

Revisionshistorik			
Version	Note	Dato	Redigeret af
v.1.00		25-05-2018	LU

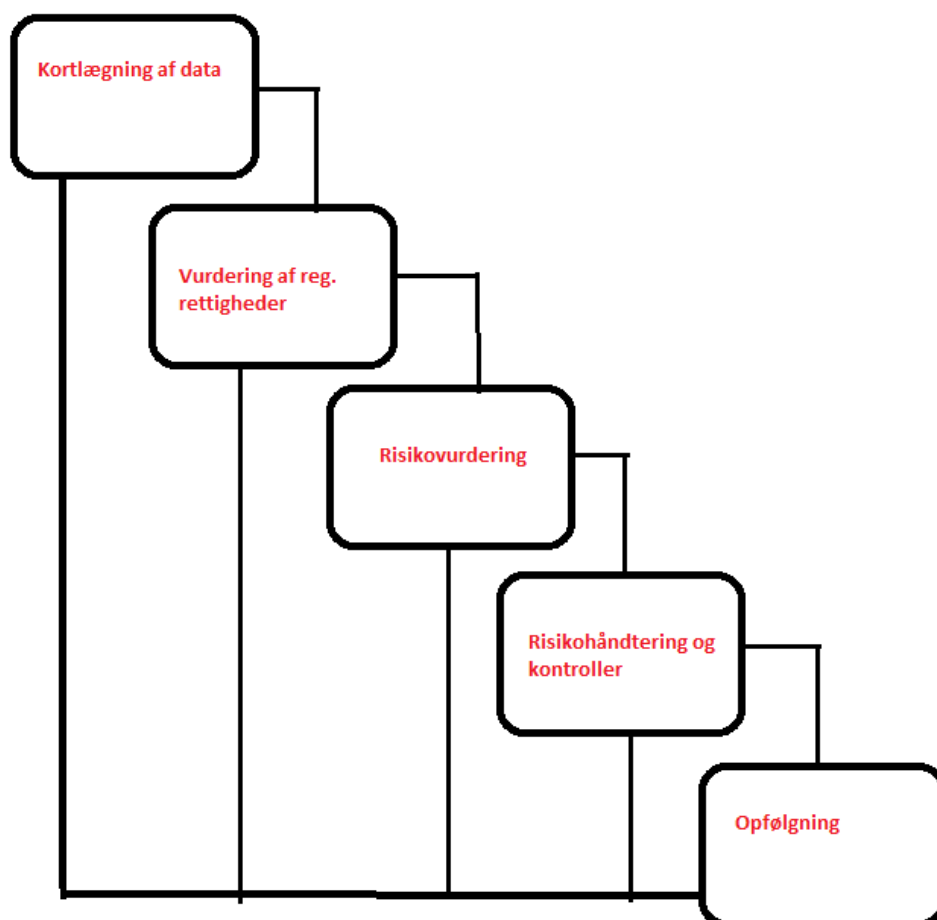
Retningslinjer om risikovurdering

En traditionel risikovurdering gennemføres ud fra den dataansvarliges eller systemansvarliges synspunkt. I en risikovurdering efter databeskyttelsesforordningen måles risikoen ved at bedømme, hvor stor sandsynlighed der er for, at en hændelse indtræffer, samt hvor store konsekvenser hændelsen kan have for den registrerede person og Vordingborg Gymnasium & HF. Det er den registrerede person, der er hovedfokus i denne risikovurdering.

En risikovurdering er således en vurdering af hvilke risici, der er forbundet med en konkret databehandling. Ud fra den foretagne risikovurdering kan Vordingborg Gymnasium & HF gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerheds-niveau, der passer til de identificerede risici.

En risikoanalyse er tilmed et øjebliksbillede. Man får et indblik i, hvordan verden ser ud på det tidspunkt, hvor man gennemfører risikoanalysen.

Nedenfor ses en illustration af hele processen bag en risikovurdering.



Hvordan gør vi?

Når Vordingborg Gymnasium & HF foretager en risikovurdering, tager vi udgangspunkt i

- *Fareidentifikation*: En identifikation af hvilke hændelser, der kan ramme den registrerede.
- *Eksponeringsvurdering*: En vurdering af, hvor eksponeret Vordingborg Gymnasium & HF er for at blive påvirket af en bestemt hændelse i relation til den konkrete databehandling.

En risikovurdering skal udføres af de personer, som har den nødvendige faglige indsigt.

Hvordan håndterer vi de identificerede risici?

Hvis Vordingborg Gymnasium & HF vurderer, at der kan være risici forbundet med en databehandling, skal vi efterfølgende afgøre, hvordan vi vil håndtere de identificerede risici. Vi skal således udarbejde en handlingsplan.

Der er som udgangspunkt fire muligheder for at håndtere risici:

1. Acceptér (risikoen accepteres, og der foretages ikke yderligere).
2. Flyt (den pågældende behandling flyttes – eksempelvis til et andet system).
3. Undgå (risikoen undgås ved at stoppe eller ændre den aktivitet, som er årsag til risikoen).
4. Kontrollér (risikoen kontrolleres ved at indføre foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne).

Det handler således om at prioritere og vælge sikkerhedsforanstaltninger, således vi nedbringer risici til et niveau, som er acceptabelt for såvel den registrerede som for skolen.

Formkrav

For at kunne overholde vores dokumentationsforpligtelse udfører vi risikovurderingen i skriftlig form.

Risikovurderingen opbevares sammen med øvrig behandlings dokumentation.

Kontrol og dokumentation

Vordingborg Gymnasium & HF skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes.

Vordingborg Gymnasium & HF skal kunne dokumentere (påvise):

- At vi foretager den fornødne risikovurdering, når vi igangsætter en behandling af personoplysninger
- At vi revurderer risikovurderingen, hvis behandlingen af personoplysninger ændrer karakter.
- At vi mindst én gang årligt gennemgår risikovurderingen
- At den løbende kontrol med denne retningslinje overholdes

Bilag 1 – Risikovurderingsskema

	Forekomst næsten usandsynlig	Forekomst mindre sandsynlig	Forekomst sandsynlig	Forekomst meget sandsynlig
Ingen konsekvens				
Lille konsekvens				
Moderat konsekvens				
Alvorlig konsekvens				

Farvekode	Risikoniveau	Handling
	Lavt	Yderligere handlinger overvejes
	Medium	Der lægges en plan for handling
	Højt	Der skal hurtigst muligt findes en løsning

Bilag 2 –risikovurderinger, der skal udføres

- **Personaleadministration**, herunder ansættelse, løn, fravær og klagesager
- **Elevadministration**, herunder fravær, forældre/værger, optagelsesproces og klagesager.
- **Ansattes behandling af personoplysninger**, særligere undervisere.
- **Eksamensadministration**
- **Studievejledning**