**Innledning:**

**Sjekkliste for behandling av personopplysninger i henhold til ny personopplysningslov (GDPR)**

**Hensikt og målgruppe**

Denne sjekklisten er ment som et praktisk redskap som universiteter og høyskoler kan anvende i arbeidet med å kartlegge dagens tilstand og å tilpasse seg kravene i den nye personopplysningslovgivningen (GDPR). Det nye lovverket trer i kraft fra 25. mai 2018.

Målgruppen er ansatte ved universiteter og høyskoler som deltar i lokale GDPR-prosjekter eller som har ansvaret for at systemer og tjenester er tilpasset det nye lovverket, for eksempel system- eller tjenesteeiere/-ansvarlige.

**Innhold og oppbygning**

Sjekklisten inneholder 25 spørsmål om sentrale krav som stilles til den behandling av personopplysninger som universiteter og høyskoler er ansvarlige for (behandlingsansvarlig). Sjekklisten må gjennomgås for hvert enkelt system/tjeneste hvor det behandles personopplysninger, for eksempel om studenter, ansatte, gjester eller deltakere i forskningsprosjekter.

Under hvert spørsmål følger en hjelpetekst som gir en kort forklaring til hva spørsmålet handler om. Deretter følger tre felter som institusjonene må fylle ut. Det første feltet gjelder hva som er status i dag på det området som spørsmålet omhandler. Det andre feltet gjelder hvilke eventuelle avvik som finnes mellom statusen på området og de krav som den nye personopplysningsloven (GDPR) stiller. Det tredje feltet omhandler en beskrivelse av hvilke tiltak som eventuelt må iverksettes for at institusjonen skal kunne overholde de krav som gjelder på det området som spørsmålet omhandler. Til slutt lenkes det til ressurser som kan være nyttige for å forstå reglene bedre og i arbeidet med å avdekke og lukke eventuelle regelavvik.

Institusjonene oppfordres til å melde inn ressurser, det vil si løsninger på konkrete oppgaver, slik at de kan deles med resten av sektoren.

**Utfylling og prioritering**

Det anbefales at sjekklisten fylles ut av personer med god kjennskap til hvert enkelt system eller tjeneste (og til hvordan det brukes), for eksempel system- eller tjenesteeiere/-ansvarlig. Det vil være en fordel at system- eller tjenesteeiere/-ansvarlig (ved behov) kan få hjelp til å utfyllingen fra lokalt ansatte som har særlig kompetanse på den nye lovgivningen (GDPR).

Etter som universiteter og høyskoler er ansvarlige for et stort antall systemer og tjenester, bør de viktigste prioriteres. Dette er systemer eller tjenester i administrasjon, undervisning eller forskning som behandler store mengder personopplysninger om mange registrerte. Nedenfor finnes lenke til en oversikt over systemer eller tjenester som bør prioriteres.

**Lukking av avvik**

Dersom kartleggingen av behandling av personopplysninger i systemer eller tjenester avdekker viktige avvik fra det nye lovverket, må disse avvikene lukkes. Institusjonene må derfor avsette ressurser for lukking av eventuelle avvik (mellom dagens tilstand og lovverkets krav). Allokering av ressurser til lukking av avvik bør inngå som en del av planleggingen av det lokale GDPR- og kartleggingsarbeidet.

**Samarbeidsgruppen for GDPR i UH-sektoren**

Kort om gruppen og hvem som er med.

Ressurser: Lenke til (i) norsk oversettelse av forordningen, (ii) Datatilsynets veiledningssider, (iii) forklaring av grunnleggende begreper i forordningen (Ceres), (iv) oversikt over systemer/tjenester som bør prioriteres.

**Sjekkliste for behandling av personopplysninger ved [navn på institusjonen]**

**Gjelder for [navn på system/tjeneste]**

1. **Hvem er ansvarlig for at systemet, applikasjonen eller tjenesten (og tilhørende arbeidsprosesser) er tilpasset kravene i GDPR?**

Navn på system-, applikasjons- eller tjenesteansvarlig:

1. **Hvilke typer personopplysninger behandles i systemet, applikasjonen eller tjenesten og hva brukes opplysningene til (formål)?**

*Hjelpetekst: Det må finnes en oversikt over hvilke hovedtyper personopplysninger som systemet, applikasjonen eller tjenesten behandler. Dernest må det beskrives hva opplysningene skal brukes til (formål). Formålet må (der hvor det er mulig) være såpass tydelig definert at det tydelig fremgår hva opplysningene skal brukes til, hva de ikke skal brukes til og hvilke opplysninger som er nødvendige/relevante for den aktuelle bruken (formålet). Formålet kan for eksempel være studieadministrasjon (FS) eller lønnsutbetaling og personaladministrasjon (lønns- og personalsystem).*

Gjør rede for hvilke typer personopplysninger som behandles i systemet, applikasjonen eller tjenesten:

Gjør rede for hva opplysningene i systemet, applikasjonen eller tjenesten brukes til:

Beskriv tiltak for lukking av eventuelle avvik, for eksempel at formålet for bruken av opplysningene må vurderes/defineres:

1. **Behandles sensitive (særskilte) personopplysninger i systemet, applikasjonen eller tjenesten?**

*Hjelpetekst: Behandling av sensitive personopplysninger er ikke lenger konsesjonspliktig etter de nye personvernreglene. Det må likevel kartlegges/avklares om sensitive personopplysninger behandles i systemet, applikasjonen eller tjenesten. Det vil blant annet ha betydning for hvor strenge krav som skal stilles til informasjonssikkerheten i systemet, applikasjonen eller tjenesten og om det er nødvendig å gjennomføre en personvernkonsekvensutredning.*

Gjør rede for hvilke typer sensitive personopplysninger som eventuelt behandles i systemet, applikasjonen eller tjenesten:

Ressurser: Lenke til dokument med definisjon av sensitive personopplysninger.

1. **Inneholder systemet, applikasjonen eller tjenesten opplysninger som strengt tatt ikke er nødvendige/relevante, og finnes det rutiner for kontroll av dette?**

*Hjelpetekst: Opplysningene som registreres og behandles i systemet, applikasjonen eller tjenesten skal være nødvendige/relevante for det opplysningene er tenkt brukt til (formål). Det er derfor ikke anledning til å registrere og behandle overskuddsinformasjon, det vil si opplysninger som ikke er nødvendige/relevante. Det skal finnes rutiner for kontroll av opplysningenes nødvendighet/relevans og for sletting av eventuell overskuddsinformasjon.*

Gjør rede for om det finnes rutiner for kontroll av nødvendighet/relevans:

Gjør rede for eventuell overskuddsinformasjon:

Beskriv tiltak for lukking av eventuelle avvik, for eksempel etablering av rutiner for gjennomgang og sletting av overskuddsinformasjon:

1. **Omtrent hvor mange registrerte (studenter, ansatte, osv.) finnes det opplysninger om i systemet, applikasjonen eller tjenesten?**

*Hjelpetekst: Systemet, applikasjonen eller tjenesten kan for eksempel inneholde opplysninger om alle studenter eller alle ansatte (oppgi ca. antall).*

Oppgi hvem (studenter, ansatte, osv.) og hvor mange det er registrert opplysninger om:

1. **Hvilken lovlig grunn (behandlingsgrunnlag) gjelder for behandling av opplysninger i systemet, applikasjonen eller tjenesten?**

*Hjelpetekst: Behandling av personopplysninger defineres som et inngrep i den enkeltes personvern. Det må derfor finnes en lovlig grunn (behandlingsgrunnlag) for all behandling av personopplysninger. Hvilke behandlingsgrunnlag som er aktuelle, listes opp i forordningens artikkel 6 og artikkel 9 (gjelder for behandling av sensitive personopplysninger). Samtykke fra ansatte/studenter eller hjemmel i universitets- og høyskoleloven er eksempler på behandlingsgrunnlag. Andre viktige lovlige grunner er at behandling av personopplysninger er nødvendig for å utøve offentlig myndighet, for eksempel fatte enkeltvedtak, for å ivareta forpliktelser i avtaler som institusjonen har inngått eller for å drive forskning. I tillegg finnes en rekke andre lovlige grunner som listes opp i artikkel 6 og 9.*

Gjør rede for lovlig grunn (behandlingsgrunnlag):

Beskriv tiltak for lukking av eventuelle avvik (lovlig grunn mangler og må defineres):

Ressurs: Lenke til norsk oversettelse av personvernforordningen.

1. **Anvendes opplysningene til noe helt annet enn det de opprinnelig skulle brukes til (gjenbruk), og hva er den lovlige grunnen til det?**

*Hjelpetekst: Opplysninger som er innsamlet for et bestemt formål, for eksempel adgangskontroll for fysisk sikring av bygninger/rom, kan ikke senere anvendes til et helt annet og uforenelig formål, for eksempel at passeringsdata fra adgangskontrollsystemet benyttes til kontroll med de ansattes arbeidstid/tilstedeværelse. Dette kan likevel gjøres dersom den enkelte har samtykket til den nye bruken eller den nye bruken er hjemlet i lov eller forskrift. Personopplysninger kan også i mange tilfeller lovlig gjenbrukes til arkiverings- og forskningsformål.*

Gjør rede for hvilke formål opplysningene gjenbrukes til:

Gjør rede for om det er gitt samtykke eller foreligger lovhjemmel for den nye bruken:

Beskriv tiltak for lukking av eventuelle avvik, for eksempel at ulovlig gjenbruk avsluttes:

1. **Finnes det rutiner for kvalitetssikring, for eksempel oppdatering eller feilretting, av personopplysninger i systemet, applikasjonen eller tjenesten?**

*Hjelpetekst: Det skal finnes rutiner for kvalitetssikring av personopplysninger i forbindelse med førstegangs innsamling/registrering av personopplysninger og ved endring av opplysningene i systemet, applikasjonen eller tjenesten.*

Gjør rede for om det finnes rutiner for kvalitetssikring:

Beskriv tiltak for lukking av eventuelle avvik (etablere rutiner for kvalitetssikring):

1. **Hvor lenge er det nødvendig å lagre opplysningene og finnes det rutiner for sletting, eventuelt arkivering?**

*Hjelpetekst: Personopplysninger som institusjonen ikke lenger har konkret bruk for skal slettes fra systemet, applikasjonen eller tjenesten. Det vil derfor ikke være lovlig å oppbevare personopplysninger med tanke på at de kan komme til nytte i fremtiden (da skal opplysningene eventuelt samles inn på nytt). Personopplysninger som er arkivverdige er unntaket fra sletteplikten (de skal ikke slettes).*

Gjør rede for hvor lenge opplysningene oppbevares:

Gjør rede for om det finnes rutiner for sletting eller arkivering av opplysningene:

Beskriv tiltak for lukking av eventuelle avvik, for eksempel at lagringstiden må endres:

1. **Utleveres opplysninger til andre aktører/virksomheter og hva er grunnlaget for utleveringen?**

*Hjelpetekst: Det kan tenkes at enkelte opplysninger som er registrert i systemet, applikasjonen eller tjenesten utleveres til andre aktører/virksomheter. Dette kan være andre offentlige organisasjoner som har behov for dem i sin saksbehandling eller virksomhet, for eksempel skatteetaten, NAV eller DBH. Institusjonen må ha oversikt over hvilke opplysninger som utleveres og hvilket lovlig grunnlag (behandlingsgrunnlag) som utleveringen baserer seg på (vanligvis hjemmel i lov eller forskrift).*

Gjør rede for hvilke andre aktørene/virksomhetene som er mottakere av opplysningene:

Gjør rede for hvilke opplysninger som utleveres til andre aktører/virksomheter:

Gjør rede for det lovlige grunnlaget for utleveringen:

Beskriv tiltak for lukking av eventuelle avvik, for eksempel at utleveringsgrunnlaget må avklares:

Det utleveres ikke opplysninger til andre aktører/virksomheter:

1. **Er det laget en personvernerklæring for systemet, applikasjonen eller tjenesten?**

*Hjelpetekst: Personvernerklæringer gir de registrerte, for eksempel studenter eller ansatte, grunnleggende informasjon om ulike forhold knyttet til bruken av opplysninger om dem i systemet, applikasjonen eller tjenesten. Denne informasjonen er avgjørende for at de registrerte skal kunne ivareta andre rettigheter de har etter lovverket, blant annet retten til innsyn i egne opplysninger.*

Gjør rede for om personvernerklæring finnes og hvor den i så fall er publisert:

Beskriv tiltak for lukking av eventuelle avvik her (etablering av erklæringer der hvor dette mangler):

Ressurser: Lenke til eksempel på personvernerklæring - FS.

1. **Finnes det rutiner/løsninger for ivaretakelse av retten til å kreve innsyn i, retting og sletting av egne opplysninger?**

*Hjelpetekst: Systemer, applikasjoner eller tjenester skal tilrettelegges slik at de registrertes rett til innsyn, retting og sletting kan ivaretas på en så enkel måte som mulig (innebygd personvern). De registrerte, for eksempel studenter eller ansatte, har rett til å få endret unøyaktige opplysninger og at ufullstendige opplysninger blir supplert med utfyllende informasjon. Retten til sletting gjelder for eksempel når samtykke trekkes tilbake og når opplysningene ikke lenger er nødvendige for formålet. De registrerte har ikke krav på sletting av opplysninger som er oppbevaringspliktige.*

Gjør rede for om slike rutiner/løsninger finnes:

Gjør rede for hvilke rutiner/løsninger som eventuelt mangler:

Beskriv tiltak for lukking av eventuelle avvik (etablering av manglende rutiner/løsninger):

Ressurser: Lenke til Datatilsynets veileder om de registrertes rettigheter.

1. **Finnes det rutiner/løsninger for ivaretakelse av retten til å protestere mot og å kreve begrenset behandling av egne opplysninger?**

*Hjelpetekst: De registrerte, for eksempel studenter og ansatte, har rett til å protestere mot at opplysninger om dem behandles. Retten til å protestere gjelder når den lovlige grunnen for behandlingen av opplysningene er (i) utførelse av en oppgave i allmenhetens interesse, (ii) utøvelse av offentlig myndighet og (iii) ivaretakelse av en berettiget interesse. De registrerte har rett til å kreve begrensninger i bruken av egne opplysninger. Denne retten gjelder blant annet når de registrerte bestrider opplysningenes riktighet, og ikke ønsker at opplysningene skal brukes før feil/mangler er rettet. Riktigheten av opplysningene må da kontrolleres og eventuelt feil/mangler korrigeres før opplysningene igjen kan brukes.*

Gjør rede for om slike rutiner/løsninger finnes:

Gjør rede for hvilke rutiner/løsninger som eventuelt mangler:

Beskriv tiltak for lukking av eventuelle avvik (etablering av manglende rutiner/løsninger):

Ressurser: Lenke til Datatilsynets veileder om de registrertes rettigheter.

1. **Finnes rutiner/løsninger for varsling ved retting, sletting eller begrenset behandling av personopplysninger?**

*Hjelpetekst: Opplysninger om enkeltpersoner kan i mange tilfeller bli gjenbrukt på tvers av systemer, applikasjoner eller tjenester. Det betyr at dersom krav om retting, sletting eller begrenset behandling av personopplysninger etterkommes, må opplysningene også rettes, slettes eller ikke behandles i alle andre systemer, applikasjoner eller tjenester hvor de samme opplysningene benyttes. Det må derfor finnes rutiner/løsninger for varsling om dette, spesielt der hvor opplysningene blir utlevert til eksterne aktører/virksomheter.*

Gjør rede for om slike rutiner/løsninger finnes:

Gjør rede for hvilke rutiner/løsninger som eventuelt mangler:

Beskriv tiltak for lukking av eventuelle avvik (etablering av manglende rutiner/løsninger):

Ressurser: Lenke til Datatilsynets veileder om de registrertes rettigheter.

1. **Finnes det rutiner/løsninger for ivaretakelse av retten til dataportabilitet?**

*Hjelpetekst: De registrerte, for eksempel studenter eller ansatte, har rett til dataportabilitet, inkludert direkte overføring av egne opplysninger til systemer, applikasjoner eller tjenester som driftes av eksterne aktører/virksomheter. Retten til dataportabilitet gjelder bare dersom den lovlige grunnen for behandlingen er samtykke fra den enkelte eller er basert på avtale med den registrerte, for eksempel arbeidsavtale. Retten gjelder der hvor det er tilrettelagt (teknisk) for slik dataoverføring.*

Gjør rede for om slike rutiner/løsninger finnes:

Gjør rede for hvilke rutiner/løsninger som eventuelt mangler:

Beskriv tiltak for lukking av eventuelle avvik (etablering av manglende rutiner/løsninger):

Retten gjelder ikke for systemet, applikasjonen eller tjenesten:

Ressurser: Lenke til Datatilsynets veileder om de registrertes rettigheter.

1. **Finnes det rutiner/løsninger som å ivareta rettigheter som gjelder ved helautomatiserte beslutninger?**

*Hjelpetekst: Det kan tenkes at institusjonen fatter vedtak om den registrerte, for eksempel ansatte eller studenter, ved hjelp av helautomatiserte beslutningssystemer. Bruk av slike beslutningssystemer vil bare være lovlig under visse forutsetninger, for eksempel dersom den registrerte har gitt sitt samtykke til automatisert saksbehandling eller dersom automatiseringen er hjemlet i lov/forskrift. Ved automatisert saksbehandling har den registrerte rett til å kreve manuell kontroll av beslutningen, til å uttrykke sine synspunkter i saken og til å bestride resultatet av saksbehandlingen.*

Gjør rede for om slike rutiner/løsninger finnes:

Gjør rede for hvilke rutiner/løsninger som eventuelt mangler:

Beskriv tiltak for lukking av eventuelle avvik (etablering av manglende rutiner/løsninger):

Det skjer ikke helautomatisert saksbehandling i dette systemet, applikasjonen eller tjenesten:

Ressurser: Lenke til Datatilsynets veileder om de registrertes rettigheter.

1. **Finnes det rutiner/løsninger for ivaretakelse av kravet om innebygd personvern?**

*Hjelpetekst: Innebygd personvern omfatter tekniske og organisatoriske tiltak som har til hensikt å overholde reglene i forordningen og å unngå krenkelser av den enkeltes personvern. Reglene om innebygd personvern gjelder både for egenutviklede systemer, applikasjoner eller tjenester og ved innkjøp/anskaffelse av «hyllevare». Innebygd personvern må derfor tas hensyn til både i utviklings- og anskaffelsesprosesser. Kravet til innebygd personvern kan blant annet inkludere rutiner for ivaretakelse av de registrertes rettigheter, tekniske løsninger for innsyn (for eksempel min-side-funksjonalitet), logging av oppslag i systemer/tjenester, rollebasert tilgangsstyring, automatisk sletting av opplysninger, anonymisering av opplysninger eller kryptering av opplysninger som på lagres eller som overføres via internettet.*

Gjør rede for eksisterende løsninger for innebygd personvern:

Gjør rede for innebygde personvernløsninger som planlegges eller bør etableres:

Ressurs: Lenke til Datatilsynets veileder om innebygd personvern.

1. **Driftes systemet, applikasjonen eller tjenesten – eller deler av det – av en ekstern leverandør, og er det inngått databehandleravtale med leverandøren?**

*Hjelpetekst: Eksterne leverandører (databehandlere) kan være andre UH-institusjoner eller kommersielle selskaper, blant annet leverandører av skytjenester eller andre nettbaserte tjenester. Det skal inngås databehandleravtaler med eksterne leverandører som behandler personopplysninger som institusjonen er ansvarlig for. Databehandleravtaler kan bare inngås dersom det først er gjennomført en risikovurdering av informasjonssikkerheten i systemet, applikasjonen eller tjenesten, og det konkluderes med at informasjonssikkerheten er tilfredsstillende. Dersom risikovurderingen viser at informasjonssikkerheten ikke er tilfredsstillende, vil det ikke være lovlig å anvende det aktuelle systemet, applikasjonen eller tjenesten (selv om det inngås en databehandleravtale).*

Gjør rede for om databehandleravtale er inngått og hvor den eventuelt oppbevares:

Beskriv tiltak for lukking av eventuelle avvik (inngåelse av manglende avtaler):

Problemstillingen er ikke relevant for systemet, applikasjonen eller tjenesten:

Ressurser: Lenke til sjekkliste og mal for databehandleravtaler.

1. **Finnes det rutiner for oppfølging av eksterne leverandører (databehandlere), spesielt kontroll med at vilkår i databehandleravtaler overholdes?**

*Hjelpetekst: Forholdet til eksterne leverandører (databehandlere) skal forvaltes av institusjonen. Forvaltningen omfatter kontroll med at avtalevilkår overholdes av leverandøren, spesielt med tanke på informasjonssikkerheten. Viktige endringer i systemet, applikasjonen eller tjenesten skal meldes til og godkjennes av institusjonen. Slike endringer kan utløse behov for at det gjennomføres en ny risikovurdering av informasjonssikkerheten for å avdekke om den fortsatt er tilfredsstillende. Rapporter fra sikkerhetsrevisjoner hos leverandøren skal være tilgjengelig for og gjennomgås av institusjonen.*

Gjør rede for om slike rutiner finnes:

Gjør rede for eventuelle rutiner som mangler:

Beskriv tiltak for lukking av eventuelle avvik (etablering av manglende rutiner):

1. **Vil personopplysninger bli overført til land utenfor EU/EØS, og hva er i så fall grunnlaget for overføringen?**

*Hjelpetekst: Det er i utgangspunktet forbudt å overføre personopplysninger til land utenfor EU/EØS-området. Slik overføring kan for eksempel skje i forbindelse med bruk av skytjenester eller andre typer nettbaserte tjenester. Overføringen vil likevel være lovlig dersom den skjer (i) til land som EU har definert som godkjente mottakerland, (ii) det inngås egne avtaler som regulerer overføringen av opplysningene (EUs standardavtaler for overføring) eller (iii) det finnes et annet lovlig overføringsgrunnlag, for eksempel til selskaper (i land utenfor EU/EØS) som har innført og har fått godkjent bedriftsinterne regler for behandling av personopplysninger (binding corporate rules).*

Gjør rede for land utenfor EU/EØS som opplysningene overføres til:

Gjør rede for grunnlaget for overføringen:

Beskriv tiltak for lukking av eventuelle avvik, for eksempel etablering av overføringsgrunnlag:

Problemstillingen er ikke relevant for systemet, applikasjonen eller tjenesten:

Ressurser: Lenke til oversikt over godkjente mottakerland og EUs standard overføringsavtaler.

1. **Blir sikkerheten til opplysningene i systemet, applikasjonen eller tjenesten håndtert i henhold til de krav som stilles i ledelsessystemet for informasjonssikkerhet?**

*Hjelpetekst: KDTO har laget et rammeverk for ledelsessystem for informasjonssikkerhet som anbefales av Kunnskapsdepartementet, jf. tildelingsbrevet til institusjonene. Ledelsessystemet skal gi toppledelsen styring og kontroll med informasjonssikkerheten ved egen institusjon, og omfatter en rekke aktiviteter. Eksempler på slike aktiviteter er ledelsens gjennomgang, risikovurderinger, melding og håndtering av avvik, sikkerhetsrevisjoner og varsling av sikkerhetshendelser til Datatilsynet. Mange av disse aktivitetene skal gjennomføres (helt eller delvis) på system-/tjenestenivå.*

Gjør rede for hvordan krav til informasjonssikkerheten ivaretas for systemet, applikasjonen eller tjenesten:

Gjør rede for hvilke krav som eventuelt ikke ivaretas:

Beskriv tiltak for lukking av eventuelle avvik:

Ressurser: Lenke til KDTOs rammeverket, DIFIs veileder for internkontroll/informasjonssikkerhet og KDTOs veileder om kravene til informasjonssikkerhet i GDPR.

1. **Er det gjennomført risikovurdering av informasjonssikkerheten til personopplysningene i systemet, applikasjonen eller tjenesten og er nødvendige sikringstiltak iverksatt?**

*Hjelpetekst: Risikovurderinger av informasjonssikkerheten i systemer, applikasjoner eller tjenester er det viktigste redskapet for å avdekke og redusere trusler mot uautorisert tilgang til personopplysninger (konfidensialitet), uautorisert endring eller sletting av opplysningene (integritet) og at opplysningene ikke er tilgjengelige for de som har rettmessige behov for tilgang til dem (tilgjengelighet). Sikringstiltak skal iverksettes dersom risikovurderingene viser at informasjonssikkerheten ikke er tilfredsstillende, det vil si at risikoen for brudd på konfidensialiteten, integriteten eller tilgjengeligheten vurderes å være uakseptabel høy.*

Gjør rede for om og eventuelt når siste risikovurdering av systemet/tjenesten ble gjennomført:

l

Gjør rede for om nødvendige sikringstiltak ble iverksatt:

Beskriv tiltak for lukking av eventuelle avvik (plan for gjennomføring av manglende risikovurderinger eller for etablering av nødvendige sikringstiltak):

Ressurs: Lenke til KDTOs veileder for gjennomføring av risikovurderinger, til Datatilsynets veileder og til risikovurderinger som kan deles med sektoren.

1. **Er det etablert og innført rutiner/løsninger for melding av avvik og sikkerhetsbrudd?**

*Hjelpetekst: Avvik fra lokale rutiner for behandling av personopplysninger og brudd på informasjonssikkerheten til opplysningene skal meldes som avvik. Avvikene skal håndteres slik at ønsket/normal tilstand gjenopprettes så fort som mulig. Det må derfor finnes rutiner/løsninger for melding og håndtering av avvik og sikkerhetsbrudd. Rutinene/løsningene må være kjent blant studenter/ansatte og de må anvendes når behovet oppstår. Til slutt må det finnes rutiner for varsling av Datatilsynet og de registrerte (studenter, ansatte, osv.) ved alvorlige brudd på sikkerheten til personopplysninger.*

Gjør rede for om slike rutiner/løsninger finnes:

Gjør rede for eventuelle rutiner/løsninger som mangler:

Beskriv tiltak for lukking av eventuelle avvik (etablering av manglende rutiner/løsninger):

Ressurs: Lenke til retningslinjer for varsling av Datatilsynet og de registrerte.

1. **Finnes det rutiner/metodikk for gjennomføring av personvernkonsekvensutredninger og konsultasjon med Datatilsynet?**

*Hjelpetekst: For enkelte systemer, applikasjoner eller tjenester vil det være pålagt å gjennomføre utredninger av personvernkonsekvenser. Konsekvensutredningene skal vurdere risikoen for at bruken av systemet, applikasjonen eller tjenesten kan føre til at institusjonen ikke greier å ivareta sine personvernplikter og de registrertes rettigheter, og hvilke tiltak som i så fall bør iverksettes for å unngå dette. Dersom utredningen viser at det er stor risiko for at plikter/rettigheter ikke kan ivaretas på en god nok måte, skal Datatilsynet kontaktes for rådgiving/veiledning om hva som bør gjøres for å løse problemet (konsultasjon). Datatilsynet vil publisere en liste over hva som vil omfattes av kravet om konsekvensutredning. En slik liste foreligger ikke per dags dato.*

Gjør rede for om det finnes slike rutiner/metodikk:

Gjør rede for eventuelle rutiner/metodikk som mangler:

Beskriv tiltak for lukking av eventuelle avvik (etablering av manglende rutiner/metodikk):

Ressurser: Lenke til Datatilsynets veileder om utredning av personvernkonsekvenser og Utredningsinstruksens veileder for vurdering av personvernkonsekvenser. Lenke til Datatilsynets liste når den blir publisert.

1. **Er det utnevnt et ombud for behandling av personopplysninger ved institusjonen (personvernombud)?**

*Hjelpetekst: Statlige universiteter og høyskoler er pålagt å utnevne personvernombud for behandlinger av personopplysninger i administrasjon, undervisning og forskning. Ombudet skal være uavhengig. Ombudet skal blant annet føre kontroll med at reglene i det nye lovverket overholdes og gi råd til institusjonen i spørsmål knyttet til behandling av personopplysninger.*

Sett inn navn og kontaktinformasjon til personvernombudet:

Beskriv tiltak for lukking av eventuelle avvik (plan for utnevnelse av ombud):

Ressurser: Lenke til Datatilsynets veileder om personvernombud.

**Protokoll med oversikt over behandlinger**

Den nye personopplysningslovgivningen (GDPR) stiller krav om at det føres en oversikt over behandlingen av personopplysninger ved institusjonen (protokoll, jf. artikkel 30). Oversikten skal blant annet inneholde informasjon om formålet med behandlingen av personopplysningene, hvem opplysningene gjelder (de registrerte), om opplysningene vil bli overført til land utenfor EU/EØS, lagringstiden og hvilke sikringstiltak som er etablert.

Ved at denne sjekklisten fylles ut for hvert system, applikasjon eller tjeneste som behandler personopplysninger, vil dette kravet være ivaretatt.