UTKAST

Databehandleravtale mellom <instans> og Universitetet i Oslo, om behandling av personopplysninger i KADA

I henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016, Artikkel 28 og 29, jf. Artikkel 32-36, inngås følgende avtale

mellom

……

(behandlingsansvarlig)

og

Universitetet i Oslo, USIT

Org.nr 971035854

(databehandler)

16.09.2023

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter i henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, samt om oppheving av direktiv 95/46/EF.

Avtalen skal sikre at personopplysninger ikke brukes ulovlig, urettmessig eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Avtalen regulerer databehandlers forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med bruk av/behandling i KADA.

Ved motstrid skal vilkårene i denne avtalen gå foran databehandlers personvernerklæring eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler i forbindelse med bruk av/behandling i KADA.

2. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å forenkle hverdagen til studenter og fagpersoner ved å gi de en samlet oversikt over sine kalenderdata.

Kalenderdata oppstår i flere systemer, blant annet Timeplanlegging (TP), Felles Studentsystem (FS) og Exchange. Målet med KADA er å samle alt dette i Exchange, slik at hver person har en samlet oversikt over sine kalenderhendinger i sin personlige kalender i Exchange.

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål uten at dette på forhånd er godkjent av behandlingsansvarlig.

Databehandler kan ikke overføre personopplysninger som omfattes av denne avtalen til samarbeidspartnere eller andre tredjeparter uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. punkt 10 i denne avtalen.

3. Instrukser

Databehandler skal følge de skriftlige og dokumenterte instrukser for forvaltning av personopplysninger i KADA som behandlingsansvarlig har bestemt skal gjelde.

Universitetet i Oslo, ved USIT, forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av KADA til behandling av personopplysninger.

Databehandler forplikter seg til å varsle behandlingsansvarlig dersom databehandler mottar instrukser fra behandlingsansvarlig som er i strid med bestemmelsene i gjeldende norsk personopplysningslovgivning.

4. Opplysningstyper og registrerte

KADA samler inn personopplysninger fra flere system. KADA skaper ikke personopplysninger selv. Unntaket er en generert id for kvar kalenderaktivitet som KADA oppretter i Exchange.

Fra Felles Studentsystem (FS):

- Alle aktive undervisingsmeldinger til en person. Brukes for å legge inn undervisningsaktiviteter i kalenderen til studenter og fagpersoner. (Også kalt timeplan, eller emne).
- Alle aktive partipåmeldinger til en person. Brukes for å kunne legge inn gruppeundervisning i kalenderen til studenter og fagpersoner.
- Alle aktive vurderingsmeldinger til en person. Brukes for kunne legge inn når en student har eksamen.
- Alle roller en person har til ulike studieelement. Brukes for å kunne vedlikeholde kalenderen til fagpersoner, for eksempel foreleser og gruppelærer.
- Hvilke kull, klasse og studieprogram hver person er registrert på. Brukes for å kunne legge inn studieaktiviteter som er blitt registrert på kull, klasse eller studieprogram i Exchange.
- Personen sitt brukernavn. Brukes for å knytte person mot riktig brukerkonto i Exchange.
- Meldinger om endringer på en person sine registreringer. Brukes for å kunne legge til, endre og slette kalenderhendinger hendingsbasert.

Fra Timeplansystemet (TP):

- Detaljer om undervisning og andre møter. Dette er ikke personopplysninger, men det kobles mot data fra FS for å vite hva som skal legges i Exchange kalenderen til personen.

Fra Cerebrum:

- Personen sine brukernavn. Brukes til å knytte identitet mot riktig identitet i FS.
- Primær e-postadresse. Brukes for å knytte seg til riktig kalender i Exchange.

Fra Exchange:

- Identifikatorer til eksisterende kalenderhendinger som KADA allerede har lagt inn. KADA leser ikke andre kalenderhendinger fra Exchange, men spør spesifikt etter kalenderhendinger ut ifra hvilken identifikator som er lagret i KADA. Når KADA legg inn kalenderhendinger, genererast en id, som lagres på aktiviteten i Exchange, og som senere brukes for å kunne hente ut, redigere og slette kalenderhendingen.
- Eksisterende kalenderhendinger som KADA har oppretta i hver brukers personlige kalender. Disse har KADA produsert tidligere, men personen har full tilgang til å endre disse, så di kan inneholde endringer gjort av personen. KADA overskriver alle slike endringer gjort av bruker.

Grunnet tekniske begrensninger i tilgangsstyringen i Exchange, har KADA også tilgang til å lese alle kalenderaktiviteter hos hver bruker. KADA leser ikke disse kalenderaktivitetene selv om den har tilgang.

Personopplysningene gjelder følgende registrerte:

- Studenter hos databehandler som følger timeplanlagt undervisning
- Ansatte hos databehandler med rolle som fagperson i forbindelse med timeplanlagt undervisning

5. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretakelse av den registrertes rettigheter i henhold til gjeldende norsk personopplysningslovgivning.

Den registrertes rettigheter inkluderer retten til informasjon om hvordan hans eller hennes personopplysninger behandles, retten til å kreve innsyn i egne personopplysninger, retten til å kreve retting eller sletting av egne personopplysninger og retten til å kreve at behandlingen av egne personopplysninger begrenses.

I den grad det er relevant, skal databehandler bistå behandlingsansvarlig med å ivareta de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

Databehandler er erstatningsansvarlig overfor de registrerte dersom feil eller forsømmelser hos databehandler påfører de registrerte økonomiske eller ikke-økonomiske tap som følge av at deres rettigheter eller personvern er krenket.

6. Tilfredsstillende informasjonssikkerhet

Databehandler skal iverksette tilfredsstillende tekniske, fysiske og organisatoriske sikringstiltak for å beskytte personopplysninger som omfattes av denne avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler skal gi egne ansatte tilstrekkelig informasjon om og opplæring i informasjonssikkerhet slik at sikkerheten til personopplysninger som behandles på vegne av behandlingsansvarlig blir ivaretatt.

Se Universitetet i Oslo sitt Ledelsessystem for informasjonssikkerhet (LSIS) for prinsipper, retningslinjer og andre føringer som KADA styres etter.

7. Taushetsplikt

Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, kan gis slik tilgang. Databehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Ansatte hos databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør. Taushetsplikten omfatter ansatte hos tredjeparter som utfører vedlikehold (eller liknende oppgaver) av systemer, utstyr, nettverk eller bygninger som databehandler anvender for å levere tjenesten.

Behandlingsansvarlig skal sørge for tilsvarende tilgangskontroll og taushetsplikt om den dokumentasjon databehandler tilgjengeliggjør overfor behandlingsansvarlig.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos behandlingsansvarlig, databehandler og tredjeparter. Universitetet i Oslo er underlagt offentleglovas bestemmelser om offentlig innsyn.

8. Tilgang til sikkerhetsdokumentasjon

Databehandler plikter på forespørsel å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til gjeldende norsk personopplysningslovgivning.

Databehandler plikter på forespørsel å gi behandlingsansvarlig tilgang til annen relevant dokumentasjon som gjør det mulig for behandlingsansvarlig å vurdere om databehandler overholder vilkårene i denne avtalen.

Behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

9. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ugrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd.

Varselet til behandlingsansvarlig skal som minimum inneholde informasjon som beskriver sikkerhetsbruddet, hvilke registrerte som er berørt av sikkerhetsbruddet, hvilke personopplysninger som er berørt av sikkerhetsbruddet, hvilke strakstiltak som er iverksatt for å håndtere sikkerhetsbruddet og hvilke forebyggende tiltak som eventuelt er etablert for å unngå liknende hendelser i fremtiden.

Behandlingsansvarlig er ansvarlig for at Datatilsynet blir varslet når dette er påkrevd.

10. Underleverandører

Databehandler plikter å inngå egne avtaler med underleverandører som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med denne avtalen.

I avtaler mellom databehandler og underleverandører skal underleverandørene pålegges å ivareta alle plikter som databehandleren selv er underlagt i henhold til denne avtalen og lovverket. Databehandler plikter å forelegge avtalene for behandlingsansvarlig på forespørsel.

Databehandler skal kontrollere at underleverandører overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos underleverandører er kjent med sine forpliktelser og oppfyller disse.

Databehandler kan ikke engasjere underleverandører for å oppfylle denne avtalen uten at det på forhånd er skriftlig godkjent av behandlingsansvarlig.

Databehandler er erstatningsansvarlig overfor behandlingsansvarlig for økonomiske tap som påføres behandlingsansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører.

11. Overføring til land utenfor EU/EØS

Ingen personopplysninger skal overføres til tredjeland uten at det på forhånd er skriftlig godkjent av behandlingsansvarlig.

12. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Sikkerhetsrevisjoner skal omfatte databehandlers sikkerhetsmål og sikkerhetsstrategi, sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, etablerte tekniske, fysiske og organisatoriske sikringstiltak og arbeidet med informasjonssikkerhet hos underleverandører til denne avtalen. Det skal i tillegg omfatte rutiner for varsling av behandlingsansvarlig ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene på forespørsel.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal behandlingsansvarlig informeres om hvilken revisor som benyttes og få tilgang til oppsummeringer av revisjonsrapportene på forespørsel.

13. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å tilbakelevere og slette alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til denne avtalen. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Sletting skal skje ved at databehandler sletter personopplysninger innen 120 dager etter avtalens opphør. Dette gjelder også for sikkerhetskopier av personopplysningene.

Databehandler skal dokumentere at sletting av personopplysninger er foretatt i henhold til denne avtalen. Dokumentasjonen skal gjøres tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler dekker alle kostnader i forbindelse med tilbakelevering og sletting av de personopplysninger som omfattes av denne avtalen.

14. Mislighold

Ved mislighold av vilkårene i denne avtalen som skyldes feil eller forsømmelser fra databehandlers side, kan behandlingsansvarlig si opp avtalen med øyeblikkelig virkning.

Databehandler vil fortsatt være pliktig til å tilbakelevere og slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 13 ovenfor.

15. Erstatning

Behandlingsansvarlig kan kreve erstatning for økonomiske tap som feil eller forsømmelser fra databehandlers side, inkludert mislighold av vilkårene i denne avtalen, har påført behandlingsansvarlig, jf. også punkt 5 og 10 ovenfor.

Databehandler er erstatningsansvarlig for direkte økonomisk tap, herunder administrative overtredelsesgebyr og erstatningskrav som rettes mot behandlingsansvarlig, som kan tilbakeføres til brudd på databehandlerens forpliktelser i henhold til denne avtalen. Samlet erstatning per kalenderår er begrenset til et beløp som tilsvarer Hovedavtalens samlede årlige vederlag ekskl. merverdiavgift.

Har databehandler eller noen denne svarer for utvist grov uaktsomhet eller forsett, gjelder ikke de ovennevnte erstatningsbegrensningene.

16. Avtalens varighet

Denne avtalen gjelder så lenge databehandler forvalter personopplysninger på vegne av behandlingsansvarlig.

Avtalen kan sies opp av begge parter med en gjensidig frist på 6 måneder.

16. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er: Joakim Hovlandsvåg.

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er: _____.

17. Lovvalg og tvisteløsning

Partenes rettigheter og plikter etter denne avtalen bestemmes i sin helhet av norsk rett. Eventuelle tvister som springer ut av denne avtalen skal først søkes løst gjennom forhandlinger.

Dersom partene ikke oppnår enighet gjennom forhandlinger, skal tvisten løses med bindende virkning av Kunnskapsdepartementet. Hver av partene kan forlange at tvisten oversendes departementet.

***

Denne avtale er i 2 – to - eksemplarer, hvorav partene har hvert sitt.

16.09.2023

Sted og dato

På vegne av behandlingsansvarlig	På vegne av databehandler
……..	……
(Navn)	Gard Thomassen
(Tittel)	IT-direktør
(Virksomhet)	Universitetet i Oslo, USIT

16.09.2023