Kryptering af e-mails

Datatilsynet udgav i sommeren 2018 en nyhed, hvor de varslede skærpet praksis i forhold til transmission af personoplysninger med e-mail via internettet.

Beskeden lød: "*Fremadrettet vil det således være Datatilsynets opfattelse, at det normalt vil være en passende sikkerhedsforanstaltning – for både offentlige og private aktører – at anvende kryptering ved transmission af fortrolige og følsomme personoplysninger med e-mail via internettet*".

Kryptering er imidlertid ikke i sig selv et krav. Kravet består i, at data transmitteres fra et sted til et andet på en tilpas sikker måde i forhold til den risikovurdering, man har foretaget på transmissionen. Den vurdering hænger i høj grad sammen med, hvilken type data vi sender og ikke mindst i hvilken mængde/størrelsesorden.

Der er ingen tvivl om, at det for mange virksomheder vil være nemmest (og mest hensigtsmæssigt) at sætte fuld kryptering op, men virkeligheden er en anden for jer.

Herunder kommer vi med et bud på, hvordan I via andre metoder og alternativer kan opnå en sikker transmission af følsomme og fortrolige personoplysninger uden de vilde IT-tekniske færdigheder og ikke mindst økonomi.

1. Altid en konkret vurdering

I skal altid tage udgangspunkt i en konkret vurdering af de oplysninger, I sender. Langt hen ad vejen har I måske mulighed for at vurdere på et overordnet niveau, ex. på typer af afsendelser, men hvis ikke må I lave en vurdering fra udsendelse til udsendelse.

Spørg jer selv:

- Hvilken data har vi med at gøre?
- Hvilke data sender vi og hvor følsomme/fortrolige er de?
  (Husk: Vi snakker kun om følsomme og fortrolige personoplysninger i forhold til kryptering).
- Hvor mange data sender vi?
- Hvor hyppigt?
- Kunne vi sende/overføre samme data med andet end mail?
  Og vigtigst:
- Hvad siger vores risikovurdering?

2. Risikobaseret tilgang

For at kunne vurdere risikoen forbundet med transmissionen af de konkrete oplysninger skal I stille jer selv ovenstående spørgsmål, som vil hjælpe jer med at stilling til, hvor meget sikkerhed der skal kobles på afsendelsen.
Når vi snakker risikovurdering, er det altid i forhold til den registrerede, altså: Hvilken konsekvens ville det have for den registrerede (typisk spejderen/den frivillige), at de oplysninger vi sender ender i de forkertes hænder?
Når I har vurderet den risiko, kan I også nemmere vurdere, hvilken type kryptering/anden sikkerhed I vil lægge på afsendelsen.
I mange af de tilfælde I sidder med vil det altså være rigeligt eksempelvis at sætte password på et Word-dokument inden det sendes.

3. Tekniske vs. organisatoriske foranstaltninger

Datatilsynet uddyber på deres hjemmeside hvilke muligheder der er for at opsætte tekniske foranstaltninger og fokuserer på især to typer af krypteringer: Kryptering på transportlaget og end-to-end kryptering. Datatilsynet kommer selv med en uddybende forklaring på de to typer kryptering på deres hjemmeside her.

Det vil imidlertid også være ok at imødekomme kravet gennem organisatoriske foranstaltninger. Dette forudsætter dog en tydelig instruks, ex. fra bestyrelse til ledere og opfølgning på om instruksen bliver fulgt gennem kontrol, ex. stikprøver. Dette er ikke anderledes end for andre organisatoriske foranstaltninger, I måtte have implementeret under jeres tidligere GDPR-arbejde.

4. Alternativer til kryptering

Så længe sikkerheden omkring transmissionen af personoplysningerne er på plads, kan vi sagtens finde alternativer til de tekniske foranstaltninger.

Overvej om følgende kunne give en tilstrækkelig sikkerhed (set i forhold til pkt. 1 og 2):

- Sæt en lås på dokumentet med følsomme/fortrolige oplysninger inden det sendes ud. Koden formidles ex. over telefon eller pr. SMS.
- Kan der linkes ind til dokumentet, som ligger på en platform beskyttet af password og evt. rettighedsstyring?
- Kan oplysningerne overbringes på andre (og sikrere) måder end pr. mail?
- Andet: Brug jeres fantasi 😊

5. Tænk jer om

- Husk at I har ansvaret for de mails og oplysninger, I sender ud og derfor også ansvaret for om oplysningerne er tilstrækkeligt sikret.
- Lav overordnede vurderinger hvor det er muligt og ellers fra udsendelse til udsendelse.
- *Hav en risikobaseret tilgang når I nedfælder jeres retningslinjer for udsendelse af følsomme og fortrolige oplysninger. Og hav ikke mindst den registreredes rettigheder for øje.*
- Sørg for at ingen er i tvivl om de retningslinjer I har vedtaget.
- Følg op på om jeres retningslinjer overholdes.