medlemsland.

En fransk virksomhed kan således behandle oplysninger ikke bare om fysiske personer i Frankrig, men også om personer, der befinder sig i andre EU-medlemslande.

Reglerne om anmeldelse af et brud på persondatasikkerheden er grundlæggende de samme, uanset om anmeldelsen skal ske i det ene eller andet EU-medlemsland.

Forordningens bestemmelser om hvilken tilsynsmyndighed i EU, der er kompetent til at behandle anmeldelsen, indebærer imidlertid, at den kompetente myndighed til at modtage og behandle anmeldelsen ikke nødvendigvis er dér, hvor den del af den dataansvarlige virksomhed, der er ansvarlig for bruddet, er beliggende.

Den kompetente myndighed er tilsynsmyndigheden i det land, hvor hovedvirksomheden ligger, eller det land, hvor den del af virksomheden, der træffer alle beslutninger om virksomhedens behandling af personoplysninger, er placeret.

Den kompetente tilsynsmyndighed kaldes for den ledende tilsynsmyndighed.

Det betyder, at når et brud på sikkerheden omhandler oplysninger om fysiske personer i mere end ét EU-medlemsland, vil den dataansvarlige skulle foretage anmeldelse til den ledende tilsynsmyndighed.

Dataansvarlige virksomheder med grænseoverskridende behandlinger bør derfor foretage en vurdering af, hvilken tilsynsmyndighed blandt EU's medlemslande, der er virksomhedens ledende tilsynsmyndighed. Dette bør noteres i virksomhedens beredskabsplan vedrørende brud, så virksomheden ikke skal bruge tid på at undersøge disse forhold i forbindelse med et brud.

Hvis den dataansvarlige ikke har nået at foretage denne vurdering, bør den underrette tilsynsmyndigheden i det land, hvor bruddet er sket.

Når den dataansvarlige anmelder et brud på persondatasikkerheden til den ledende tilsynsmyndighed, bør den samtidig orientere om, at bruddet omfatter etableringer i andre EU-medlemslande og i hvilke EU-medlemslande, der er fysiske personer, der er berørt af bruddet.

Når den ledende tilsynsmyndighed – det kan f.eks. være CNIL i Frankrig – har modtaget anmeldelsen, herunder oplysningerne om, at fysiske personer i andre EU-medlemslande er berørt af et brud på persondatasikkerheden, er det tilsynets ansvar at underrette de relevante tilsynsmyndigheder i de respektive medlemslande.

Eksempel:

En virksomhed med hovedvirksomhed i Frankrig tilbyder via sin hjemmeside onlinesalg af tøj.

Ved en fejl kommer virksomheden til på hjemmesiden – i forbindelse med en opdatering af siden – at offentliggøre en oversigt over virksomhedens kundedatabase. Oversigten indeholder kundernes fulde navn, ligesom der fremgår bl.a. betalings-, kontakt- og adresseoplysninger på kunderne.

Virksomheden har kunder i Frankrig, men en del af kunderne befinder sig også i andre EU-medlemslande, og ud fra den offentliggjorte oversigt kan virksomheden konstatere, at kunder bosat i henholdsvis Tyskland, Belgien og Holland har været berørt af lækagen.

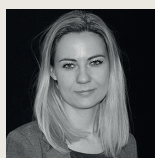
Virksomheden vurderer, at dette brud på persondatasikkerheden skal anmeldes, og den foretager derfor en anmeldelse til CNIL.

I anmeldelsen markeres, at personer i de ovenfor angivne EU-medlemslande har været berørt.

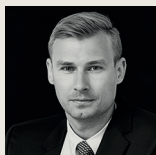
CNIL skal herefter underrette tilsynsmyndighederne i Tyskland, Belgien og Holland.



Henrik Christian Strand



Pernille Kristensen



Michael Gravesen



Bianca Britt Nielsen

Skal vi hjælpe dig?

Hvis du oplever brud på persondatasikkerheden, er vores specialister klar til at hjælpe med at anmelde bruddet til den relevante tilsynsmyndighed.