blicher
INSPIRATION

Dato skrevet:
6. December 2018

Dato for download:
17. August 2022

# Datatilsynet skærper praksis for e-mail af fortrolige personoplysninger

Gældende fra 1. januar 2019 stiller Datatilsynet krav om, at private virksomheder skal anvende kryptering ved "transmission" af fortrolige og følsomme personoplysninger med e-mail via internettet. Hidtil har kravet alene omfattet offentlige virksomheder.

Det er afsenderen, der ud fra en risikovurdering skal vurdere hvilken sikkerhed, der er nødvendig. Ifølge datatilsynet bør de dataansvarlige dog som udgangspunkt anse risikoen for høj – og sende e-mails med fortrolige oplysninger sikkert. Dette skyldes, at afsendere af e-mails, der sendes over det åbne internet, normalt ikke har kontrol over, hvilke servere mailen passerer – herunder, hvor de er placeret.

Afsendelse af sikker mail kan teknisk ske enten ved kryptering af selve forsendelsen af data eller ved kryptering af indholdet.

Ved krypteringen af forsendelsen data er det selve transporten, der er sikret. Mails ligger derimod læsbare på både modtagers og afsenders mailserver. Metoden kan sammenlignes med et gammeldags brev, hvor brevet både kan åbnes af uvedkommende på adressen eller være fejladresseret. Men selve transporten af brevet kan man normalt regne for sikker – ganske vist lidt afhængigt af postbuddet. Modsat, hvis man sender et åbent postkort svarende til en mail, hvor forsendelsen ikke er sikret ved kryptering.

Som en yderligere sikkerhed er det muligt at kryptere indholdet inden afsendelse. Heraf kan mailen kun læses af den modtager, der har en krypteringsnøgle – og ligger umiddelbart ikke læsbart for andre på mailserverne.

Blicher kan sikre mails ved transporten og har mulighed for at kryptere selve indholdet enten ved aftalt kode, nem-id eller anvendelse af krypteringsprogram. Fortrolige mails vil som minimum blive afsendt med tilvalg af mindst en af krypteringsformerne.