[Konsekvensanalyse – DPIA](http://www.risikoanalyser.dk/konsekvensanalyse-dpia.html)

## Beskrivelse af dette dokument

Formålet med dette dokument er at støtte processen med udførslen af konsekvensanalyse for et eller flere behandlingsområder, hvor behandlingen af personoplysningerne, enten på baggrund af omfanget, følsomheden eller kombinationen heraf, vurderes at kunne medføre en høj risiko for de registrerede, hvis risikoen ikke afbødes og mindskes korrekt.

## Identifikation af behovet for en PIA

*Behandles der personoplysninger på stor skala? (vurdering)*

* **Ja**/Nej (beskriv om behandlingen af personoplysninger efter vandværkets vurdering drejer sig om stor skala)

*Behandles der følsomme personoplysninger?*

* **Nej**. (rettes såfremt vandværket behandler følsomme personoplysninger om forbrugere)

*Behandles personoplysninger i realtid?*

* **Ja/Nej** (beskriv om personoplysningerne behandles i realtid eller om der er mennesker der bistår med sagsbehandlingen og kan finde og rette eventuelle fejl)

*Behandles der personoplysninger om svage / særligt udsatte?*

* **Nej**, dog kan det i sjældne tilfælde komme til vandværkets opmærksomhed, at der er tale om svage / særligt udsatte borgere.

*Behandles der personoplysninger med ny/uprøvet teknologi (eksv. kunstig intelligens)?*

* **Nej**. (rettes såfremt vandværket behandler personoplysninger om forbrugeremed ny/uprøvet teknologi)

**Ud fra en samlet vurdering af ovenstående vurderes behovet for en formel DPIA ikke at være til stede, da der ikke forventes at være en høj risiko for de registrerede. Vi udfører dog risikovurderinger for alle behandlingsaktiviteter i fortegnelsen. [hvis vandværket i modsat fald konkluderer, at der er tale om en eller flere behandlingsaktiviteter der må forventes at medføre en høj risiko, fortsætter vandværket med at udfylde resten af dokumentet]**

## Formålene med behandlingen

*Beskriv her hvilke(t) formål der søges opnået med behandlingen af personoplysninger. Formålet/ene skal bl.a. lægge til grund for vurdering af muligheder for dataminimering, opbevaringsfrister mv. Så det er vigtigt at tænke holistisk og både på forretningen og personerne.*

## Beskrivelse af den påtænkte behandling

*Hvordan påtænker man at behandle personoplysningerne? Beskriv hele livscyklus, herunder indsamling, processering, opbevaring, videregivelse, sletning/anonymisering.*

### Indsamling

### Processering og opbevaring

### Videregivelse

### Sletning/anonymisering

### Datasættet (kategorier af personoplysninger)

## Beskrivelse af nødvendigheden og rimeligheden af behandlingen

*Beskriv her hvorfor behandlingen er nødvendig og hvordan man kan sikre rimeligheden i behandlingen (eksempelvis dataminimering)*

## Identifikation af risikoen for negativ påvirkning af personernes privatliv og rettigheder

*Hvad kunne tænkes at være problematisk for de personer som oplysningerne omhandler? Tag udgangspunkt i konfidentialitet (hvad sker der hvis data offentliggøres utilsigtet), integritet (hvad sker der hvis oplysningerne ændres utilsigtet) og tilgængelighed (hvad sker der hvis data bliver midlertidigt eller permanent utilgængelige)*

### Konfidentialitet (datalækage)

### Integritet (utilsigtet ændring)

### Tilgængelighed (midlertidig / permanent utilgængelige data)

*Giver det mening, på baggrund af den beskrevne risiko, at inddrage eksterne stakeholders, eksempelvis en fokusgruppe af de privatpersoner der er i målgruppen eller måske endda eksterne eksperter i form af forskere og interesseorganisationer med ekspertise indenfor privacy engineering, for at afdække mulighederne for privacy?*

## Identifikation af anvendte løsninger til at håndtere privacy og evaluering af dem

*Beskriv måden data forventes behandlet på og tag stilling til hver del – systemer og processer – og beskriv eventuelle svage punkter.*

## Implementering af forebyggende eller korrigerende foranstaltninger

*Beskriv hvilke ting der forventes at kunne reducere de identificerede risici forbundet med behandlingen.*

Med udgangspunkt i ovenstående har vi identificeret behov for:

## Mulighed for at vælge privatlivsfremmende teknologier

Kan formålene for behandlingen opnås med et mere begrænset datasæt?

Kan pseudonymisering hjælpe?

Kan kryptering eller one-way hashing hjælpe?

## Plan for håndtering af risikoen

*Beskriv den forventede resterende risiko. Hvis den resterende risiko vurderes som høj, skal datatilsynet høres inden behandlingen igangsættes.*

## Integration af resultaterne fra konsekvensanalysen i compliance arbejdet

*Beskriv hvordan man forestiller sig den løbende opfølgning skal ske. (Årshjul / compliance)*

Konsekvensanalysen genbesøges og opdateres årligt af {person i vandværket der følger op på efterlevelse af databeskyttelsesforordningen}.

## Revisionshistorik

Version Note Dato Redigeret af

V0.9 Første udkast til skabelon 13. august 2017 Tor Valstrøm

V0.91 Alle sektioner tilrettet 30. oktober 2017 Tor Valstrøm

V0.92 Opdatering af sektioner efter feedback 10. november 2017 Tor Valstrøm

V0.93 Opdatering af skabelon 19. februar 2018 Tor Valstrøm

## Referencer

Dokumentet indeholder elementer og inspiration fra følgende:

1. Datatilsynets “12 spørgsmål som dataansvarlige allerede nu med fordel kan forholde sig til”
2. EU forordning 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (”Persondataforordningen”)
3. WP248 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (4. April 2017)
4. DI’s skabelon for Privacy Impact Assessment
5. ISO/IEC 27002:2013 Information Technology — Security Techniques — Code of practice for Information Security Management <http://www.iso.org>
6. Information Security Forum (ISF) – Standard of Good Practice for Information Security (SOGP) 2011 <https://www.securityforum.org/>