Sen varsling av databrudd til Datatilsynet ga overtredelsesgebyr på 2,5 millioner

Petter Bjerke
Partner, Faggruppeleder personvern og immaterialrett

William Myhr
Advokatfullmektig

Plikten til å varsle om databrudd (personopplysningssikkerheten) og eventuelt berørte er en sentral plikt i henhold til GDPR.

Vi har nå fått en av de første sakene i Norge som går på gebyr for unnlatelse av å ikke melde fra i tide.

Leverandøren av medisinsk utstyr, Argon Medical Devices, Inc. meldte ifra om databrudd 67 dager etter at de ble klar over et databrudd. GDPR pålegger virksomheter å melde ifra til tilsynsmyndigheter innen 72 timer etter virksomheten ble klar over databruddet. Datatilsynet mente at Argon Medical Devices, Inc. meldte ifra alt for sent og ga virksomheten et overtredelsesgebyr på 2,5 millioner.

Sakens bakgrunn

24. september 2021 sendte Argon Medical Devices, Inc. avviksmelding til Datatilsynet om at de i perioden 21. mai 2021 til 14. juni 2021 hadde blitt utsatt for et cyber-angrep. Hendelsen medførte at angriperen fikk uautorisert tilgang til personopplysninger til alle ansatte i Europa, herunder en norsk ansatt.

Sikkerhetshendelsen ble først oppdaget 14. juni 2021, og en intern etterforskning ble iverksatt. I begynnelsen av den interne etterforskningen var hovedfokuset på selskapets virksomhet i USA. Den 19. juli 2021 ble imidlertid selskapet klar over at bruddet også involverte europeiske ansatte.

Argon Medical Devices, Inc. foretok derfor en vurdering av om databruddet var meldepliktig og kom til at bruddet måtte meldes inn. Datatilsynet mottok imidlertid avviksmelding først 24. september 2021.

Datatilsynets syn på saken

Da Datatilsynet mottok avviksmeldingen, etterspurte tilsynet mer informasjon om hva selskapet gjorde av tiltak mellom 19. juli 2021 og til Datatilsynet mottok avviksmelding 21. september 2021. Til dette svarte Argon Medical Devices, Inc. at de under denne perioden drev intern etterforskning. Argon Medical Devices, Inc. anførte at de først fikk fullstendig oversikt da de meldte inn databruddet til Datatilsynet og at de derfor hadde opptrådt innenfor 72-timers fristen som gjelder for meldepliktige databrudd.

Datatilsynet var uenige i dette og mente at 72-timers fristen begynner å løpe når virksomheten blir klar over at det har skjedd et brudd, og ikke når virksomheten har den fulle oversikten over bruddet.

Datatilsynet mente derfor at virksomheten hadde brutt 72-timers fristen og ga et overtredelsesgebyr på 2,5 millioner kroner. I skjerpende retning vektla Datatilsynet at virksomheten ikke hadde gitt presis nok informasjon i sin korrespondanse med Datatilsynet og at det kun var en oppmerksom undersøkelse av avviksmeldingen fra tilsynets side som avdekket at 72-timers fristen var brutt. Videre vektla tilsynet at personopplysningene som var blitt utsatt, som lønn- og stønadsopplysninger, var av en sensitiv karakter.

Avgjørelsen kan leses i sin helhet her.

Hva kan man lære av avgjørelsen?

Avgjørelsen fra Datatilsynet viser viktigheten av å håndtere databrudd på en god måte.

For det første må virksomheter ha gode rutiner på å oppdage databrudd og hvordan databrudd skal varsles. I Argon Medical Devices, Inc. rutiner var det nedfelt at databrudd kun skulle varsles når selskapet hadde den fulle oversikten. Etter GDPR og Datatilsynets vurdering var ikke dette riktig.

For det andre er avgjørelsen en viktig påminner om at databrudd skal varsles senest 72 timer etter at virksomheten har fått kjennskap til databruddet. Om virksomheten ikke har den fulle oversikten innen fristen, må det varsles løpende etter hvert som virksomheten får mer informasjon.

For det tredje viser avgjørelsen at virksomheter som er etablert utenfor EØS må være ekstra oppmerksomme på om også EU-borgere er rammet av databruddet. Om fokuset kun er nasjonalt, for eksempel amerikanske lover og regler, kan 72-timers fristen raskt overskrides.