Retningslinje om risikovurdering

Indhold

Anvendelsesområde

Retningslinje om risikovurdering er udarbejdet i overensstemmelse med kravene i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (betegnet "forordningen" i det følgende) – gældende for alle ansatte på SOSU Esbjerg, der behandler personoplysninger.

Formål

Formålet med denne retningslinje er at sikre, at SOSU Esbjerg foretager den fornødne risikovurdering ved behandling af personoplysninger.

Definitioner

Personoplysninger er enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som fx et navn, et identifikationsnummer, lokaliseringsdata, eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Den registrerede er den fysiske person, som personoplysningerne vedrører, fx medarbejdere, elever, kursister, leverandører, samarbejdspartnere og andre.

Behandling af personoplysninger skal fortolkes bredt. Begrebet "behandling" dækker over enhver aktivitet eller en række af aktiviteter, som personoplysninger gøres til genstand for. Det kan fx være indsamling, registrering, organisering, systematisering, opbevaring, ændring, søgning, formidling og sletning.

Almindelige/fortrolige personoplysninger er alle oplysninger om en identificeret eller identificerbar person, der ikke er omfattet af nedenstående kategori, fx navn, adresse, CPR-nummer, e-mail, billeder, telefonnummer.

Følsomme personoplysninger er oplysninger om helbredsforhold, fagforening, racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, seksuelle forhold og genetiske oplysninger. Der er tale om en udtømmende liste.

Dataansvarlig er den person eller myndighed/organisation, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Databehandler er den, der behandler personoplysninger på den dataansvarliges vegne – dvs. arbejder under instruks af den dataansvarlige. Databehandler er i henhold til forordningen forpligtet til at føre fortegnelse over behandlingskategorier, der føres på vegne af den dataansvarlige.

Databeskyttelsesrådgiveren (DPO) er en uafhængig person med ekspertise i databeskyttelsesret og –praksis, der skal inddrages i alle spørgsmål om databeskyttelse og rådgive om de databeskyttelsesretlige regler på SOSU Esbjerg. Databeskyttelsesrådgiverens funktion er at understøtte, at SOSU Esbjerg overholder reglerne i forordningen. Databeskyttelsesrådgiveren er ansat ved IT Center Fyn og via kontrakt tilknyttet SOSU Esbjerg som DPO.

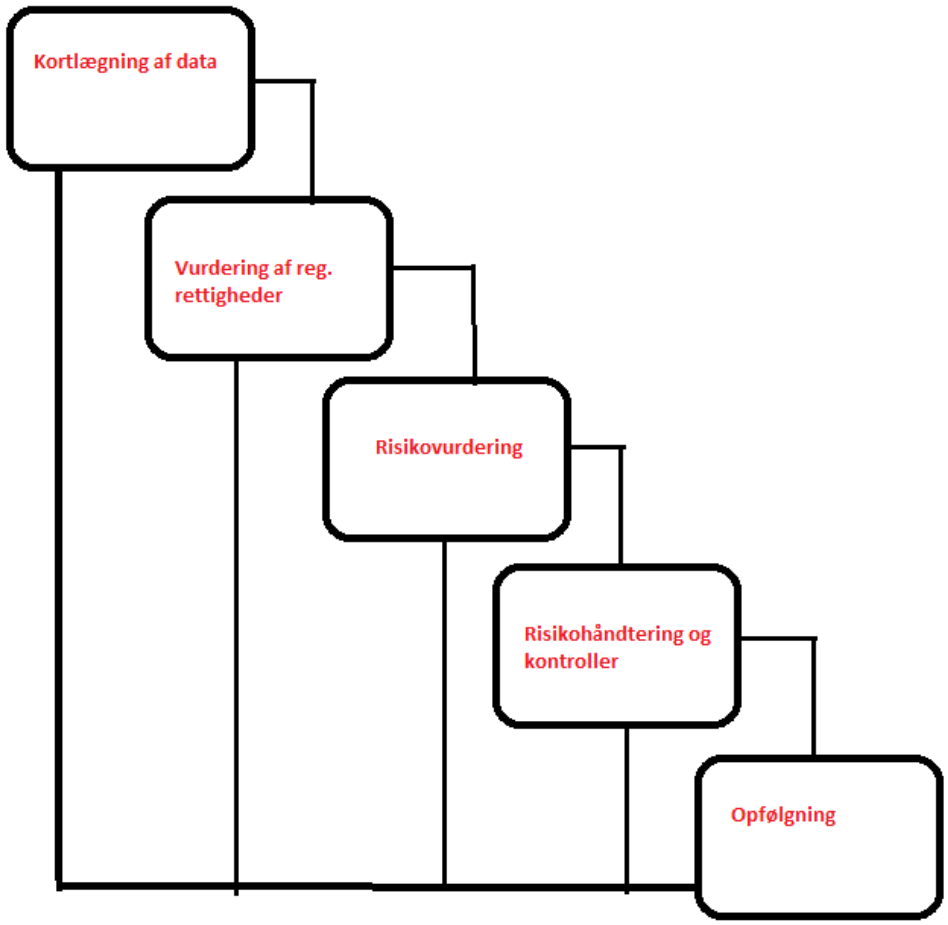
Hvad er en risikovurdering?

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 SOSU Esbjerg. 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 SOSU Esbjerg gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, 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 SOSU Esbjerg foretager en risikovurdering, tager vi udgangspunkt i:

***Fareidentifikation*:** En identifikation af, hvilke hændelser der kan ramme den registrerede.

***Eksponeringsvurdering*:** En vurdering af, hvor eksponeret SOSU Esbjerg er for at blive påvirket af en bestemt hændelse i relation til den konkrete databehandling.

Ad. Fareidentifikation

Fareidentifikationen skal vurderes ud fra den konkrete databehandling.

Eksempelvis:

Ved anvendelse af system "X " til behandling af HR-oplysninger, er der risiko for, at cpr. nr. lækkes.

Ad. Eksponeringsvurdering

Eksponeringsvurderingen skal give et indtryk af, hvor eksponeret SOSU Esbjerg er, for at ovenstående hændelser vil indtræde.

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

Hvordan håndterer vi de identificerede risici?

Hvis SOSU Esbjerg 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 – fx 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/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 behandlingsdokumentation.

Kontrol og dokumentation

SOSU Esbjerg skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af Direktør Lisbeth Nørgaard på vegne af bestyrelsen på SOSU Esbjerg.

SOSU Esbjerg skal kunne dokumentere og hermed 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

Der henvises i øvrigt til *"Procedure for intern GDPR-audit"*

Dokumentejer, godkender og versionering

Ejer: Claus Larsen

Godkender: Direktør Lisbeth Nørgaard

Dato	Version	Forfatter	Ændringsbeskrivelse
19. februar 2020	1.1	BEK	I afsnittet Kontrol og dokumentation, henvises der til "Procedure for intern GDPR-audit"
13. august 2018	1.0	BEK	-