Sjekkliste informasjonssikkerhet ved avslutning av prosjekt

Denne listen skal fylles ut ved avslutning av prosjekter for å kvalitetssikre at den tjenesten som er etablert oppfyller Oslo kommunes regelverk og lovkrav til personvern og informasjonssikkerhet.

Veiledning og forklaring av elementene i sjekklisten finnes bak sjekklisten.

Før listen fylles ut er det viktig å tydeliggjøre at begrepet «Tjenesten» refererer til den løsningen som er utarbeidet og satt i drift. Hvis Tjenesten har en verdikjede som involverer flere virksomheter (statlige, kommunale, andre), skal svaret utformes slik at det gjelder for hele verdikjeden.

Prosjektets navn	
Behandlingsansvarlig for Tjenesten er	
Systemeier for Tjenesten er	

Nr.	Oppgave	Status
1	Finnes det en oppdatert behandlingsoversikt som dekker tjenesten?	
2	Er det gjort en vurdering av behovet for å vurdere konsekvenser for de registrertes personvern (fra nå referert til som DPIA)?	
3	Hvis det er identifisert behov for DPIA, er denne utført og dokumentert?	
4	Foreligger det en ROS-analyse som viser hvilken risiko som er identifisert i den ferdige Tjenesten?	
5	Er det fastsatt krav til hva som skal anses som akseptabel risiko for Tjenesten?	
6	Er systemeiers virksomhetsleder informert om eventuell uakseptabel (rød) risiko i Tjenesten og hvilke planer som finnes for å redusere slik risiko?	
7	Er det gjennomført en sikkerhetstest/inntrengningstest av Tjenesten? Vennligst begrunn hvorfor hvis slik test ikke er gjennomført.	
8	Er prinsippene for innebygget personvern ivaretatt ved utforming av Tjenesten?	
9	Er det etablert en forvaltningsorganisasjon for Tjenesten? Er det avklart hvem som har ansvar for jevnlig kartlegging og vurdering av risiko gjennom sikkerhetstesting og ROS-analyser? Er det avsatt midler til disse tiltakene i forvaltningen?	
10	Hvis Tjenesten har en ekstern leverandør av programvare, er det inngått avtale om sikkerhetsvedlikehold av denne programvaren?	
11	Hvis Tjenesten ikke har et avtalefestet sikkerhetsvedlikehold, er ansvaret for å identifisere nødvendig sikkerhetsvedlikehold plassert og finansiert? (Slikt løpende vedlikehold er nødvendig også som følge av at det jevnlig oppdages sårbarheter i protokoller eller programvarebiblioteker som Tjenesten benytter.)	
12	Er det etablert en forvaltningsorganisasjon for Tjenesten som har ansvar for løpende utførelse av sikkerhetsoppdatering av programvare og driftsmiljø.	
13	Hvis Tjenesten, eller deler av denne, er levert av en ekstern leverandør eller driftes utenfor Oslo kommune, er det inngått Databehandleravtaler?	

En kort veiledning til sjekklisten

Nr	Oppgave
1	Alle virksomheter må ha *dokumentert* oversikt over alle behandlinger av personopplysninger i virksomheten (= behandlingsoversikt). Oversikten skal bl.a. gi oversikt over hvilke kategorier av personopplysninger som behandles, hvordan opplysningene er samlet inn og grunnlaget for å behandle personopplysninger for de ulike formål. Det må foreligge en behandlingsoversikt uansett om personopplysningene gjelder innbyggere eller ansatte. Behandlingsansvarlig er ansvarlig for oversikten. For mer informasjon om hvordan utarbeide en behandlingsoversikt, samt mal, henvises det til https://felles.intranett.oslo.kommune.no/informasjonssikkerhet/personvern/behandlingsoversikt/.
2	Mens vanlige risikovurderinger ser på virksomhetens risiko, krever den nye personvernlovgivningen at det også vurderes om en Tjeneste kan utgjøre en risiko for de registrerte (brukerne). Dette kalles å gjennomføre en DPIA (en vurdering av personvernkonsekvenser). For mer informasjon, se https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/
3	
4	Hvorfor må det gjøres en ROS-analyse av Tjenesten? Det er normalt slik at en løsning settes i drift selv om man har identifisert scenarier som viser at uheldige hendelser kan skje. Det etableres da en plan for hvilke tiltak som skal settes i verk for å redusere risiko for uheldige hendelser. Hvis risiko for en hendelse vurderes både som lav sannsynlighet og å ha lav konsekvens er det normalt å akseptere slik risiko. Større risiko vil man normalt forsøke å redusere ved å sette i verk ulike tiltak. Desto større risiko, desto raskere forsøker man å få iverksatt tiltak. Noen ganger er det vanskelig å finne kostnadseffektive tiltak for å redusere risiko. Da kan man velge å akseptere en identifisert risiko – se også punkt 6.
5	Hvordan fastsettes krav til hva som skal anses som akseptabel risiko for Tjenesten? Dette fastsettes ved at man 1. Fastsetter skalaer for hva man mener med lav eller høy sannsynlighet 2. Fastsetter skalaer for hva som skal vurderes som alvorlig eller mindre alvorlig konsekvens 3. Fastsetter hvilke kombinasjoner av sannsynlighet og konsekvens som ikke er akseptable – normalt ved å si hvilke felter i en risikomatrise som er røde (=uakseptabel), gule (=bør håndteres) eller grønne (akseptabel). Det er viktig at systemeier har godkjent de kriteriene som benyttes og at kriteriene er kjent av de behandlingsansvarlige. Systemeier må også ta stilling til om lansering er forsvarlig med den risiko som er identifisert.
6	Hva skjer hvis ROS-analysen resulterer i scenarier med uakseptabel (rød) risiko? Slik risiko må rapporteres til behandlingsansvarlig for tjenesten – normalt virksomhetsleder. Er det andre virksomheter som benytter Tjenesten vil det være naturlig å informere disse. Det er også naturlig å informere overordnet byrådsavdeling.
7	Hva er en sikkerhetstest og hvorfor bør man gjennomføre slik testing før tjenesten tas i bruk? Erfaringsmessig oppstår det feil og sikkerhetshull i utvikling av programvare. Dette kan være feil som en inntrenger/hacker kan utnytte til å hente ut informasjon, ødelegge informasjon eller servere eller spre virus til alle som besøker Tjenesten. Ved en sikkerhetstest letes det aktivt etter slike sikkerhetshull ved å bruke samme teknikker som en inntrenger vanligvis benytter. Når sikkerhetshull identifiseres kan de lukkes og risiko i tjenesten reduseres. Kravet om sikkerhetstesting er nedfelt i «Instruks for informasjonssikkerhet», kap 5.4.c

8	Hvordan oppnår man innebygget personvern i en Tjeneste? Innebygget personvern er ikke et entydig begrep i lovens forstand. Man kan finne veiledninger flere steder, for eksempel på Datatilsynets sider https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/ . Program for elektroniske tjenester har også en egen sjekkliste.
9	Hvorfor trenger man å gjøre jevnlig kartlegging av risiko? Trusselbildet utvikler seg raskt på internett og det betyr at Tjenester som var sikre nok i fjor ikke nødvendigvis har samme sikkerhet i år. Det kan være kommet nye hackerteknikker eller det kan være sårbarheter eller feil som er oppdaget i standard kommunikasjonsprotokoller eller programvare. Derfor må det arbeides jevnlig med å kartlegge endringer i risiko, gjennom både sikkerhetstesting og ROS-analyser.
10	Hvorfor må noen ha ansvar for å identifisere behov for sikkerhetsvedlikehold av programvare? Det oppdages jevnlig sikkerhetsfeil i programvaremoduler som benyttes av mange tjenester i verden. Slike oppdagelser publiseres løpende i et stort volum. Det er et stort arbeid som må utføres for å identifisere hvilke feil som kan ramme den programvaren som benyttes i kommunens Tjenester. Slikt vedlikehold leveres normalt av programvareleverandøren, som leverer nye versjoner av programmene der kjente sikkerhetshull er lukket. Hvis kjente sikkerhetshull ikke blir lukket øker risikoen for at noen utnytter dem. Derfor er det viktig å avtalefeste ansvar for denne typen vedlikehold.
11	Hvem skal vedlikeholde sikkerheten i åpen programvare eller programvare Oslo kommune har utviklet selv? Åpen programvare er gratis og det finnes ingen avtale om sikkerhetsvedlikehold. Programvaren kan bli vedlikeholdt på dugnadsbasis (eller man må gjøre det selv), men man blir nok ikke varslet om behov for sikkerhetsoppdateringer. Man er selv ansvarlig for å følge med på når det er nødvendig å modifisere programvare for å tette sikkerhetshull. Det er viktig at dette ansvaret er plassert og finansiert i forvaltningen av tjenesten.
12	Hvem skal passe på at sikkerhetsoppdateringer blir installert i driftsmiljøet? Både programvare og driftsmiljø trenger jevnlige oppdateringer og det kan være en omfattende oppgave å utføre slike endringer i et driftsmiljø. Det er viktig å følge opp at dette utføres som avtalt, om det er overfor en ekstern applikasjonsleverandør, en ekstern driftsleverandør eller en intern forvalter.
13	Når må det inngås databehandleravtaler? For systemer som behandler personopplysninger krever personvernlovgivningen at det inngås Databehandleravtaler med de partene som er involvert i behandlingen. Lovgivningen stiller strenge krav til hvordan en slik avtale kan utformes. Oslo kommune har utviklet en mal for Databehandlingsavtaler og denne skal alltid benyttes. Se https://felles.intranett.oslo.kommune.no/informasjonssikkerhet/personvern/databehandleravtaler-maler/ Formålet med avtalene er å fastslå hvordan databehandler skal behandle personopplysningene på vegne av behandlingsansvarlig. Det omfatter hvor personopplysninger skal lagres, hvor lenge databehandler skal oppbevare opplysningene, krav til informasjonssikkerhet mv.