**SJEKKLISTE**

**For vurdering og gjennomgang av nye IT-systemer og skyløsninger**

Formålet med denne sjekklisten er å gi en overordnet forståelse av hva som må evalueres i vurderingen av et nytt IT-system for å ivareta IT-sikkerhet, personvern, forvaltning og generelle anskaffelsesforhold. Hvert sjekkpunkt må derfor, etter beste evne, besvares så konkret som mulig og utdypes der det er nødvendig.

Sjekklisten har som hensikt å fungere som et verktøy personvernkontakt kan benytte når vedkommende skal bistå sin avdeling med gjennomgangen et nytt IT-system eller ny skyløsning, for å vurdere følgende:

* Om leverandøren tilfredsstiller fastsatte krav per d.d.
* Om leverandøren må implementere tiltak før kontraktsinngåelse.
* Om leverandøren er ikke en aktuell samarbeidspartner for OsloMet.

Relevant dokumentasjon tilknyttet vurderingsprosessen av IT-systemet:

* Databehandleravtale (DBA) / Data processing agreement/addendum (DPA)
* Personvernerklæringer / Privacy Policy
* Vilkår for bruk / Terms of Service
* Samsvarserklæringer / Compliance posture
  + Inneholder informasjon om hvilke nasjonale og internasjonale lov- og regelverk leverandøren etterlever, gyldige sertifiseringer og hvilke krav leverandøren oppfyller for å inneha sertifiseringene ol.
* Relevante nettsider tilknyttet leverandøren

Dersom personvernkontakter ber om bistand til vurdering og gjennomgang fra [kompetansegruppe for databehandleravtaler (DBA)](https://ansatt.oslomet.no/sok?p_p_id=com_liferay_portal_search_web_search_results_portlet_SearchResultsPortlet_INSTANCE_noymRBU4yQAA&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_com_liferay_portal_search_web_search_results_portlet_SearchResultsPortlet_INSTANCE_noymRBU4yQAA_mvcPath=%2Fview_content.jsp&_com_liferay_portal_search_web_search_results_portlet_SearchResultsPortlet_INSTANCE_noymRBU4yQAA_assetEntryId=167837404&_com_liferay_portal_search_web_search_results_portlet_SearchResultsPortlet_INSTANCE_noymRBU4yQAA_type=content), eller IT-FoU vedrørende forskningsrelaterte henvendelser (kontaktes via [IT-servicedesk](https://ansatt.oslomet.no/brukerstotte-it)), skal sjekklisten fylles ut etter beste evne i forkant og vedlegges henvendelsen.

Sjekklisten skal lagres iht. [OsloMet sin retningslinje for dokumentforvaltning](https://ansatt.oslomet.no/retningslinje-for-dokumentforvaltning).   
Sjekklister er klassifisert lavest på nivåinndelingen for dokumenter, men det anbefales å vurdere om sjekklisten skal arkiveres jf. høyere nivå dersom dokumentet tillegges en større mengde spesifiseringer og kommentarer. Sporbar arkivering er viktig for å kunne dokumentere vurderingen av IT-systemet/skyløsningen, men i tillegg for å ha informasjonen lett tilgjengelig da mye av den blir etterspurt på senere tidspunkt i bla. behandlingsprotokoll, ROS-analyse og personvernkonsekvensvurdering (DPIA) dersom en går til anskaffelse av IT-systemet.

Innhold

[1. Generelt 2](#_Toc146227774)

[2. Personopplysninger *Se Datatilsynets definisjon på en personopplysning ved behov.* 2](#_Toc146227775)

[3. Leverandør, underleverandører og dataflyt 3](#_Toc146227776)

[4. Tredjeland\* og jurisdiksjon 4](#_Toc146227777)

[5. Sikkerhetstiltak, sertifiseringer og kontroll 5](#_Toc146227778)

[6. Generelle avklaringer 6](#_Toc146227779)

# 1. Generelt

|  |  |  |
| --- | --- | --- |
| 1.1. | Systemnavn: |  |
| 1.2. | Navn på leverandør: |  |
| 1.3. | Nettside: |  |
| 1.4. | I hvilket land er leverandør etablert? |  |
| 1.5. | Hva skal systemet i hovedsak benyttes til? |  |

# 2. Personopplysninger *Se* [*Datatilsynets definisjon på en personopplysning*](https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/) *ved behov.*

|  |  |  |  |
| --- | --- | --- | --- |
| 2.1. | Hvilke alminnelige personopplysninger direkte tilknyttet den registrerte behandles?  *Dersom det ikke behandles alminnelige personopplysninger direkte tilknyttet den registrerte, gå videre til pkt. 2.2.* | Navn  Telefonnummer  Adresse  E-postadresse  Fødselsdato  IP-Adresse  Organisasjonstilknytning  Annet (spesifiser nedenfor) | |
| Spesifiseringer: | | |
| 2.2. | Behandles det alminnelige personopplysninger indirekte tilknyttet den registrerte?  *Eksempelvis beskrivelser av og kjennetegn på deres person, deres kompetanse, deres ytringer/vurderinger (f.eks. gjennom fritekstfelt i IT-systemet) ol.* | Ja | Nei |
| Er svaret på pkt. 2.2. JA, utdyp her: | | |
| 2.3. | Behandles personnummeret (11 siffer) til de registrerte? | Ja | Nei |
| 2.4. | Behandles det særlige kategorier av personopplysninger? | Ja | Nei |
| *Er svaret på pkt. 2.4. JA gå videre til pkt. 2.5. Er svaret NEI, gå videre til pkt. 2.6.* | | |
| 2.5. | Hvilke særlige kategorier av personopplysninger behandles?  *Merk! Helseopplysninger er ikke kun fysiske målbare data, men kan være verbale utsagn, atferdsmønstre ol. som sier noe om den registrerte sin psykiske helse.* | Helseopplysninger  Genetiske/biometriske  Etnisk bakgrunn  Seksuell(e) legning/forhold  Politisk tilhørighet  Religiøs oppfatning  Fagforeningsmedlemskap  Annet (spesifiser nedenfor) | |
| Spesifiseringer: | | |
| 2.6. | Hvor mange registrerte berøres av databehandlingen? | 1 - 50 | 50 - 150 |
| 150 - 500 | 500+ |
| 2.7. | Hvilke kategorier tilhører de registrerte? | Ansatte | Studenter |
| Deltagere/pasienter i forskningsprosjekt | |
| Dersom ingen av svaralternativene til pkt. 2.7. er relevant, utdyp her: | | |
| 2.8. | Behandles det personopplysninger om sårbare grupper eller personer i sårbare situasjoner?  *Eksempelvis er pasienter og barn under 16 år å anse som sårbare grupper. Sårbare situasjoner kan være varslingssaker, skikkethetssaker, fuskesaker mm. Se* [*OsloMets nettside om særlige kategorier av personopplysninger (avsnitt "Andre personopplysninger som kan være sensitive")*](https://ansatt.oslomet.no/sensitive-personopplysninger#statisk_avsnitt_aomhldqm) *for nærmere informasjon.*  *Personopplysninger som i utgangspunktet er å anse som alminnelige kan defineres som sensitive dersom de omhandler sårbare grupper eller personer i sårbare situasjoner . Dette kan medføre høyere krav til sikkerhet og krav, samt implementering av ytterligere tiltak.* | Ja | Nei |
| Er svaret på pkt. 2.8. JA, utdyp her: | | |
| 2.9. | Er formålet med behandlingen av personopplysninger avklart?  *Eksempelvis at personopplysningene må behandles for å gi den registrerte tilgang til IT-systemet.* | Ja | Nei |
| Er svaret på pkt. 2.9. JA, utdyp her: | | |
| 2.10. | Er det vurdert om OsloMet har et gyldig behandlingsgrunnlag (rettslig grunnlag) til å gjennomføre behandlingen av personopplysninger?  *Se* [*Datatilsynets gjennomgang av de ulike behandlingsgrunnlagene og når de gjelder*](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/) *ved behov.* | Ja | Nei |
| Er svaret på pkt. 2.10. JA, utdyp her: | | |
| 2.11. | Er det det avklart hvordan databehandleren i praksis skal behandle personopplysningene?  *Eksempelvis analysering, lagring, sammenstilling og kobling el.* | Ja | Nei |

# 3. Leverandør, underleverandører og dataflyt

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3.1. | Er leverandøren (databehandleren) godt etablert og en kjent aktør i sin bransje?  *Et raskt Googlesøk kan avklare om hvordan kundetype leverandøren har (f.eks. andre virksomheter i UH-sektoren), hvordan kundeomtale leverandøren har fått ol.*  *Svaret vil være NEI dersom leverandøren f.eks. er en startup-bedrift.* | | | Ja | Nei |
| Er svaret på pkt. 3.1. NEI, utdyp her: | | | | |
| 3.2. | Er IT-systemet/tjenesten en pilotering eller en del av en pilotering?  *Eksempelvis et prosjekt, nytt satsingsområde el. Ved pilotering med begrenset tidsperiode vil krav til personvern kunne reduseres noe.* | | | Ja | Nei |
| 3.3. | Benyttes det underleverandører? | | | Ja | Nei |
| *Er svaret på pkt. 3.3. JA gå videre til pkt. 3.4. Er svaret NEI, gå videre til pkt. 3.6.* | | | | |
| 3.4. | Navn: | Behandlings-lokasjon (land): | Prosessbeskrivelse:  *(f.eks. datalagring, kundeservice el.)* | Nettside: | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
| 3.5. | Hvilke personopplysninger som behandles har underleverandører tilgang til? | | | All data | Noe data |
| Er svaret på pkt. 3.5. NOE DATA, utdyp her: | | | | |
| 3.6. | Opplyser leverandøren (databehandleren) om forhold som tilsier at det foregår dataoverføringer til tredjeparter (ev. underleverandører), hvor formålet med overføringen ikke samsvarer med OsloMet (behandlingsansvarlig) sitt behandlingsformål (se pkt. 2.9.)?  *F.eks. overføring til virksomheter som utfører analyser, statistikk el.* | | | Ja | Nei |
| Utdyp nærmere, ved behov: | | | | |
| 3.7. | Er dataflyten tydelig og klargjort?  *Dette gjelder hvordan dataene flyter/forflyttes i IT-systemet/tjenesten, ev. mellom leverandør og underleverandør(er).* | | | Ja | Nei |
| Dersom det er behov for filoverføringer, integrasjoner el., spesifiser her: | | | | |

4. Tredjeland\* og jurisdiksjon **\*Land utenfor EU/EØS. F.eks. USA.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4.1. | Er leverandøren eller underleverandør(er) etablert i tredjeland, men har etablert datalagringssenter i Europa og er dermed underlagt europeisk lovgivning?  *For eksempel:*  *Amerikansk underleverandør. Etablert datalagringssenter i Nederland. Underlagt nederlandsk lovgivning (inkl. GDPR).* | Ja | Nei | Opplyses  ikke om |
| Er svaret på pkt. 4.1. JA, utdyp her: | | | |
| 4.2. | Foregår det dataoverføring til og databehandling i tredjeland?  *Datalagring er et eksempel på databehandling.* | Ja | Nei | Opplyses  ikke om |
| *Er svaret på pkt. 4.2. JA gå videre til pkt. 4.3. Er svaret NEI, gå videre til pkt. 5.* | | | |
| 4.3. | Er leverandøren eller underleverandør(er) på EU sin siste over godkjente amerikanske virksomheter å overføre personopplysninger til?  *Se* [*Datatilsynets gjennomgang av regler for overføring av personopplysninger til USA*](https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/nye-regler-for-overforing-av-personopplysninger-til-usa/) *for utfyllende informasjon og* [*Data Privacy Framework Program sin nettside*](https://www.dataprivacyframework.gov/s/participant-search) *for oppdatert liste over godkjente virksomheter.* | Ja | | Nei |
| *Er svaret på pkt. 4.3. NEI gå videre til pkt. 4.4. Er svaret JA, gå videre til pkt. 5.* | | | |
| 4.4. | Er det inngått Standard Contractual Clause (SCC) mellom leverandør og underleverandør i tredjeland?  *SCC er det vanligste overføringsgrunnlaget når personopplysninger skal overføres til tredjeland. Dersom SCC er inngått fremkommer dette normalt av DBA, ta kontakt med leverandør dersom det ikke fremkommer av tilgjengelig dokumentasjon.*  *Merk! Leverandører kan benytte seg av utdaterte DBA og referere til Privacy Shield som overføringsgrunnlag. Privacy Shield ble dømt ugyldig av EU-domstolen i 2020, dersom leverandør referer til dette må leverandør kontaktes for nærmere avklaringer.* | Ja | Nei | Opplyses  ikke om |
| 4.5. | Er det gjennomført Transfer Impact Assessment (TIA) i fm. SCC?  *TIA er en vurdering av overføringen av personopplysninger til tredjeland med SCC som overføringsgrunnlag. Dersom TIA er inngått fremkommer dette normalt av DBA, ta kontakt med leverandør dersom det ikke fremkommer av tilgjengelig dokumentasjon.* | Ja | Nei | Opplyses  ikke om |

# 5. Sikkerhetstiltak, sertifiseringer og kontroll

|  |  |  |  |
| --- | --- | --- | --- |
| 5.1. | Tilfredsstiller leverandøren OsloMet sine krav til autentisering?    *Flerfaktor-autentisering (MFA).*  *Se* [*OsloMet sin retningslinje for tilgangskontroll*](https://ansatt.oslomet.no/retningslinje-for-tilgangskontroll)*.* | Ja | Nei |
| Utdyp nærmere, ved behov: | | |
| 5.2. | Tilfredsstiller leverandøren OsloMet sine krav til tilgangsstyring?  *Eksempelvis at ansatte hos leverandør/underleverandør kun har tilgang til data de har tjenstlig behov til.*  *Se* [*OsloMet sin retningslinje for tilgangskontroll*](https://ansatt.oslomet.no/retningslinje-for-tilgangskontroll)*.* | Ja | Nei |
| Utdyp nærmere, ved behov: | | |
| 5.3. | Hvilke andre personvern- og sikkerhetstiltak er implementert hos leverandøren? | Kryptering  Backup  Dataminimering  ☐ Sletterutiner  Innsynsrett for den registrerte  Exit-strategi\*  Annet (spesifiser nedenfor) | |
| *\* Strategi/rutine for overføring av personopplysninger til nytt IT-system ved bytte av leverandør.* | |
| Spesifiseringer: | | |
| 5.4. | Innehar leverandøren noen form for sikkerhetsrelatert sertifisering?  *F.eks. ISO/IEC 27001.* | Ja | Nei |
| Er svaret på pkt. 5.4. JA, utdyp her: | | |
| 5.5. | Opplyser avtalen eller annen dokumentasjon om leverandørens rutiner for revisjon og kontroll? Dette inkludere eksterne og interne prosesser.  *Eksempelvis fastsatte revisjoner som gjennomføres årlig.* | Ja | Nei |
| Utdyp nærmere, ved behov: | | |
| 5.6. | Opplyser avtalen at leverandøren tilbyr revisjon av egen virksomhet på forespørsel fra OsloMet? | Ja | Nei |
| Utdyp nærmere, ved behov: | | |
| 5.7. | Opplyser avtalen om leverandørens avviksrutiner?  *Eksempelvis at dersom et avvik avdekkes, så varsles behandlingsansvarlig (OsloMet) snarest og Datatilsynet varsles innen fristen på 72 timer.* | Ja | Nei |
| Utdyp nærmere, ved behov: | | |

# 6. Generelle avklaringer

|  |  |  |  |
| --- | --- | --- | --- |
| 6.1. | Opplyser avtalen hvor lenge den er gyldig, samt informasjon tilknyttet oppsigelsestid, bindingstid ol.?  *Ref. oppsigelsestid skal det tilstrebes å ha dokumentasjon på hva som gjelder for OsloMet som kunde og hva som gjelder for leverandør.* | Ja | Nei |
| Utdyp nærmere, ved behov: | | |
| 6.2. | Opplyser avtalen om hvem som er økonomisk ansvarlig ved avvik?  *For eksempel:*  *Avvik inntreffer grunnet systemfeil/rutinesvikt hos leverandør, men det resulterer i at OsloMet bøtelegges av Datatilsynet da OsloMet er behandlingsansvarlig.* | Ja | Nei |
| Utdyp nærmere, ved behov: | | |
| 6.3. | Opplyser avtalen om behandlingsansvarlig (OsloMet) sine rettigheter til å avslutte samarbeidsforholdet dersom avvik inntreffer?  *Eksempelvis at oppsigelsestiden blir tilsidesatt dersom et avvik medfører store konsekvenser for OsloMet.* | Ja | Nei |
| Utdyp nærmere, ved behov: | | |
| 6.4. | Opplyser avtalen om økonomiske kostnader for leverandør som belastes OsloMet dersom virksomheten forespør bistand?  *Eksempelvis i fm. revisjoner, risiko- og sårbarhetsanalyser (ROS), personvernkonsekvensvurdering (DPIA) ol.* | Ja | Nei |
| Utdyp nærmere, ved behov: | | |