DATABEHANDLERAVTALE

mellom
Kristelig studieforbund, org. nr. 970 477 802 («databehandler»)
og
Medlemsorganisasjon/lokallag:

_____

(org. navn)

_____

(org. nr.)
(«behandlingsansvarlig»)

1 Formål

Denne avtalen regulerer behandling av personopplysninger som databehandler gjør på vegne av behandlingsansvarlig i henhold til avtalen om medlemskap i studieforbundet (heretter kalt «hovedavtalen»). Avtalen skal sikre at personopplysninger behandles i samsvar med norsk personvernlovgivning.

2 Databehandlers plikter

Databehandleren skal:

a) kun behandle personopplysninger i samsvar med behandlingsansvarliges dokumenterte instruksjoner. Behandlingsansvarlig skal straks informere databehandler dersom instruksjonene er mangelfulle eller i strid med norsk personvernlovgivning;
b) sikre at ansatte og underleverandører eller andre tredjeparter som er autorisert til å behandle personopplysninger på vegne av databehandler er underlagt taushetsplikt;
c) gjennomføre hensiktsmessige tekniske og organisatoriske tiltak som kreves i henhold til GDPR artikkel 32. Informasjonssikkerhetstiltakene er nærmere beskrevet i vedlegg 2;
d) iverksette dataminimerende tiltak, f. eks. pseudonymisering, for å begrense mengden av lagrede identifiserbare opplysninger;
e) sikre at det er inngått bindende avtale med eventuelle underdatabehandlere i henhold til GDPR artikkel 28 nr. 2 og 4;
f) varsle behandlingsansvarlig dersom personopplysninger skal overføres utenfor EØS og sikre at personopplysningene er adekvat beskyttet gjennom standard kontraktsvilkår utarbeidet av EU-kommisjonen eller andre grunnlag for overføring i henhold til GDPR;
g) gjøre all informasjon tilgjengelig på behandlingsansvarliges forespørsel (uten kostnad for behandlingsansvarlig) som er nødvendig for å dokumentere at behandlingsansvarlig og databehandler oppfyller GDPR artikkel 28. Databehandler skal legge til rette for at behandlingsansvarlig kan utføre revisjoner og inspeksjoner, enten av behandlingsansvarlig selv eller en tredjepart utpekt av behandlingsansvarlig;
h) føre protokoll (logg) over behandlingsaktiviteter denne utfører på vegne av den behandlingsansvarlige, som skal inneholde minimum den informasjon som er pålagt etter GDPR artikkel 30. Den behandlingsansvarlige kan til enhver tid kreve oversendt kopi av slik protokoll;
i) umiddelbart varsle den behandlingsansvarlige hvis databehandler mottar forespørsel fra en myndighet om å utlevere personopplysninger behandlet i henhold til denne avtalen. Databehandler plikter ikke å varsle dersom loven forbyr slik underretning;
j) bistå behandlingsansvarlig med å svare på forespørsler fra den registrerte i henhold til GDPR kapittel III (deriblant rett til informasjon, innsyn, retting og korrigering); og
k) bistå behandlingsansvarlig med å oppfylle sine forpliktelser i henhold til GDPR artikkel 32-36;

3 Varslingsrutiner

Ved datasikkerhetsbrudd skal databehandler gi melding til behandlingsansvarlig innen 48 timer. Meldingen skal minimum beskrive:

- arten av brudd på personopplysninger, herunder om mulig, kategoriene og omtrentlig antall berørte registrerte og kategoriene og omtrentlig antall berørte personopplysninger;
- navn og kontaktinformasjon til personvernansvarlig eller annet kontaktpunkt der mer informasjon kan fås;
- beskrive de sannsynlige konsekvensene av datasikkerhetsbruddet;
- beskrive tiltakene som er truffet eller foreslått for å ta hensyn til datasikkerhetsbruddet, herunder eventuelt tiltak for å redusere mulige bivirkninger.

Hvis ikke all informasjon ovenfor kan gis i første varsel, skal informasjonen gis så snart som mulig, og senest 72 timer innen datasikkerhetsbruddet har inntruffet. Behandlingssansvarlig skal sørge for at hendelsesrapporten sendes til Datatilsynet, dersom det kreves av GDPR artikkel 33.

4 Bruk av underleverandører og overføring utenfor EØS

Databehandleren har rett til å benytte underleverandører navngitt i vedlegg 1 som sine databehandlere.

Behandlingsansvarlig skal informeres om alle nye underleverandører som skal behandle personopplysninger på vegne av behandlingsansvarlig.

5 Revisjon

Hver av partene dekker sine egne kostnader forbundet med en revisjon. Hvis en revisjon avdekker ikke-uvesentlige avvik fra forpliktelsene i denne avtalen, skal alle kostnader forbundet med revisjonen dekkes av databehandleren, herunder den behandlingsansvarliges og eksterne revisorers rimelige kostnader.

6 Ansvar og erstatning

Partene er selv ansvarlig for å dekke administrative bøter og øvrige sanksjoner som ilegges som følge av brudd på personvernlovgivningen.

Dersom en part har blitt ilagt erstatningsansvar for et forhold som den andre parten står ansvarlig for skal den ansvarlige parten dekke erstatningskostnadene. Erstatningsansvaret er likevel begrenset til direkte kostnader, og ikke indirekte tap, i henhold til hovedavtalen.

7 Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig i henhold til hovedavtalen.

Ved databehandlers brudd på denne avtalen eller personvernlovgivningen kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

8 Tilbakelevering, sletting og/eller destruering ved avtalens opphør

Ved opphør av denne avtalen plikter databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av behandlingsansvarlig.

Behandlingsansvarlig kan kreve at databehandler sletter eller destruerer alle personopplysningene som behandles etter denne avtalen. Behandlingsansvarlig kan be databehandler skriftlig bekrefte til behandlingsansvarlig at sletting er gjennomført. Slettingen skal gjennomføres senest 60 dager etter

avtalens opphør. Sletting innebærer at personopplysningene slettes permanent fra alle systemer, med unntak av backup-systemet. Det er kun teknisk personale som har tilgang til backup-systemet.

9 Lovvalg og verneting

Lovvalg og verneting følger av hovedavtalen.

10 Signatur

Medlemmets signatur:

Hege Irene Fossum
Daglig leder
Kristelig studieforbund

Navn: _____

Tittel: _____

Org.: _____

Vedlegg 1: Behandlingens omfang

Formålet med behandlingen

Tilby et kursadministrasjonsverktøy (programvare) til kursarrangører, lærere og andre faglig ansvarlige. I kursverktøyet kan den enkelte bruker registrere studieplaner og kursrapporter, samt få tilbakemeldinger fra studieforbundet.

Hvilke opplysninger som behandles

Navn på registrert bruker, kontaktopplysninger (adresse, telefon, e-postadresse), kursdato, besvarelser og tilbakemeldinger som den enkelte selv legger opp i kursverktøyet.
Navn og adresse på lærer og andre faglig ansvarlige.
Navn, adresse, fødselsår og avkrysning for fremmøte på kursdeltaker.

Behandlingens art

Opplysningene lagres på server for å kunne tilby kursverktøyet. Opplysninger om kursdeltakelse (navn, fødselsdato, adresse og kursdato) rapporteres til myndighetene i henhold til dokumentasjonskravene i voksenopplæringsloven.

Kategorier av registrerte

Kursarrangørens kontaktperson, lærer og andre faglig ansvarlige for kurset og kursdeltakere.

Behandlingens varighet

Opplysningene lagres så lenge den registrerte har et aktivt kundeforhold med databehandler. Den registrerte skal varsles før opplysningene slettes og få mulighet til å overføre personopplysningene i et maskinleselig format (opplysningene skal være dataportabile).

Underdatabehandlere og overføring utenfor EØS

- Amazon Web Services EMEA SARL, Rue Plaetis 5, L-2338 LUXEMBOURG, Luxembourg.
- Amazon Web Services Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, USA.
- Cloudflare Inc., 665 3rd Street, Suite 200, San Francisco, CA 94107, USA.

Underdatabehandler står for løpende drift og vedlikehold av kursverktøyet. Databehandleren har underleverandører som overfører personopplysninger utenfor EØS, i henhold til reglene for overføring i GDPR.

Vedlegg 2: Sikkerhetstiltak

Pseudonymiseringstiltak

Opplysninger om inaktive brukere og lærere, deltakere som ikke har fullført kurs, eller deltakere på gamle kurs kan pesudonymiseres, anonymiseres eller slettes. Eier av opplysningene skal varsles minst 14 dager i forveien, og enten få anledning til å motsette seg tiltakene eller få tilbakelevert opplysningene.

Ved rapportering med statistikkformål til offentlige myndigheter overføres bare nøkkelopplysninger om kursdeltakernes kjønn og alder.

Krypteringstiltak

Tjenesten krever sikker forbindelse ved overføring av personopplysninger over internett.

Tilgangskontroll og passordrutiner

Tilgang til personopplysninger er begrenset til innloggete brukere som har bekreftet eierskapet til sin e-postadresse, og som oppfyller ett av følgende kriterier:

- Brukeren har selv registrert de aktuelle opplysningene.
- Brukeren er gitt eksplisitt tilgang til opplysninger om et bestemt kurs.
- Brukeren er ansatt i studieforbundet og har som arbeidsoppgave å behandle søknader om tilskudd eller tilby brukerstøtte til kursansvarlige og/eller lærere.
- Brukeren er administrator for systemet.

Brukere velger selv et passord, og passordet skal aldri sendes på e-post eller oppgis til andre. Passordet må være på minst 6 tegn og bør inneholde både bokstaver og tall.

Rutiner ved kritiske hendelser

Ved kritiske hendelser som hacking, fysisk skade, brann, innbrudd, strømbrudd mv. skal studieforbundet varsles uten ugrunnet opphold. Studieforbundet skal sammen med databehandlerne kartlegge omfanget av situasjonen og vurdere ytterligere varslingstiltak.

Ved tap eller eksponering av data, eller langvarige driftsforstyrrelser, skal studieforbundet sørge for at berørte parter varsles.