Klager resulterer ikke altid i medhold

Det er ikke alle klager til Datatilsynet, der resulterer i, at klager (den registrerede) får ret. Senest har Datatilsynet vurderet, at den registrerede ikke skulle have medhold i sin klage i en konkret sag om kryptering af e-mails hos Lowell Danmark A/S, da virksomheden efter Datatilsynets vurdering havde foretaget en risikovurdering, hvor fremgangsmåden omkring kryptering af e-mails blev vurderet som en passende sikkerhedsforanstaltning.

Baggrund

Datatilsynet meddelte i 2018, at private virksomheder fra 1. januar 2019 skulle kryptere e-mails , der indeholder fortrolige eller følsomme persondata. På baggrund af dette har en registreret klaget til Datatilsynet to gange i januar 2019 over Lowell Danmark A/S' behandling af oplysninger om vedkommende.

Læs mere om kryptering af e-mails
Virksomheden havde sendt oplysninger om skyldige restancer til klagers e-mailadresse. Ved afsendelsen af disse e-mails anvendte virksomheden en TLS 1.2-kryptering baseret på algoritmen AES256. Denne "opportunistisk TLS-kryptering" sikrer, at e-mails sendes krypteret under transporten til modtageren, hvis det understøttes af modtagerens e-mailklient, men hvis det ikke understøttes, sendes e-mails ukrypteret.

Virksomheden havde foretaget en risikovurdering i forhold til kryptering af e-mails i medfør af Databeskyttelsesforordningens art. 32 og fulgt denne. I risikovurderingen var der bl.a. lagt vægt på, at der anvendes sagsnumre i de pågældende e-mails, hvilket er en pseudonymisering af persondata, og at risikoen for, at oplysningerne kommer til uvedkommendes kendskab, er lav. Desuden blev der lagt vægt på, at de fleste e-mailklientversioner og tjenesteudbydere i dag kan modtage TLS 1.2-krypteringen.

Datatilsynets afgørelse

Sagen er afgjort på baggrund af Databeskyttelsesforordningens art. 32, stk. 1, hvoraf det fremgår, at den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til identificerede risici ved behandlingen af persondata.

Datatilsynet fandt, at virksomhedens behandling af persondata var i overensstemmelse med databeskyttelsesforordningens art. 32, stk. 1, bl.a. på baggrund af risikovurderingen, den anvendte kryptering, samt at klagers e-mailklient understøttede krypteringsformen, hvilket betød, at de to e-mails havde været krypteret gennem transportlaget.

Datatilsynets generelle bemærkninger

I forbindelse med afgørelsen i sagen udtaler Datatilsynet, at når der sendes fortrolige og/eller følsomme persondata, bør den dataansvarlige anvendes tvungen TLS og som minimum i version 1.2. Det er dog efter Datatilsynets opfattelse ikke i sig selv i strid med Databeskyttelsesforordningens art. 32, stk. 1, at anvende en "opportunistisk TLS-kryptering", hvis den dataansvarlige, efter en risikovurdering, har vurderet, at "opportunistisk TLS" er en passende sikkerhedsforanstaltning.

Derudover udtaler Datatilsynet, at en risikovurdering ikke kan tage udgangspunkt i, hvad en registreret eventuelt har givet tilladelse til, idet en sådan accept ikke kan sidestilles med, hvilket sikkerhedsniveau der er passende. Man kan som virksomhed med andre ord ikke samtykke sig ud af sikkerhedsniveauet.

Afgørelsen fra Datatilsynet viser, hvor vigtigt det er at foretage og dokumentere risikovurderinger, samt at have styr på sin kryptering af e-mails og undervisning af medarbejdere i, hvornår kryptering og ekstra kryptering evt. skal anvendes.

NIS PETER DALL
ADVOKAT (L), PARTNER

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

PERNILLE KIRK ØSTERGAARD
ADVOKAT, SENIORSPECIALIST

(+45) 77 40 11 74
POS@NJORDLAW.COM