Databehandleravtale

mellom

Behandlingsansvarlig:	xxx
Organisasjonsnr:	xxx
Etablert i:	
Behandlingsansvarliges kontaktinformasjon for generelle henvendelser (navn, rolle, kontaktdetaljer):	
Behandlingsansvarliges kontaktinformasjon for henvendelser om uautorisert behandling av personopplysninger (navn, rolle, kontaktdetaljer):	
Databehandler:	Visma Software AS
Organisasjonsnummer:	933646920
Etablert i:	Norge
Databehandlerens kontaktinformasjon for generelle henvendelser (navn, rolle, kontaktdetaljer):	Visma Software AS Kundesenteret@visma.com Tlf. 09101 (08-17)
Databehandlerens kontaktinformasjon for henvendelser om uautorisert behandling av personopplysninger (navn, rolle, kontaktdetaljer):	Visma Software AS Kundesenteret@visma.com Tlf. 09101 (08-17)

heretter betegnet som henholdsvis Behandlingsansvarlig, Databehandler eller Part, i fellesskap som Partene.

Innledning

Partene bekrefter herved at de har nødvendige fullmakter til å inngå denne databehandleravtalen (Databehandleravtalen). Databehandleravtalen vil utgjøre en del av og regulere all behandling av personopplysninger i tilknytning til følgende avtaler (Tjenesteavtale) mellom partene:

- ***Avtale om bruksrett og leie av Huldt & Lillevik Lønn 5.0 Cloud***

Databehandleren behandler personopplysninger i henhold til Visma Privacy Statement, tilgjengelig på https://www.visma.com/privacy-statement/, som gjelder for alle selskaper i Visma-konsernet.

Definisjoner

Definisjonene av personopplysning, sensitiv personopplysning, behandling av personopplysning, den registrerte, behandlingsansvarlig og databehandler skal forstås slik de brukes og tolkes i henhold til gjeldende personvernlovgivning, inkludert personvernforordningen av 4. mai 2016 - General Data Protection Regulation (GDPR) som gjelder for denne Databehandleravtalen og i Norge fra 25 mai 2018.

Formål

Databehandleravtalen regulerer Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige, og beskriver hvordan Databehandleren gjennom tekniske og organisatoriske virkemidler skal bidra til å sikre den registrertes rettigheter på vegne av den Behandlingsansvarlige.

Formålet med Databehandlerens behandling av personopplysninger er å oppfylle Tjenesteavtalen og Databehandleravtalen.

Ved eventuell motstrid mellom bestemmelser om behandling av personopplysninger har Databehandleravtalen forrang over Tjenesteavtale eller andre avtaler inngått mellom Partene. Denne Databehandleravtalen varer like lenge som Partene har en gyldig Tjenesteavtale som inkluderer behandling av personopplysninger.

Databehandlerens plikter

Databehandler skal bare behandle personopplysninger på vegne av og i henhold til instruksjoner fra Behandlingsansvarlig. Ved å inngå denne Databehandleravtalen instruerer Behandlingsansvarlig Databehandler om å behandle personopplysninger på følgende måte: i) bare i henhold til gjeldende lovgivning, ii) for å oppfylle alle plikter i henhold til Tjenesteavtale, iii) som instruert via Behandlingsansvarlig sin bruk av Databehandlers ordinære tjenester og iv) som spesifisert i denne Databehandleravtalen.

Databehandleren har ved avtaleinngåelsen ingen grunn til å anta at det foreligger regulatoriske hindringer mot å følge instruksjonene fra Behandlingsansvarlige. Dersom Databehandleren ved et senere tidspunkt blir klar over at Behandlingsansvarliges instruksjoner eller behandling av personopplysninger strider mot gjeldende personvernlovgivning, skal Databehandleren melde dette til Behandlingsansvarlige.

Typen personopplysninger og kategorier av registrerte som er gjenstand for behandling under denne Databehandleravtalen er angitt i Appendix A.

Databehandleren skal sikre konfidensialitet, integritet og tilgjengelighet til personopplysningene i

henhold til de regulatoriske krav som gjelder for Databehandleren. Dette inkluderer å implementere systematiske, organisatoriske og tekniske virkemidler for å sikre et tilstrekkelig nivå for sikkerhet. Ved avgjørelsen av hva som er et tilstrekkelig nivå skal hensyn til den teknologiske utviklingen og kostnaden ved implementering av tiltak veies mot risikoen ved behandlingen og typen personopplysninger som behandles.

Databehandleren skal ved tekniske og organisatoriske virkemidler bistå Behandlingsansvarlig med å ivareta Behandlingsansvarliges plikter under GDPR artikkel 32 til 36, samt bistå i arbeidet med å behandle forespørsler fra registrerte i henhold til GDPR kapittel III. Pliktens omfang avgrenses av formen for behandling av personopplysninger og hvilken informasjon som er tilgjengelig for Databehandleren.

Behandlingsansvarlige kan kreve informasjon om de sikkerhetstiltak, dokumentasjon og annen informasjon om hvordan Databehandleren behandler personopplysninger. Dersom Behandlingsansvarlige ber om mer informasjon enn det som Databehandleren tilgjengeliggjør for å oppfylle kravene til rollen som Databehandler i henhold til gjeldende personvernlovgivning, kan Databehandleren kreve betaling for slike eventuelle tilleggstjenester.

Databehandleren og dennes ansatte skal sørge for konfidensialitet ved behandling av personopplysninger som behandles i henhold til denne databehandleravtalen. Denne plikten gjelder også etter at avtalen opphører.

Databehandleren vil gjennom å varsle Behandlingsansvarlig uten ugrunnet opphold om brudd på personopplysningssikkerheten, muliggjøre etterlevelse av gjeldende personvernlovgivning vedrørende varsling av tilsynsmyndigheter og registrerte.

Videre vil Databehandleren, i den utstrekning det er praktisk mulig og lovlig, varsle Behandlingsansvarlig om;

i) innsynsbegjæringer fra registrerte,

ii) innsynsbegjæringer fra offentlige myndigheter

Databehandleren vil kun besvare forespørsler fra registrerte i den grad Behandlingsansvarlig har gitt tillatelse til det. Databehandleren vil kun varsle Behandlingsansvarlig om innsynsbegjæringer fra offentlige myndigheter i den grad slikt varsel er lovlig, samt kun utlevere informasjon til offentlige myndigheter dersom rettslig pålegg foreligger.

Databehandleren har ikke eierskap til eller kontroll med hvorvidt og hvordan Behandlingsansvarlig velger å benytte seg av eventuelle tredjeparts integrasjoner via Databehandlers API, via direkte databasekobling eller lignende. Ansvaret for slike integrasjoner med tredjepart påhviler utelukkende Behandlingsansvarlig.

Behandlingsansvarliges plikter

Ved å signere Databehandleravtalen bekrefter Behandlingsansvarlig:

- All behandling av personopplysninger i forbindelse med Tjenesteavtalen skal foregå i overensstemmelse med gjeldende lovgivning.
- Behandlingsansvarlig har rett til å behandle personopplysninger og til å gi Databehandleren og dennes underleverandører adgang til å behandle personopplysninger.
- Behandlingsansvarlig er ansvarlig for at personopplysningene som overlates til Databehandleren er lovlig innsamlet, er korrekte og tilstrekkelige.
- At alle regulatoriske krav vedrørende varsel til eller tillatelse fra tilsynsmyndigheten for behandlingen av personopplysninger er oppfylt.
- At forpliktelsen til å formidle relevant informasjon til registrerte vedrørende behandlingen av personopplysninger er oppfylt.
- At sensitive personopplysninger kun vil bli behandlet som en del av bruk av tjenestene under Tjenesteavtalen der dette er uttrykkelig avtalt i Appendix A til Databehandleravtalen.

- At Behandlingsansvarlig vil ha et oppdatert register over typen personopplysninger og kategorier av registrerte som behandles i forbindelse med Tjenesteavtalen.

Bruk av underleverandører og overføring av personopplysninger

Som en del av leveransen under Tjenesteavtale vil Databehandleren bruke underleverandører. Slike underleverandører kan være andre selskaper i Visma-konsernet eller eksterne tredjeparter. Underleverandørene kan befinne seg innenfor eller utenfor EU/EØS-området. Databehandleren har plikt til å påse at underleverandører påtar seg tilsvarende forpliktelser som de som følger av denne Databehandleravtalen. All bruk av underleverandører skal skje i samsvar med Visma Privacy Statement.

Behandlingsansvarlig har rett til å be om en oversikt over hvilke underleverandører av Databehandler som har tilgang til personopplysninger. Slik oversikt kan inntas i Appendix B eller gis på Visma sine dedikerte nettsider for personvern.

Dersom underleverandøren er lokalisert utenfor EU/EØS gir Behandlingsansvarlig fullmakt til Databehandleren til å sikre lovlig overføringsgrunnlag for overføringen av personopplysninger ut av EU/EØS på vegne av Behandlignsansvarlig, herunder ved å gjøre bruk av EU standardavtaler eller Privacy Shield ordningen.

Behandlingsansvarlig vil bli varslet før Databehandleren endrer underleverandør som behandler personopplysninger. Dersom det er klart at den nye underleverandøren ikke oppfyller gjeldende personvernlovgivning, så kan Behandlingsansvarlig si opp Databehandleravtalen. Slik oppsigelse kan gi Behandlingsansvarlig rett til å terminere Tjenesteavtalen helt eller delvis i tråd med Tjenesteavtalens bestemmelser om terminering, der det særlig skal vektlegges i hvilken grad den aktuelle behandlingen av personopplysninger er en nødvendig del av Tjenesteavtalen. Endring av underleverandør vil i seg selv ikke bli ansett som et brudd på Tjenesteavtale.

Ved å undertegne denne Databehandleravtalen samtykker Behandlingsansvarlig til den bruk av underleverandører som er beskrevet ovenfor.

Sikkerhet

Databehandler skal sørge for et høyt sikkerhetsnivå i sine produkter og tjenester. Dette skal skje ved organisatoriske, tekniske og fysiske sikkerhetstiltak, i henhold kravene til informasjonssikkerhet som fremgår av GDPR artikkel 32.

Visma konsernets rammeverk for personvern skal sikre personopplysningenes konfidensialitet, integritet, robushet og tilgjengelighet. Følgende tiltak er særlig viktig i denne forbindelse:

- Klassifisering av personopplysninger for å vurdere sikkerhetstiltakene på bakgrunn av risikovurderinger.
- Vurdere bruk av kryptering og pseudomisering for å avhjelpe risiko
- Begrense tilgang til personopplysninger til personell som trenger tilgang for å oppfylle plikter i henhold til denne Databehandleravtalen eller Tjenesteavtale.
- Systemer som avdekker, retter, forhindrer og rapporterer avvik
- Benytte sikkerhetsrevisjoner til å analysere hvorvidt de til enhver tids gjeldende tekniske og organisatoriske tiltak for å beskytte personopplysninger er tilstrekkelig, sett i lys av gjeldende lovgivning.

Rett til tilsyn

Behandlingsansvarlig kan revidere Databehandler sin etterlevelse av denne Databehandleravtalen inntil en gang i året. Hvis lovgivning som Behandlingsansvarlig er underlagt krever det, kan Behandlingsansvarlig kreve flere revisjoner.

For å be om revisjon må Behandlingsansvarlig sende en detaljert tilsynsplan minimum 4 uker i forkant av ønsket tilsynsdato, med oversikt over forslagets omfang, varighet og oppstart. Hvis tredjeparter skal gjennomføre tilsynet, skal dette som hovedregel avtales mellom Partene. Hvis Behandlingsansvarlig behandling av personopplysninger skjer i et "multitenant" miljø eller lignende, aksepterer Behandlingsansvarlig likevel at tilsynet gjennomføres av en tredjepart utpekt av Databehandler.

Hvis tilsynets omfang er behandlet i ISAE, ISO eller lignende rapport av kvalifisert tredjepart i løpet av de siste 12 månedene, og Databehandler bekrefter at det ikke finnes kjente endringer fra dette, skal Behandlingsansvarlig akseptere disse rapportene i stedet for å forespørre nytt tilsyn.

I alle tilfeller skal tilsyn utføres i samråd med virksomhetens ordinære åpningstider, i henhold til virksomhetens retningslinjer og ikke forstyrre den ordinære virksomheten. Behandlingsansvarlig er ansvarlig for kostnader forårsaket av sitt tilsyn. Dersom Behandlingsansvarlige ber om mer assistanse enn den som tilbys av Databehandleren for å oppfylle gjeldende personvernlovgivning, kan Databehandleren kreve betaling for denne tilleggstjenesten.

Varighet

Databehandleravtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig i henhold til Tjenesteavtale.

Databehandleravtalen opphører i forbindelse med avslutning av Tjenesteavtale. Ved opphør av Databehandleravtalen, skal Databehandler slette eller returnere personopplysninger som er behandlet på vegne av Behandlingsansvarlig i tråd med Tjenesteavtale. Med mindre annet er avtalt mellom Partene, skal arbeidet forbundet med dette kompenseres basert på; i) kompleksiteten ved forespørselen og ii) betaling for medgått tid.

Databehandler kan beholde personopplysninger etter opphøret av Databehandleravtalen i henhold til gjeldende lovgivning, underlagt de samme typer tekniske og organisatoriske tiltak som skissert i denne Databehandleravtalen.

Endringer og ugyldighet

Endringer i Databehandleravtalen skal inkluderes i et eget endringsvedlegg og signeres av begge Parter for å være gyldig.

Hvis bestemmelser i Databehandleravtalen kjennes ugyldig, skal ikke dette påvirke de øvrige bestemmelsene i Databehandleravtalen. Partene skal erstatte den ugyldige bestemmelsen med en gyldig bestemmelse som reflekterer intensjonen til Partene bak bestemmelsen.

Mislighold

Begge parter har et individuelt ansvar og skal holdes selvstendig ansvarlig for å betale alle bøter eller erstatning som ilegges den respektive Part i henhold til GDPR. Ansvaret for øvrige brudd på Databehandleravtalen eller GDPR reguleres av den Tjenesteavtale som foreligger mellom Partene. Dette gjelder også for avvik forårsaket av Databehandler sine underleverandører.

Gjeldende rett og verneting

Databehandleravtalen er underlagt norsk rett ved norske domstoler med Oslo tingrett som avtalt verneting.

****

Denne Databehandleravtalen i ett eksemplar med kopi til hver av Partene.

Behandlingsansvarlig:

Signatur::	
Signert av:	
Tid og sted:	

Databehandler:

Signatur:	
Signert av:	CEO, Erlend Sogn
Tid og sted:	07.05.2018 Oslo

Vedlegg A - Kategorier av registrerte og personopplysninger

1. *Kategorier av registrerte og personopplysninger*

Oversikt

Aktuelle tjenester	Hensikt og varighet	Data subjekter og kategorisering av persondata.	Behandlingsprosesser
Huldt & Lillevik Lønn Cloud	Huldt & Lillevik Lønn levert som en skytjeneste via vår Citrix plattform. Leveransen inkluderer tilgang til programvaren, oppgraderinger, backup, sikkerhet og driftsplattform, så lenge kunden har et abonnement på avtalen.	Hovedelmentet er de ansatte, med tilhørende relevante opplysninger for arbeidsforholdet, avlønning og offentlig rapportering. Transaksjonsdata kan omfatte fravær/ferie/timer/lønn/utlegg/reise påleggstrekk/fagforeningskontigent	Lagring av data, backup av data

a. Kategorier av registrerte
   - *i.* kundens sluttbruker
   - i. ansatt hos kunde
   - ii. kontaktpersoner av kunde
   - iii. andre kategorier?

b. Kategorier av personopplysninger
   - i. kontaktinformasjon som navn, telefon, adresse, epostadresse mv.
   - ii. jobbrelatert informasjon som tittel, arbeidsgiver, utdannelse etc.
   - iii. økonomisk informasjon som kortnummer, faktura, konto etc.

2. *Særlige kategorier av personopplysninger (sensitive personopplysninger)*

Denne delen er bare relevant hvis Databehandler skal behandle sensitive personopplysninger som angitt under av Behandlingsansvarlig som del av Tjenesteavtalen.

Databehandler skal på vegne av Behandling behandle følgende sensitive personopplysninger:	***Yes***	***No***
rase, etnisitet, politisk eller filosofisk tilhørighet eller religion		N
at en person har vært eller er siktet/dømt for kriminalitet		N
helseopplysninger	Y	

seksuell orientering		N
Fagforeningsmedlemskap	Y	
genetisk eller biometrisk data		N

Vedlegg B - Oversikt underleverandører

Underleverandører av Databehandler med tilgang til personopplysninger ved signering av Databehandleravtalen inkluderer:

Navn	**Land**	**Overføringsgrunnlag hvis underleverandør er lokalisert utenfor EU**	**Assisting the Processor with**
Visma ITC AS	Oslo, Norway	Gjelder ikke innen EU	Lagring server