Kryptering af e-mails til GDPR

Databeskyttelsesforordningen, som trådte i kraft den 25. maj 2018, medførte en skærpelse af kravene til virksomheders behandling af personoplysninger.

En problemstilling, som særligt gav vanskeligheder, var spørgsmålet om videregivelse af personoplysninger elektronisk, primært ved brug af mails.

Datatilsynet fastslog hurtigt efter forordningens ikrafttræden, at personfølsomme eller fortrolige oplysninger alene kunne videregives ved brug af krypteret mails. Udveksling af mails med personfølsomme eller fortrolige oplysninger mellem virksomheder og til det offentlige kan i praksis ske ved brug af medarbejdersignaturer via NemID. Dette er en sikker løsning, som medfører en høj grad af beskyttelse.

Det er imidlertid ikke alle, der kan modtage mails, som er krypteret ved medarbejdersignaturer, og særligt private modtagere kan ikke benytte denne løsning.

Der er også andre krypteringsløsninger på markedet, men der er imidlertid mange, særligt gratis mailudbydere, som heller ikke kan modtage krypterede mails via andre krypteringsløsninger.

Mange mails sendes dog automatisk med TLS-kryptering, men man kan ikke være sikker på, at mailen er TLS-krypteret, hvis modtagermailen ikke understøtter TLS.

Datatilsynets afgørelse
Datatilsynet har den 26. juni 2019 truffet afgørelse i en sag, hvor en virksomhed havde fremsendt fortrolige oplysninger uden kryptering. Virksomheden havde benyttet TLS-kryptering med en indstilling, hvor mailen blev leveret krypteret hos modtageren, hvis modtagerens mail understøttede kryptering. Hvis modtagerens mail ikke understøttede kryptering, blev mailen afleveret ukrypteret.

Datatilsynet fastslog bl.a., at det ikke i sig selv var i strid med Databeskyttelsesforordningen, om en virksomhed benyttede en kryptering af mails, som var afhængig af modtagerens mailsystem/tjenesteudbyder. Virksomheden havde dog pligt til at foretage en behørig risikovurdering og overveje, om opsætningen af kryptering udgjorde en passende sikkerhedsforanstaltning.

Drachmanns råd
Afgørelsen fra Datatilsynet fastslår, i tråd med tidligere afgørelser, at virksomhedens risikovurdering er meget vigtigt ved vurderingen af, om virksomheden overholder Databeskyttelsesforordningen. Det er derfor en rigtig god ide at sikre, at virksomheden i sin risikovurdering tager stilling til:

- Hvad kan gå galt
- Hvornår kan det gå galt
- Hvor stor er risikoen for, at det går galt
- Er risikoen for, at det går galt proportional med foranstaltningen

Spørgsmål kan rettes til
Advokat (L), partner
Sissel Egede-Pedersen
sep@drachmann.com