Kvalitetssikring av KS' digitaliseringsprosjekter
Sjekkliste informasjonssikkerhet og personvern

Versjon 1.0 - 25.02.2018

Det er krav om innebygget personvern i tråd med personopplysningsloven. Innebygd personvern betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Det er både kostnadsbesparende og mer effektivt enn å endre et ferdig system.

De aller fleste prosjekter i KS' regi handler om personopplysninger. Norsk lovverk stiller strenge krav til håndtering av personopplysninger og prosjektene må sørge for at disse kravene blir oppfylt. For å skape løsninger og tjenester med tilstrekkelig personvern og informasjonssikkerhet, må prosjektene gjennomføre en rekke aktiviteter. Dette arbeidet er ofte mer omfattende enn man ser for seg på forhånd og kan kreve mer spesialistkompetanse og ressurser enn forventet. Ofte oppdager man sent i prosjektene at dette arbeidet ikke er tilstrekkelig planlagt, finansiert eller bemannet. Det fører til forsinkelser, budsjettoverskridelser og merarbeid. Dette kan i verste fall store bøter.

En annen utfordring kan oppstå ved etablering av forvaltningsorganisasjon. Det vil påløpe kostnader og være behov for ressurser i forbindelse med risikostyring, oppfølging av leverandørers sikkerhetsarbeid og løpende sikkerhetsvedlikehold gjennom hele systemets levetid. Hvis disse oppgavene ikke har nødvendige rammer, eller hvis ansvaret for oppgavene ikke er plassert, øker tjenestens risikonivå raskt.

Hensikten med at prosjektene besvarer denne sjekklisten er å kunne fastslå at:

- arbeidet med personvern og informasjonssikkerhet er planlagt, finansiert og organisert ved prosjektets oppstart.
- det er etablert nødvendige roller og styring som sikrer at personvern- og informasjonssikkerhetsaktiviteter blir utført.
- ved etablering av drift og forvaltningsorganisasjon ivaretas også oppgaver knyttet til personvern og informasjonssikkerhet.

Sjekklisten består av tre deler. Den første delen er spørsmål som må kartlegges og avklares allerede i konseptfasen/planleggingsfasen. Del tro er spørsmål rundt ansvar, styring og finansiering av arbeidet med personvern og informasjonssikkerhet. Den siste delen spør mer konkret om hvilke aktiviteter som er identifisert og planlagt av prosjektet.

Del 1 Kartlegges allerede i konseptfasen

	Del 1 Kartlegges allerede i konseptfasen Avklare behov for informasjonssikkerhet og personvern[1] Gjennomføre DPIA dersom kravene er til stede (Data Protection Impact Assessment - DPIA)[2] Du må alltid avklare spørsmålene: • Har din virksomhet spesielle føringer eller retningslinjer for informasjonssikkerhet og personvern som prosjektet må forholde seg til? Dette kan være spesielle krav for sektor, bransje eller en intern sikkerhetspolicy. • Er noen av de identifiserte behovene for informasjonssikkerhet eller personvern knyttet til et spesifikt konsept slik at dette kan påvirke konseptvalget? Identifiser i så fall behovene for hvert av konseptene. • Er noen av behovene kritiske?

[1] https://www.prosjektveiviseren.no/avklare-behov-informasjonssikkerhet-og-personvern
[2] https://www.datatilsynet.no/regelverk-og-skjema/veiledere/vurdering-av-personvernkonsekvenser/

	• Er det noen av behovene som gjør at et konsept ikke kan gjennomføres? Sørg for at noen i prosjektet har ansvar for informasjonssikkerhet og personvern. Vurder å innhente ekstern kompetanse på områdene dersom dette ikke finnes internt i virksomheten
1	**Hva er behovet for informasjonssikkerhet og personvern?** Prosjektet må ha et bevisst forhold til informasjonssikkerhet og personvern fra starten av. Hvis tiltak må legges på til slutt, blir det ofte økte kostnader og forsinkelser i prosjektet og løsningene kan ofte bli dårligere kvalitetsmessig. I konseptfasen vurderes overordnede behov for informasjonssikkerhet og personvern for å sikre konfidensialitet, integritet og tilgjengelighet og vurdere om arbeidsområdet kan være omfattet av regelverk eller avtaler som stiller spesielle krav til sikkerhetstiltak. Noen løsninger vil kunne omfattes av sikkerhetsloven, for eksempel om det samles inn store menger personopplysninger eller hvis sikkerhetsgradert informasjon skal behandles. Dette må ivaretas særskilt.
2	**Skal personvernkonsekvenser (DPIA) vurderes?** En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de som er registrert i løsningen ivaretas. Dette er en plikt etter det nye personvernregelverket. Artikkel 35 definerer når det er påkrevd å gjøre en DPIA, hva den skal inneholde og hvem som skal gjennomføre den. Vi har laget en veileder som går gjennom regelverket.

Del 2 Ansvar, styring og finansiering av personvern og informasjonssikkerhet.

	Del 2 Ansvar, styring og finansiering av personvern og informasjonssikkerhet. Alle spørsmål må være besvart for at KS' fagråd for informasjonssikkerhet skal kunne vurdere og gi råd til prosjektet.
1	**Skal prosjektet utvikle fri programvare eller etablere en tjeneste / felleskomponent?** Hvis prosjektet ikke skal etablere en tjeneste/felleskomponent, er det ikke nødvendig å besvare spørsmål 2 eller siste punkt under spørsmål 3.
2	**Hvem er behandlingsansvarlig for opplysninger som håndteres av tjenesten/felleskomponenten? Hvordan skal dette behandlingsansvaret ivaretas – vennligst beskriv styringsmidlene.** Normalt vil det være den enkelte kommune/fylkeskommune som er behandlingsansvarlig og som dermed har et selvstendig ansvar for at personvern og informasjonssikkerhet er ivaretatt. For å ivareta dette ansvaret må det etableres en styringsstruktur som gir den enkelte kommune/fylkeskommune innsyn i forhold rundt risiko og mulighet for å påvirke hva som skal være akseptabel risiko. Dette kan for eksempel realiseres gjennom en referansegruppe som involveres i risikovurderinger og oppfølging av funn.
	Hvem er ansvarlig for at personvern og informasjonssikkerhet ivaretas i prosjektet? **Hvem er ansvarlig for at personvern og informasjonssikkerhet ivaretas ved idriftssettelse?**

	Hvem er ansvarlig for at personvern og informasjonssikkerhet ivaretas i videre forvaltning? Her ber vi om at rollene beskrives slik at det fremgår hvilke organisasjoner som har hvilke roller på området informasjonssikkerhet og personvern. I samarbeidsprosjekter kan det ofte være en utfordring å få rollene beskrevet. Som et minimum må det beskrives: • Hvem er ansvarlig for at løsningen oppfyller relevante lovkrav, herunder at prosjekt og forvaltningsorganisasjon er underlagt et styringssystem for informasjonssikkerhet? • Hvem har fastsatt hvilket prosjektstyringsrammeverk prosjektet skal benytte? • Hvem er ansvarlig for at personvern- og informasjonssikkerhetsaktiviteter er finansiert og bemannet med forsvarlig kompetanse? • Hvem er ansvarlig for at de underleverandører som velges, er i stand til å oppfylle kravene som er stilt på området informasjonssikkerhet og personvern. • Hvem er ansvarlig for at risiko i løsningen over tid er akseptabel i henhold til de krav som behandlingsansvarlig har stilt.
4	**Hvilket prosjektstyringsrammeverk benyttes i prosjektet?** Et prosjektstyringsrammeverk kan gi god hjelp i å planlegge riktige sikkerhetsaktiviteter til riktig tid i prosjektet. Her viser vi til DIFIs anbefalte rammeverk for prosjekter[3] (se mer detaljer i del 2). Eller angi et annet rammeverk som er valgt.
5	**Er det øremerkede midler i prosjektet til informasjonssikkerhet og personvern?**
6	**Er det planlagt en sikkerhetstest/inntrengningstest av løsningen før den tas i bruk?**

Del 3 – Prosjektaktiviteter på området personvern og informasjonssikkerhet

	Del 3 – Prosjektaktiviteter på området personvern og informasjonssikkerhet Her ber vi om mer detaljer om hvordan arbeidet med personvern og informasjonssikkerhet er planlagt ivaretatt gjennom prosjektet. Punktene følger samme struktur som prosjektveiviseren til DIFI, jf. prosjektveiviseren.no.
1	**Avklare behov for informasjonssikkerhet og personvern** Et hvert digitaliseringsprosjekt har behov for å sikre informasjon, spørsmålet er bare i hvilken grad. For at prosjektet skal ivareta dette på best mulig måte, må behovene for sikring avklares. Krav til sikring av informasjon avgjøres av relevant lovverk, bransjens norm og bedriftens egne rutiner og retningslinjer. Derfor må et hvert prosjekt kartlegge og analysere hvilken informasjon som skal behandles. Det er først når man har oversikt over hvilken informasjon et produkt/en tjeneste er planlagt å behandle, at man kan si noe særlig om hvilke krav som stilles til sikring av den aktuelle informasjonen. Planlegger prosjektet en eller annen form for behandling av informasjon om enkeltpersoner, enten det handler om brukernavn og passord, helseopplysninger eller økonomiske transaksjoner, så vil det

[3] https://www.datatilsynet.no/regelverk-og-skjema/veiledere/vurdering-av-personvernkonsekvenser/

	stilles ulike krav til sikring på grunnlag av dette. Helseopplysninger krever f.eks. som regel av man følger Norm for informasjonssikkerhet i helsesektoren. Skulle det være informasjon som er eller kan bli gradert etter sikkerhetsloven, vil dette stille andre krav, osv. Dermed kan det også være lurt for et hvert prosjekt å avklare og avgrense hvilken informasjon som faktisk skal behandles, da dette kan få stor effekt på prosjektet. Jf. for øvrig prosjektveiviseren.no for utfyllende informasjon[4]
2	**Ivareta informasjonssikkerhet og personvern i prosjektplanlegging, anskaffelser og kontraktsinngåelser** Basert på behovene man avdekker vil det være nødvendig å planlegge ivaretakelse av informasjonssikkerhet og personvern i prosjektgjennomføring, og i forvaltning, drift og vedlikehold av produktet/tjenesten. Følgende aktiviteter må gjennomføres: • Beskriv hvordan prosjektorganisasjonen planlegger å ivareta informasjonssikkerhet og personvern • Beskriv prosjektets planlagte produkter for ivaretakelse av informasjonssikkerhet og personvern • Beskriv prosjektets tekniske rammer og sikkerhetsarkitektur for ivaretakelse av informasjonssikkerhet og personvern • Beskriv behovet for ivaretakelse av informasjonssikkerhet og personvern gjennom avtaleverk og kontraktsmessige forhold. Jf. for øvrig prosjektveiviseren.no for utfyllende informasjon.[5]
3	**Følge opp informasjonssikkerhet og personvern i prosjektgjennomføringen** Etter hvert som prosjektplanen blir gjennomført blir det behov for å følge opp at produktene for ivaretakelse av informasjonssikkerhet og personvern er produsert og oppdatert. En risikovurdering bør f.eks. utvikle seg med prosjektet etter hvert som tekniske forutsetninger, funksjonelle krav og avtalemessige eller praktiske forhold endrer seg. Sørg for at følgende blir fulgt opp: • Før avslutning av en fase, sjekk at produkter for ivaretakelse av informasjonssikkerhet og personvern er levert og oppdatert • Nødvendige avtaler og kontraktsmessige forhold for ivaretakelse av informasjonssikkerhet og personvern er gjennomgått, formalisert og undertegnet • Overlevering til forvaltning, drift og vedlikehold er planlagt for å ivareta informasjonssikkerhet og personvern gjennom hele produktets/tjenestens livsløp Jf. for øvrig prosjektveiviseren.no for utfyllende informasjon[6] og til Datatilsynets veileder[7].
4	**Trygge testdata**

[4] (https://prosjektveiviseren.no/avklare-behov-informasjonssikkerhet-og-personvern)
[5] (https://prosjektveiviseren.no/ivareta-informasjonssikkerhet-og-personvern-i-prosjektplanleggingen)
[6] (https://www.prosjektveiviseren.no/følge-opp-informasjonssikkerhet-og-personvern-i-prosjektgjennomføringen)
[7] (https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/)

	Alle personopplysninger benyttet til testformål skal være pseudonymisert, avidentifisert eller anonymisert. Pseudonymisering vil si at enkelte direkte identifiserende parametere erstattes med pseudonymer, som fremdeles vil være unike indikatorer. Avidentifisering vil si at alle personentydige kjennetegn er fjernet fra opplysningene, slik at de ikke lenger kan knyttes til en enkeltperson. Anonymisering er å gjøre personopplysninger anonyme. Vennligst beskriv hvordan prosjektet planlegger å ivareta testdata på en trygg måte.