GYMNASIEFÆLLESSKABET

Vejledning om sikker mail

Hvornår er der krav om brug af sikker mail?

Når en skole sender eller modtager e-mails med personoplysninger af fortrolig og/eller følsom karakter skal det ske via en sikker mailforbindelse. Det er et krav, der følger af persondataloven og som fra maj 2018 vil blive videreført i EU-databeskyttelsesforordningen.

E-mails med personoplysninger af fortrolig eller følsom karakter udveksles fx som led i elevoptag, fravær, SPS, studievejledning, frafald, sanktioner, udveksling af oplysninger med andre skoler, kommunikation med UU-vejlederen, eksamensafholdelse, indberetninger til UVM eller til censorbanken, personalesager, refusionsanmodninger, mv.

En personoplysning er fortrolig, hvis oplysningen er af en sådan karakter, at den efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab.

Følgende personoplysninger er *altid* fortrolige:

- cpr-nummer, oplysninger om en persons racemæssige eller etniske baggrund, politiske, religiøse eller filosofiske overbevisning, fagforeningsmæssige tilhørsforhold, helbredsforhold, seksuelle forhold, oplysninger om strafbare forhold og væsentlige sociale problemer, oplysninger om interne familieforhold, f.eks. stridigheder, selvmordsforsøg og ulykkestilfælde.

Følgende oplysninger *kan* være fortrolige:

- oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold.

Hvis personoplysningerne i mailen er fuldt anonymiserede, er der ikke krav om brug af sikker mail. Der er heller ikke krav om brug af sikker mail, hvis mailen ikke sendes det åbne internet. Dette er tilfældet, hvis mailen er bestemt til en modtager på samme domæne eller på samme mailserver som afsenderen. Hvis man er i tvivl om dette er tilfældet, kan man kontakte sin lokale it-vejleder.

Hvordan sendes mail sikkert?

For at e-mailkorrespondancen bliver sikker, skal både afsender og modtager have en sikker mail-løsning.

Den sikre mail-løsning kan være etableret på flere måder, fx

- Skolen har en integration mellem sit almindelige mailsystem og Digital Post/e-Boks, som gør at medarbejderne via opslag på modtagerens cpr-nr. eller cvr-nr. kan sende mails sikkert ind modtagernes digitale postkasse. Denne model kræver således, at man kender modtagerens cpr.nr. eller cvr.nr., for at man kan kommunikere sikkert
- Den enkelte medarbejder har installeret et NemID på sin individuelle mailkonto, som gør at medarbejderen kan slå modtagerens sikre mail adresse op i en liste over sikre certifikater hos NemID. Hvis der er tale om en modtager, man ofte kommunikerer sikkert med, kan certifikatet tilføjes mailkontoens adressebog
- Både afsender og modtager er tilknyttet samme tunnelmail. Denne løsning kræver køb af en serviceaftale med et af de private firmaer, der udbyder tunnelmail-løsninger
- Skolen har en ”sikkermail”-adresse på sin hjemmeside, som der kan sendes sikkert til. Det kan være en fælles funktionspostkasse for hele institutionen (fx. sikkermail@[*]-gym.dk) eller softwaren kan tilføjes de individuelle medarbejderpostkasser, der allerede anvendes til mailkorrespondance. Hvis

løsningen med én fælles funktionspostkasse vælges, skal den sikre mail fordeles manuelt til den korrekte fysiske modtager. Der findes også mailfordelingssystemer, der kan indstilles til automatisk at videresende mails fra fællespostkassen til den enkelte modtager. Hver skole bør lade adressen på sin(e) sikre mailpostkasse(r) fremgå tydeligt og lettilgængeligt på sin hjemmeside, fx. på forsiden sammen med øvrige formelle oplysninger som adresse, CVR-nr., mv. eller under punktet "Kontakt". Er den sikre e-mail stilet til en bestemt medarbejder, kan dette angives i e-mailens emnefelt, som fx kan navngives "*Fortroligt. Skal videresendes til [x medarbejder]*", hvorved de øvrige medarbejdere, der måtte have adgang til indbakken i den sikre fællespostkasse, bliver advaret om, at mailen ikke er til dem men skal videresendes. Endvidere *kan* afsender i særlige tilfælde (fx hvis der er tale om særligt følsomme personoplysninger eller en hastehenvendelse) vælge at sende en adviseringsmail (uden fortrolige og følsomme personoplysninger) til modtagerens egen (usikre) mailadresse med information om, at der nu ligger en mail i den fælles postkasse og venter på at blive fordelt.

Da man ikke altid på forhånd kan vide, hvilken form for sikker mail-løsning, modtageren benytter, bør man som afsender spørge modtageren om dette. Der er dermed behov for en dialog forud for at mailen med fortrolige eller følsomme personoplysninger afsendes – i hvert fald hvis der er tale om en skole eller en modtager, som man ikke normalt kommunikerer med.

<u>Reglerne</u>

Det følger af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Af sikkerhedsbekendtgørelsens § 14 følger endvidere, 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.

Dette betyder bl.a., at en offentlig myndighed ikke må sende fortrolige og følsomme personoplysninger via det åbne internet, med mindre fremsendelsen sker krypteret.

Et mailsystem må endvidere kun indeholde følsomme eller fortrolige oplysninger, hvis

- Adgangen til mailsystemet er begrænset til de brugere, som er autoriseret dertil
- Adgangskontrolsystemet er aktiveret, således at en bruger kun har adgang til sin postkasse efter afgivelse af password
- Der er sletterutiner i såvel afsenders "sendt post" som i modtagers "indbakke" samt efterfølgende i papirkurven
- Der er truffet sædvanlige sikkerhedsmæssige foranstaltninger, herunder bl.a. beskyttelse mod uvedkommendes adgang til lokalnet og postserver i form af opdateret firewall, antivirus, mv.
- Der senest 1 måned efter afslutningen af sagsbehandlingen sker overførsel af evt. følsomme personoplysninger til et system, der kan foretage systemlogning af autoriserede brugeres anvendelse af de følsomme personoplysninger. Overførslen er ikke er krav, hvis de følsomme personoplysninger kan anonymiseres fuldt ud eller slettes effektivt senest 1 måned efter afslutningen af sagsbehandlingen

Maj 2017

Astrid Levin, jur. konsulent