Bøder efter de nye databeskyttelsesregler

Det er efterhånden et stykke tid siden, at den nye databeskyttelsesforordning trådte i kraft. Hidtil har det danske Datatilsyn kun udstedt ganske få bøder for overtrædelse af det gamle regelsæt, og bøderne har maksimalt lydt på 25.000 kr. Efter de nye databeskyttelsesregler kan overtrædelse heraf medføre bøder på op til 20 mio. euro eller fire pct. af den overtrædende virksomheds samlede globale årlige omsætning – alt efter hvilket beløb der er højest.

Der er endnu ikke udstedt bøder efter det nye regelsæt herhjemme, men dette ændrer sig formentlig meget snart. Mens vi venter på de første danske bøder, er der i udlandet så småt begyndt at blive udstedt bøder efter persondataforordningens regelsæt. Der kan spores en tendens i retning af et højere bødeniveau end hidtil set.

Maksimale bøder udstedt efter det tidligere regelsæt

Det engelske datatilsyn, Information Commissioner's Office (ICO), udstedte i efteråret 2018 en bøde til en global koncern, Equifax Ltd, for ikke at formå at beskytte personoplysninger for op imod 15 millioner UK-statsborgere (globalt blev 146 millioner ramt) under et cyberangreb i 2017. Bøden lød på 500.000 GBP, hvilket er den højeste bøde, som kunne tildeles efter det gamle regelsæt.

Bødeniveauet blev fastsat efter tilsvarende kriterier, som skal anvendes efter persondataforordningen, særligt med fokus på antallet af ofre, typen af de lækkede personoplysninger, samt manglende efterlevelse af egne politikker og kontroller og af de grundlæggende principper om blandt andet dataminimering. Det må derfor forventes, at en tilsvarende sag, efter ikrafttrædelsen af persondataforordningen, vil resultere i en markant højere bøde.

Tilsvarende blev Facebook i efteråret 2018 tildelt en bøde af ICO lydende på de maksimale 500.000 GBP efter det tidligere regelsæt. Elizabeth Denham, kommissær hos ICO, udtalte i den forbindelse, at såfremt bøden havde været udstedt efter de nye persondataretlige regler, så havde den været betydeligt større. Det var således alene på grund af begrænsningen på 500.000 GBP, at bøden ikke blev større. Dette må ses som en klar indikation på, at tilsynsmyndighederne er parate til at gøre brug af muligheden for at udstede væsentlig større bøder efter persondataforordningens ikrafttræden.

Der skal ikke meget til

Der skal mindre til, end de fleste tror, før bødehammeren falder. ICO har efter det tidligere regelsæt udstedt en bøde til Heathrow Airport lydende på 120.000 GBP, fordi Heathrow Airport havde mistet et ukrypteret USB-stik, hvorpå de opbevarede større mængder personoplysninger. Dette viser, at der ikke nødvendigvis skal meget til, før en overtrædelse af databeskyttelseslovgivningen medfører en bødestraf. Virksomheder bør derfor prioritere at få styr på sin persondata-compliance for at undgå bøder.

Bøder udstedt i udlandet efter persondataforordningen

Det portugisiske datatilsyn har efter persondataforordningen tildelt et portugisisk hospital en bøde på 400.000 euro for overtrædelse af principperne om fortrolighed, integritet og dataminimering. På trods af, at bøden blev pålagt et offentligt hospital, er der tale om overtrædelse af principper, som gælder for både offentlige og private virksomheders håndtering af persondata.

I Tyskland har et datatilsyn (LfDI) tildelt en bøde på 20.000 euro til virksomheden Knuddles, som havde forsømt at kryptere sine brugeres adgangskoder til virksomhedens datingsite. Den relativt lave bøde blev udmålt under hensyntagen til den høje grad af samarbejdsvillighed, som blev udvist af virksomheden – særligt kan det nævnes, at virksomheden selv havde henvendt sig til tilsynet efter hackerangrebet og det deraf følgende læk af ukrypterede adgangskoder.

Seneste nyt

Den franske tilsynsmyndighed, Commission Nationale de l'Informatique et des Libertés (CNIL), har netop udstedt en bøde på 50 mio. euro til Google LLC for manglende overholdelse af persondataretten. Bøden, som er den første CNIL udsteder efter det nye regelsæt, er udstedt på baggrund af to brud på overholdelse af persondataforordningen.

Det ene brud består i, at Google LLC ikke overholder kravet om gennemsigtighed eller giver tilstrækkelige oplysninger til brugerne og Google LLC's brug af persondata. Dette begrunder CNIL bl.a. med, at de oplysninger, der gives, ikke er let tilgængelige, idet de unødvendigt er delt ud over flere dokumenter. Et andet argument fra CNIL's side af er, at de beskrevne formål med behandlingen og kategorierne af behandlet persondata er for uklare.

Det andet brud består i, at Google LLC mangler hjemmel til at målrette reklamer, da samtykket som brugeren giver, ikke er tilstrækkeligt oplyst, samt at det ikke er tilstrækkeligt specifikt og utvetydigt. Størrelsen på bøden skyldes alvoren af bruddene på de grundlæggende principper i persondataforordningen; gennemsigtighed, oplysning og samtykke, samt at bruddene er sket løbende over tid, samt fortsat sker på tidspunktet for bødens udstedelse.

Ingen administrative bøder fra det danske Datatilsyn

Efter ovenstående betragtninger skal der dog gøres opmærksom på, at det danske Datatilsyn ikke kan udstede administrative bøder. Det kræves altså, at sagen overgives til politiet eller anklagemyndigheden, før der kan udstedes en bøde. På trods af dette forhold må der dog stadig forventes en harmonisering på området mellem EU-landene, hvilket alt andet lige må betyde langt højere og hyppigere bøder for overtrædelser af persondatalovgivningen end hidtil set i Danmark.

NIS PETER DALL
ADVOKAT (L), PARTNER

(+45) 77 40 10 18
NPD@NJORDLAW.COM