Innledning til mal for databehandleravtaler ved bruk av tjenester i Dataporten

Nedenfor følger mal for databehandleravtaler ved bruk av tjenester som tilbys via Dataporten. Malen kan anvendes av universiteter og høyskoler når de bestiller tjenester til bruk i administrasjon, forskning eller undervisning. Den baserer seg på Datatilsynets veiledninger og generelle forslag til databehandleravtaler. Disse er tilgjengelige på http://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/.

Behandlingsansvarlig og databehandlere

I henhold til personopplysningsloven med forskrift, er universiteter og høyskoler ansvarlige for å sikre personvernet til enkeltpersoner – studenter, ansatte, gjester og respondenter eller informanter i forskning – når institusjonene behandler personopplysninger[1] om dem. Universiteter og høyskoler defineres derfor i loven som behandlingsansvarlige. Leverandører av tjenester som behandler opplysninger om enkeltpersoner på vegne av (etter bestilling fra) universiteter eller høyskoler, blir i loven definert som databehandlere.

Tjenester som tilbys via Dataporten vil vanligvis behandle opplysninger om enkeltpersoner på vegne av (etter bestilling fra) universiteter eller høyskoler. Institusjonene er dermed behandlingsansvarlige for disse personopplysningene, mens tjenesteleverandørene er databehandlere for institusjonene.

Databehandleravtaler

Behandlingsansvarlig (universitet eller høyskole) er, ifølge personopplysningsloven, pålagt å inngå databehandleravtaler med hver enkelt databehandler (tjenesteleverandør). Hensikten med avtalene er å ivareta personvernet til studenter, ansatte, gjester og respondenter eller informanter i forskning når andre enn institusjonene selv behandler opplysninger om dem. Slike avtaler skal inngås både med norske og utenlandske tjenesteleverandører.

I databehandleravtalene skal behandlingsansvarlig (universitet eller høyskole) stille krav til:

- hvordan tjenesteleverandører håndterer personopplysninger om studenter, ansatte, gjester og respondenter eller informanter i forskning,

[1] Med personopplysninger menes alle opplysninger og vurderinger som kan knyttes til en bestemt og identifiserbar enkeltperson. Personopplysninger kan foreligge som tekst, bilder, lyd- eller videoopptak.

- hvordan tjenesteleverandører sikrer opplysningene mot uautorisert innsyn, eksponering, endring, sletting, tap eller ødeleggelse (informasjonssikkerhet).

Den behandlingsansvarlige (universitet eller høyskole) har også et ansvar for å følge opp at vilkårene i avtalene blir overholdt av tjenesteleverandørene.

Samtidig har tjenesteleverandørene et selvstendig ansvar for at personopplysninger som de behandler på vegne av (etter bestilling fra) universiteter eller høyskoler blir tilfredsstillende sikret mot uautorisert innsyn, eksponering, endring, sletting, tap eller ødeleggelse (informasjonssikkerhet).

Risikovurdering

Før universiteter eller høyskoler inngår databehandleravtaler med leverandører av tjenester som tilbys via Dataporten, er institusjonene pålagt å foreta risikovurdering av hver enkelt tjeneste. Risikovurderingen skal avgjøre om det er forsvarlig av hensyn til personvernet og informasjonssikkerheten å ta tjenesten i bruk.

Universiteter og høyskoler er videre pålagt å gjennomføre nye risikovurderinger dersom (a) tjenestenes oppbygning/virkemåte eller (b) institusjonenes bruk av tjenestene endres på vesentlige måter.

Avtaletilpasning

Vær oppmerksom på at malen for databehandler nedenfor er en generell anbefaling om hvordan slike avtaler kan utformes. Det kan derfor være behov for å tilpasse malen slik at den passer bedre for spesifikke tjenester i Dataporten. Hvert enkelt universitet eller høyskole må vurdere om slike tilpasninger er nødvendige, gjerne i samarbeid med aktuelle tjenesteleverandører. Dette gjelder særlig der hvor det i malen er markert med gult.

UNINETT kan bistå institusjonene med råd og veiledning i forbindelse risikovurderinger av tjenestene og tilpasninger av avtalemalen til spesifikke tjenester.

Databehandleravtale for <navn på tjeneste>

I henhold til personopplysningslovens § 13, jf. § 15 og personopplysningsforskriftens kapittel to, inngås følgende avtale mellom

<Navn på vertsorganisasjonen>, heretter kalt behandlingsansvarlig

og

<navn på tjenesteleverandør>, *leverandøren* av <navn på tjeneste>, som databehandler

1. Avtalens hensikt

Avtalen regulerer rettigheter og plikter etter Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven), og forskrift av 15. desember 2000 nr. 1265 (personopplysningsforskriften).

Avtalen regulerer <navn på tjenesteleverandør> sin håndtering av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, lagring og utlevering, i forbindelse med bruken av <tjeneste>.

Avtalen skal sikre at personvernet til de registrerte (studenter, ansatte, osv.) ikke krenkes ved behandling av personopplysninger i <navn på tjeneste>.

Vilkårene i denne avtalen går foran vilkår i andre avtaler inngått mellom behandlingsansvarlig og <navn på tjenesteleverandør> knyttet til <navn på tjeneste>.

2. Formål og formålsbegrensning

Formålet med <navn på tjenesteleverandør> sin behandling av personopplysninger på vegne av behandlingsansvarlig, er å levere og administrere <navn på tjeneste>.

Personopplysninger som <navn på tjenesteleverandør> behandler i <tjeneste> vil ikke bli brukt til andre formål enn dette.

3. Personopplysninger som behandles

<Navn på tjenesteleverandør> behandler følgende personopplysninger på vegne av behandlingsansvarlig i <navn på tjeneste>:

<her listes personopplysninger som behandles i tjenesten>

Eksempel:

- Epostadresse og portrettbilde.
- Bruker-ID
- Organisasjonstilhørighet
- Gruppetilhørighet (fag og studieretning)

4. Databehandlers plikter

<Navn på tjenesteleverandør> vil følge de instrukser for behandling av personopplysninger som behandlingsansvarlig har bestemt skal gjelde. Den behandlingsansvarliges instrukser er uttømmende beskrevet i denne avtalen.

Behandlingsansvarlig har rett til tilgang til og innsyn i de personopplysninger som <navn på tjenesteleverandør> håndterer på dennes vegne. Det samme gjelder for alle IT-løsninger som <navn på tjenesteleverandør> benytter til behandling av personopplysninger i <navn på tjeneste>. <Navn på tjenesteleverandør> vil gi nødvendig bistand til dette.

<Navn på tjenesteleverandør> vil bistå den behandlingsansvarlig ved ivaretakelse av den registrertes rettigheter, spesielt innsyn i, retting og sletting av personopplysninger, jf. personopplysningsloven kapittel III og IV.

5. Bruk av underleverandør

Alternativ 1: Dersom tjenesteleverandøren ikke benytter underleverandører:

<Navn på tjenesteleverandør> benytter ikke underleverandører eller andre tredjeparter til behandling av personopplysninger i forbindelse med administrasjon og levering av <navn på tjeneste>.

Alternativ 2: Dersom tjenesteleverandøren benytter underleverandører:

<Navn på tjenesteleverandør> benytter følgende underleverandører eller andre tredjeparter til behandling av personopplysninger i forbindelse med administrasjon og levering av <navn på tjeneste>:

- <navn på underleverandør a>
- <navn på underleverandør b>
- etc…

Følgende avtaler eksisterer mellom <navn på tjenesteleverandør> og underleverandører:

- <avtaler>

Behandlingsansvarlig vil på forespørsel få tilgang til nevnte avtaler.

Dersom <navn på tjenesteleverandør> tar i bruk nye underleverandører skal behandlingsansvarlig informeres om og godkjenne dette.

6. Sikkerhet

<Navn på tjenesteleverandør> vil til enhver tid sørge for at informasjonssikkerheten til personopplysninger som behandles på vegne av behandlingsansvarlig i <navn på tjeneste>, er tilfredsstillende, jf. personopplysningsloven § 13 og personopplysningsforskriften kapittel to.

<Navn på tjenesteleverandør> vil dokumentere arbeidet med informasjonssikkerhet etter forespørsel fra behandlingsansvarlig.

<Navn på tjenesteleverandør> gjør jevnlig risikovurderinger av behandlingen av personopplysninger i <navn på tjeneste>. Nødvendige tekniske, fysiske eller organisatoriske sikringstiltak vil bli etablert for å forhindre ødeleggelse og tap eller uautorisert endring, eksponering og tilgang til personopplysninger.

Avviksmelding etter personopplysningsforskriftens § 2-6 skal skje ved at <navn på tjenesteleverandør> melder avviket til behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet.

<Navn på tjenesteleverandør> vil holde personopplysninger fra ulike behandlingsansvarlige forsvarlig adskilt fra hverandre. <Navn på tjenesteleverandør> vil dokumentere dette på forespørsel fra behandlingsansvarlig.

<Navn på tjenesteleverandør> vil loggføre all autorisert og forsøk på uautorisert bruk av personopplysninger i <navn på tjeneste>, jf. personopplysningsforskriften § 2-16. Loggene

oppbevares i minimum 3 måneder. Behandlingsansvarlig vil på forespørsel få tilgang til loggene.

Kun ansatte hos <navn på tjenesteleverandør> som har tjenstlige behov for tilgang til personopplysningene i <navn på tjeneste>, har slik tilgang. <Navn på tjenesteleverandør> vil dokumentere rutiner og retningslinjer for tilgangsstyring på forespørsel fra behandlingsansvarlig.

Ansatte hos <navn på tjenesteleverandør> har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Taushetsplikten gjelder også etter avtalens opphør.

Valgfri tekst:

For nærmere beskrivelse av sikringstiltak i <navn på tjeneste>, se vedlegg XX til denne avtalen.

7. Sikkerhetsrevisjoner

<Navn på tjenesteleverandør> vil jevnlig gjennomføre sikkerhetsrevisjoner av behandlingen av personopplysninger i <navn på tjeneste>. Behandlingsansvarlig vil gis tilgang til oppsummeringer av revisjonsrapportene.

Behandlingsansvarlig kan selv gjennomføre sikkerhetsrevisjoner av <navn på tjeneste> hos <navn på tjenesteleverandør>. <Navn på tjenesteleverandør> vil gi behandlingsansvarlig nødvendige bistand ved slike revisjoner. Kostnadene som dette medfører for <navn på tjenesteleverandør> vil faktureres behandlingsansvarlig.

8. Sletting av personopplysninger

Ved opphør av denne avtalen vil <navn på tjenesteleverandør> slette alle personopplysninger som behandles på vegne av behandlingsansvarlig og som omfattes av denne avtalen.

9. Avtalens varighet

Avtalen gjelder så lenge <navn på tjenesteleverandør> behandler personopplysninger på vegne av behandlingsansvarlig.

Ved brudd på denne avtale kan den behandlingsansvarlige pålegge <navn på tjenesteleverandør> å stoppe den videre behandlingen av personopplysninger med øyeblikkelig virkning.

10. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar <navn på lokal tingrett> som verneting. Dette gjelder også etter opphør av avtalen.

***

Denne avtale er akseptert og undertegnet av <navn på vertsorganisasjon> og <navn på tjenesteleverandør>.