Vedlegg 3 til bransjestandard for personopplysningsloven

Mal for personvernkonsekvensvurdering (DPIA)

|  |
| --- |
| Hva er hensikten med malen?  En vurdering av personvernkonsekvenser skal sikre at personvernet til de registrerte blir ivaretatt.  Å gjennomføre en personvernkonsekvensvurdering skal bidra til at virksomheten:   * Håndterer risikoer behandlingen innebærer for den registrerte nå og i fremtiden (til forskjell fra risiko for den enkelte virksomhet) * Identifiserer behov for risikoreduserende tiltak * Demonstrere og dokumentere ansvarlighet ovenfor ledelsen, Datatilsynet, evt. personvernombudet og de registrerte |

Dokumentasjon og ajourhold

|  |  |
| --- | --- |
| **Grunnleggende informasjon** | |
| Tema/område/formål |  |
| Risikoeier |  |
| Vedlegg | Vedlegg 1: Beskrivelse av sannsynlighet- og konsekvensnivå  (Legg til evt andre vedlegg som kan gi utdypende informasjon) |
| Referanse til lagringssted av vurderingene og annen dokumentasjon |  |

|  |  |  |
| --- | --- | --- |
| **Deltagere** | | |
| Navn | Rolle | Enhet |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| **Eksterne deltagere** | |
| Representant for brukere |  |
| Representant for databehandler |  |
| Begrunnelse for evt. manglende involvering av eksterne: |  |

|  |  |  |
| --- | --- | --- |
| **Endringslogg** | | |
| Dato for første versjon | |  |
| Evt. dato for oppdatering | Endringer | Godkjent av eier |
|  |  |  |
|  |  |  |

1. Behandlingen av personopplysninger

|  |  |
| --- | --- |
| **Overordnet oversikt over behandlingen** | |
| Gi en kort, overordnet presentasjon av denne behandlingen. | |
| *Hvorfor behandle personopplysninger? Hva er formålet med behandlingen?* |  |
| Eventuelle avgrensninger for denne vurderingen |  |
| Gi en beskrivelse av behandlingens livsløp (steg for steg). Flytdiagram kan med fordel brukes. |  |

|  |  |
| --- | --- |
| **Behandlingens art og omfang** | |
| Hvem skal det samles inn personopplysninger om? |  |
| Hvilke kategorier av personopplysninger skal behandles?  *(Personalia, adresse/*  *kontaktinfo/Helseopplysninger/*  *Logger/økonomiske opplysninger/annet?* |  |
| Hvor mange brukere er omfattet? | (Beskriv her et ca. antall dersom dere ikke har presist antall.) |
| Hvordan er utvalget bestemt? |  |

|  |  |
| --- | --- |
| **Behandlingens nødvendighet og proporsjonalitet** | |
| * Behandlingen må være nødvendig – derfor må det vurderes kan gjennomføres på en annen eller mindre inngripende måte. * Det skal være et rimelig forhold mellom det inngrepet som gjøres i personvernet og de fordeler som oppnås ved behandlingen av personopplysninger. | |
| Beskriv vurderingene og avveiingene som er gjort: |  |

1. Relaterte krav og prosesser

|  |  |  |  |
| --- | --- | --- | --- |
| **Behandlingsoversikt** | | | |
| Er behandlingsaktiviteten allerede beskrevet i virksomhetens behandlingsoversikt? | Ja | Nei | Delvis |
| Hvis ja – gi referanse til behandlingen |  | | |
| Hvis nei eller delvis, angi hvem som sørger for å oppdatere og når dette forventes utført |  | | |

|  |  |
| --- | --- |
| **Rettslig grunnlag** | |
| For å sikre at behandlingen er lovlig, trengs en nærmere beskrivelse av det rettslige grunnlaget for den spesifikke behandlingen. | |
| Hva er det rettslige grunnlaget for denne behandlingen? |  |

|  |  |
| --- | --- |
| **Risikovurdering** | |
| Det skal gjennomføres en risikovurdering av informasjonssikkerheten tilknyttet personopplysningene, det som i personopplysningsloven kalles personopplysningssikkerheten. | |
| Referanse til relevante risikovurderinger (lenke eller vedlegg) |  |

1. Konsekvenser for den enkelte

I dette steget skal man identifisere og vurdere aktuelle personvernkonsekvenser basert på flere scenarioer. Det er viktig å ta perspektivet til de registrerte og vurdere hvordan behandlingen kan påvirke deres personvern. For inspirasjon, vises det til vedlegg 4 i Veileder og bransjestandard for personvern i energibransjen.

|  |  |  |  |
| --- | --- | --- | --- |
| **Relevante scenario** | | | |
| **Sett inn personvernscenario er vurdert som relevante i vurderingen av personvernkonsekvenser. For inspirasjon, vises det til vedlegg 4 i Veileder og bransjestandard for personvern i energibransjen.**   1. **Beskriv scenariet - tilpasset det som er relevant for den aktuelle behandlingen** 2. **Beskriv gjerne en kort begrunnelse for valgt sannsynlighets- og konsekvensnivå** 3. **Sett deretter inn fastsatt sannsynlighet- og konsekvensnivå for den aktuelle behandlingen.** | | | |
| **Nr** | **Personvernscenario** | **Konsekvens** | **Sannsynlighet** |
| **1** |  | **2** | **5** |
| **2** |  | **2** | **4** |
| **3** |  | **4** | **5** |
| **4** |  | **2** | **5** |
| **5** |  | **2** | **3** |
| **6** |  | **2** | **5** |
| **7** |  | **3** | **1** |
| **8** |  | **3** | **1** |
| **9** |  | **3** | **1** |
| **10** |  | **Velg et nivå.** | **Velg et nivå.** |
| **11** |  | **Velg et nivå.** | **Velg et nivå.** |

3.1 Risikobilde før tiltak

Plott inn hvor de ulike scenarioene vil befinne seg etter at tiltakene fra tabellen over er gjennomført. Det er dette risikobildet risikoeier må vurdere om kan akseptere eller ikke.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SANNSYNLIGHET** | Nesten sikkert |  | |  |  |  | |  |
| Sannsynlig |  | |  |  |  | |  |
| Moderat |  | |  |  |  | |  |
| Lite sannsynlig |  | |  |  |  | |  |
| Meget lite sannsynlig |  | |  |  |  | |  |
|  |  | Ubetydelig | | Lav | Moderat | Alvorlig | | Svært alvorlig |
|  |  | | **KONSEKVENS** | | | |

3.2 Tiltak

3.2.1 Tabell for risikoreduserende tiltak

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltak** | | | |
| Tabellen oppdateres etter vedlegg 1 er gjennomgått og tiltak er bestemt. | | | |
| Risikoreduserende tiltak | For hvilke(t) scenario? | Ansvarlig | Frist |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

3.2.2 Risikobilde etter tiltak

Plott inn hvor de ulike scenarioene vil befinne seg etter at tiltakene fra tabellen over er gjennomført. Det er dette risikobildet risikoeier må vurdere om kan akseptere eller ikke.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SANNSYNLIGHET** | Nesten sikkert |  | |  |  |  | |  |
| Sannsynlig |  | |  |  |  | |  |
| Moderat |  | |  |  |  | |  |
| Lite sannsynlig |  | |  |  |  | |  |
| Meget lite sannsynlig |  | |  |  |  | |  |
|  |  | Ubetydelig | | Lav | Moderat | Alvorlig | | Svært alvorlig |
|  |  | | **KONSEKVENS** | | | |

1. Avslutning

4.1 Vurdering og råd fra personvernombudet (Om virksomheten har dette)

Personvernombudet skal gi sine råd og anbefalinger for å beskytte de registrertes personvern før endelig godkjenning hos risikoeier.

|  |  |  |
| --- | --- | --- |
| **Personvernombud** | | |
| Spørsmål for personvernombudet | Tilstrekkelig? | Kommentarer |
| Personvernscenarioene slik de er beskrevet? | Ja  Nei |  |
| Risikoreduserende tiltak | Ja  Nei |  |
| Andre tilbakemeldinger |  | |
| Anbefaler personvernombudet at arbeidet går videre som planlagt? Eventuelt behov for å fremme saken til forhåndskonsultasjon til Datatilsynet? | | |
|  | | |

4.2 Endelig godkjenning

|  |  |  |  |
| --- | --- | --- | --- |
| **Endelig godkjenning** | | | |
| Vurderingen skal godkjennes av risikoeier. Eventuell restrisiko er akseptert ved godkjenning. | | | |
| Er anbefalinger fra PVO fulgt? | Ja | | Nei |
| Dersom nei, hvorfor ikke? |  | | |
| Er vurderingene av personvernkonsekvens i sin helhet godkjent? | Ja | | Nei |
| Dato |  | Signatur |  |

Beskrivelse av sannsynlighet- og konsekvensnivå

|  |  |  |
| --- | --- | --- |
| Sannsynlighetsnivå | | |
| **Nivå** | **Beskrivelse** | **Veiledning** |
| **1** | Meget lite sannsynlig | Mindre enn 10 % sannsynlig og/eller inntreffer hvert 5. år eller sjeldnere |
| **2** | Lite sannsynlig | 10-30 % sannsynlig og/eller inntreffer hvert år eller sjeldnere |
| **3** | Moderat sannsynlig | 30-60 % sannsynlig og/eller inntreffer 2-4 ganger per år |
| **4** | Sannsynlig | 60-90 % sannsynlig og/eller inntreffer månedlig |
| **5** | Nesten sikkert | Over 90 % sannsynlig og/eller inntreffer ukentlig |

|  |  |  |
| --- | --- | --- |
| Konsekvensnivå | | |
| **Nivå** | **Beskrivelse** | **Veiledning** |
| **1** | Konsekvensen for den registrertes personvern er ubetydelig | * Forbigående, mindre økonomisk tap for den registrerte * Midlertidig og begrenset tap av den registrertes omdømme * Den registrertes rett til personvern utfordres i en svært kort periode og uten å involvere særlige kategorier/sårbare grupper |
| **2** | Konsekvensen for den registrertes personvern er lav | * Midlertidige eller mindre alvorlige helsemessige konsekvenser for den registrerte * Forbigående økonomisk tap for den registrerte * Midlertidig eller begrenset tap av den registrertes omdømme * Den registrertes rett til personvern utfordres i en kort periode eller uten å involvere særlige kategorier/sårbare grupper * Den registrertes tillit til virksomheten utfordres midlertidig |
| **3** | Konsekvensen for den registrertes personvern er moderat | * Midlertidige eller noe mer alvorlige helsemessige konsekvenser for den registrerte * Økonomisk tap av noe varighet for den registrerte * Midlertidige eller noe mer alvorlige tap av den registrertes omdømme * Den registrertes rett til personvern krenkes i en større periode eller involverer særlige kategorier/sårbare grupper * Den registrertes tillit til virksomheten utfordres |
| **4** | Konsekvensen for den registrertes personvern er alvorlig | * Varige eller alvorlige helsemessige konsekvenser for den registrerte * Økonomisk tap av betydelig varighet for den registrerte * Varig eller alvorlig tap av den registrertes omdømme * Den registrertes rett til personvern krenkes alvorlig i en større periode og involverer særlige kategorier/sårbare grupper * Den registrerte taper tilliten til virksomheten |
| **5** | Konsekvensen for den registrertes personvern er svært alvorlig | * Tap av liv for den registrerte * Varige og alvorlige helsemessige konsekvenser for den registrerte * Varig og betydelig økonomisk tap for den registrerte * Varig og alvorlig tap av den registrertes omdømme * Den registrertes rett til personvern krenkes på en svært alvorlig måte * Den registrerte og samfunnet taper tilliten til virksomheten |