Databehandleravtale

Datakontroller: <kundenavn>

og

Databehandler:

EasyISP Fauske
Org nr. 980989240
Falkensteinsvegen 13
6809 Førde

DATABEHANDLERAVTALEN – DPA

som gjelder databehandlerens behandling av personopplysninger på vegne av datakontrolleren.

1. **Hensikt**

1.1 Databehandleren kan bare behandle personopplysninger til det formål som er nødvendig for å oppfylle databehandlers forpliktelser, og i denne forbindelse levere tjenestene som er beskrevet i hovedavtalen.

2. **Datakontrollers plikter**

2.2 Datakontroller garanterer at personopplysninger blir behandlet til legitime og objektive formål, og at databehandler ikke behandler mer personopplysninger enn nødvendig for formålet.

2.3 Datakontroller er ansvarlig for å sikre at det finnes et gyldig juridisk grunnlag for behandling på tidspunkt for overføring av personopplysninger til databehandler. På forespørsel fra databehandler, må datakontroller skriftlig redegjøre for og/eller levere dokumentasjon på grunnlaget for databehandlingen.

2.4 I tillegg garanterer datakontroller at datasubjektene som personopplysningene omhandler har fått tilstrekkelig informasjon om behandling av deres personopplysninger.

2.5 I tilfelle datakontroller instruerer en underleverandør utpekt i overensstemmelse med paragraf 4.1 direkte, må datakontroller umiddelbart varsle databehandler om dette. Databehandler skal på ingen måte være juridisk ansvarlig for databehandling foretatt av en underleverandør i overensstemmelse med slike instruksjoner.

3. **Databehandlers forpliktelser**

3.1 All behandling av personopplysningene levert av datakontroller utført av databehandler fra datakontrolleren må være i samsvar med disse instruksjonene fra datakontrolleren, og databehandleren er dessuten forpliktet til å overholde all lover og forskrifter for sikring av data.

Databehandler om informere datakontroller om juridiske krav forut for behandling. Men dette gjelder ikke hvis lovgivningen forbyr slik informasjon på bakgrunn av offentlighetens interesse. Databehandler må umiddelbart informere datakontroller hvis, etter databehandlers skjønn, hvis en instruksjon bryter EUs forordning for personvern, eller datasikkerhetsreglene til et medlemsland i EU.

3.2 Databehandler må ta alle nødvendige tekniske og organisatoriske sikkerhetstiltak, herunder eventuelle tilleggstiltak som kreves for å sikre at personopplysningene som er

angitt i punkt 1.2, ikke utilsiktet eller ulovlig destrueres, går tapt eller svekkes eller blir gjort kjent for uautoriserte tredjeparter, misbrukt eller på annen måte behandlet på en måte som strider mot dansk personvernlovgivning.

3.3 Databehandler må sikre at ansatte autorisert til å behandle personopplysninger har skrevet under avtale om konfidensialitet eller tilsvarende.

3.4 Etter ønske fra datakontroller må databehandler oppgi og/eller dokumentere at databehandler overholder alle kravene i gjeldende personvernlovgivning, inkludert dokumentasjon vedrørende databehandlers dataflyt, samt prosedyrer/retningslinjer for behandling av personopplysninger

3.5 Med hensyn til type behandling, må databehandleren så langt som mulig bistå kontrolleren med hensiktsmessige tekniske og organisatoriske tiltak for å oppfylle datakontrollerens plikt til å svare på forespørsler om utøvelse av registrerte rettigheter som fastsatt i kapittel 3 i EUs forordning for personvern.

3.6 Hvis databehandleren behandler personopplysninger i en annet EU medlemsland, må databehandleren overholde kravene til sikkerhet gjeldende for det aktuelle medlemslandet.

3.7 Databehandler må varsle datakontroller ved mistanke om at kravene til sikring av personopplysninger er brutt, eller ved andre uregelmessigheter i forbindelse med behandling av personopplysninger. Databehandler har en frist på 24 timer til å varsle datakontroller om sikkerhetsbrudd, løpende fra det tidspunktet databehandler blir oppmerksom på sikkerhetsbruddet. Hvis etterspurt av datakontrolleren må databehandleren hjelpe datakontrolleren med å klargjøre omfang av sikkerhetsbruddet, inkludert utarbeidelse av eventuelle meldinger til det danske Datatilsynet og/eller datasubjektene.

3.8 Databehandleren må overfor datakontrolleren gjøre tilgjengelig all informasjon nødvendig for å demonstrere etterlevelse av artikkel 28 i EUs forordning for personvern og avtalen. I denne forbindelse gir databehandleren tillatelse til og bidrar i revisjoner, inkludert inspeksjoner, gjennomført av datakontrolleren eller annen revisor med oppdrag gitt av datakontrolleren.

3.9 I tillegg til det ovennevnte må databehandleren bistå datakontrolleren med å sikre overholdelse av datakontrollerens forpliktelser i henhold til artikkel 32-36 i EUs forordning for personvern. Denne hjelpen vil ta hensyn til type behandling og type informasjon tilgjengelig for databehandleren.

4. Overføring av data til underleverandør eller tredjepart

4.1 Databehandler må overholde betingelsene i artikkel 28, paragraf 2.4 i EUs forordning for personvern for å engasjere en annen databehandler (underleverandør).

Dette medfører at databehandleren ikke engasjerer en annen databehandler (underleverandør) for gjennomføring av avtalen uten en spesifikk eller generell skriftlig forhåndsgodkjenning fra datakontroller.

4.2 Datakontroller gir herved databehandleren en generell godkjenning til å inngå avtaler med underleverandører. Databehandler må varsle datakontroller om alle endringer i underleverandører. Datakontroller kan komme med rimelige og relevante innsigelser mot slike endringer. Hvis databehandler fortsatt å ønske å bruke en underleverandør som datakontroller har innvendinger mot, har partene rett til å si opp avtalen og, hvis det er

relevant, hovedavtalen med kortere varsel, jfr. 6.2. Under denne perioden kan datakontrolleren ikke kreve at databehandleren ikke bruker den aktuelle underleverandøren.

4.3 Databehandlere må pålegge underleverandører de samme påleggene som fremsatt i denne avtalen. Dette utøves gjennom en avtale eller en annen lovgivning under EU-lov eller loven i et medlemsland. Det må sikres at det foreligger tilstrekkelige garantier fra underleverandøren for gjennomføring av hensiktsmessige tekniske og organisatoriske tiltak på en slik måte at behandlingen vil oppfylle kravene i EUs forordning for personvern ("back-to-back"-vilkår).

4.4 Hvis underleverandøren ikke oppfyller sine forpliktelser til datasikkerhet, forblir databehandleren ansvarlig overfor datakontrolleren for utførelsen av underleverandørens forpliktelser.

4.5 Databehandleren kan på vegne av datakontrolleren inngå databehandlingsavtaler med underleverandører innenfor EU/EØS. Når det gjelder underleverandører utenfor EU/EØS kan databehandleren inngå standardavtaler som oppfyller kravene i Kommisjonsvedtak 2010/87/EU av 5. februar 2010 vedrørende standard avtalevilkår for overføring av personopplysninger til databehandlere i tredjeplan (Standardavtaler), eller i overensstemmelse med EU/US Privacy Shield.

4.6 Datakontrolleren gir herved databehandleren en generell rett til å inngå standardavtaler med underleverandører utenfor EU/EØS på vegne av datakontrolleren.

5. Ansvar

5.1 Partenes ansvar styres av hovedavtalen.

5.2 Partenes ansvar for skade under denne avtalen styres av hovedavtalen.

6. Effektiv data og terminering

6.1 Denne avtalen blir gyldig på samme tidspunkt som hovedavtalen.

6.2 I tilfelle oppsigelse av hovedavtalen, vil denne avtalen også bli sagt opp.

Databehandleren forblir imidlertid bundet av forpliktelsene som er fastsatt i denne avtalen, så lenge databehandleren behandler personopplysninger på vegne av datakontrolleren.

I situasjonen som beskrevet under pkt. 5.2 har partene rett til å si opp hovedavtalen og avtalen med varsel på 1 (én) måned som slutter ved utgangen av en måned.

6.3 Ved opphør av behandlingstjenesten er databehandler forpliktet til, på forespørsel fra datakontroller, å slette eller returnere alle personopplysninger til datakontrolleren, samt slette eksisterende kopier, med mindre lagring av personopplysningene er pålagt av EU eller nasjonal lovgivning.

7. Styrende lov og jurisdiksjon

7.1 Eventuelle krav eller tvist som oppstår fra eller i forbindelse med denne avtalen, må avgjøres av en kompetent domstol i første instans i samme jurisdiksjon som angitt i hovedavtalen.

Vedlegg 1
Kategorier datasubjekter, typer personopplysninger og instruksjoner

1. Kategorier datasubjekter:

- Databehandleren behandler kontaktopplysninger til datakontrollerens faktiske, potensielle eller tidligere kunder og eller medlemmer, ansatte, leverandører, forretnings- og samarbeidspartnere og tilknyttede selskaper.
- Databehandleren gjør sine systemer tilgjengelig for datakontrolleren som en hostet tjeneste, og det er ikke mulig for databehandleren å fastslå alle kategorier datasubjekter. Hvis datakontrolleren hoster opplysninger om andre kategorier datasubjekter hos databehandleren, er det datakontrollerens plikt å registrere denne informasjonen.

2. Typer personopplysninger:

- Kontaktinformasjon inkludert e-postadresse
- IP-adresse
- Domenenavn
- Brukernavn
- Medlemsinformasjon
- Analyse- og bruksdata
- Ordrehistorikk og informasjon
- Kontakter
- Kommunikasjon
- Støtte
- Bilder
- Andre typer personopplysninger kan forekomme

3. Instruksjoner

Tjeneste

Databehandleren kan behandle personopplysninger som omhandler datasubjekter i den hensikt levere, utvikle, administrere og styre tjenester i hovedavtalen, inkludert sikre stabilitet og oppetid på våre servere og tilfredsstille juridiske krav.

Sikkerhet

Databehandleren skal sikre konfidensialitet, integritet og tilgjengelighet av personopplysninger. Databehandleren skal implementere systemrelaterte, organisatoriske og tekniske tiltak for å sikre tilstrekkelig sikkerhetsnivå, hvor type tiltak og kostnad ved implementering ses i forhold til type personopplysninger og risiko ved behandling av disse.

Databehandleren må levere høy grad av sikkerhet på sine tjenester og produkter. Denne sikkerheten leveres gjennom tekniske, organisatoriske og fysiske sikringstiltak, som inkluderer:

- Samlokaliserte bygninger og kontorer er sikret med egnet tilgangskontroll, som sikrer at bare autoriserte medarbeidere har adgang.
- Relevant antivirusbeskyttelse er på plass.
- Tilgang og innlogging er rollebaser eller personbasert, og personer og systemer har ikke større tilgang enn det som er nødvendig for å utføre sine oppgaver.
- Sikkerhetskopi av systemer som behandler personopplysninger.
- Endringslogger.
- Kommunikasjon over Internett mellom systemer som håndterer personopplysninger er kryptert.
- Klassifisering av personopplysninger for å sikre implementering av sikkerhetstiltak som korresponderer med risikovurderingen.
- Bruk av systemer og prosesser som øker sikkerheten i håndtering av personopplysninger.

Databehandleren har rett til å ta ytterligere beslutninger om nødvendige tekniske og organisatoriske sikkerhetstiltak som må implementeres for å sikre riktig sikkerhetsnivå med hensyn til personopplysningene.

Lagringsperiode

Personopplysninger lagret/hostet i våre systemer blir slettet eller anonymisert innen en rimelig tidsperiode etter at datakontrolleren har sagt opp hovedavtalen. Unntak er opplysninger hvor det foreligger juridiske pålegg om lagringstid.

Denne typen opplysninger vil typisk bli slettet innen åtte uker, men kan bli slettet tidligere.

Andre typer opplysninger som blir lagret i logger etc, blir slettet etter rimelig rid, vanligvis innen 8 uker.

Plassering av data

Personopplysninger lagret/hostet i databehandlerens systemer befinner seg i datasentre i Norge. Datakontroller gir herved databehandleren tillatelse til å flytte data til andre datasentre innenfor EU dersom databehandleren finner dette relevant, og hvis samme nivå av sikkerhet og oppetid kan garanteres.