DANSK OPLYSNINGS FORBUND

Ny Østergade 7, 1. sal
4000 Roskilde
Tlf. 70 20 60 20
www.danskoplysning.dk
post@danskoplysning.dk

Afsendelse af e-mails med personoplysninger

Siden 2008 har Datatilsynet anbefalet, at man anvender kryptering ved afsendelse af fortrolige og følsomme personoplysninger via e-mail, men i 2019 er det blevet et krav.
Selvom e-mail afsendelse af disse oplysninger ikke direkte er omtalt i GDPR, vurderer Datatilsynet, at krypteringen er den eneste måde at overholde GDPR krav om ”passende sikkerhedsforanstaltninger”.

Hvad er fortrolige og følsomme personoplysninger?

Kategorien ”følsomme personoplysninger” er klart defineret og omfatter: Race, etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data, helbredsoplysninger, seksuelle forhold, seksuel orientering.
På den anden side er kategorien ”fortrolige personoplysninger” meget mere uklar og er i den sidste ende en vurderingssag. Mens følsomme personoplysninger er altid fortrolige, er en fortrolig oplysning ikke altid følsom. En ikke-følsom personoplysning kan i visse situationer også være fortrolig, hvis det vurderes som sådan.
Principielt er en oplysning fortrolig, hvis det vurderes, at oplysningen objektivt bør kunne forlanges unddraget offentlighedens kendskab. Personhenførbare oplysninger, som ikke kan nægtes udleveret efter offentlighedsloven, er ikke fortrolige.
Datatilsynet har dog vurderet, at CPR nr. er en fortrolig oplysning.

Hvad er kryptering?

Når en e-mail sendes over internettet, har brugeren ingen kontrol over, hvilke ruter og maskiner mailen passerer undervejs, og hvem der eventuelt vil kunne læse mailen. For at forhindre dette har man to muligheder: at kryptere transporten af de datapakker, som indeholder mailen (kryptering på transportlaget); eller at selve mailens indhold krypteres hos afsenderen og kun kan læses af modtageren, der har en passende nøgle (end-to-end kryptering).
Hvilken type kryptering, man skal bruge, er en vurderingssag. Men efter vores opfattelse – og i overensstemmelse med Datatilsynets krav – er kryptering på transportlaget passende for langt de fleste aftenskolers virke.

Hvad er kryptering på transportlaget?

Man kan sammenligne e-mailsystemet med et almindeligt, fysisk postsystem. At sende en ukrypteret e-mail over Internettet svarer til, at man sender et åbent postkort. Alle, som kommer i kontakt med postkortet, vil kunne læse indholdet, uden at afsenderen eller modtageren er beviste om det.
Hvis man til gengæld smider kortet i en lukket konvolut, så forhindrer man, at uvedkommende læser indholdet (hvis konvolutten brydes, vil forsendelsen fejle). Indpakningen vil dog kun sikre forsendelsen, mens den transporteres. På

destinationen vil enhver, der har adgang til postkassen stadigvæk kunne læse brevet.
Og det er overordnet principperne bag kryptering på transportlaget.
Det mest udbredte krypteringsprotokol for transportlaget er TLS (Transport Layer Security), som tilføjer et ekstra sikkerhedslag til almindelig mailkommunikation. For at etablere en sikker transport kræves det dog, at både afsenderens og modtagerens mail-server understøtter TLS (primært TLS 1.2 eller nyere, som er minimumskrav fra Datatilsynet). De fleste store mail-udbydere (Microsoft, Google mm.) understøtter TLS 1.2 kryptering som standard.

Hvad er end-to-end kryptering?

I sin basisform består end-to-end kryptering af et nøglepar (offentlig og privat), som både afsenderen og modtageren er i besiddelse af. Afsenderen bruger modtagerens offentlige nøgle for at kryptere indholdet af mailen, og modtageren bruger sin private nøgle for at afkode mailen. Indholdet af mailen er således krypteret og beskyttet hele vejen fra én bestemt afsender til én bestemt modtager.
Denne form for kryptering kræver dog en del fra både modtageren og afsenderen: Begge skal have et nøglepar og kende hinandens offentlige nøgle, og deres e-mailklienter skal desuden understøtte og indrettes til denne form for kommunikation. De mest kendte variationer for denne krypteringsform er OpenPGP standard og S/MIME (certifikater).
Grundet kompleksiteten og de tekniske krav, der stilles til både afsenderen og modtageren, vurderer vi dog ikke, at denne form for kryptering reelt er noget der pt. kan implementeres hos aftenskolerne.

Brugbare alternativer

NemID/e-Boks

Alle personer i Danmark har en e-Boks, som tilgås via NemID og virksomheder kan (mod betaling) bruge e-Boks' gateways (PostNord eller KMD) til afsendelse.
Man kan også sende sikre mails til for eksempel kommune eller bank med NemID direkte fra de fleste mailprogrammer (ikke alle er understøttet). På NemID's hjemmeside kan du læse mere om deres sikker e-mail løsning (https://www.nemid.nu/dk-da/kom_i_gang_med_nemid/sikker_e-mail/).
.

Kryptering af vedhæftede dokumenter

Nogle gange er det ikke selve e-mailen, men de vedhæftede dokumenter, der indeholder følsomme eller fortrolige informationer. Det er meget nemt at beskytte Office-dokumenter (Word, Excel mm.) med en adgangskode.
Word: Filer -> Oplysninger -> Beskyt dokument -> Kryptér med adgangskode (Skriv adgangskoden, bekræft og gem).
Excel: Fil -> Info -> Beskyt projektmappe -> Kryptér med adgangskode (Skriv adgangskoden, bekræft og gem).

Hvis der er flere filer, eller hvis der ønskes yderligere beskyttelse, kan der med fordel bruges forskellige arkiveringsprogrammer, som muliggør kryptering. De findes i både gratis og betalte udgaver, men en af de mest kendte er **WinRAR**, som muliggør arkivering, kryptering og beskyttelse af større mængde filer i én ZIP/RAR fil. Betalt version koster ca. 300 kr. (engangsudgift).
Fælles for dokument-/filbeskyttelse med kryptering er, at filerne kun kan åbnes, hvis man kender adgangskoden. Derfor er en fornuftig og sikker distribuering af denne adgangskode mindst ligeså vigtig som dokumentbeskyttelse.

Anbefalinger til aftenskolerne

Det er vigtigt at understrege, at Datatilsynet pt. kun stiller krav til kryptering af følsomme og fortrolige informationer (herunder CPR). Almene, ikke-følsomme og ikke-fortrolige informationer er ikke omfattet af dette krav.
Det betyder i praksis, at skolerne i første omgang skal overveje, om det overhovedet er nødvendigt at sende disse informationer via mail. For eksempel:

Afsendelse af deltagerlister til undervisere.

- Underviseren har under ingen omstændigheder brug for deltagernes CPR (som er fortrolig oplysning).
  Derudover kan man overveje, hvilke øvrige oplysninger underviseren reelt har brug for. Dette relateres overordnet til GDPR og ikke kun mailafsendelse. Folk skal have adgang til de oplysninger, de har brug for, og intet mere.
- Brug UnderviserNet eller andre platforme.
  Hvis man bruger DOF's administrationssystem, har man også adgang til UnderviserNet. Ved at bruge dette platform til distribuering af deltagerlister mm., reduceres antallet af afsendte mails.

Afsendelse af deltagerlister til kommuner

- Kommuner har i nogle tilfælde brug for deltagerlister, som indeholder fortrolige oplysninger, herunder CPR. Da dette er et krav fra kommunen, er kommunen forpligtet til at definere leveringsformen. Alle kommuner har en NemID-postkasse eller kan tilgås via virk.dk eller kommunens egen hjemmeside.
  Snak med kommunen, hvordan den ønsker listerne modtaget.
- Kommuner har ikke krav på CPR, hvis det ikke er tale om udenbys deltagere. Gør kommunen opmærksom på dette.

Afsendelse af deltagerlister til andre deltagere

- Disse lister bør per definition ikke indeholde følsomme eller fortrolige informationer, og derfor kan afsendelse klares via almindelig mail.
- Vær dog opmærksom på de øvrige krav i GDPR, at der skal være et sagligt formål med behandlingen af personoplysninger.
  Den nemme måde er at indhente mundtligt eller skriftligt samtykke fra deltagere på, at deres personoplysninger (normalt kun navne og eventuelt mail/telefonnummer) må deles med andre deltagere.

Afsendelse af lønsedler og andre dokumenter til undervisere

- Foreningerne i DOF kører normalt løn hos DOF, og vi leverer lønsedler direkte til et sikkert intranet.
- Hvis foreningen alligevel ønsker at maile lønsedler eller andre dokumenter med fortrolige informationer til undervisere, bør det ske med underviserens samtykke. Her kan dokumentkryptering komme på tale.

Modtagelse af oplysninger fra deltagere, undervisere og andre

- Det er vigtigt at informere (på hjemmesiden, mundtligt eller i mailen) deltagere og undervisere, at ukrypteret afsendelse af mails med fortrolige informationer udgør en sikkerhedsrisiko.
- Hvis skolen anvender DOF's administrationssystem og de tilhørende online tilmeldingssystemer, bør du bede deltagere om at bruge online tilmeldingsform, som er sikker.
- Modtagelse af underviserens CPR kan med fordel klares via telefon og helt uden om mailsystemet.

Undersøg kryptering på transportlaget

- Hvis man ikke kan undgå at sende eller modtage mails med fortrolige oplysninger, skal man undersøge om kryptering på transportlaget er understøttet.
- Microsoft Office 365 (Outlook) understøtter TLS 1.2. Det betyder, at kryptering på transportlaget hos skoler, der bruger DOF's mailsystem, er sat til som standard.
- Gmail og andre store mailudbydere understøtter også TLS 1.2. Tjek altid med mailudbyderen, om dette er sandt.
- Hvis skolen er sikker på, at skolens mailudbyder understøtter TLS 1.2, skal den anden part af mail-kommunikationen gøres opmærksom på, at de skal tjekke deres mailudbyder, hvis de ønsker at sende/modtage fortrolige oplysninger via mail.
- Informér deltagere/undervisere om ovenstående på skolens hjemmeside og evtentuel som en del af skolens persondatapolitik.
- Brug online værktøjer til at teste modtagerens og afsenderens TLS understøttelse. Du kan også manuelt tjekke hver enkel mail.