KONFIDENSIELT
RISIKOVURDERING
PESONOPPLYSNINGSLOVEN
FOR

_____

Vi har i det følgende dokumentert at virksomheten har foretatt en vurdering for å identifisere risiko for uønskede hendelser som kan ha betydning for personvernet i forbindelse med den behandling som foretas av personopplysninger. Risikovurderingen vil bli løpende oppdatert.

Risikovurdering er en kartlegging av risikofaktorer og hvilken sannsynlighet det er for at disse kan inntreffe. Tre enkle spørsmål er kjernen i risikovurderingen: Hva kan gå galt? Hva er sannsynligheten for at det kan inntreffe? Hva er konsekvensen hvis det inntreffer? I etterkant av denne vurderingen, bør følgende spørsmål stilles: Hva kan gjøres for å hindre det/redusere risikoen? Hva kan gjøres for å redusere følgene dersom det skjer?

Vår risikovurdering foretas i 4 trinn:

Trinn 1: Kartlegging som av alle mulige risikofaktorer
Tenk gjennom nøye hva som kan være risikofaktorer: For eksempel: Hvem kan legge inn data i systemet – hvem har innsyn i data - er rutiner for bruk av systemet gode nok (eksempel utlevering av data) og godt nok dokumentert?

Trinn 2: Sannsynlighet og konsekvens
Vi skal vurdere hver risikofaktor i forhold til hvor sannsynlig det er at noe går galt. Er det noe som kan skje ofte, en sjelden gang eller er det svært lite sannsynlig? En mulig inndeling av sannsynlighet er:

- Meget liten: Hendelsen inntreffer 1 gang pr. 50. år eller sjeldnere.
- Liten: Hendelsen inntreffer 1 gang pr 10. år eller sjeldnere.
- Moderat: Hendelsen inntreffer årlig eller sjeldnere.
- Stor: Hendelsen inntreffer flere ganger i året.
- Svært stor: Hendelsen inntreffer en gang i uka eller oftere.

Hva vil konsekvensen være dersom noe går galt? Noen utfall vil være mer alvorlige enn andre. En mulig inndeling av konsekvens er:

- Ubetydelig: Hendelsen kan medføre mindre avvik fra interne anbefalinger om behandlingen, men ikke brudd på regelverk
- Liten: Hendelsen kan medføre avvik fra interne rutiner – men ikke brudd på regelverk
- Moderat: Hendelsen kan medføre betydelig avvik fra interne rutiner, men ikke dirkete brudd på regelverk.
- Alvorlig: Hendelsen kan medføre avvik fra regelverk og/eller at personopplysninger kommer på avveie
- Svært alvorlig: Hendelsen kan medføre alvorlig brudd på regelverk og/eller at mengder av personopplysninger og/eller sensitive personopplysninger

kommer på avvei

Konsekvens av en hendelse vil i første rekke være knyttet til brudd på interne rutiner og brudd på personopplysningsregelverket. I tillegg vil konsekvens også avhenge av hvor mange personer som berøres. Personvernkonsekvens må rangeres høyere, eksempelvis ett nivå, dersom hendelsen får følger for mange mennesker eller det er tale om sensitive personopplysninger. Dette selv om følgene for den enkeltes personvern vurderes som liten.
.
Trinn 3: Tiltak
Hensikten er å vurdere behovet for og eventuelt iverksette tiltak for å bringe risikoen ned på et akseptabelt nivå. Vi må gå igjennom listen over risikofaktorene. Følgende spørsmål kan stilles:

- Er det mulig å fjerne en gitt risikofaktor fullstendig?
- Er det mulig å redusere sannsynligheten for at det skjer?
- Hva kan gjøres for å redusere konsekvensen dersom det skjer?
- Er lover, forskrifter og interne retningslinjer fulgt?
- Skriv ned aktuelle tiltak for hver av risikofaktorene som er avdekket.

Eksempel på tiltak kan være: Fysisk sikring av data - klar ansvarsfordeling – bedre rutinebeskrivelser – endring i IT-infrastruktur.

Trinn 4: Videre arbeid
Alle tiltakene som er opplistet i risikovurderingen, kan sannsynligvis ikke gjennomføres med en gang. Det bør settes opp en prioritert liste over det som må gjøres, slik at tiltak kan følges opp i prioritert rekkefølge. Det er viktig at det framgår tydelig hva som skal gjøres, når det skal være gjort, og hvem som har ansvaret for at det blir gjennomført. En enkel handlingsplan kan settes opp.

Basert på vår risikovurdering som følger under, er det foretatt en overordnet risikovurdering for virksomheten. Konklusjonene fra gjeldende risikovurdering er følgende:

> *Dersom opplysninger skulle komme på avveie antas dette å kunne virke integritetskrenkende på den opplysningene gjelder, noe avhengig av hvilke opplysninger dette gjelder. Risikoen for at opplysninger skulle komme på avveie vurderes som relativt liten gitt at de etablerte sikkerhetsrutiner følges og at andre tekniske og fysiske sikkerhetsbarrierer fungerer som forutsatt. Det vil, som alltid, være viktig at de som har tilgang følger gjeldende rutiner, da brudd på dette kan resultere i at opplysninger kommer på avveie.*

Risikovurdering for: _____	**Gradering 1-4**	**S x K = Risiko (R)**		Forventet effekt av gjennomført tiltak (forventet ny R)		Opplevd effekt av gjennomført tiltak (faktisk ny R)

	S = Sannsynlighet for at trussel inntreffer	**K= Konsekvens** av at trussel inntreffer			Ledelsens aksept av risiko er 3 generelt sett, men kan avvike på spesielle felt etter beslutning		Etterlevelse – risikojustering basert på kontroll av etterlevelse (føres inn etter neste kontroll)	

FORHOLD OG KRAV Hva må vurderes?	**TRUSSELBESKRIVELSE** Hva kan skje, hva kan gå galt? Beskrivelse av trussel, årsak og virkning.				**MÅL/ TILTAK** Risiko ≥ X: Forebyggende / skadebegrensende Beskrivelse av mål og tiltak		**KVITTERING** Tiltak i kraft.	
• konfidensialitet	Interne uten behov får tilgang	3	1	3	Saksbehandlingssystemet kan begrense tilgang	**2**	X	
• konfidensialitet	Interne uten behov får tilgang - sensitive	3	2	6	Saksbehandlingssystemet kan begrense tilgang	**3**	X	
• konfidensialitet	Benyttes utenfor behandlingsgrunnlag (formålet)	3	2	6	Bevissthet om bruk/ formål og retningslinjer for bruk	**3**	X	
• konfidensialitet	Benyttes utenfor behandlingsgrunnlag (formålet) - sensitive	3	3	9	Bevissthet om bruk/ formål og retningslinjer for bruk	**4**	X	
• konfidensialitet	Interne uten behov får tilgang	3	1	3	Server begrenser tilgang for områder/ filer	**2**	X	
• konfidensialitet	Interne uten behov får tilgang - sensitive	3	2	6	Server begrenser tilgang for områder/ filer	**3**	X	
• konfidensialitet	Eksterne får tilgang	2	3	6	Systemet tilgangsbeskyttet med brukernavn/ passord	**2**	X	
• konfidensialitet	Eksterne får tilgang - sensitive	2	4	8	Systemet tilgangsbeskyttet med brukernavn/ passord	**2**	X	

•	konfidensialitet	Eksterne får tilgang	2	3	6	Krav til passord/ brukernavn på mobile enheter, samt krav til mulighet for fjernsletting	**4**	X	
•	konfidensialitet	Eksterne får tilgang - sensitive	2	4	8	Krav til passord/ brukernavn på mobile enheter, samt krav til mulighet for fjernsletting	**5**	X	
•	konfidensialitet	Eksterne får tilgang	2	3	6	Kontorlokale låst med ingen tilgang for eksterne	**1**	X	
•	konfidensialitet	Eksterne får tilgang - sensitive	2	4	8	Kontorlokale låst med ingen tilgang for eksterne. Egne rutiner for tilgangskontroll.	**2**	X	
•	integritet	Opplysningene slettes	1	3	3	Data tas back-up av løpende, forpliktelser i leverandøravtale om rekonstruksjon av data	**1**	X	
•	integritet	Opplysningene er udatert/feil	3	2	6	Rutiner om oppdatering av pasientopplysninger	**4**	X	
•	tilgjengelighet	Lagringsmedia ødelegges	1	4	4	Krav og rutiner for løpende back-up annen lokasjon. Periodisk validering av backup-medier.	**1**	X	