JUSTITSMINISTERIET

Folketinget
Social-, Indenrigs- og Børneudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 22. marts 2018
Kontor: Databeskyttelseskontoret
Sagsbeh: Mia Schumacher
Sagsnr.: 2018-0032/42-0053
Dok.: 676762

Hermed sendes besvarelse af spørgsmål nr. 283 (Alm. del), som Folketingets Social-, Indenrigs- og Børneudvalg har stillet til justitsministeren den 2. marts 2018. Spørgsmålet er stillet efter ønske fra ikkemedlem af udvalget (MFU) René Gade (ALT).

Søren Pape Poulsen

/

Jakob Lundsager

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 283 (Alm. del) fra Folketingets Social-, Indenrigs- og Børneudvalg:

> "Vil ministeren oplyse, hvem der har ansvaret for, at krypterede e-mails fra borgere og virksomheder forbliver krypterede, som Datatilsynet foreskriver det, når de modtages af offentlige institutioner, og vil ministeren oplyse, hvordan ministeren vil håndtere problemstillingen med, at offentlige institutioners mailsystemer ikke er krypterede, og de dermed bryder persondataloven?"

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Datatilsynet, hvortil jeg henholder mig:

> "Datatilsynet forstår spørgsmålet således, at der spørges til, hvem der har ansvaret for, at e-mails sendt i krypteret form fra borgere og virksomheder, også forbliver krypterede, efter at de er modtaget i en offentlig institutions mailsystem, og dermed også er krypterede, så længe de er lagret i eller på anden vis behandles i en offentlig institutions mailsystem.
>
> Persondataloven indeholder en række bestemmelser om såkaldt behandlingssikkerhed, det vil sige krav til, hvordan personoplysninger skal beskyttes mod uvedkommendes adgang, misbrug eller anden behandling i strid med loven.
>
> Generelt gælder det, at dataansvarlige og databehandlere skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven, jf. lovens § 41, stk. 3.
>
> Justitsministeriet har endvidere i medfør af persondatalovens § 41, stk. 5, udstedt bl.a. en bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles af den offentlige forvaltning (sikkerhedsbekendtgørelsen). Datatilsynet har endvidere udarbejdet en vejledning, som knytter sig til den oprindelige bekendtgørelse (sikkerhedsvejledningen).
>
> Af bekendtgørelsens § 14 fremgår det, at der kun må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger. Det fremgår af sikkerhedsvejledningen hertil bl.a., at "De særlige sikkerhedsfor-

anstaltninger skal træffes efter myndighedens vurdering af sikkerhedsrisici i det konkrete tilfælde, herunder med hensyntagen til karakteren af de omhandlede oplysninger. For at kunne fastlægge sikkerhedsniveauet er det nødvendigt, at den dataansvarlige foretager en samlet risikovurdering, som omfatter alle elementer i kommunikationsforbindelsen."

I Datatilsynets praksis og i sikkerhedsvejledningen stilles krav til offentlige myndigheder om anvendelse af kryptering ved transmission af følsomme og fortrolige personoplysninger over åbne net (f.eks. internettet).

Datatilsynet har ikke stillet et generelt krav om, at krypterede e-mails fra borgere og virksomheder skal forblive krypterede, efter at de er modtaget og så længe de behandles i en offentlig institutions mailsystem.

Hvis den dataansvarlige offentlige institution i en konkret situation imidlertid vurderer, at efterlevelse af kravene i f.eks. persondatalovens § 41, stk. 3, forudsætter, at e-mails forbliver krypterede efter modtagelse, da er det den dataansvarliges ansvar at sikre, at det i så fald også sker."

Som Datatilsynet bemærker, er der således ikke et generelt krav om, at krypterede e-mails fra borgere og virksomheder skal forblive krypterede, efter at de er modtaget, og så længe de behandles i en offentlig institution. Det kan således ikke lægges til grund, at der er tale om brud på persondatalovens regler, hvis offentlige institutioners mailsystemer ikke er krypterede.