



1 år med GDPR: En god idé, men ikke gratis

Orientering fra Faglig udviklingsafdeling

Datatilsynet markerede 1-årsdagen for GDPR med en nyhed om afgørelse om PFA Pension, hvor der udtales kritik. Praksis er siden 25. maj 2018 dannet ved Datatilsynets vejledninger, ligesom Datatilsynet har udtalt kritik, og der er faldet bøder. I mange virksomheder har man løbet ualmindeligt stærkt for at følge med og blive klar. Vi kigger her nærmere på, hvorfor afgørelsen om PFA Pension ikke endte med bøde, men kun kritik og samler op på interessante erfaringer fra det første år med GDPR.

Mange bække små: 66 brud på persondatasikkerheden

I starten af februar 2019 havde PFA Pension anmeldt 66 brud på persondatasikkerheden. Det er helt i tråd med et af forordningens nye principper, nemlig anmeldelsespligten. Så langt, så godt. Når der bliver anmeldt brud på persondatasikkerheden, er det op til Datatilsynet at beslutte, om der skal følges yderligere op. Og det valgte man at gøre i PFA Pensions tilfælde.

62 af bruddene vedrører vedhæftning af forkerte dokumenter eller fremsendelse af dokumenter til forkert modtager. Det er repræsentativt for typen af brud, som er mest almindelig, læs mere om det [her](#). Det vil sige, at de enkelte brud typisk vedrører blot en enkelt person, dvs. det samlede antal berørte personer er ikke voldsomt højt. PFA Pension og Datatilsynet er dog enige om, at antallet af brud er for højt, og PFA Pension var da også på eget initiativ gået i gang med en række mindre tekniske og organisatoriske foranstaltninger for at øge sikkerhedsniveauet.

Sagen ender som nævnt i en kritik, som er Datatilsynets mildeste sanktionsform. Datatilsynet vælger tilsyneladende at statuere et eksempel og derved skabe opmærksomhed om, at denne form for brud ikke er acceptable, selvom de ikke er i den mest alvorlige ende af skalaen, samt at enkle forbedringer ofte er nok til at undgå dem.

Hvad udløser bøder?

I den alvorlige ende af skalaen har Datatilsynet indstillet i hvert fald 2 bøder: Den første på 1,2 mio. kr. til Taxa 4x35 fra marts måned og den seneste fra juni på 1,5 mio. kr. til IDesign. Vi har tidligere beskrevet [Taxa 4x35 afgørelsen](#), som begrundes med, at taxaselskabet havde gemt næsten 9 millioner personhenførbare taxature i op til fem år og uden nogen god grund. Bøden til IDesign begrundes med, at virksomheden ikke har overholdt databeskyttelsesforordningens krav om sletning. IDesign har således behandlet oplysninger om ca. 385.000 kunders navn, adresse, telefonnummer, e-mail og købhistorik i længere tid end nødvendigt. I praksis har IDesign aldrig slettet data fra systemet, og man havde heller ikke formuleret slettefrister for persondata. Læs evt. mere om sagen hos [Datatilsynet](#).

I begge sager har Datatilsynet desuden udtalt alvorlig kritik.

Ønske om tilbageholdenhed på bøder

Både ITB og DI har budt GDPR velkommen, bl.a. fordi det er en forudsætning for at skabe et velfungerende digitalt indre marked i EU. Denne positive indstilling ændrer dog ikke noget ved, at man gerne ser, at de store bøder bliver nedtonet til fordel for mere rådgivning, så virksomhederne kommer lettere og billigere i mål med deres GDPR. Birgitte Hass, som er adm. direktør i ITB, udtaler:

"Naturligvis skal banditterne kunne straffes, men at give store bøder for små fodfejl er ikke den rigtige vej at gå. Her burde fokus i stedet ligge på vejledning og hjælp"

Store GDPR-omkostninger i it-branchen, både nu og fremover

GDPR's 1-årsfødselsdag har givet flere erhvervsorganisationer anledning til at samle op på medlemmernes, altså danske virksomheders, erfaringer. IT Brancheforeningen, ITB, har lavet en [undersøgelse](#) blandt 159 af deres medlemmer.

Undersøgelsen viser, at 88% af branchen nåede at blive klar inden fristen. Det har krævet en ekstra indsats, som vurderes at have kostet 4.374 kr. pr. medarbejder. Virksomhederne vurderer, at det er en omkostning, der til en vis grad er kommet for at blive, og gennemsnitligt regner man med, at det årligt vil koste 3.253 kr. pr. medarbejder fremover. Det er ITB's vurdering, at bødefrygt og usikkerhed om reglerne har ført til en vis overimplementering og dermed gjort omkostningsniveauet unødigt højt.

Det er ikke for sent: God guide fra EU

Der er ingen grund til at fortvivle, hvis man endnu ikke er på plads med GDPR: det er bedre at komme sent i mål end at blive liggende på ruten. For den absolutte nybegynder har EU lavet en meget overskuelig video om GDPR, den kan du se [her](#).

Der er også god hjælp at hente i Beierholms række af [artikler](#) eller på [Datatilsynets hjemmeside](#).

Læs mere om EU's databeskyttelsesforordning på vores hjemmeside via dette LINK.

Tilmeld en kollega til Beierholms nyhedsmail via dette LINK