SAMARBEIDSAVTALE

BILAG 2

Databehandleravtale for behandling av personopplysninger i Altinn

VERSJON 4.1 – 24.02.2020

1. Partsforhold

Denne databehandleravtalen er inngått mellom Digitaliseringsdirektoratet som forvalter av Altinn, heretter betegnet ASF, og <Tjenesteeier> som tjenesteeier i Altinn-samarbeidet, heretter betegnet <Tjenesteeier>.

2. Avtalens formål

Avtalens formål er å regulere rettigheter og plikter etter lov av 15.06.18 nr 38 om behandling av personopplysninger (personopplysningsloven, jf. EU forordning 2016/679/EC av 27.04.16 om vern av fysiske personer i forbindelse med behandling av personopplysninger og fri utveksling av slike opplysninger (General Data Protection Regulation) (personvernforordningen). Avtalen skal sikre at personopplysninger om brukerne av Altinn ikke brukes urettmessig eller kommer uberettigede i hende, og at deres rettigheter blir ivaretatt, samt sikre at personopplysninger behandles i samsvar med de til enhver tid gjeldende krav i henhold til lov, forskrift eller annet regelverk,

Avtalen regulerer partenes behandling av personopplysninger i Altinn-løsningen, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

Databehandleravtalen er en del av Altinn Samarbeidsavtale mellom partene for bruk av Altinn. Begreper og definisjoner i avtalen skal forstås på samme måte som i personopplysningsloven.

3. Formål med behandling av personopplysninger

Formålet med behandling av personopplysninger i Altinn-løsningen, er autentisering, autorisasjon og elektronisk samhandling mellom tjenesteeierne og fysiske/juridiske personer. De personopplysninger som behandles vil være knyttet til autentisering, autorisasjon og den enkelte tjenesteeiers skjema/tjeneste, og vil inneholde opplysninger i relasjon til dette.

- Kategorier av registrerte

De registrerte vil i hovedsak være personer i roller registrert i Enhetsregisteret eller personer som er delegert tilgang til rettigheter eller roller i Altinn fra rolleinnehavere i Enhetsregisteret. Videre vil de registrerte kunne være privatpersoner som bruker Altinn i forbindelse med kontakt med offentlige myndigheter.

- Kategorier av registrerte opplysninger

Brukerens innboks i Altinn-løsningen vil kunne inneholder skjema/tjenester fra tjenesteeierne med opplysninger som faller inn under personvernforordningens artikkel 9, eksempelvis fagforeningsmedlemsskap eller helseopplysninger. Videre vil innboksen også kunne inneholder opplysninger om straffbare forhold, jf. artikkel 10.

Altinn er en offentlig felleskomponent som kan benyttes av statlige etater, kommuner og fylkeskommuner, samt andre offentlige virksomheter (tjenesteeiere). Det vil derfor potensielt behandles personopplysninger om hele Norges befolkning. I tillegg kommer personopplysninger om utenlandske statsborgere som har en kommunikasjon med norske myndigheter gjennom Altinn.

Nær sagt alle tenkelige typer personopplysninger behandles i Altinn. Navn, fødselsnummer, fysiske og elektroniske adresser og kontaktinformasjon. Konfidensiell informasjon, helseopplysninger og andre kategorier personopplysninger, jf. GDPR art. 9 og 10.

Databehandler skal kun behandle opplysninger i henhold til formålet som tjenesteeier har definert

4. Behandlingsansvar

Digitaliseringsdirektoratet v/ASF som behandlingsansvarlig:
Lagring av grunndataregister:

- Det sentrale folkeregister (DSF)

Utdrag fra det Det sentrale folkeregisteret (DSF) i henhold til tillatelse fra Skattedirektoratet: Navn, fødsels- og D-nummer, adresse.

- Kontakt- og reservasjonsregisteret (KRR):

Navn, fødsels- og D-nummer, epostadresse og/eller mobilnummer.

- Enhetsregisteret (ER):

Navn, fødsels- og D-nummer, adresse, roller i ER, varslingsadresse (e-postadresse og mobilnummer).

Lagring av personopplysninger for å kunne utføre korrekt kontroll av autentisering og autorisasjon til data. Dette er fødselsnummer/D-nummer, navn, mobil, e-post, pinkoder, brukernavn, brukerID, roller og rettigheter til tjenester.

Lagring av loggdata med personopplysninger i forbindelse med brukeraktiviteter (Tiltrodd tredjeparts arkiv). Loggdatabasen er ikke direkte tilgjengelig for bruker eller andre, men kan utleveres på forespørsel. Loggdatabasen inneholder IP-adresser, intern brukerID, tidspunkt for innlogging, aktivitetshistorikk. Personopplysninger i tjenesteeiernes tjenester/skjema lagres ikke i loggdatabasen.

Lagring av personopplysninger i brukerens innboks. Innboksen inneholder brukerens lagrede/innsendte skjema/tjenester fra de ulike tjenesteeierne i Altinn-samarbeidet. Skjemadata vil kunne inneholde personopplysninger som faller inn under artikkel 9.

Etter innlogging: tilgjengeliggjøring av personopplysninger på visningssider i Altinn: profilsider, aktivitetslogg, samtykkeside.

Tjenesteeier som behandlingsansvarlig:

Tjenesteeier er behandlingsansvarlig for personopplysninger som behandles i løsningen ved bruk av tjenesteeiers tjenester i Altinn, herunder data som behandles under utfylling, mellomlagring, videresending, innsending og utsending til og fra tjenesteeier, samt til preutfylling. Dette inkluderer alle funksjoner i løsningen tilknyttet en sluttbrukers bruk av tjenester i løsningen, og ved bruk av Altinns funksjoner for tjenesteeiere.

Tjenesteeier er videre behandlingsansvarlig for personopplysninger som behandles i tjenesteeiers egne systemer ved forespørsler på informasjon fra Altinn, uavhengig av hvilket teknisk grensesnitt og funksjonalitet som benyttes i løsningen. Dette kan eksempelvis være utveksling av autorisasjonsinformasjon.

5. Partenes plikter

Digitaliseringsdirektoratet v/ASF er databehandler på vegne av den enkelte tjenesteeier for de behandlinger tjenesteeier er behandlingsansvarlig for i Altinn-løsningen,

ASF plikter å bistå tjenesteeier i forbindelse med krav fra den registrerte om innsyn i registrerte opplysninger, jf personvernforordningen artikkel 15.

Ved sikkerhetshendelser som innebærer brudd på personopplysningssikkerheten, jf. personvernforordningen artikkel 4 nr.12, skal tjenesteeier informeres uten ugrunnet opphold, jf. bilag 3 Tjenesteavtale.
Tjenesteeier er ansvarlig for oppfølging av feilsendte meldinger, herunder sletting i innboks, informasjon til berørte og varsling til Datatilsynet.

<Tjenesteeier> innestår for å ha rettslig grunnlag etter personopplysningsloven for bruken av disse personopplysningene, jf. personopplysningsloven§ 1, jf. personvernforordningen artikkel 6 nr, 1e) og artikkel 9 og 10.

<Tjenesteeier> skal godtgjøre overfor ASF at <Tjenesteeier> har hjemmel til å motta ønskede folkeregisteropplysninger før utlevering kan finne sted.

Begge parter skal sørge for å ivareta krav til protokoll over behandlingsaktiviteter, jf. personvernforordningen artikkel 30.

Bruk av underleverandører
Databehandler gis en generell tillatelse til å gjøre bruk av underleverandør til behandling av personopplysninger. ASF er overfor <Tjenesteeier> ansvarlig for at underleverandører utfører sine oppgaver i overensstemmelse med denne avtalen og personopplysningsloven, samt de krav <Tjenesteeier> har satt for de aktuelle tjenestene

Overføring av personopplysninger til tredjeland
ASF skal kun overføre personopplysninger til et land utenfor EU-/EØS-området og EU-godkjente tredjeland, eller til internasjonale organisasjoner, slik det er beskrevet i dokumenterte instruksjoner fra den behandlingsansvarlige.

ASF skal ha avtaler med skyleverandører som ivaretar norsk og europeisk personvernreglement. En overføring til ikke-godkjente tredjeland kan bare skje dersom skyleverandøren har gitt nødvendige garantier i tråd med GDPR kap V.

Ved å ta i bruk Altinns skybaserte tjenester, godtar Tjenesteeier at det kan bli behov for support fra en skyleverandørs support-senter og underleverandører, som kan befinne seg i tredjeland.

6. Sikkerhetstiltak

ASF er forpliktet til å ivareta det ansvar for informasjonssikkerhet som tilligger databehandler i henhold til personopplysningslovens § 1, jf. personvernforordningen artikkel 32,

- ✓ Sikring av konfidensialitet; beskyttelse mot at uvedkommende får innsyn i opplysningene
- ✓ Sikring av integritet; beskyttelse mot utilsiktet endring av opplysningene
- ✓ Sikring av tilgjengelighet; sørge for at tilstrekkelige og relevante opplysninger er til stede

ASF plikter for øvrig å etterkomme krav til databehandlingen som ellers følger av relevante lover og forskrifter. Databehandlingen vil i tillegg utføres i henhold til gjeldende systemdokumentasjon og øvrige rutinebeskrivelser for Altinn-tjenesten. Oppstiller aktuelle tjenester tilleggskrav til sikkerhet, skal det før tjenestene besluttes lagt inn i Altinn, avklares mellom ASF og tjenesteeier om ytterligere sikkerhetstiltak som tilfredsstiller disse kravene kan dekkes.

Dokumentasjon på dette skal på forespørsel være tilgjengelig for <Tjenesteeier>, Datatilsynet og Personvernnemnda. Ved krav til behandling som ikke dekkes av gjeldende Altinn-løsning må endring eller videreutvikling behandles i Samarbeidsavtalens fora.

ASF forplikter seg til aktivt å opprettholde en forståelse for relevante trusler og risiko, og å vedlikeholde tilstrekkelige sikkerhetstiltak ut fra et besluttet risikonivå. Tjenesteeier skal varsles dersom det oppstår vesentlige endringer i risikobildet. Overordnet oversikt over tiltak skal oppdateres i protokoll over behandlingsaktiviteter for Altinn-løsningen.

Videre skal <Tjenesteeier> administrere tilganger som <Tjenesteeier>s egne ansatte/konsulenter har til informasjon i dokumentasjon om Altinn-løsningen og i servicedialogen mellom tjenesteeierne og ASF. Tilgangen skal være styrt i henhold til tjenstlig behov.

7. Sikkerhetsrevisjoner

Det skal gjennomføres årlig sikkerhetsrevisjoner av Altinn-løsningen. <Tjenesteeier> kan be om utlevering av de sikkerhetsrevisjoner som viser hvordan Altinn håndterer <Tjenesteeier>s data, etter de retningslinjer som foreligger hos Altinn sentralforvaltning.

Tjenesteeier kan i tillegg be om at det foretas sikkerhetsrevisjon. I så fall har tjenesteeier plikt til å dekke alle utgifter forbundet med utøvelsen av en slik revisjon.

ASF kan bare inngå avtaler med skyleverandører som har tilstrekkelig sikkerhet til å ivareta ASF sitt samlede databehandleransvar overfor Tjenesteeierne. For skybaserte tjenester i Altinn, utøves sikkerhetsrevisjoner og sertifisering av skyleverandørene av kvalifiserte og uavhengige tredjeparter. ASF og Tjenesteeier har kontinuerlig tilgang til sikkerhetsrapporter og annen sikkerhetsrelatert dokumentasjon om skyleverandør og de skybaserte tjenestene.

8. Vedlegg

Tjenesteeier er behandlingsansvarlig for egne tjenester i Altinn-løsningen.
Som vedlegg til denne avtalen skal tjenesteeier utarbeide og ajourholde oversikt over egne skjema/tjenester hvor formålet med og varigheten av behandlingen, behandlingens art, typen personopplysninger og kategorier av registrerte skal angis.

9. Avtalens varighet

Avtalen varer så lenge ASF behandler personopplysninger på vegne av <Tjenesteeier> i henhold til Samarbeidsavtalen.

10. Opphør

Ved opphør av denne avtalen skal ASF tilbakelevere alle personopplysninger som er behandlet på vegne av tjenesteeier, og slette egne kopier. Kostnader som oppstår i forbindelse med uthentingen vil <Tjenesteeier> selv måtte bære.

11. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til den personen som er merkantilt ansvarlig for Altinn samarbeidsavtale på vegne av <Tjenesteeier>.

Digitaliseringsdirektoratet
v/ Altinn Sentralforvaltning

Brønnøysund, <dato>

Sted, dato

_____
Andreas Rafaelsen, avdelingsdirektør

_____