Retningslinjer for brug af mail – for aktive.

1. E-mailadressen er personlig – dvs. at det kun er dig som person, der må have adgang til den og kende kodeordet.

2. Mailen kan nemt tilgås fra alle browsere på: www.portal.office.com.

3. **Personoplysninger**
   I skal være særligt opmærksomme på ikke at sende personoplysninger ukrypteret pr. mail – personoplysninger deles op i to kategorier:

   3.1. Følsomme personoplysninger
   Oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering. Det er kun de oplysninger, der er nævnt her, der anses for følsomme oplysninger i forordningen.

   3.2. Almindelige personoplysninger
   De personoplysning, der ikke falder ind under kategorien ”følsomme personoplysninger”, kan kaldes ”almindelige personoplysninger. Almindelige personoplysninger kan f.eks. være identifikationsoplysninger som f.eks. navn og adresse, oplysninger om økonomiske forhold, kundeforhold eller andre lignende ikke-følsomme oplysninger.

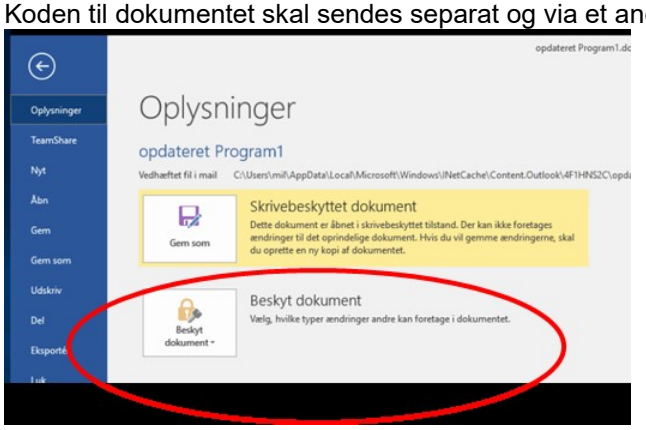
   3.3. Betydning i IDA: Hvis en person står omtalt som medlem af IDA er det en følsom oplysning, da det fortæller om personens fagforeningsmæssige tilhørsforhold.

      3.3.1. Hvornår skal vi kryptere dokumenter, når vi sender dem pr mail?
      Svar: Når dokumenterne indeholder følsomme personoplysninger. Indeholder dokumentet almindelige personoplysninger er det fortsat god stil at kryptere.

      Datatilsynet skriver: ”Brug og håndtering af personoplysninger skal foregå betryggende og med et passende niveau af sikkerhed og privatlivsbeskyttelse. Sikkerhedsniveauet skal afspejle den konkrete risiko for, at oplysningerne stjæles, mistes, skades, eller behandles ulovligt.”

      3.3.2. Hvordan kan et dokument krypteres inden afsendelse?
      Svar: Det er god stil at kryptere alle dokumenter med følsomme persondata og persondata i større omfang (medlemslister). I Office-programmerne gøres det under menuen Filer.

Koden til dokumentet skal sendes separat og via et andet medie, f.eks. sms eller messenger.



3.3.3. Hvad er udtrykkeligt samtykke, og hvordan sikrer vi, at vi har det?
Svar: Når en person har afgivet et samtykke, som er utvetydigt og de har mulighed for at trække det tilbage. Samtykket skal være let tilgængeligt og forståeligt. Man sikrer bedst et samtykke ved at få det skriftligt eller elektronisk. Et mundtligt samtykke er også gyldigt, men sværere at bevise senere.

3.3.4. Må vi i bestyrelsen sende referater fra vores bestyrelsesmøder/generalforsamlinger til hinanden i bestyrelsen og netværkskoordinatoren uden at kryptere?
Svar: Særligt hvis dokumentet indeholder følsomme personoplysninger, skal det krypteres. Indeholder dokumentet almindelige personoplysninger kan I vurdere om en kryptering er nødvendig i forhold til om oplysningerne kan misbruges, jf. Datatilsynets anvisning som står under punkt 1.

3.3.5. Interne deltagerlister med tlf. nr. og mailadresse. Skal den krypteres, når den sendes ud til bestyrelsesmedlemmer eller samarbejdspartnere?
Svar: Det vil være god stil og det vil sikre et tilpas sikkerhedsniveau i forhold til at undgå at persondata falder i forkerte hænder.

3.3.6. Må jeg anvende Dropbox eller anden privat delingstjeneste?
Svar: Ja, hvis der ikke ligger persondata, der stammer fra IDA heriblandt deltagerlister. Har I aftalt i bestyrelsen, at I anvender en delingstjeneste, så kan I godt dele referater og andre dokumenter fra bestyrelsesarbejdet..

Derudover bør I jævnligt holde jer opdaterede på aktivguiden på ida.dk – den opdateres løbende.