Sikkerhedsgruppen

# Arbejdsgang for risikovurdering

Der skal foretages en risikovurdering, når:

* Vi indkøber et nyt IT-system, som skal indeholde personoplysninger
* Når vi tager ny teknologi i brug (det kan fx være, at en del af arbejdsgangen bliver digital eller automatiseret)
* Når vi starter et nyt projekt eller på anden måde påbegynder en ny type behandling af personoplysninger
* Når vi ændrer arbejdsgange, hvis det kan have betydning for risikoen for den registrerede
* Hvis der indføres væsentlige ændringer i et af kommunens IT-systemer, herunder hvis data flyttes til et land uden for EU.

Omfanget samt følgerne af risikovurderingen afhænger af, hvilke typer af personoplysninger der skal beskyttes samt, hvilken af de ovenstående ændringer, der er tale om. Som udgangspunkt vil der kræves indføring af tekniske- og organisatoriske foranstaltninger, når der behandles følsomme- og/eller fortrolige personoplysninger, uanset hvilken af ovenstående ændringer, der foretages.

**Risikovurdering ”in a nutshell”**

Risikotal er sandsynlighed for at en trussel sker, gange konsekvensen for det sker.

R= S \* K

**Eksempel:**

En lejlighed har en dør uden lås. Den skal risikovurderes i forhold til truslen indbrud.

**Konsekvensen** er meget stor ved indbrud, det giver jeg tallet **5** ud af 5.

**Sandsynligheden** for indbrud sættes til **4** ud af 5 (hvis jeg boede et andet sted ville sandsynligheden enten være større eller mindre).

Risikoen for indbrud er derfor = **20 (4\*5)**

Jeg vurderer at risikoen er for høj.

Jeg laver en handleplan med tekniske tiltag, og organisatoriske tiltag.

Som teknisk tiltag sættes en lås i døren.

Som organisatorisk tiltag taler vi med alle i husstande om at låse døren, og tjekke den er låst.

Efter de mitigerende tiltag er lavet er sandsynligheden ændret fra 4 til **2**. Konsekvensen for indbrud er stadig **5**

Risikoen er nu = **10** (2\*5)

Risikoen på 10 bliver nu accepteret.

Risikovurderingen foretages efter nedenstående procedure.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Opgave** | **Beskrivelse** | **Henvisning/Værktøjer** | **Udførende** | **Ansvarlig** | **Rådgivende** | **Informeret** |
| **Opstart** | System-/procesejer kontakter informationssikkerhedsgruppen med henblik på, at der udarbejdes en risikovurdering. Dette gøres ved at oprette en sag om ”nyindkøb eller genanskaffelse af IT-teknologi eller digitale løsninger” på IT-serviceportalen.  Hvis der er tale om risikovurdering af et system, som allerede er taget i brug, bør risikovurderingen påbegyndes så snart man bliver opmærksom på det. I øvrigt følges proceduren som var det et nyt system. |  | System-/procesejer | System-/procesejer |  | Informationssikkerhedsgruppen |
| **Organisering** | Informationssikkerhedsgruppen kontakter system-/procesejer og giver information om, hvem der kan understøtte risikovurderingen samt information om, hvordan risikovurderingen kommer til at foregå.  Hvis der er behov for, at system-/procesejer forbereder eller leverer noget, får de ligeledes besked om dette. Herved kan system-/procesejeren indkalde de relevante deltagere til et møde, hvor risikovurderingen kan udføres. |  | Informationssikkerhedsgruppen | Informationssikkerhedsgruppen |  | System-/procesejer |
| **Risikovurdering** | Ved risikovurderinger kan Ishøj Kommunes værktøj til risikovurdering bruges. Værktøjet er et Excel ark, hvor der er angivet forskellige trusler. Ud fra en dialog mellem informationssikkerhedsgruppen og fagområdet tilføjes evt. øvrige trusler, som er relevante i det konkrete tilfælde.  Ud fra hver trussel angives sandsynlighed samt konsekvens, så man finder risikotallet. Hvis risikotallet er grønt, er niveauet acceptabelt. Hvis risikotallet er gult, skal risikoen overvåges eller mitigeres (dvs. nedsættes). Hvis risikotallet er rødt, skal der iværksættes foranstaltninger, som mitigerer risikoen. | Retningslinje for risikovurdering og konsekvensanalyse  Ishøj Kommunes værktøj til risikovurdering | System-/procesejer  &  Informationssikkerhedsgruppen | System-/procesejer |  |  |
| **Risikotal** | Når du har foretaget en risikovurdering, vil du få et risikotal. Risikotallet er det tal, der udtrykker, om personoplysningerne er beskyttet tilstrækkeligt. Risikotallet skal vurderes mod Ishøj Kommunes beslutning omkring risikotolerance jf. retningslinjer for risikovurdering og konsekvensanalyse. | Retningslinje for risikovurdering og konsekvensanalyse  Ishøj Kommunes værktøj til risikovurdering | System-/procesejer  og  Informationssikkerhedsgruppen | System-/procesejer |  |  |
| **Foranstaltninger** | På baggrund af risikovurderingen beslutter system-/procesejeren, hvilke foranstaltninger der skal iværksættes for at nedsætte risici samt hvilke risici, system-/procesejer er villig til at acceptere.  **Grøn (<5)**  Hvis risikotallet er grønt, behøver man som udgangspunkt ikke at beskytte oplysningerne yderligere.  **Gul (6-8)**  Ved en mellem risiko vurderer ledelsen fra gang til gang, om man kan acceptere risikoen eller om man vil gøre noget for at nedbringe den, eksempelvis ved at indføre ekstra foranstaltninger.  **Rød (>8)**  Hvis risikotallet er højt, skal risikoejer iværksættes mitigerende foranstaltninger, som nedsætter risikoen.  **Risikoejer**  System- eller procesejer er risikoejer. Det betyder, at det er system- eller procesejer, som efterfølgende skal beslutte, hvilke foranstaltninger der skal iværksættes for at beskytte personoplysningerne samt, hvilke risici området er villige til at acceptere.  Hvis system-/procesejer accepterer en høj risiko (9 eller derover) efter der er foretaget mitigerende foranstaltninger, skal områdets centerchef samt sikkerhedsgruppen orienteres om risikoen samt bevæggrundene for beslutningen, og der skal foretages en konsekvensanalyse. | Retningslinje for risikovurdering og konsekvensanalyse | System-/procesejer |  | DPO |  |
| **Konsekvensanalyse** | Hvis risikovurderingen viser, at der er en høj risiko for de registrerede forbundet med behandlingen, skal der – udover risikovurderingen – også udarbejdes en konsekvensanalyse, som også kaldes en DPIA (data protection impact assessment).  I konsekvensanalysen går man i dybden med konsekvenserne for de registrerede og mulige foranstaltninger for at mindske risikoen. Hvis det ikke er muligt at mindske risikoen for de registrerede, skal man søge Datatilsynet om tilladelse til at udføre behandlingen.  Det er et krav i GDPR, at kommunens databeskyttelsesrådgiver (DPO) inddrages i forbindelse med konsekvensanalyser. | Retningslinje for risikovurdering og konsekvensanalyse | System-/procesejer  &  DPO | System-/procesejer |  |  |
| **Journalisering** | Den samlede risikovurdering samt tilhørende beslutninger om håndtering af risici journaliserer på IT-systemet sag i SBSYS. | Retningslinje for risikovurdering og konsekvensanalyse | System-/procesejer | System-/procesejer |  |  |
| **Årlig gennemgang af risikovurderinger** | Risikovurderinger bør gennemgås årligt for at sikre, at personoplysningerne fortsat er beskyttede. Hvis risikobilledet har ændret sig, kan det være nødvendigt at introducere nye foranstaltninger. | Retningslinje for risikovurdering og konsekvensanalyse | System-/procesejer | System-/procesejer |  |  |

# Procesdiagram for risikovurdering