Har du styr på din kryptering af e-mails fra 1. januar 2019?

Datatilsynet skærper sin praksis fra 1. januar 2019, og det betyder i realiteten, at alle arbejdsmails, der indeholder følsomme eller fortrolige personoplysninger, skal krypteres. Krypteringskravet er en praktisk minimumsstandard for sikkerhedskravet til behandling af personoplysninger som følge af GDPR. Kravet rammer især den private sektor, da offentlige myndigheder allerede er omfattet af tilsvarende krav.

I løbet af de næste måneder skal virksomheder, foreninger, fonde og andre ikke-offentlige dataansvarlige implementere kryptering af mails, som indeholder følsomme og/eller fortrolige oplysninger. Formålet er at højne sikkerheden for behandling af personoplysninger ifølge databeskyttelsesloven og GDPR. Krypteringen skal gøre det mere besværligt for hackere og andre at få adgang til indholdet af mails, der ikke vedkommer dem. Det er en skærpelse af Datatilsynets tidligere praksis, som alene anbefalede kryptering.

Krypteringskravet forventes at påvirke rigtig mange i den private sektor, fordi langt de fleste virksomheder ikke anvender krypteringsløsninger i forbindelse med e-mails i dag. For eksempel vil HR-afdelinger, sundhedsklinikker, långivervirksomhed og fonde med uddeling til privatpersoner blive påvirket af det nye krav.

Men hvad ligger der i krypteringskravet?

Hvilke personoplysninger kræver kryptering?

Det er alene mails, der indeholder følsomme eller fortrolige personoplysninger, der skal krypteres.

Følsomme personoplysninger er et begreb, der stammer direkte fra GDPR og omfatter oplysninger om:

- Race og etnisk oprindelse
- Politiske holdninger
- Religiøs eller filosofisk overbevisning
- Medlemskab i en fagforening
- Alkoholmisbrug
- Seksualitet

Fortrolige personoplysninger er ikke defineret direkte i GDPR, hvilket gør begrebet til en ren dansk fortolkning. Datatilsynet har meldt ud, at i hvert fald følgende oplysninger er fortrolige:

- CPR-numre
- Oplysninger, som er omfattet af en lovbestemt tavshedspligt

Andre oplysninger kan efter omstændighederne også være fortrolige. Datatilsynet har i den forbindelse oplyst, at der må lægges vægt på den almindelige opfattelse af, om en oplysning skal beskyttes. I praksis kan det være vanskeligt at foretage denne vurdering – specielt hvis vurderingen ikke er understøttet af principper eller interne retningslinjer hos private dataansvarlige. Uden dette, vil medarbejderne selv skulle foretage vurderingen.

Vi anbefaler for den enkelte virksomhed en generel stillingtagen til krypteringskravet. I vurderingen kan der med fordel tages udgangspunkt i den registreredes situation.

Tre eksempler på, hvad der i praksis vil være underlagt krypteringskravet:

- Kopi af pas, kørekort og sygesikringsbevis
- Gældsforhold
- Kontooplysninger

Hvilken kryptering kræves?

Der findes mange forskellige typer af kryptering, men Datatilsynet har udmeldt, at den private sektor som minimum skal have såkaldt "TLS"-kryptering, hvilket står for Transport Layer Security. I skrivende stund er minimumskravet TLS version 1.2, som er den næst-nyeste version.

TLS har dog den svaghed, at det ofte kun er transporten mellem dig og din/jeres mailserver, der krypteres. Når mailen skal fra mailserveren til modtageren, er den ikke altid krypteret. Det er derfor vigtigt at indstille TLS krypteringen korrekt, så hele transporten er sikret.

På baggrund af flere henvendelser om krypteringskravet, offentliggjorde Datatilsynet den 20. september en beskrivelse af nogle af de tekniske aspekter af krypteringskravet. Du kan læse beskrivelsen her.

Fordi der er tale om en minimumsgrænse, vil TLS 1.2 ikke per definition være tilstrækkelig. GDPR stiller krav om, at jo større sikkerhedsrisiko, der er for den registrerede, desto større sikkerhed skal man implementere. Mere sikre former for kryptering kan derfor blive relevant, herunder eksempelvis "end-to-end" kryptering, som betyder, at modtageren skal have en dekrypteringsnøgle for at kunne låse mailen op.

Det kan være en besværlig omgang og andre løsninger kan med fordel tænkes ind i disse situationer, for eksempel at lade modtageren hente beskeder via en platform, hvor der kræves sikkert login, som alternativ til mail.

Det bør ligeledes indgå i vurderingen af behovet for kryptering, at det ikke kun er mails som sendes, der skal krypteres. Hvis man anmoder om, eller må forvente at modtage fortrolige eller følsomme oplysninger pr. mail, skal man også stille en mulighed til rådighed, der gør det muligt at modtage mails krypteret.

Hvordan kommer jeg videre?

I kan med fordel gribe krypteringskravet an på følgende måde:

1. Find ud af, hvilke personoplysninger der behandles via mailsystemet.
2. Undersøg, om behandlingen omfatter følsomme oplysninger, som de er defineret i GDPR eller oplysninger, som må forventes at blive opfattet som fortrolige af de registrerede.
3. Vil I fortsætte med behandling af følsomme og/eller fortrolige personoplysninger via mails, skal der etableres en kryptering, der som minimum lever op til TLS version 1.2. Spørg din IT-leverandør.
4. Hvis I har flere medarbejdere, der skal håndtere mails, anbefaler vi at udarbejde retningslinjer, som gør det muligt for medarbejderne at navigere sikkert i det daglige arbejde. Spørg os.

Vil du vide mere?

Hvis du har nogen spørgsmål til kryptering af e-mails, er du velkommen til at kontakte NJORDS persondatateam.

NJORDs persondatateam har betydelig erfaring med den komplicerede lovgivning inden for persondata og omfattende ekspertise i at samarbejde på tværs af alle juridiske discipliner og på tværs af landegrænser.

Vi yder rådgivning til offentlige myndigheder og til private virksomheder med en kommerciel tilgang til håndtering af persondataretlige problemstillinger. Du kan læse om vores GDPR-produkter her.