Notat

Kirkeministeriet

Folkekirkens It

Dato: 28. november 2021

Akt nr. 198082

Sagsbehandler: Torben Stærgaard

Om en ændret forståelse af "sikker kommunikation" i henhold til databeskyttelsesforordningens krav

Forståelsen med hensyn til at efterleve krav i databeskyttelsesforordningen ved digital kommunikation mellem på den ene side folkekirken (fra en Kirkenets-pc) og på den anden side dens medlemmer samt med borgere har hidtil været den, at almindelige e-mails ikke har måttet indeholde hverken fortrolige eller følsomme personoplysninger. Konkret er det blevet udmøntet i vejledninger fra stifter om at neutralisere indholdet, eksempelvis ved ikke at nævne ord som "konfirmation" og "dåb", da man kan ellers kunne risikere at nævne følsomme oplysninger om modtageren.

Efter Kirkeministeriets drøftelser med Datatilsynet er der sket en præcisering af, hvordan e-mails kan anvendes på en måde, så kravene i databeskyttelses-forordningen opfyldes.

Dette betyder, at alle e-mails sendt fra en Kirkenet-postkasse er tilstrækkeligt sikre og kan indeholde ovennævnte oplysninger uden yderligere tiltag.

Med udgangspunkt i denne forståelse lægges der op til, at Kirkeministeriet udsender en vejledning til folkekirkens ansatte og menighedsråd m.fl.

Vejledningen skal præcisere den "nye forståelse" men også tydeliggøre, at det stadig er den dataansvarlige – dvs. den kirkebogsførende sognepræst eller menighedsrådet – der skal sikre sig, at modtageren er den rette.

Med udsendelse af en vejledning fra Kirkeministeriet lægges der op til, at der sker en ajourføring af vejledninger på DAP og diverse hjemmesider således, at der skabes klarhed om disse spørgsmål.

Sikre e-mails fra Kirkenet-postkasser

Datatilsynet har i møder i oktober 2021 oplyst

- 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
- at kryptering med TLS-protokollen som minimum baseres på version 1.2 samt at det skal sikres, at TLS gennemtvinges. Det betyder, at e-mailen ikke sendes fra afsender på Kirkenettet, medmindre modtagers posthus (uden for Kirkenettet) anvender TLS 1.2.

Det betyder, at brugere af Kirkenettet, eksempelvis præster og kordegne, som sender fra en "km.dk" adresse, og menighedsråd, som sender fra en "sogn.dk" adresse, frit kan kommunikere med andre e-mailadresser, idet e-mails afsendt fra Kirkenettet netop opfylder disse krav.

Når en Kirkenetbruger trykker på "send-knappen" sker der i første omgang det, at Kirkenettets e-mail system kontakter modtagerens e-mail system for at sikre, at dette anvender TLS 1.2. Og først når dette bekræftes, sendes e-mailen.

Bekræftes det ikke, vil afsenderen få et advis om at e-mailen ikke kan sendes fra Kirkenettet.

Til udtrykket "frit kan kommunikere" skal der knyttes den forudsætning, at Kirkenettets afsender skal være sikker på, hvem vedkommende kommunikerer med, altså på modtagerens identitet.

Endelig bemærkes det, at i de tilfælde, hvor e-mail sendes med mange personoplysninger på én gang, vil det være hovedreglen, at der skal anvendes løsninger, som sikrer kryptering både hos afsender og modtager samt under transporten.

Denne yderligere beskyttelse er også tilgængelig ved brugen af Kirkenet-postkasser og vil fremgå af den vejledning Kirkeministeriet udgiver.

Sikker kommunikation med konfirmander
Ifølge Datatilsynet er den sikre fremgangsmåde ved konfirmandtilmelding den, at forældrene først foretager tilmeldingen via Folkekirken.dk, hvor forældrene via NemID/MitID oplyser konfirmandens navn og mailadresse. Herefter vil kommunikation med konfirmander kunne ske frit med e-mail – så længe det sker fra Kirkenettet – fordi afsender ved, hvem modtager præcist er, og fordi e-mailen ikke kan afsendes fra Kirkenets-pc'en, medmindre konfirmandens mail anvender den krævede TLS-protokol.

SMS er ikke en sikker kommunikationsform
Kommunikation af fortrolige eller følsomme oplysninger via SMS er ikke sikker, da SMS'er ikke sendes krypteret. Disse må derfor ikke indeholde fortrolige eller følsomme oplysninger.

I stedet for SMS kan benyttes App'en Signal, som findes på alle Kirkenet-pc'er. Kommunikationen med Signal er krypteret og derfor sikker.

Udlevering af oplysninger om afdøde til pårørende og bedemænd
I forhold til kirkekontorernes betjening af bedemænd og pårørende i forbindelse med anmodning om begravelse/ligbrænding, er det efter Datatilsynets opfattelse i overensstemmelse med databeskyttelsesforordningen, at kirkekontoret kan oplyse de pågældende, hvorvidt afdøde var medlem af folkekirken[1].

Tilsvarende er det også tilsynets opfattelse, at i de tilfælde, hvor der ikke umiddelbart er nære slægtninge til afdøde, og hvor kommunen – som oftest via en bedemand – indgiver anmodning om begravelse eller ligbrænding, vil det være i overensstemmelse med forordningen at oplyse bedemanden om eventuelle nære slægtninge, såfremt sådanne vil kunne ses i Den digitale Kirkebog.

[1] Hjemlen hertil er databeskyttelsesforordningens artikel 6, stk. 1, litra e (*offentlig myndighedsudøvelse)* samt artikel 9, stk. 2 (undtagelsesbestemmelserne) litra f (*behandlingen er nødvendig, for at et retskrav kan fastlægges, gøres gældende eller forsvares*) og litra g (*behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser*).

Også i disse tilfælde er det en forudsætning, at kirkontoret eller præsten sikrer sig, at bedemanden kan sandsynliggøre at vedkommende optræder som anmelder på vegne af kommunen. Det kan eksempelvis ske ved, at vedkommende kan oplyse navn og CPR-nr. på afdøde, eller ved at bedemanden kan forevise en dødsattest.

Gives svaret pr. e-mail kan det sendes fra en Kirkenet's-pc og i den forbindelse kan det overvejes at sende med Digital Post til bedemandens CVR-nr.