Læsetid
ca. 8 min.

4 KRYPTERINGSFORMER DU SKAL KENDE TIL

Send 100% sikre e-mails med et tryk på en knap

DPG e-bog om e-mail sikkerhed
Udgivet Sept 2019

DPG

Hvornår skal jeg sende sikkert?

I 2008 hørte du måske første gang om, at personfølsomme oplysninger skulle beskyttes, når du sendte dem digitalt på fx e-mail.

I dag er der flere standarder, du skal efterleve på det danske og internationale marked efter Databeskyttelsesdataloven trådte i kraft i maj 2018. Det kan virke som en jungle med de nye krav.

Flere afdelinger som HR, Økonomi og Jura sidder til daglig med behandling af personfølsomme oplysninger. Det kan være svært at gennemskue, hvornår det er okay at sende en e-mail almindeligt og hvornår den skal være krypteret.

Her giver vi dig et overblik over de fire krypteringsformer, som du kan bruge til at efterleve GDPR og overholde reglerne for transport af personfølsomme oplysninger.

DPG

Hvilke oplysninger skal krypteres?

Følsomme personoplysninger

- Helbredsoplysninger
- Seksuelle forhold
- Race
- Etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold
- Genetiske data
- Biometriske data

Personnummer

- Medarbejderens CPR-nummer

Strafbare forhold

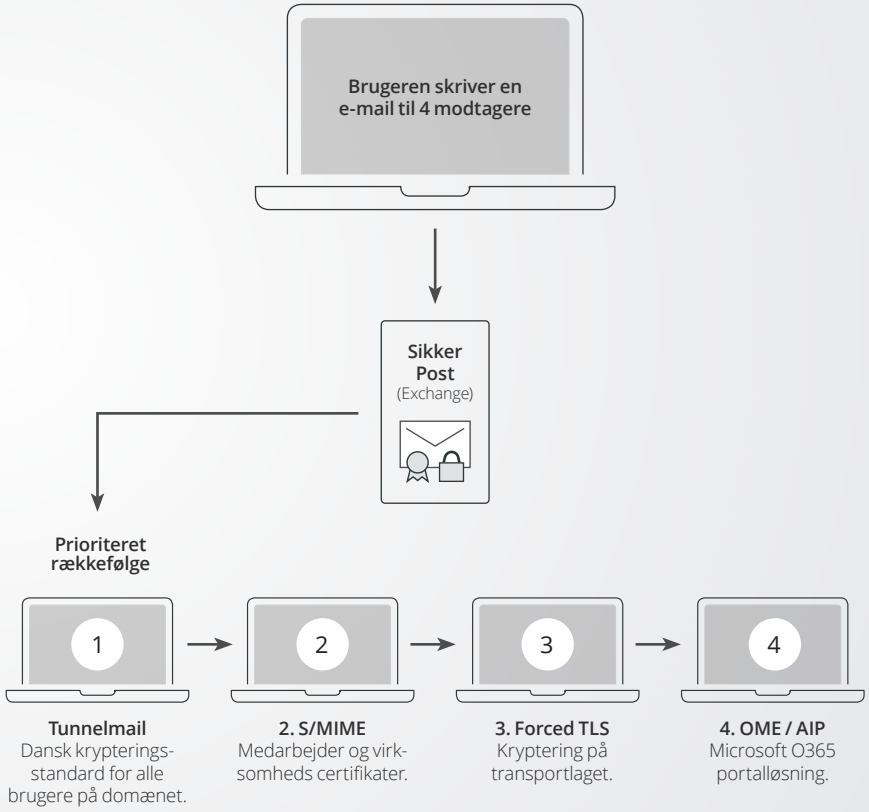
- Oplysning om at en medarbejder har begået (eller er politianmeldt for) et strafbart forhold.
- Oplysning om overtrædelse af lovgivningen, uden at det har udløst (eller kan udløse) et egentlig strafansvar, som fx sanktion eller rettighedsfrakendelse.
- Oplysninger på straffeattest eller børneattest.

Kilde: Datatilsynet.dk – Vejledning om databeskyttelse i forbindelse med ansættelsesforhold

De 4 krypterings-former

Har du hørt om de fire krypteringsformer **S/MIME, Tunnelmail, TLS og OME**? Hvis ikke får du i næste afsnit en gennemgang af dem i et let forstå-eligt sprog.

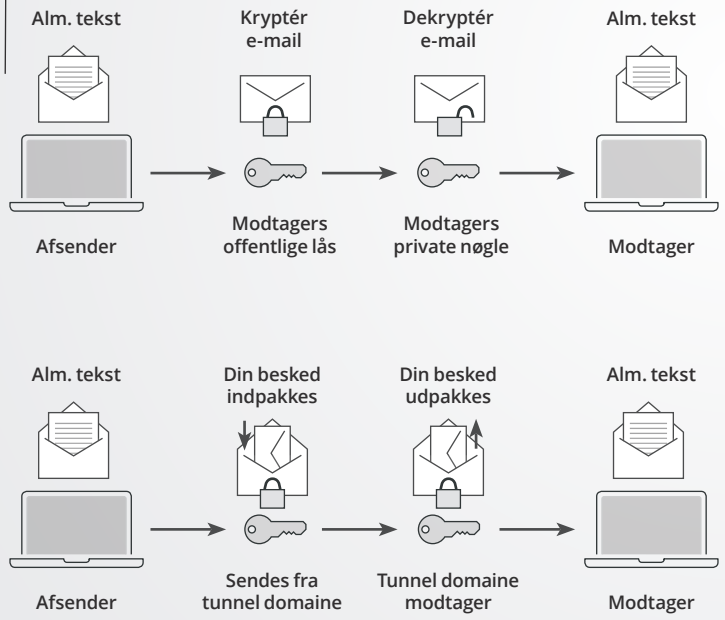
Til dig som har helt styr på de fire former, har vi gemt nogle tekniske tips sidst i bogen, så du kan opnå det fulde udbytte med kryptering.



1 S/MIME kryptering

S/MIME kaldes SikkerPost, SikkerMail, Krypteret signeret mail.

Det er en standard fra 90'erne. Indført i det offentlige Danmark i 2008. Denne krypteringsform er typisk anvendt i Danmark med brug af NEMID certifikater, som både kan være medarbejder- og virksomhedscertifikater. S/MIME kan du anvende manuelt i fx din Outlook, men den kan også håndteres automatisk af krypteringsløsninger som DPG.



FAKTA
Datatilsynet betegner disse som END2END kryptering (stærk kryptering)

Hvilken type data må jeg sende?
Du må sende alle typer af personfølsomme data og mængder med disse løsninger.

STÆRK KRYPTERING

2 Tunnelmail kryptering

Tunnelmail er en dansk standard baseret på S/MIME kryptering.

Tunnelmail er domæne til domæne kryptering. Det vil sige, at alle brugere på et domæne, der er tilmeldt tunnelmail-listen kan kommunikere med alle andre brugere på et andet domæne, som også er tilmeldt tunnelmail-listen. Det fjerner behovet for at alle brugere behøves et certifikat. Metoden er transparent for afsender/modtager.

99% af alle offentlige danske virksomheder er på løsningen samt et par tusind andre virksomheder.

Er din virksomhed på tunnelmail-listen? Når du er på listen, kan du kommunikere med alle medarbejdere i det offentlige direkte og sikkert.

3 TLS 1.2 kryptering

Dette er en international standard.

TLS 1.2 er brugt næsten alle steder i dag. Med TLS krypteres data ikke, men forbindes mellem to mailsystemer, der udveksler mails. Det vil sige, at data kan læses af alle der er i forbindelse med e-mailen. Det er ikke kun en specifik modtager, der kan læse mailen.

De fleste mailsystemer i dag tilbyder en opportunistisk tilgang til TLS. Det er ikke nok at have TLS på dit system, din modtager skal også have TLS for at kunne modtage din mail. Faldgruppen her er, at du i standard mailsystemer ikke kan gennemtvinge TLS på enkelte forsendelser, der indeholder personfølsomme data. Konsekvensen er, at du kan komme til at sende noget ukrypteret.

DPG SikkerPost kan tilsikre brugen af "Force" TLS.

FAKTA
Datatilsynet betegner det som kryptering på transportlaget (svag kryptering), uden mulighed for authentication.

Hvilken type data må jeg sende? Du må sende begrænset mængder personfølsomme data.

SVAG KRYPTERING

4 OME kryptering

Portalløsninger - OME
(office message encryption fra Microsoft)

Portalløsninger benyttes til at aflevere personfølsomme data til modtagere, der ikke er i stand til at modtage krypteret post under normale forudsætninger, som beskrevet i krypteringsform 1-3.

Rent praktisk sendes et link til modtageren, der henviser til en sikker portal, hvor modtageren kan tilgå personfølsomme oplysninger og besvare henvendelsen sikkert.

For modtagerens synspunkt er brugeroplevelsen ikke lige så let tilgængelig som at modtage en e-mail, da man først skal logge ind på portalen.

FAKTA
Datatilsynet betegner det som END2END kryptering (stærk kryptering)

Hvilken type data må jeg sende? Du må sende alle typer af personfølsomme data og mængder med denne løsning.

Husk dog på i portalløsningen at modtageren ikke kan valideres på baggrund af en e-mailadresse uden certifikat.

STÆRK KRYPTERING

Resumé af de 4 krypteringsformer

Nu er du blevet klog på de fire krypteringsformer og hvilken slags data du skal sende krypteret. Du får lige en kort opsamling på de fire former, så du kan huske dem.

S/MIME

S/MIME var krypteret signeret mail, som du typisk anvender, når du bruger NEMID certifikater.

Tunnelmail

Tunnelmail handlede om domæne til domæne kryptering, hvor brugere på et domæne, der er tilmeldt tunnelmail-listen kan kommunikere med alle andre brugere på et andet domæne, som også er tilmeldt tunnelmail-listen.

TLS 1.2

Med TLS krypteres data ikke, men forbindes mellem to mailsystemer, der udveksler mails. Det vil sige, at data kan læses af alle, der er i forbindelse med e-mailen.

OME

Den sidste krypteringsform OME var en portalløsning, hvor modtageren kan tilgå personfølsomme data og svare på beskeden.

For dig som er teknisk

Vi har spurgt vores Tekniske Teamleder, Gregers Blach, hvad du skal tænke ekstra over ved nogle af de fire krypteringsformer.

Tech tips fra Gregers

VIL DU GERNE BRUGE TUNNELMAIL?

For at kunne sende og modtage tunnelmail, skal du være kunde hos en systemleverandør, som tilbyder tunnelmail. Din leverandør vil sikre, at dit maildomæne oprettes på alle leverandørernes tunnelmail-lister, så du kan udveksle tunnelmail med alle maildomæner på tunnelmail-listerne.

KAN DINE MODTAGERPUNKTER TERMINERE MED TLS?

Inden afsendelse af en sikker mail, laves der med en løsning som DPG et tjek på modtagerdomænets MX record for at sikre, at alle modtagerpunkter kan terminere/forbinde med TLS. Kan blot ét modtagerpunkt ikke terminere med TLS, kan DPG ikke garantere en sikker forsendelse, og vil derfor ikke tillade afsendelse af mailen. DPG opererer derfor med garanteret/påkrævet TLS og ikke blot opportunistisk TLS.

DPG

Hvad er DPG SikkerPost?

Skal du sende sikker digital post til både private og offentlige modtagere?

Timengo DPG tilbyder en SikkerPost løsning, der integrerer med Exchange Online, Office 365 og Exchange On-Premise. Løsningen er registreret i Microsoft OCP katalog (Partnerkatalog). Grundet vores tætte samarbejde og integration med Microsoft løsningerne.

Kommunikationsløsningen gør det nemt for den enkelte bruger i virksomheden at overholde GDPR og retningslinjer fra Datatilsynet vedr. transport af personfølsomme data. Klik på 'Send sikkert' knappen i Outlook og løsningen gør resten for dig ved automatisk at kombinere forskellige krypteringsformer.

SikkerPost løsningen benytter S/MIME, tunnelmail, OME/AIP, Forced TLS til Exchange/Outlook. Ved hjælp af integration til e-Boks får du mulighed for at sende e-mail direkte i e-Boks til CPR- og CVR-numre.

Læs mere om den digitale kommunikationsløsning på
www.sikker-post.dk

Send e-Boks beskeder med DPG

Timengo DPG løsningen integrere direkte med e-Boks uden om distributionsleddet. Det vil sige, du har en direkte forbindelse til e-Boks fra din Outlook eller et andet mailsystem. Timengo DPG er samarbejdspartner til e-Boks, så vi kan let oprette jeres virksomhed som afsender i e-Boks.

Som afsender i e-Boks opnår du en sikker kommunikation direkte til dine kunders foretrukne digitale postkasse. Samtidig effektiviserer du omkostningstunge papirprocesser og arbejdsgange – uden at forringe dit serviceniveau. Du kan sende alt fra lønsedler, kontrakter, indkaldelser til undersøgelser/operationer, div. opgørelser/oversigter og meget mere – altsammen CPR/CVR valideret. Du leverer blot uddata og e-Boks håndterer resten.

Vil du vide mere om e-Boks integration og aftaler kan du læse mere på **www.sikker-post.dk/send-sikkert-med-e-boks-integration**

Du kan også ringe direkte på **+45 7020 6280** eller skrive til vores Salgsdirektør Andreas Mortensen på **salg@sikker-post.dk**. Tak fordi du læste med.

Ring på +45 7020 6280

Eller besøg vores hjemmeside
www.sikker-post.dk