VEJLEDNING

RISIKOVURDERING

**Hvorfor en risikovurdering?**

Datasikkerhed kan siges at være Databeskyttelsesforordningens hovedformål. De sikkerhedsforanstaltninger, den enkelte virksomhed eller den enkelte organisation skal foretage for at sikre datasikkerheden, skal vælges ud fra og på baggrund af en konkret risikovurdering. Forordningen opstiller ikke en række faste krav til, hvordan hver virksomhed eller organisation skal håndtere deres datasikkerhed. Forordningen lader det være op til den enkelte virksomhed eller organisation at vurdere hvilke sikkerhedsforanstaltninger, der skal til for at sikre datasikkerheden.

Datasikkerheden skal altså sikres ved en risikobaseret tilgang. Det vil sig, at det er de risici som er forbundet med en bestemt behandling af personoplysninger, som spiller en afgørende rolle for hvilke foranstaltninger, man som dataansvarlig konkret skal iværksætte. Ikke alle virksomheder eller organisationer er ens, og risikoen for at der sker brud på datasikkerheden varierer i et meget stort omfang. Derfor skal sikkerhedsforanstaltninger fastlægges alt efter hvilke risici der foreligger for den enkelte virksomhed eller organisation.

Det som skal underlægges en vurdering er de risici, der foreligger for de registreredes rettigheder. Vurdering handler om, hvilke risici en virksomhed eller en organisation udsætter den registreredes personoplysninger for.

**Eksempel på opbygning af en risikovurdering:**

Databeskyttelsesforordningen stiller ikke krav til hvor detaljeret eller hvor grundig denne risikovurdering skal være. Forordningen siger blot, at den dataansvarlige skal fastlægge et *passende sikkerhedsniveau* i forhold til de risici, som er relevante for den konkrete persondatabehandling.

Til at starte med er det en god ide at skabe et overblik over informationsaktiverne i virksomheden eller i organisationen. Dette skyldes, at disse informationsaktiver bør være omdrejningspunkt for selve risikovurderingen. Et informationsaktiv er der, hvor personoplysningerne behandles. Dette kan være it-systemer, servere, kommunikationskanaler og lignende.

Når man skal sikre datasikkerheden er der tre ting som er essentielle. Disse tre ting drejer sig om fortrolighed, tilgængelighed og integritet.

Fortrolighed indebærer, at der skal forhindres uautoriseret adgang til eller videregivelse af personoplysninger. Det betyder, at uvedkommende ikke får fat i eller kendskab til personoplysninger.

Tilgængelighed vil sige, at personoplysningerne skal sikres mod en uautoriseret begrænsning af adgangen til oplysninger for de personer som har en retmæssig adgang hertil.

Integritet indebærer, at informationer skal sikres mod uautoriseret ændring eller ødelæggelse.

1. **en konsekvensvurdering**

Når man påbegynder sin risikovurdering, er det en god idé at tage udgangspunkt i hvert enkelt informationsaktiv. Her kan man så fastlægge konsekvensen, hvis det antages, at informationsaktivet taber fortrolighed, tilgængelighed og integritet. Denne konsekvens kan f.eks. vurderes som høj, medium eller lav.

1. **en sandsynlighedsvurdering**

Herefter kan man med fordel identificere de trusler, som hver af informationsaktiverne eventuelt står overfor. Hertil kan der igen laves en høj, medium eller lav vurdering af, hvor stor sandsynligheden er for at truslen bliver en realitet. Dette kaldes også for ”trusselsvurdering”.

1. **en sårbarhedsvurdering**

Der er formentlig allerede opsat eksisterende sikkerhedsforanstaltninger i virksomheden eller organisationen. Disse sikkerhedsforanstaltninger mildner truslerne, som er blevet fastlagt.

Det næste trin er at fastlægge og identificere disse eksisterende sikkerhedsforanstaltninger, samt at fastlægge deres virkning på nedsættelsen af sandsynligheden og konsekvenserne, som er fastlagt jf. ovenfor.

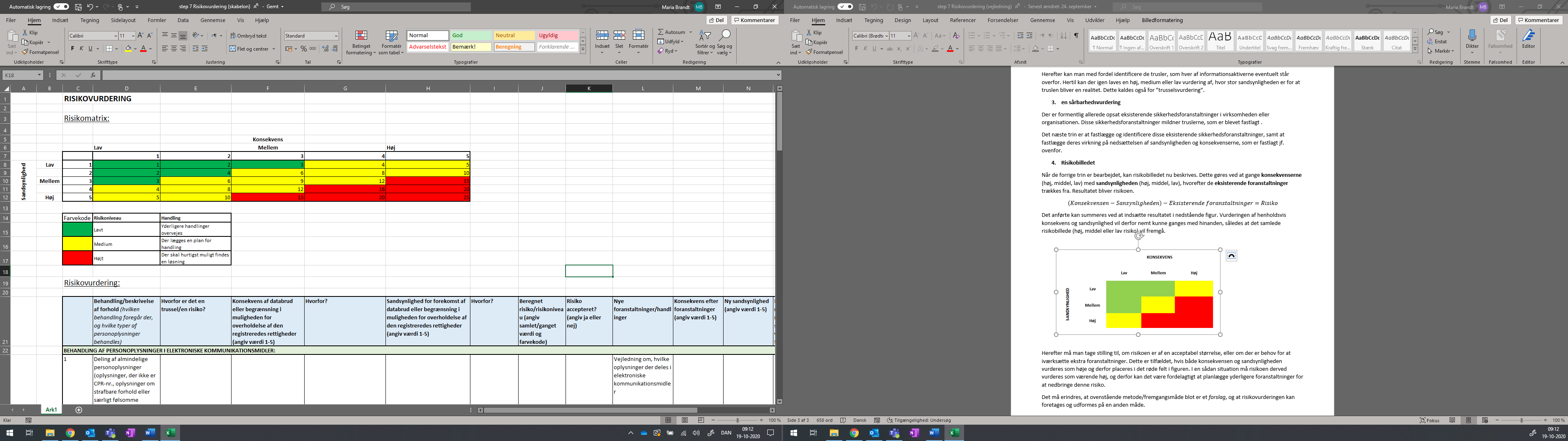
1. **Risikobilledet**

Når de forrige trin er bearbejdet, kan risikobilledet nu beskrives. Dette gøres ved at angive en værdi mellem 1-5 for **konsekvensen**, og det samme for **sandsynligheden**. 1 er lav konsekvens/sandsynlighed og 5 er høj konsekvens/sandsynlighed (jf. nedenstående risikomatrix). Herefter ganges de to tal:

*Konsekvens x sandsynlighed = risiko*

Du har nu en risiko på mellem 1 og 25. Nedenstående risikomatrix definerer om din samlede risiko for den enkelte trussel er lav, mellem eller høj.

Risikomatrix:



Herefter må man tage stilling til, om risikoen er af en acceptabel størrelse, eller om der er behov for at iværksætte ekstra foranstaltninger. Dette kan være tilfældet, hvis både konsekvens og sandsynlighed vurderes som høje og derfor placeres i det røde felt i figuren. I en situation, hvor risikoen vurderes som værende høj, kan det være fordelagtigt at planlægge yderligere foranstaltninger for at nedbringe denne risiko. De nye foranstaltninger beskrives i risikovurderingen, og der beregnes herefter en ny risiko. Den nye risiko beregnes på samme vis som ovenstående.

Det må erindres, at ovenstående metode/fremgangsmåde blot er et *forslag*, og at risikovurderingen kan foretages og udformes på en anden måde.