Indhold

[1. Indhold 1](#_Toc38956520)

[2. Introduktion 1](#_Toc38956521)

[3. Målgruppe 1](#_Toc38956522)

[4. Hvad skal risikovurderes? 1](#_Toc38956523)

[5. Hvordan udføres risikovurderingen? 2](#_Toc38956524)

[6. Eksempler på risici 2](#_Toc38956525)

[6.1 Fanen ”Hjælpeværktøj” 2](#_Toc38956526)

[6.2 Eksempler på risici 2](#_Toc38956527)

[7. Supplerende materiale 2](#_Toc38956528)

# Introduktion

Denne institutionelle anvisning definerer håndteringen af risikovurderinger på DMJX. Risikovurderinger er typisk kendt fra it-sikkerhed, hvor DMJX vurderer *sin risiko* for fx et systemnedbrud, produktionstab og lignende. I en persondatamæssig er metoden den samme, men her vurderer DMJX *de registreredes risiko*.

Målet med anvisningen er både at definere håndteringen af risikovurderingerne på DMJX, men også at skabe klarhed. Derfor vil anvisningen blive opdateret løbende. Det betyder, at du altid skal finde og følge den seneste opdaterede anvisning.

# Målgruppe

De primære målgrupper for anvisningen er GDPR-koordinatorer, forskere eller projektansvalige. Forholdet mellem GDPR og anden lovgivning er et vanskeligt tilgængeligt område, og i langt de fleste tilfælde vil der fortsat skulle tages stilling til sletning eller dataminimering ved den konkrete behandlingsproces. Dataminimering eller evt. frist for sletning skal derfor fastsættes i dialog med GDPR-teamet.

# Hvad skal risikovurderes?

Alle de behandlingsaktiviteter, der skal laves fortegnelser på, skal der også laves risikovurderinger på. Dvs. **indsamling** af data eks. ved spørgeskema, interview, høstning af data eller andre datakilder. **Opbevaring** og behandling af data eks. i statistikprogram, interviewlydfil.

# Hvordan udføres risikovurderingen?

Du udfører risikovurderingen på følgende måde:

1. Hent skabelonen for risikovurdering
2. Gem den på rette placering hvor diu opbevare dine projektdokumenter
3. Udfyld risikovurderingen – se og følg anvisningen i feltet ”Guide” i skemaet (se evt. det følgende afsnit 5, hvor du kan hente inspiration i hvilke risici, der typisk kan være).
4. Sørg for at iværksætte nye tiltag på de risici, som er enten gule eller røde – og sørg for at prioritere de værste risici først. Er risikoen fortsat rød (høj), så skal du kontakte DMJX’s DPO.
5. Har du spørgsmål så kontakt DMJX’s DPO dpo@dmjx.dk

# Eksempler på risici

Se excelark for ricisikovurdering

## Fanen ”Hjælpeværktøj”

I regnearket for risikovurdering kan du under fanen ”Hjælpeværktøj” få lidt støtte til at identificere trusler/risici for din behandlingsaktivitet. Du bruger de forskellige tabeller til at spørge: ”Hvordan kan et menneske ’indefra’ ved et ’uheld’ gøre noget, der resulterer i ’brud på fortroligheden’ ved hjælp af ’tekniske midler’? Dette kunne fx være ”Sende mail til forkert modtager”, ”Give for vid adgang til dine forskningsdata. Eks studerende”, ”Offentliggøre forskningsrapport uden at have anonymiseret personoplysninger tilstrækkeligt”.

## Eksempler på risici

Alle behandlingsaktiviteter er forskellige, så der er derfor ikke muligt at lave en udtømmende liste med risici/trusler. Her er dog nogle eksempler, du kan lade dig inspirere af:

1. Tab/deling af adgangskode
2. Tildele uvedkommende adgang til persondata
3. Sende uvedkommende data
4. Placering af persondata i gratis it-værktøjer
5. Utilstrækkelig anonymisering af data, hvis anonymisering var påkrævet.
6. Hacking
7. Phishing
8. Tab af hardware
9. Indbrud

# Supplerende materiale

Datatilsynets introduktion til risikovurderinger: <https://www.datatilsynet.dk/emner/persondatasikkerhed/risikovurdering/>

Datatilsynet vejledning om risikovurderinger: <https://www.datatilsynet.dk/media/7900/vejledende-tekst-om-risikovurdering.pdf>