Vedlegg E – Eksempel kundeinformasjon personvern

Personopplysninger i it's learning

1 Innledning

1.1 Formål

Denne informasjonspakken fra it's learning as skal hjelpe databehandlingsansvarlige ved brukersted til å gjennomføre sine lovpålagte oppgaver i henhold til personvern ved bruk av læringsplattformen it's learning.

Informasjonspakken skal veilede databehandlingsansvarlig gjennom vurderinger og aktiviteter som etter lov må gjennomføres ved bruk av it's learning og tilsvarende verktøy, samt gi tilstrekkelig informasjon om personverntema som inntreffer ved bruk av it's learning.

Den behandlingsansvarlige ved brukerstedet er ansvarlig for å etterleve lovens krav. Personopplysningsloven forvaltes av Datatilsynet (www.datatilsynet.no) og har tilhørende personopplysningsforskrift med veiledninger. På internettsidene til Datatilsynet finnes mye informasjon om etterlevelse av personopplysningslovens krav. Som eksempel kan følgende trekkes frem:

- **Sikkerhetsbestemmelser**
  Sikkerhetsbestemmelsene i personopplysningsforskriften stiller konkrete krav til virksomhetene
- **Risikovurdering**
  Datatilsynet har laget en veiledning om risikovurdering av informasjonssystemer
- **Veiledning for kommuner og fylker**
  Veilederen for informasjonssikkerhet er rettet inn mot kommuner og fylkeskommuner, men kan også brukes av andre virksomheter som behandler personopplysninger
- **Tynne klienter**
  Dette dokumentet er en veileder for bruk av terminaltjener/tynne klienter (terminaler uten egen lagringsenhet og programvare) for å skille samtidige brukere i åpne og sikre soner
- **Kryptering**
  Når sensitive personopplysninger overføres over eksterne datanett krever Datatilsynet at informasjonen beskyttes gjennom bruk av kryptering
- **Konsesjonssøknader**
  Ved behandling av konsesjonssøknader vurderer Datatilsynet om behandlingsansvarlig med rimelighet kan sies å ha ivaretatt plikten til forholdsmessig sikring av personopplysningene

Hvorfor er personopplysningsloven viktig for deg?

Personopplysningsloven gjelder for alle foretak som benytter personopplysninger. Foretakene er selv ansvarlig for å etterleve krav i loven.

Generelt sett og uavhengig av læringsprogramvaren it's learning stilles det klare krav til organisasjoner og foretak som bruker personopplysninger. Som et utgangspunkt må følgende hovedaktiviteter utføres og dokumenteres:

- Behandlingsansvarlig må identifiseres. Dette er vanligvis foretakets øverste leder. Dette er den som er personlig ansvarlig dersom personopplysninger brukes i strid med loven

- Prosesser der personopplysninger inngår må beskrives. Formål med bruk av personopplysninger må dokumenteres. Melding foretas til Datatilsynet og kan utføres på Datatilsynets hjemmesider. For it's learning-relaterte behandlinger, se kap. 2.
- Risikovurdering av behandlingene skal utføres. Vinklingen på risikovurderingen skal være sett i forhold til den registrerte. Se mer om dette i kap. 3
- Internkontrollsystem skal etableres og dokumenteres. Veiledning for hva et slikt internkontrollsystem skal inneholde kan finnes på Datatilsynets hjemmesider. Mer informasjon om dette finnes i kap. 4

Organisasjonen/foretaket er selvstendig ansvarlig for å etterleve lovens krav. Dette ansvaret kan ikke overføres til leverandør. Dette dokumentet er kun ment som en veiledning og fritar ikke institusjonen for noen av sine forpliktelser iht. personopplysningsloven ved bruk av it's learning.

1.2 Ansvar

Behandling av opplysninger og vurderinger som kan knyttes til en enkeltperson og som helt eller delvis skjer med elektroniske virkemidler, er det sentrale virkeområdet for Personopplysningsloven (Lov av 14. april 2000 om behandling av personopplysninger). Personopplysningsloven gjelder bare behandling av opplysninger og vurderinger som kan knyttes til fysiske personer.

Det er den behandlingsansvarlige - den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes - som må sørge for at lovens bestemmelser etterleves. I forholdet mellom kunden og it's learning as vil kunden være behandlingsansvarlig, dette til tross for at it's learning as ved utformingen av systemet har stor påvirkning på hvilke opplysninger som kan registreres og hvordan de registrerte opplysningene kan behandles.

Kunden må sikre at behandlingen har et grunnlag i personopplysningsloven. Ettersom systemet muliggjør omfattende registrering av informasjon om brukeren vil behandlingen kreve et samtykke fra brukeren dersom innhenting av opplysningene ikke kan hjemles i annen lovgivning. Samtykket skal være en frivillig, uttrykkelig og informert erklæring fra brukeren om at han eller hun godtar behandling av opplysninger om seg selv (§8 og §11).

Det er også kunden som må melde behandlingen eller eventuelt søke Datatilsynet om konsesjon dersom det er identifisert bruk av personopplysninger som er meldepliktige. Utgangspunktet er at meldeplikt gjelder for behandling av ikke-sensitive personopplysninger, mens behandling av sensitive personopplysninger som ikke er avgitt uoppfordret er underlagt konsesjonsplikt. Loven har en rekke unntak fra meldeplikten som kan medføre at Datatilsynet ikke behøver å motta melding om foretakets bruk av personopplysninger.

Som leverandør av ASP-tjenester, vil it's learning as behandle personopplysninger på kundens vegne, it's learning as er derfor en databehandler for kunden. Databehandleren er i loven (§ 13) pålagt selvstendige plikter med hensyn til informasjonssikkerhet ved behandlingen. Personopplysningsloven § 15 krever at det foreligger en skriftlig avtale mellom databehandleren og den behandlingsansvarlige hvor det reguleres på hvilken måte databehandleren kan behandle personopplysningene.

1.3 Definisjoner

Emne	Definisjon
Personopplysningsloven (POL)	Lov om behandling av personopplysninger, 14. april 2000 nr. 31

Personopplysningsforskriften (POF)	Forskrift til personopplysningsloven, 15. desember 2000 nr. 1265 Ikrafttredelse 01.01.2001
Behandling av person-opplysninger	Jfr. POL §2 Definisjoner Enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter
Databehandlingsansvarlig	Jfr. POL §2 Definisjoner Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Det er kunde som er behandlingsansvarlig og som i forhold til brukerne av system må sikre grunnlaget for behandlingen.
Databehandler	Jfr. POL §2 Definisjoner Den som behandler personopplysninger på vegne av den behandlingsansvarlige. I forhold til læringsplattformen er it's learning as databehandler på vegne av kunden.
Personopplysning	Jfr. POL §2 Definisjoner Opplysninger og vurderinger som kan knyttes til en enkeltperson
Samtykke	Samtykke er hovedregel i personopplysningsloven. Loven er bygget på prinsippet om enkeltindividets selvråderett over personopplysninger om seg selv. Samtykket skal være frivillig i den forstand at tjenester ikke kan nektes som følge av at den enkelte ikke vil oppgi personopplysninger ut over det som er lovmessig hjemlet. Samtykket skal være informert slik at alle kan ha forutsetninger til å forstå hva avgivelse av personopplysninger innebærer og hva de skal brukes til.

1.4 FAQ

Datatilsynet har på sine hjemmesider (www.datatilsynet.no) dokumentert de mest vanlige spørsmålene som tilsyns- og sikkerhetsavdelingen får.

- **Er fødselsnummer sensitiv eller taushetsbelagt informasjon?**
  I henhold til personopplysningsloven, så er ikke fødselsnummer ansett å være en sensitiv opplysning. Det er heller ikke taushetsbelagt (ref. forvaltningsloven §13). Fødselsnummer kan imidlertid bare brukes når det er saklig behov og det er umulig å identifisere personer ved andre metoder.
  Et vanlig spørsmål i forbindelse med læringsplattformer angr nødvendighet av bruk av fødselsnummer i forbindelse med integrasjon mot elev-/studentadministrative systemer, katalogtjenester m.m. Siden fødselsnummer er identiteten som gjør det mulig å koble disse systemene sammen er det en vanlig tolkning at dette er et saklig behov for bruk av fødselsnummer.

- **Når kan innsyn nektes fra eleven (i fht. foresatte etc.)?**
  Se kap. 5.1

- **Hvor ofte skal risikovurdering utføres?**
  Risikovurdering skal gjøres årlig eller ved endringer/nyinstalleringer som kan påvirke prosesser der personopplysninger inngår. Se kap. 3 for utfyllende opplysninger og metodikk.

- **Gjennomgang av brukere i it's learning**
  Gjennomgang av brukermassen i it's learning bør gjøres jevnlig. Brukere skal etter en viss periode med inaktiv bruk slettes. Denne gjennomgangen er spesielt aktuell der brukere i it's learning ikke er koblet mot et studentadministrativt system.
  En vanlig tolkning er at elever/studenter som har fullført et studie ved en utdanningsinstitusjon må fjernes fra systemet fordi det ikke lenger er saklig behov for å lagre disse personopplysningene.

  I de tilfeller der it's learning er integrert mot studentadministrative system vil denne koblingen håndtere sletting av brukere som ikke lenger er knyttet til utdanningsinstitusjonen. Her er det viktig å understreke at en slik sletting kun legger brukere i it's learnings "søppelbøtte" og at permanent sletting må foretas av systemadministrator.

- **Innmelding av behandlinger**
  For de prosesser der personopplysninger inngår og som ikke er unntatt melde- og konsesjonsplikt, gjelder det at de skal innmeldes til Datatilsynet når de opprettes, etter endringer i prosessen og jevnlig hvert tredje år dersom ingen endring er gjort med prosessene. Bruk av it's learning vil i utgangspunktet ikke medføre meldeplikt. Her er det imidlertid læringsinstitusjonens eget ansvar å etterse at bruken ikke medfører innhenting av personopplysninger som utløser meldeplikt

- **Oppbevaringstid for backup**
  Det er den enkelte behandlingsansvarlig ved læringsinstitusjonen som er ansvarlig for å etterse at backuprutinene hos databehandler ikke medfører konflikt vedrørende oppbevaringstid av lagrede data. Dialog må inngås med databehandler og enighet må oppnås om en maksimal oppbevaringstid som er innenfor akseptabel tid for lagring av også slettet informasjon. Hvor lenge dette er vil variere etter hvilken hjemmel slik oppbevaring har. Dersom oppbevaring av backup- taper har som formål å sikre at man har bevis i ulike klagesaker hjemlet i utdanningsloven, så er det dette som vil gjelde. Dersom slik hjemmel ikke kan benyttes så vil lagringen kunne hjemles i driftstekniske behov og lagringstiden vil måtte bli noe kortere.

2 Kartlegging av personopplysninger

2.1 Innledning

Lov om behandling av personopplysninger ble gjort gjeldende fra 01.01.2001. Loven setter blant annet krav til beskrivelse av kontrollmiljøet i virksomheter som behandler personopplysninger.

Vedlagt følger oversikt over prosesser der det inngår personopplysninger som fremkommer som følge av bruk av programvaren it's learning. Prosessene der det inngår personopplysninger er dokumentert på et generelt grunnlag. Institusjonen som tar i bruk læringsløsningen må på eget selvstendig grunnlag kartlegge sin bruk av personopplysninger. Dokumentasjonen herfra kan med fordel benyttes i dette arbeidet.

2.2 Databehandler

Institusjonen vil fremstå som behandlingsansvarlig i forhold til de arbeidsprosesser der det inngår bruk av personopplysninger. Formålet med bruk av personopplysninger og hvilke hjelpemidler som skal brukes må dokumenteres. Behandlingsansvarlig er ansvarlig for at dette utføres.

Etter POL § 2 er en databehandler ”den som behandler opplysninger på vegne av den behandlingsansvarlige”. Dette innebærer at databehandler kan være en formelt sett annen juridisk enhet enn behandlingsansvarlig.

I praksis er databehandler den som har ansvar for drift, vedlikehold og informasjonssikkerhet til databaser inneholdende personopplysninger.

Personopplysningslovens § 15 stiller krav til skriftlig inngått avtale som regulerer databehandlers plikter. Avtalen skal inneholde en erklæring fra databehandler om etterlevelse av lovens krav. Det anbefales at tilsvarende avtaler inngår med de ”interne databehandlere” som bidrar med drift av databaser etc.

Databehandler er selvstendig ansvarlig for å etterleve krav i personopplysningsloven.

Behandlingsansvarlig som eier personopplysningene er på sin side ansvarlig for at persondata kun utveksles med foretak som etterlever personopplysningslovens krav.

2.3 Kartlegging av behandlinger

Innledning

Etter personopplysningsloven er institusjonen som er behandlingsansvarlig pålagt å utarbeide en oversikt over alle prosesser der personopplysninger inngår (kartlegge behandlinger), utarbeide en risikovurdering og etablere et styringssystem for informasjonssikkerhet (internkontroll). Arbeidet med å kartlegge de ulike prosessene der personopplysninger inngår danner således grunnlaget for å møte krav oppstilt i personopplysningsloven.

Ved innføring av it's learning vil kunden som et utgangspunkt ikke få konsesjons- eller meldepliktig behandling av personopplysninger. Dette avhenger imidlertid av at informasjonen som legges inn i elæringssystemet ikke er personopplysninger i en systematisk form (eksempelvis bruk av elæringssystemet til forskningsdokumentasjon knyttet til personer, etc.). Institusjonen som tar læringssystemet i bruk er selvstendig ansvarlig for å etterse at bruken av læringssystemet ikke går ut over de initielt beskrevne personopplysningsprosessene.

En rekke behandlinger er i lov og forskrift unntatt fra konsesjons- og meldeplikt. Dette gjelder også for elev- og studentopplysninger ved skoler og universiteter mv (Forskrift om behandling av personopplysninger §7-20). Utdanningsinstitusjonen må gjøre en selvstendig vurdering av om bruken av personopplysninger i it’s learning er meldepliktig eller untatt meldeplikt.

Identifiserte behandlinger

Det er kundens eget ansvar å identifisere de behandlinger av persondata som kommer inn under kundens behandlingsansvar. Men for å lette dette arbeidet foreslår dette dokumentet typiske behandlinger av personopplysninger som kan finne sted etter innføring av læringsplattformen:

1. Bruk av læringsplattform til utdanningsformål
2. IT-drift
3. Administrasjon av brukere i læringsplattformen

Bruk av læringsplattform til utdanningsformål

Behandlingen

Formålet med denne behandlingen er å gi den enkelte læringsinstitusjon anledning til å benytte læringsplattformen som en integrert del av sin undervisning. Studenter og lærere skal benytte it's learning til kommunikasjon seg imellom, til lagring av egen studieproduksjon på eget brukerområde og egenpublisert studiemateriale innenfor læringsinstitusjonen, og for læringsinstitusjoner som inngår i et avtaleregulert samarbeid.

Hjemmelsgrunnlaget

Hjemmel for behandling av relevante opplysninger vil følge av POL § 8 første ledd bokstav a, d og f, som åpner for behandling av personopplysninger.

Konsesjons- eller meldeplikt

Elektronisk behandling av personopplysninger vil være unntatt meldeplikt jfr. POF §§ 7-11, 7-16, 7-20 og 7-21.

Kunden sin behandlingsansvarlig er selvstendig ansvarlig for vurdering av om denne behandlingen er meldepliktig til Datatilsynet for den spesifikke bruksmåten av læringssystemet.

IT-drift

Behandlingen

Formålet med behandlingen er å overvåke og drifte it-systemene med tilhørende maskin- og programvare for å opprettholde tilgjengelighet og informasjonssikkerhet. Logger registrerer aktivitet i IT-systemene. Logger administreres av systemadministrator for databasen som derfor er å anse som databehandlere etter loven, med de forpliktelser dette pålegger dem.

Behandlingen dekker også teknisk assistanse gitt til brukere der dette er forhåndsavtalt. Parametre unik for den enkelte bruker benyttes der dette er nødvendig. Help desk vil da få tilgang til den enkelte brukers profil i det tidsrommet som assistanse er nødvendig, basert på samtykke fra bruker.

Hjemmelsgrunnlaget

Dette tiltaket er hjemlet i POL § 8 b). Begrensinger er pålagt for oppbevaring av IT-logger i lov.

Konsesjons- eller meldeplikt

Opplysninger som finnes i IT-loggene vil være unntatt fra både konsesjons- og meldeplikt, jfr. POF §§ 7-11, 7-16, 7-20 og 7- 21. Unntaket forutsetter at opplysningene bare blir brukt til å administrere systemet eller for å avdekke/oppklare brudd på sikkerheten i systemet. Unntaket gjelder følgelig ikke ved registrering tenkt benyttet til kontroll- eller overvåkingsformål.

Dokumentasjon av rutiner knyttet til informasjonssikkerhet skal lagres i minst 5 år, mens hendelsesregister skal lagres i minst tre måneder, jf. POF § 2- 16. Rutiner for oppbevaring av IT-logger bør finnes tilgjengelig.

Rutiner for oppbevaring, beskyttelse og gjennomgang av logger bør finnes tilgjengelig.

Kunden sin behandlingsansvarlig er selvstendig ansvarlig for vurdering av om denne behandlingen er meldepliktig til Datatilsynet for den spesifikke bruksmåten av læringssystemet.

Administrasjon av brukere i læringsplattformen

Behandlingen

Formålet med behandlingen er å føre kontroll med tilgangen til læringssystemet gjennom utstedelse og distribusjon av personlig brukernavn og passord. Den fysiske adgangskontrollen til databaser utøves av databehandler.

Administratorkommunikasjon er kryptert (https). Institusjonen kan på selvstendig grunnlag slå på kryptering for vanlig brukerkommunikasjon.

Hjemmelsgrunnlaget

Hjemmel for behandling av relevante opplysninger vil følge av samtykke fra den enkelte bruker og POL § 8 første ledd bokstav a, d og f, som åpner for behandling av personopplysninger.

Konsesjons- eller meldeplikt

Opplysninger som finnes i tilknytning til brukeradministrasjon i it's learning vil være unntatt fra både konsesjons- og meldeplikt, jfr. POF §§7-11, 7-16, 7-20 og 7-21.

Kunden sin behandlingsansvarlig er selvstendig ansvarlig for vurdering av om denne behandlingen er meldepliktig til Datatilsynet for den spesifikke bruksmåten av læringssystemet.

2.4 Behandlingsmatrise

Formål/ kategori	**Behandling/ type aktivitet**	**Hjemmel**	**Konsesjonsplikt**	**Meldeplikt**	**Behandlings- ansvarlig**	**Lovpålagt Taushets- plikt**	**Antall registrerte (personer eller transaksjoner)**	**K/T/I***
Undervisning	**It's learning** • Fag/kursarbeid • Prosjektarbeid • Kommunikasjon	Samtykke (Avtaleforhold), POL §8 bokstav a og f. (Opplærings- loven, Universitets- loven)	Nei (forutsatt ikke sensitive opplysninger)	Nei, POF §§7-7, 7-11, 7-16, 7-20 og 7-21	Behandlingsansvarlig	Nei	Vurderes av den enkelte institusjon	K/T/I
Drift av systemet	**IT-Drift** - Overvåkning av drifts parametre - Drift av produksjonsmiljøet - Feilretting - Aktivitetslogg (Identifikasjon, tidsregistrering) -Brukerassistanse	Samtykke (Avtaleforhold), POL §8 bokstav a og f. (Opplærings- loven, Universitets- loven)	Nei (forutsatt ikke sensitive opplysninger)	Nei, POF §§7-7, 7-11, 7-16, 7- 20 og 7-21	Behandlingsansvarlig	Nei	Vurderes av den enkelte institusjon	K/I
Tilgangskontroll	**Brukeradministrasjon** - Tilgang til IT-systemer - Identifikasjon - Tidsregistrering	Samtykke (Avtaleforhold), POL §8 bokstav a og f. (Opplærings- loven, Universitets- loven)	Nei (forutsatt ikke sensitive opplysninger)	Nei, POF §§7-7, 7-11, 7-16, 7-20, 7-21	Behandlingsansvarlig	Nei	Vurderes av den enkelte institusjon	K/T/I

*K=Konfidensialitet, I=Integritet og T=Tilgjengelighet i forhold til viktighet for de registrerte

2.5 Hvem har tilgang til hvilke data

Se oversikt for hvem som har tilgang til hvilke data

3 Risikovurdering

3.1 Formål og hensikt

Formålet med risikovurdering er å undersøke hvorvidt den risiko som avdekkes er innenfor de akseptkriterier for behandling av personopplysninger som er fastlagt av virksomheten. Personopplysningsforskriften krever at den behandlingsansvarlige skal gjennomføre slike vurderinger for å klarlegge sannsynlighet for og konsekvenser av sikkerhetsbrudd (POF §2- 4). I tillegg kan Datatilsynet gi pålegg om sikring av personopplysninger og fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger (POF §2- 2). Risikovurderingen skal videre ligge til grunn for prosedyrer og instrukser som skal sikre personvernet og inngå som en del av internkontrollsystemet.

Risikovurderinger bør gjennomføres årlig og skal gjennomføres ekstraordinært ved endringer som har betydning for informasjonssikkerheten, eksempelvis endringer i informasjonssystemet som læringsverktøyet er en del av eller endringer i trusselbildet. Resultatet av risikovurderingen skal i henhold til POF §2-4 dokumenteres.

I risikovurderingen bør det legges vekt på sikring av informasjonens tilgjengelighet, konfidensialitet og integritet/kvalitet. I tillegg bør organisatoriske forhold som påvirker sikkerheten - i hovedsak rutiner knyttet til informasjonsbehandlingen vurderes.

3.2 Ansvar

Det er databehandlingsansvarlig som har ansvar for at risikovurdering blir utført jevnlig og ved endringer som kan påvirke informasjonssikkerheten.

3.3 Forenklet risikovurdering - bruk av personopplysninger

Generelt

Behandling av personopplysninger er i utgangspunktet ikke sentralt i institusjonens hverdag. Selv om det ikke er et hovedanliggende for institusjonen å behandle personopplysninger så bør det etterstrebes å ha en høy standard på måten personopplysninger oppbevares, brukes, oppdateres og videreformidles.

Institusjonen er blant annet gjennom personopplysningsloven pålagt å ha et internkontrollsystem i bruk for å holde en høy standard på måten personopplysninger behandles. Risikovurdering skal inngå i et internkontrollsystem for behandling av personopplysninger.

Institusjonen skal etter pålagte krav gjennomføre en kartlegging av de personopplysningsbehandlingene som utføres. Denne kartleggingen skal dokumenteres i internkontrollsystemet. På bakgrunn av denne kartleggingen skal Datatilsynet meldes der dette er påkrevd. For å sikre at kartleggingen og melding til Datatilsynet representerer nåsituasjonen for behandling av personopplysninger, skal denne forenklede risikovurderingen sikre at endringer i og nye IT- systemer, utlevering og annen ny bruk av personopplysninger dekkes av internkontrollsystemet. Dersom denne forenklede risikovurderingen viser at eksisterende rutiner ikke er dekkende, så må det sørges for at et tilstrekkelig internkontrollmiljø er på plass før behandlingen av personopplysninger starter opp.

Når skal du fylle ut en forenklet risikovurdering for behandling av personopplysninger?

En slik vurdering skal alltid foretas når personopplysninger ønskes benyttet til et annet formål enn de er innhentet for. Eksempel på dette kan være:

- markedsaktiviteter som ønsker å gjøre bruk av brukerinformasjon
- innføring av nye IT-løsninger som henter personinformasjon fra andre IT-systemer der informasjonen har blitt samlet inn til et annet spesifikt formål
- en ønsket utlevering av statistisk informasjon til eksterne institusjoner

Definisjoner

Emne	Definisjon
Akseptabel risiko	Kriterier basert på forskrifter, standarder, erfaring og/eller teoretisk kunnskap som legges til grunn for beslutninger om akseptabel risiko. Akseptkriterier kan uttrykkes med ord eller være tallfestet.
Konsekvens	Mulig følge av en uønsket hendelse. Konsekvens kan uttrykkes med ord eller som en tallverdi for omfanget av skader.
Sannsynlighet	Sannsynligheten for en hendelse uttrykker muligheten for at denne hendelsen skal inntreffe og angis ved Lav, Middels eller Høy.
Risiko	Uttrykk for den fare som uønskede hendelser representer for den enkelte person sine elektroniske personopplysninger. Risiko uttrykkes ved sannsynligheten for og konsekvensene av de uønskede hendelsene (Trusler og årsaker)
Konfidensialitet	Det at informasjon ikke er tilgjengelig for uautoriserte personer eller ikke godkjente systemer.
Integritet	Det at informasjon ikke blir endret eller ødelagt på en uautorisert måte. (Informasjonen representerer det den gir seg ut for).
Tilgjengelighet	Det at informasjon eller dataressurser er til stede og anvendelige etter behov.

Punktvis veiledning til Risikovurdering - personopplysninger its learning**, Forenklet risikovurdering**

A. Beskrivelse av prosjektet

Denne seksjonen skal inneholde en kort beskrivelse av prosjektet. En slik beskrivelse skal eksempelvis inneholde:

- Ansvarlig
  Navnet på leder som er ansvarlig for prosjektet/løsningen
- Institusjon og Avdeling
  Navnet på institusjon og avdeling som prosjektet/løsningen sorterer under
- Formål
  Hvilket formål prosjektet/løsningen er ment å dekke
- Analyseobjekt
  Hvilke grupper informasjon inngår i prosjektet/løsningen?
- Målgruppe
  Hvem skal få tilgjengelig resultatet/informasjonen fra prosjektet/løsningen?

- Tidsavgrensning
  Når startes opp og eventuelt avsluttes prosjektet/løsningen?

Benytt gjerne eget ark til å beskrive prosjektet/løsningen. Forsøk å gjøre dette så kort og konsist som mulig.

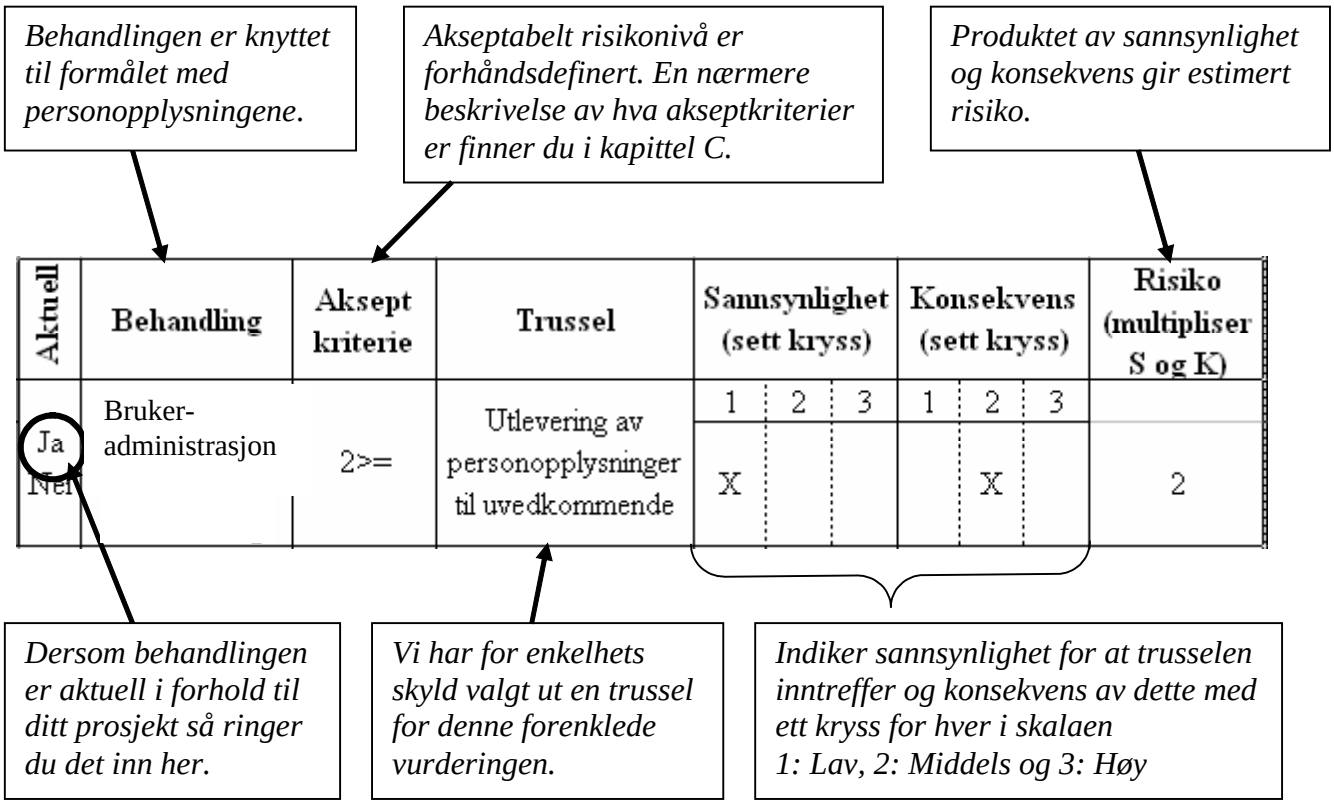
B. Risikovurderingsmatrise

I Risikovurdering - personopplysninger its learning er de forhåndsdefinerte behandlingene kartlagt. Denne forenklede risikovurderingen skal verifisere at kartleggingen og konsesjon/melding til Datatilsynet fremdeles er dekkende. Derfor må det til enhver tid sørges for at det foreligger oppdatert informasjon om nye prosjekter (forskning) og nye løsninger (tekniske og organisatoriske) som berører personopplysninger i institusjonen.

Følgende behandlinger er definert og meldt til Datatilsynet:

Behandling/Formål	Beskrivelse
Bruk av læringsplattform til utdanningsformål	Formålet med denne behandlingen er å gi den enkelte læringsinstitusjon anledning til å benytte læringsplattformen som en integrert del av sin undervisning. Studenter og lærere skal benytte it's learning til kommunikasjon seg imellom, til lagring av egen studieproduksjon på eget brukerområde og egenpublisert studiemateriale innenfor læringsinstitusjonen, og for læringsinstitusjoner som inngår i et avtaleregulert samarbeid.
IT-drift	Formålet med behandlingen er åovervåke og drifte it-systemene med tilhørende maskin- og programvare for å opprettholde tilgjengelighet og informasjonssikkerhet. Logger registrerer aktivitet i IT-systemene. Logger administreres av systemadministrator for databasen som derfor er å anse som databehandlere etter loven, med de forpliktelser dette pålegger dem. Behandlingen dekker også teknisk assistanse gitt til brukere der dette er forhåndsavtalt. Parametre unik for den enkelte bruker benyttes der dette er nødvendig. Help desk vil da få tilgang til den enkelte brukers profil i det tidsrommet som assistanse er nødvendig, basert påsamtykke fra bruker.
Administrasjon av brukere i læringsplattformen	Formålet med behandlingen er å føre kontroll med tilgangen til læringssystemet gjennom utstedelse og distribusjon av personlig brukernavn og passord. Den fysiske adgangskontrollen til databaser utøves av databehandler. Administratorkommunikasjon er kryptert (https). Institusjonen kan på selvstendig grunnlag slåpåkryptering for vanlig brukerkommunikasjon.
Annet?	Dersom ingen av de overnevnte behandlingene/formålene dekker behovet, så bør behandlingsansvarlig kontaktes for videre gjennomgang.

Eksempel på utfylling i risikovurderingsmatrisen



Vi ser av dette eksempelet at estimert risiko er lik akseptabel risiko. Dette medfører at det ikke er påkrevd å iverksette sannsynlighets- eller konsekvensreduserende tiltak.

Eksempler på sannsynlighets- og konsekvensreduserende tiltak

Sannsynlighetsreduserende tiltak

- Opplæring i informasjonssikkerhet og den registrertes rettigheter til innsyn og utlevering av personopplysninger
- Kvalitetskontroll av informasjon av to uavhengige ledd før utlevering
- Merking av informasjon som sensitiv
- Ikke la sensitiv informasjon ligge fremme på skrivebordet

Konsekvensreduserende tiltak

- Dobbel konvolutt ved postforsendelse
- Behandle personrelatert informasjon på egne PCer frakoblet nettet
- Nedlåsing av personrelatert informasjon
- Konfidensiell informasjon sendes ikke på e-post

C. Eksisterer det gap mellom identifisert risiko og akseptabel risiko?

Akseptkriterier må bestemmes og dokumenteres.

D. Korrigerende tiltak er iverksatt og hensyntatt i prosjektet.

Der man gjennom utfylling av punkt B, Risikovurderingsmatrise, har funnet gap mellom identifisert og akseptabel risiko, skal en foreslå korrigerende tiltak slik at risikoen blir akseptabel i forhold til behandling av personopplysninger. Når tiltakene er iverksatt og hensyntatt i prosjektet/løsningen, signeres punkt D ut.

E. Signering

Gjennomfører av forenklet risikovurdering signerer her.

Vedlegg

Risikovurdering - personopplysninger its learning.xls

4 Internkontroll

4.1 Innledning

Personopplysningsloven §14 krever at den som behandler personopplysninger skal etablere et internkontrollsystem. Internkontrollsystemet skal systematisere prosedyrer og instrukser som sørger for at loven og tilhørende regelverk er kjent blant ansatte og blir fulgt. Databehandlingsansvarlig har ansvar for at dette etableres, dokumenteres og vedlikeholdes. Dokumentasjonen over internkontrollsystemet skal være tilgjengelig for de ansatte og for Datatilsynet. Datatilsynet tilbyr en sjekkliste for internkontroll på sine websider (www.datatilsynet.no)

For enheter som benytter it's learning, vil som regel følgende regelverk være relevant (listen er ikke uttømmende):

- Personopplysningsloven (POL)
- Personopplysningsforskriften (POF)
- Opplæringsloven
- Universitetsloven
- Forvaltningsloven - Lov om behandlingsmåten i forvaltningssaker (som forvaltningsorgan regnes et hvert organ for stat og kommune)

4.2 Samtykke

Bruk av it's learning muliggjør omfattende registrering av personopplysninger. I henhold til personopplysningsloven, krever dette samtykke fra brukeren (POL §§8 og 11).

it's learning har utviklet et forslag til samtykkeklausul.

4.3 Innsyn, retting og sletting av personopplysninger

4.4 Taushetserklæring

Medarbeidere hos den behandlingsansvarlige skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten skal også omfatte annen informasjon med betydning for

informasjonssikkerheten. For brukere av it's learning bør det for eksempel vurderes om administratorer og systemadministratorer med utvidet tilgang til personopplysninger skal undertegne taushetserklæring.

4.5 Avviksbehandling

Uautorisert utlevering, bruk, endring eller sletting av personopplysninger skal registreres i henhold til en avviksrutine.

4.6 Informasjonssikkerhet

Informasjonssikkerhet omfatter alle tiltak som virksomheten iverksetter for å sikre dens informasjon. Informasjonssikkerhetsarbeidet bidrar således til å sikre og øke selskapets verdier, samt beskytte informasjonen mot utilsiktet endringer eller avsløringer.

Informasjonssikkerhet defineres med begrepene tilgjengelig, konfidensialitet og integritet:

- **Tilgjengelighet** - sikre at brukere har tilgang til de korrekte ressursene eller informasjon til rett tid og i riktig omfang.
- **Konfidensialitet** - hindre uautorisert personell tilgang til informasjon og ressurser.
- **Integritet** - sikre kvalitet på informasjonens gyldighet, nøyaktighet og fullstendighet.

Sikkerhetsmål og sikkerhetsstrategi bør formuleres og forankres i en sikkerhetspolicy som hensyntar ovenfor nevnte aspekter. Ansvar for sikkerhet må plasseres på rett instans.

5 Personvernproblemstillinger

5.1 Foreldretilgang til barns bruker og foresattes rolle

it's learning har ikke en spesifikk bruker-rolle tilpasset foreldre. Foreldrene kan inntil barnet er myndig få innsyn i barnets it's learning- bruker, men dette kan nektes av eleven når vedkommende har nådd myndighetsalder. Imidlertid bør eleven etter fylte 15 år samtykke til denne type innsyn. Dersom barnets modenhet før fylte 15 år tilsier det, bør samtykke fra barnet innhentes før foreldrepålogging tillates.

Dersom sensitiv informasjon/kommunikasjon foregår mellom lærer og elev i it's learning, kan det være problematisk å gi foreldre tilgang til elevens brukerområde. Dette kan anses som et taushetspliktsproblem for lærer.

I de tilfeller det ønskes at foreldre skal opprettes som egne brukere, bør det vurderes hvor hensiktsmessig dette vil være da vedkommende kan få adgang til å kommunisere med alle elever som er opprettet som it's learning-brukere ved skolen. Brukerfeil kan også lett føre til at foreldre får tilgang til annen informasjon som de ikke normalt sett skal ha tilgang til.

it's learning as har utviklet et forslag til brev til foresatte.

5.2 Oppbevaringstid for backup

Backup av data tas hver natt og det lagres opp til 3 versjoner av hver datafil. I avtale mellom leverandør og kunde, spesifiseres det at personopplysninger umiddelbart slettes når avtalen mellom partene opphører. Dette gjelder de operative data, mens backup av dokumenter og annet blir lagret i 3 år.

Opphold i studier og klageformål er viktige argumenter for oppbevaring av backup i så lang tidsperiode. Ved opphold i studier (fødselspermisjon og annet), ønsker studenten å ta opp igjen sine studier ved endt permisjon uten å

risikere å miste sitt påbegynte arbeid. Hva gjelder klagesaker, så kan begge parter ha behov for å hente frem data og dokumenter fra en tid tilbake for å argumentere for sine syn.

Datatilsynet mener det er uklart når et dokument anses slettet dersom det kan fremhentes igjen fra backup 3 år senere. Datatilsynet mener at en bruker skal kunne stole på at et dokument faktisk er slettet.

5.3 Redaktøransvar

Alle brukere i it's learning har et "mine webfiler"-område. Filer som ønskes offentliggjort lagres her og er åpent tilgjengelig for alle. Dette innebærer at støtende, ærekrenkende og annet ulovlig materiale kan tilgjengeliggjøres herfra og spres via kundens system. Dette kan ramme personvernet på flere måter og databehandlingsansvarlig bør ha tenkt gjennom reaksjoner/sanksjoner og ha et bevisst forhold til dette for å møte de tilfeller der dette eventuelt kan oppstå.

5.4 IT-logg

All anvendelse av it's learning blir logget. Formålet med dette er å registrere bruk og eventuelle forsøk på misbruk av informasjonssystemet. Forsøk på ikke-autorisert tilgang samt andre sikkerhetsbrudd vil kunne spores og tiltak kan settes i verk på grunnlag av dette.

5.5 Foretakssamarbeid ved bruk av it's learning

I de tilfellene der to foretak (for eksempel utdanningsinstitusjoner, kommuner e.l.) ønsker å samarbeide ved bruk av it's learning av en slik art at brukere kan kommunisere på tvers av foretak så må en slik bruk av informasjon avklares på forhånd. De behandlingsansvarlige må inngå avtale om formålet med bruken av it's learning på tvers av institusjonene/foretakene og en hjemmel for slik bruk må etableres (samtykke fra brukerne er det mest nærliggende i utgangspunktet).

Årsaker til en løsning som beskrevet over, kan være mindre læringsinstitusjoner eller kommuner som kan ha en administrativ effekt av å samordne tjenester knyttet til it's learning.

Dersom det kun dreier seg om å vise kurskatalog på tvers av institusjoner/foretak vil dette gå inn under behandlingen 'Bruk av læringsplattform til utdanningsformål' som foreligger ferdig kartlagt og risikovurdert.

5.6 Kan it's learning benyttes til å lagre sensitive data?

Systemet er ikke bygget med tanke på å oppfylle krav som stilles til behandling av sensitive personopplysninger. Det er derfor leverandørens klare anbefaling at systemet ikke benyttes til å lagre data av denne art. Kunden bør legge klare føringer for sine sluttbrukere av systemet for å hindre at denne type data kan bli registrert.