Vedlegg 2 - Databehandleravtale

Table of contents

1 Innledning
2 Bilagets hensikt
3 Formål
4 Behandlingsansvarliges plikter
5 Databehandlers plikter
6 Bruk av underleverandører
7 Sikkerhet
8 Sikkerhetsrevisjoner
9 Avtalens varighet
10 Ved opphør
11 Erstatning og ertatningsansvar
12 Meddelelser
13 Lovvalg og verneting
14 Signatarer

1 Innledning

Databehandleravtale i henhold til personvernlovgivningen, General Data Protection Regulation (heretter GDPR) Eurpopaparlamentets- og rådsforordningen (EU) 2016/679 vedrørende Avtale mellom:

Rolle	Kunde	Leverandør
Navn		
Org.nr.		

2 Bilagets hensikt

Bilagets hensikt er å regulere rettigheter og plikter etter personvernlovgivning, GDPR, av 20. juli 2018. Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende, sikre de registrertes rettigheter og ivareta personvernprinsippene i henhold til artikkel 5.

Bilaget regulerer databehandlers bruk av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

3 Formål

Formålet med databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig, er kun å levere og administrere.

Personopplysninger som overføres til databehandler kan ikke brukes til andre formål enn levering og administrasjon.

Type personopplysninger som databehandleren behandler i forbindelse med levering og administrasjon av er hovedsakelig:

- Kjønn (MR/MS prefix)
- Fornavn
- Etternavn
- Fødselsdato
- E-post
- Telefon kontor/privat/mobil
- Ansattnummer, kostnadssted, avdeling
- Postadresse
- Kredittkortinformasjon
- Passinformasjon

Avtalen omfatter følgende behandlinger: Innsamling, oppbevaring, bearbeiding av personopplysninger for å kunne oppfylle formålet med Avtalen.

Databehandleren kan kun behandle personopplysninger gjort tilgjengelig av behandlingsansvarlig til de formål som er bestemt av behandlingsansvarlig og i samsvar med de vilkår som fremgår av denne avtale. Formålet er å tilby.

Behandlingens formål kan ikke endres av noen av partene uten at det gjennomføres en endring av Avtalen i henhold til Bilag 6.

4 Behandlingsansvarliges plikter

Behandlingsansvarlig er ansvarlig for at personopplysninger blir behandlet i samsvar med personvernforordningen og personopplysningsloven (jf. artikkel 24)

5 Databehandlers plikter

Databehandler skal følge de rutiner og instrukser for behandlingen som behandlingsansvarlig til enhver tid har bestemt skal gjelde.

Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Databehandler plikter å bistå behandlingsansvarlige med å overholde forpliktelsene etter artikkel 32-36 som er relevante i dette avtaleforholdet

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Databehandler plikter å ivareta at kun de med tjenstlig behov får tilgang til opplysningene. Denne bestemmelsen gjelder også etter avtalens opphør.

Databehandler skal levere et system som har innebygget personvern og personvern som standardinnstilling, ref. GDPR artikkel 25.

6 Bruk av underleverandører

Dersom databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos databehandler skal dette avklares og avtales skriftlig med behandlingsansvarlige før behandlingen av personopplysninger starter.

Underleverandør skal pålegges de samme pliktene om vern av personopplysninger som er fastsatt i denne databehandleravtalen. Databehandler har det fulle ansvaret for at underdatabehandler oppfyller sine forpliktelser overfor den behandlingsansvarlige.

Samtlige som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

En avtale med underleverandører vedlegges denne Avtalen.

7 Sikkerhet

Databehandler skal treffe alle tiltak som er nødvendig for å sikre informasjonssikkerhet i tråd med kravene i GDPR artikkel 32. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Den behandlingsansvarlige kan kreve innsyn av dokumentasjonen, etter

en skriftlig varsling på minimum 14 dager.

Personopplysninger skal ikke overføres, lagres eller speiles til land utenfor EØS-området uten at dette er skriftlig avtalt med behandlingsansvarlig på forhånd. Dette gjelder ikke dersom norsk lov pålegger databehandler en konkret behandling av personopplysninger.

Avviksmelding etter personvernlovgivningen skal skje ved at databehandler melder avviket til behandlingsansvarlig, uten grunnet opphold, slik at behandlingsansvarlig kan oppfylle sitt krav, etter GDPR artikkel 33 og 34, og melde avviket innen 72 timer til Datatilsynet og umiddelbart ved høy risiko til den registrerte. Dette gjelder hendelser som berører konfidensialitet, integritet og tilgjengelighet.

8 Sikkerhetsrevisjoner

Behandlingsansvarlig skal avtale med databehandler at det gjennomføres sikkerhetsrevisjoner periodisk for systemer og lignende som omfattes av denne Avtalen. Databehandler skal muliggjøre og bidra til revisjoner og inspeksjoner som gjennomføres av den behandlingsansvarlige eller en annen på dennes vegne.

Revisjonen kan blant annet omfatte gjennomgang av rutiner, stikkprøvekontroll, mer omfattende stedlige kontroller og andre egnede kontrolltiltak.

Behandlingsansvarlig skal så vidt mulig gi Databehandler varsel i rimelig tid ved krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. Revisjon skal likevel skje umiddelbart dersom behandlingsansvarlig har behov for det. Eksempelvis ved tilsyn fra datatilsynet eller andre kritiske hendelser.

9 Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig.

10 Ved opphør

Databehandler skal dokumentere skriftlig at sletting og/eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

Ved brudd på denne avtale eller personopplysningsloven kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning

Ved opphør av denne avtalen;
Plikter databehandler etter den behandlingsansvarliges valg, å forsvarlig slette eller tilbakelevere alle personopplysninger til den behandlingsansvarlige og slette eksisterende kopier, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at personopplysningene lagres.Ved opphør av Avtalen deaktiveres alle profiler på Kunden.

For online brukerprofiler gjelder sletting innen 30 dager etter registrert forespørsel, og for sletting av brukerprofiler fra kryptert backup, gjelder sletting innen 180 dager basert på eksisterende backup-syklus. Sletting av opplysninger gjennomføres såfremt annen lovgivning ikke pålegger oppbevaring av opplysningene.

11 Erstatning og ertatningsansvar

Rett til erstatning og erstatningsansvar reguleres av GDRP artikkel 82. Øvrige bestemmelser om erstatningsansvar er regulert i Hovedavtalen eller gjeldende ordrebekreftelse hos Databehandler.

12 Meddelelser

Meddelelser etter denne avtalen skal sendes gjennom kommunikasjonmodulen i Mercell.

13 Lovvalg og verneting

Lovvalg og verneting reguleres av Hovedavtalen.

14 Signatarer