Hvornår er sikkert sikkert nok?
Pragmatisk metode til vurdering af risici

Datatilsynet og Rådet for Digital Sikkerhed udgiver vejledende tekst om risikovurdering, som præsenterer en pragmatisk metode, som de fleste små og mellemstore virksomheder let vil kunne benytte sig af.

GDPR introducerede princippet om ansvarlighed, forstået på den måde, at ansvaret for korrekt og sikker behandling af persondata i høj grad uddelegeres til de dataansvarlige. Det gør det muligt for de dataansvarlige at sørge for sikkerhedsniveauer, der passer til de forskellige persondata: ikke unødigt sikkert, ikke for usikkert.

Et fornuftigt og letforståeligt princip, som det dog kan være mere besværligt at føre ud i livet: For hvordan vurderer man, hvornår sikkert er sikkert nok? Og hvis der er flere typer persondata og flere systemer, hvordan skaber man så overblik?

Datatilsynet og Rådet for Digital Sikkerheds vejledende tekst om risikovurdering præsenterer en pragmatisk metode, som de fleste små og mellemstore virksomheder let vil kunne benytte sig af. Her følger en kort introduktion til metoden, som er todelt:

1. Risici kortlægges og kvantificeres ved en risikofaktor – og bliver derved sammenlignelige
2. Risici håndteres – og risikofaktoren genberegnes.

Simpel opskrift på kortlægning af risici

Start med at identificere og liste de processer og it-systemer, som behandler persondata; det som i denne terminologi kaldes **informationsaktiver**. Det kan f.eks. være CRM-system, økonomisystem og HR-system. Du kan med fordel anvende et regneark, f.eks. den skabelon, som stilles til rådighed i artiklen.

For hvert informationsaktiv gennemgås som minimum disse:

1. Risiko, som beskrives ud fra, hvad der kan påvirke personoplysningernes
   - Fortrolighed – beskyttelse mod uautoriseret adgang eller videregivelse
   - Tilgængelighed – er autoriserede personer sikre på at kunne tilgå data?
   - Integritet – beskyttelse mod uautoriseret ændring eller ødelæggelse.

2. Konsekvens
   - Beskriv med ord, hvad konsekvensen er, hvis informationsaktivet mister fortrolighed, tilgængelighed eller integritet
   - Angiv, hvor alvorlige konsekvenserne er på en selvvalgt skala, f.eks. 1 – 5, hvor den mest alvorlige konsekvens kunne være, at virksomhedens eksistens er truet, f.eks. hvis man risikerer en stor GDPR-bøde.

3. Sandsynlighed
   - Beskriv med ord, hvor sandsynligt det er, at risikoen faktisk vil finde sted. Tag højde for de sikkerhedstiltag, der allerede er sat i værk, for de er naturligvis med til at mindske sandsynligheden
   - Angiv sandsynligheden på en selvvalgt skala, f.eks. 1 – 5, hvor 1 er "usandsynlig", og 5 er "vil blive udnyttet".

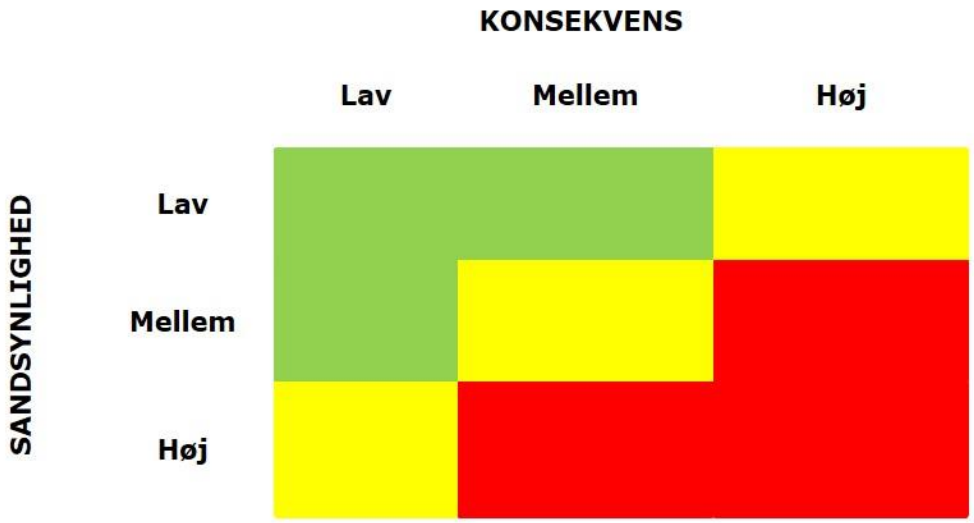
4. Beregnet risiko
   - For hvert informationsaktiv beregnes nu risikofaktoren ved at gange værdien for konsekvens med værdien for sandsynlighed
   - Hvis du har brugt 5-skalaen, vil risikofaktoren kunne ligge mellem 1 og 25.

Håndtering af risici

Der er ikke nogen gylden regel for, hvornår risikofaktorer er så høje, at der skal gøres noget. Det er op til den enkelte virksomhed og især virksomhedens ledelse at lægge sig fast på, hvor store risici man er villig til at acceptere. Når I har haft den diskussion, kan I med fordel lave jeres egne tommelfingerregler for, hvordan I håndterer forskellige niveauer af risici.

Eksempelvis kan I bruge en kombination af tal og farvekoder:

- Grøn 1 – 5: Risikoen kan uden videre accepteres
- Gul 6 – 10: Her vurderer man, typisk ledelsen, fra sag til sag, om der skal gøres noget
- Rød over 10: Her skal der altid gøres noget for at håndtere risikoen.



Når de kritiske risici er håndteret, går man tilbage til start og laver en ny risikovurdering, hvis resultat ledelsen bør orienteres om og sige god for.

En tilbagevendende øvelse og vigtig dokumentation

Risikovurderingen er noget, man regelmæssigt kommer tilbage til, f.eks. en gang om året eller efter behov, hvis der sker ændringer eller opdateringer i virksomhedens informationsaktiver, eller trusselsbilledet ændrer sig.

Det er vigtigt at italesætte risikovurderingen som en naturlig og nødvendig del af virksomhedens daglige drift, fordi den er med til at skabe indsigt i og opmærksomhed om forhold, som ikke nødvendigvis springer i øjnene, men som i yderste konsekvens kan have meget negative konsekvenser.

Endelig er risikovurderingen også god dokumentation for de valg, man som dataansvarlig har truffet, f.eks. hvis Datatilsynet skulle komme på besøg, eller hvis kunder, medarbejdere eller andre interessenter søger indsigt i, hvordan man behandler deres personoplysninger.

Læs mere om EU's databeskyttelsesforordning på vores hjemmeside via dette LINK.

Tilmeld en kollega til Beierholms nyhedsmail via dette LINK