Utdannings-
direktoratet

Veiledning for risikovurdering ved en DPIA

Når du skal gjennomføre en risikovurdering ved en DPIA, skal du beskrive risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å håndtere risikoene.

ARTIKKEL | SIST ENDRET: 09.12.2021

De registrertes rettigheter og friheter kan være retten til privatliv, ytringsfrihet, tanke-, tros- og religionsfrihet, og retten til ikke å bli diskriminert. At den registrerte ikke har mulighet til å utøve sine rettigheter, har manglende kontroll over bruken av personopplysninger, utsettes for diskriminering, svindel, ID-tyveri, økonomiske tap, tap av omdømme eller annen betydelig økonomisk eller sosial ulempe er eksempler på at rettighetene og frihetene ikke er godt nok ivaretatt.

Dersom det er sannsynlig at en behandling vil medføre en høy risiko for personers rettigheter og friheter, skal behandlingsansvarlig gjøre en DPIA før behandlingen starter. Dette gjelder særlig ved bruk av ny teknologi, og det skal her tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.

Risikoen skal være spesifikk for behandlingen DPIAen gjelder for.

For å gjøre risikovurderingen i en DPIA kan du bruke vedlagte Excel-mal.

Slik gjør du det

- Identifiser trusler som kan føre til uønskede hendelser og hvordan disse kan skje. Dette skal du gjøre ut fra den registrertes perspektiv
- Anslå alvorlighetsgraden for hver risiko, særlig ut fra hvordan en eventuell hendelse vil påvirke den registrerte

- Anslå sannsynligheten for at en hendelse skjer
- Beskriv iverksatte tiltak for å redusere risikoen for en hendelse, og nye tiltak for å redusere risiko

Eksempler på trusler

Manglende reell åpenhet

Manglende reell åpenhet kan for eksempel være at virksomheten ikke gir informasjon, eller ikke klarer å forklare behandlingene de gjør med personopplysningene.

Eksempler på risikoer

- dere gir ikke den registrerte regelmessig informasjon om behandlingen
- dere gir ikke forståelig og fullstendig informasjon om hva personopplysningene brukes til, og om dataflyt
- dere gir ikke den registrerte informasjon om sikkerhetsbrudd
- dere gir ikke den registrerte tilstrekkelig informasjon om sikkerhetstiltakene for å beskytte personopplysningene, eller om programvare eller algoritmer som benyttes

Manglende forutsigbarhet

Manglende forutsigbarhet ved behandlingen kan for eksempel være at behandlingen er utenfor det den registrerte forventer.

Eksempler på risikoer

- dere forteller ikke på en fullstendig eller forståelig måte hvilket formål dere har med behandlingen
- dere gir ikke klar eller tilstrekkelig informasjon om hvorfor en person er utvalgt hvis dere registerer personopplysninger til forskning
- dere følger ikke prinsippet om dataminimering
- dere følger ikke reglene om sletting av personopplysningene

Manglende reell medbestemmelse

Manglende reell medbestemmelse handler om at den registrerte for eksempel ikke får informasjon eller innsyn.

Eksempler på risikoer

- dere bruker innsamlet informasjon til andre formål enn det den registrerte har samtykket til
- dere gir ikke innsynsmuligheter til den registrerte, og den registrerte får ikke reell mulighet til retting, sletting eller tilbaketrekking av samtykke

Eksempel på tiltak

Velg tiltak for å håndtere risikoene for de registrertes rettigheter og interesser. Identifiser eller bestem hva slags tiltak som kan håndtere/minimere risikoene.

Generelle tiltak kan typisk være

- krav om fornyet samtykke
- innhenting av registrertes syn på behandlingen
- forsterket informasjon, som løpende informasjon, informasjon i flere kanaler, eller spesifikk informasjon om kobling mellom datasett og resultat av kobling
- særskilt tilrettelagt innsynsportal
- særskilte dataminimeringstiltak, som monitorering bare i bestemte tidsrom eller spesifikke områder, øyeblikksbilder istedenfor kontinuerlig monitorering, eller å avstå fra behandling av spesifikke opplysninger
- tilrettelegging for dataportabilitet
- automatisk sletting eller anonymisering
- hindre kobling mellom datasett

Spesifikke sikkerhetstiltak for personopplysninger kan være

- kryptering
- anonymisering
- tilgangskontroll
- sporbarhet

Generelle sikkerhetstiltak for systemet der dere utfører behandlingen kan være

- operativ sikkerhet
- backup
- sikkerhet på hardware
- teknisk og fysisk sikring

Organisatoriske tiltak kan være

- policy
- rutiner
- prosjektledelse
- personellhåndtering og opplæring
- håndtering av hendelser og brudd
- forhold til tredjeparter

Ut fra tiltakene må dere avgjøre om de identifiserte risikoene er håndtert og akseptable. Hvis ikke må dere foreslå ytterligere tiltak og revurdere nivået for hver risiko i lys av de nye tiltakene for å fastslå restrisiko.