

## **1 Behandlingens formål og omfang**

Formålet med denne Databehandleravtalen er å regulere rettighetene og forpliktelsene i henhold til personvernforordningen og personopplysningsloven (jf. artikkel 24) (samlet kalt "Forskriftene"). Denne Databehandleravtalen skal sikre at personopplysninger behandles av Databehandleren i samsvar med Forskriftene.

Denne Databehandleravtalen inngås som en del av eller med henvisning til partenes avtale om levering av en eller flere IT-tjenester fra Databehandleren til den Dataansvarlige (Leveringsavtalen).

Ved Databehandleravtalens ikrafttredelse gis Databehandleren fullmakt til å behandle personopplysninger på vegne av den Dataansvarlige som en del av ytelsen i de avtalte IT-tjenestene, på de vilkårene som er angitt i Databehandleravtalen (Instruks). Databehandleren skal ikke behandle personopplysningene som er overlatt til den, til andre formål enn å utføre IT-tjenestene som er avtalt i Leveringsavtalen.

Ved uoverensstemmelse mellom Leveringsavtalen og denne Databehandleravtalen, skal Databehandleravtalen ha forrang.

Den Dataansvarliges Instruks kan suppleres i bilag 1.

## **2 Behandlingens varighet**

Databehandleren kan behandle personopplysningene som er overlatt til den så lenge det er relevant for Databehandlerens utførelse av de avtalte oppgaver og forpliktelser overfor den Dataansvarlige etter Leveringsavtalen.

## **3 Omfattede typer av personopplysninger og kategorier av registrerte**

De typer personopplysninger som leveres til Databehandleren for behandling, og de kategorier av registrerte som personopplysningene vedrører og hvordan personopplysningene skal behandles av den Dataansvarlige, er angitt i bilag 1.

## **4 Databehandlerens forpliktelser**

Databehandleren påtar seg forpliktelsene som fremgår av punkt 5-15 nedenfor ved behandling av personopplysninger på vegne av den Dataansvarlige.

Databehandleren skal gi den Dataansvarlige tilgang til sikkerhetsdokumentasjonen, og bistå den Dataansvarlige, slik at den Dataansvarlige kan oppfylle kravene i henhold til Forskriftene.

Den Dataansvarlige skal, med mindre annet er avtalt eller følger av gjeldende lov, ha tilgang til og innsikt i de behandlede personopplysningene og systemene for slik behandling. Databehandleren skal bistå den Dataansvarlige i dette.

Med mindre noe annet er spesifisert særskilt, forplikter Databehandleren seg til å gjennomføre den avtalte behandlingen i samsvar med avtalte forpliktelser uten å motta annen vederlag enn det som er avtalt i Leveringsavtalen.

Uavhengig av om det er angitt at Databehandleren har krav på særskilt vederlag for å utføre en forpliktelse eller en tjeneste, har Databehandleren ikke krav på betaling for sine tjenester dersom tjenestene skal utføres som en direkte følge av Databehandlerens brudd på Databehandleravtalen eller gjeldende personopplysningslov.

## **5 Behandling i henhold til Instruksen**

Databehandleren og alle som utfører arbeid for Databehandleren og som har tilgang til den Dataansvarliges personopplysninger, kan kun behandle personopplysningene i henhold til vilkårene i den Dataansvarliges Instruks, med mindre behandlingen kreves i henhold til EU-lov eller nasjonal lovgivning som gjelder for Databehandleren. I så fall skal Databehandleren underrette den Dataansvarlige om det lovpålagte kravet før behandlingen utføres, med mindre en slik underretning vil være i strid med loven.

## **6 Endring av Instruks**

Med mindre annet er avtalt mellom partene med hensyn til endringer i Instruksen, gjelder følgende:

- Endringer i Instruksen skal gjøres i samsvar med endringsprosedyren i Leveringsavtalen, men den Dataansvarlige kan alltid ensidig instruere Databehandleren om å avslutte videre behandling av personopplysningene som er overlatt til Databehandleren.
- Databehandleren har rett til betaling av alle kostnader som er direkte knyttet til endringer i Instruksen, inkludert kostnader for gjennomføring og økte kostnader for levering av tjenester etter Leveringsavtalen.
- Endringene i Instruksen anses bare å gjelde etter at endringene er implementert.
- Databehandleren kan avslå en endring i Instruksen. Databehandleren skal da opphøre med ytterligere behandling av den Dataansvarliges personopplysninger og, etter den Dataansvarliges valg, enten slette eller returnere dataene i samsvar med punkt 14 nedenfor. Databehandleren er da fritatt fra å utføre sine leveringsforpliktelser i henhold til Leveringsavtalen, men Leveringsavtalen for øvrig fastholdes.

## **7 Overføring til tredjeland eller internasjonale organisasjoner**

Databehandleren skal kun overføre personopplysninger til et tredjeland dersom dette følger av Instruksen eller det kreves av EU-lov eller nasjonal lovgivning som gjelder for Databehandleren. I så fall skal Databehandleren underrette den Dataansvarlige om det lovpålagte kravet før overføringen utføres, med mindre en slik underretning vil være i strid med loven.

Personopplysninger skal kun overføres dersom en slik overføring er i samsvar med EU-lov eller nasjonal lovgivning som gjelder for Databehandleren.

Den Dataansvarliges godkjenning av overføring av personopplysninger til et tredjeland, kan foreligge i bilag 1.

I den utstrekning en godkjent overføring til en underdatabehandler krever at den Dataansvarlige inngår en standardkontrakt, skal den Dataansvarlige bistå med å inngå denne på egen regning på Databehandlerens forespørsel. I så tilfelle skal den Dataansvarlige rapportere en slik overføring til det norske Datatilsynet. Overføringen kan iverksettes etter en slik rapportering.

## **8 Taushetsplikt**

Databehandleren skal sørge for at personer som har fullmakt til å behandle den Dataansvarliges personopplysninger, har forpliktet seg til å fortrolighet eller er underlagt en behørig lovbestemt taushetsplikt. Denne taushetsplikten skal gjelde også etter denne Databehandleravtalen oppsigelse eller utløp.

## **9 Sikkerhetsforanstaltninger**

Databehandleren skal igangsette og gjennomføre hensiktsmessige tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som samsvarer med risikoen for behandlingsvirksomheten som utføres av Databehandleren for den Dataansvarlige.

De tekniske og organisatoriske tiltakene skal fastsettes under hensyntagen til den nyeste teknikken, kostnadene ved implementering og arten, omfanget, konteksten og formålene med behandlingen, samt risikoen for varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og friheter.

Ved vurderingen av det aktuelle sikkerhetsnivået skal det tas særlig hensyn til risikoen som behandlingen utgjør, særlig som følge av utilsiktet eller ulovlig ødeleggelse, tap, endring, uautorisert viderefremming eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Databehandleren skal oppfylle kravene til tilfredsstillende sikkerhet som fremgår av personopplysningsloven og personopplysningsforskriften, særlig lovens §§ 13-15 med tilhørende forskrifter. Databehandleren skal dokumentere rutiner og andre målinger for å oppfylle disse forpliktelsene. Slik dokumentasjon skal foreligge på forespørsel fra den Dataansvarlige.

## **10 Bruk av en annen databehandler**

Databehandleren skal ikke bruke en annen databehandler (underdatabehandler) uten skriftlig forhåndsgodkjenning fra den Dataansvarlige.

Databehandleren skal varsle den Dataansvarlige om eventuelle planlagte endringer vedrørende tilføyelse eller utskiftning av underdatabehandlere senest fjorten (14) dager før planlagt påbegynt bruk av underdatabehandler. Slike endringer skal godkjennes skriftlig av den Dataansvarlige, men en godkjenning skal ikke nektes uten rimelig grunn.

Hvis Databehandleren bruker en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den Dataansvarlige, skal Databehandleren pålegge underdatabehandleren de samme databeskyttelsesforpliktelsene som er spesifisert i denne Databehandleravtalen, især skal det gis nødvendige garantier for at underdatabehandleren skal gjennomføre passende tekniske og organisatoriske tiltak på en slik måte

at behandlingen oppfyller kravene i Forskriftene. Hvis den anvendte underdatabehandleren ikke overholder sine databeskyttelsesforpliktelser, forblir Databehandleren fullt ut ansvarlig overfor den Dataansvarlige for utførelsen av underdatabehandlerens forpliktelser.

## **11 Skyløsninger**

Hvis Databehandleren behandler den Dataansvarliges personopplysninger i en hybridløsning, noe som forstås som at det i den Dataansvarliges IT-miljø inngår komponenter som er plassert i Databehandlerens datasentre og komponenter som er plassert utenfor Databehandlerens datasentre (heretter Skyen), avtales følgende:

Hvis Databehandleren leverer en løsning til den Dataansvarlige hvor det inngår en Skydel, må Databehandlerens underleverandør på denne Skydelen oppbevare og behandle den Dataansvarliges personidentifiserbare opplysninger i overensstemmelse med underleverandørens gjeldende standardvilkår, jf. nærmere de spesielle vilkårene om dette i bilag 2.

Hvis Databehandlerens leveranser inngår i en hybridløsning, hvor den Dataansvarlige har avtalerelasjon direkte til en eller flere leverandører av Skyttelser, og Databehandleren skal behandle, men ikke oppbevare den Dataansvarliges personopplysninger i Skydelen, skjer Databehandlerens behandling i henhold til denne Avtalen mens Databehandleren ikke er ansvarlig for oppbevaringen og behandlingen av data hos en annen Skyleverandør.

Dette punkt 11 har forrang foran avsnitt 10 ovenfor, som handler om generell bruk av underdatabehandlere.

## **12 Bistand til den Dataansvarlige**

Den Dataansvarlige skal avtale med Databehandleren om å ha regelmessige sikkerhetsrevisjoner av systemer, rutiner og andre krav for å sikre overholdelse av denne Databehandleravtalen og Forskriftene. Ytterligere detaljer om slike sikkerhetsrevisjoner og hvor ofte en sikkerhetsrevisjon skal utføres, fremgår av bilag 1.

På den Dataansvarliges spesifikke forespørsel og under hensyntagen til behandlingens art, skal Databehandleren bistå den Dataansvarlige så langt det er mulig med passende tekniske og organisatoriske tiltak, med oppfyllelse av den Dataansvarliges forpliktelse til å svare på forespørsler om utøvelse av de registrertes rettigheter som er fastsatt i lovgivningen om personopplysningslovgivningen.

Hvis en registrert fremsetter en forespørsel til Databehandleren om utøvelse av sine rettigheter, skal Databehandleren varsle den Dataansvarlige om dette uten unødig forsinkelse.

Under hensyntagen til behandlingens art og opplysningene som er tilgjengelige for Databehandleren, skal Databehandleren også bistå den Dataansvarlige ved en bestemt forespørsel for å sikre overholdelse av den Dataansvarliges forpliktelser med hensyn til:

a) Gjennomføring av hensiktsmessige tekniske og organisatoriske tiltak

- b) Sikkerhetsbrudd
- c) Formidling av brudd på den registrertes personopplysningssikkerhet
- d) Gjennomføring av konsekvensanalyser
- e) Forutgående konsultasjon med tilsynsmyndighetene.

Databehandleren har krav på separat vederlag for tjenester etter dette punkt 12.

### **13 Varsel om brudd på personopplysningssikkerheten**

Databehandleren skal uten unødig forsinkelse varsle den Dataansvarlige etter å ha blitt kjent med brudd på personopplysningssikkerheten som beskrevet i Forskriftene § 2-6.

Meldingen skal inneholde de faktiske forholdene i forbindelse med brudd på personopplysningssikkerheten, dets innvirkninger og de tiltak som er truffet.

Den Dataansvarlige skal rapportere til det norske Datatilsynet innen 72 timer, jfr. GDPR § 33.

### **14 Sletting og tilbakelevering av behandlede personopplysninger**

Ved opphør av tjenestene i henhold til Leveringsavtalen skal Databehandleren slette eller tilbakelevere til den Dataansvarlige, etter den Dataansvarliges valg, alle personopplysninger og slette eksisterende kopier, inkludert sikkerhetskopier av slike data (hvis dette er i den Dataansvarliges besittelse), med mindre EU-lov eller nasjonal lovgivning krever at Databehandleren oppbevarer personopplysningene.

På den Dataansvarliges forespørsel skal Databehandleren innen rimelig tid avgi en erklæring om at de behandlede personopplysningene er tilbakelevert eller slettet i samsvar med den Dataansvarliges valg, eller at Databehandleren må oppbevare personopplysningene, i hvilket tilfelle erklæringen skal inneholde Databehandlerens erklæring om at oppbevaringen utføres etter vilkårene i Databehandleravtalen.

### **15 Dokumentasjon på overholdelse av Databehandlerens forpliktelser**

Databehandleren skal overfor den Dataansvarlige stille til rådighet all nødvendig informasjon for å dokumentere at kravene i Databehandleravtalen overholdes. Databehandleren skal gi tilgang og bidra til revisjoner, herunder inspeksjoner, utført av den Dataansvarlige eller en annen revisor som er godkjent av den Dataansvarlige.

Hvis revisjonen utføres av en annen revisor enn den Dataansvarlige selv, skal denne andre revisoren være uavhengig og ikke en konkurrent til Databehandleren og skal være underlagt fortrolighet og taushetsplikt, enten ved lov eller i henhold til en konfidensialitetsavtale som Databehandleren kan støtte seg på direkte overfor denne andre revisoren.

Databehandleren skal omgående underrette den Dataansvarlige en instruks om å stille opplysninger tilgjengelig eller gi tilgang til revisjoner eller inspeksjoner etter Databehandlerens oppfatning strider mot personopplysningslovgivningen eller databeskyttelsesbestemmelser i annen EU-lovgivning eller nasjonal lovgivning.

Databehandleren har krav på separat vederlag for å bidra til revisjon etter dette punkt 15.

I den utstrekning den Dataansvarlige stiller spesielle krav til Databehandlerens dokumentasjon, er disse kravene og Databehandlerens vederlag for å innfri dem, angitt i bilag 1.

## **16 Samarbeid med tilsynsmyndigheter**

Databehandleren skal på forespørsel samarbeide med det norske Datatilsynet og eventuelle andre tilsynsmyndigheter i utførelsen av sine oppgaver. Databehandleren har rett til å gi Tilsynsmyndighetene tilgang til alle personopplysninger og opplysninger som kreves for å utføre Tilsynsmyndighetenes oppgaver.

Ved Databehandlerens valg skal enten den Dataansvarlige eller Databehandleren treffe de nødvendige tiltak for å sikre at vedtak fra Tilsynsmyndigheten blir etterkommet. Eventuelle endringer vedrørende sikkerhetsnivået skal håndteres som en endring. Den Dataansvarlige skal varsle Tilsynsmyndighetene om de tiltakene som er truffet for å etterkomme beslutningen.

Hvis Tilsynsmyndighetene gir Databehandleren et pålegg, skal Databehandleren etterkomme pålegget på den angitte måten innenfor den angitte fristen.

Databehandleren har rett til separat vederlag for tid og materialer som forbrukes for sine tjenester og leveranser etter dette punkt 16.

## **17 Den Dataansvarliges forpliktelser**

Den Dataansvarlige påtar seg følgende forpliktelser og ansvar:

- Sikre at personopplysningene som overlates til Databehandleren for behandling, kan behandles lovlig i den utstrekning som er nødvendig for at Databehandleren skal oppfylle sine forpliktelser i henhold til Leveringsavtalen eller annen separat Instruks.
- Sikre at det gjennomføres hensiktsmessige konsekvensanalyser av den Dataansvarliges behandlingsaktiviteter, og at Databehandleren er blitt varslet om omfanget og resultatene av denne i relevant omfang.
- Sikre at det er foretatt en hensiktsmessig forutgående konsultasjon med Datatilsynet i Norge før behandlingen starter.
- Opplyse om den Dataansvarlige har utpekt en Databeskyttelsesrådgiver og en representant. I så fall skal den Dataansvarlige informere Databehandleren om relevante kontaktdetaljer. Databehandleren kan ha dialog med Databeskyttelsesrådgiveren og representanten vedrørende Databehandlerens behandling av personopplysninger for den Dataansvarlige uten å skulle betale vederlag til den Dataansvarlige.
- Foreta tilstrekkelig overvåking av Databehandleren.

## **18 Databehandling utenfor Instruksen**

Databehandleren kan behandle personopplysninger utenfor den Dataansvarliges Instruks i tilfeller der dette er påkrevd etter EU-lovgivning eller nasjonal lovgivning som gjelder for Databehandleren.

Hvis personopplysninger behandles utenfor instruksen, skal Databehandleren underrette den Dataansvarlige om årsaken. Underrettelsen må foretas før behandlingen utføres og må inneholde en henvisning til de rettslige kravene som ligger til grunn for behandlingen. Underrettelse skal ikke skje dersom en slik underrettelse ville være i strid med EU-lovgivning eller nasjonal lovgivning.

## **19 Ansvar og ansvarsbegrensning**

Partenes ansvar i henhold til Databehandleravtalen reguleres av Leveringsavtalen. Art. 82 i den generelle databeskyttelsesforskriften gjelder mht. ansvaret overfor tredjepart.

## **20 Merknader**

Partene er enige om at merknader i henhold til denne Databehandleravtalen skal være skriftlige, til følgende personer:

For den Dataansvarlige:

For Databehandleren:

## **21 Lov og verneting**

Denne Databehandleravtalen skal styres av og tolkes i samsvar med norsk lov. Partene samtykker i valg av Oslo byrett som verneting, med mindre annet er avtalt i Leveringsavtalen.

## **Bilag 1: Ytterligere spesifikasjoner vedrørende databehandling**

Følgende behandlingsaktiviteter er omfattet av Databehandleravtalen: Implementering, drift, support og vedlikehold av IT-løsningen (som beskrevet i særskilte avtaler mellom Partene), som kan innebære adgang til personopplysninger.

Den Dataansvarliges sikkerhetsprosedyrer for oppkobling via fjerntilgang skal etterleves.

### **Typer av personopplysninger**

Typer personopplysninger som behandles i sammenheng med levering av tjenester iht. Leveranseavtalen:

1. Alminnelige personopplysninger, herunder, navn, adresse, telefonnumre, e-mail adresse, bankkonto, kredittkortopplysninger, bilder, økonomiske forhold, opplysninger om lønnsforhold, lønnslipper, sosiale forhold og andre identifikasjonsopplysninger.
2. Personnummer.

### **Kategorier av registrerte personer**

Kategorier av registrerte, identifiserte eller identifiserbare fysiske personer som Databehandlerens handlinger vedrører:

1. Ansatte
2. Kunder
3. Samarbeidspartnere og andre interessenter som den Dataansvarlige måtte ha.

### **Underdatabehandlere som brukes**

Databehandleren anvender de underdatabehandlere, som fremgår av understående liste.

Dersom underdatabehandlere legges til, tas bort eller byttes ut fra denne listen vil Databehandleren informere om endringen til den Dataansvarlige til samme e-postadresse som denne Databehandleravtalen er sendt til.

Den Dataansvarlige skal straks underrette Databehandleren, hvis opplysninger om endringer av listen over underdatabehandlere skal sendes til en annen e-postadresse.

Det er den Dataansvarliges ansvar å gjøre seg kjent med endringer av underdatabehandlere, ved å følge eventuelle henvisninger i denne e-post, når Databehandleren sender e-post med informasjon som beskrevet ovenfor.



Når Databehandleren har sendt en e-post med informasjon som beskrevet ovenfor, har Databehandleren informert den Dataansvarlige om endringer av underdatabehandlere som beskrevet i Databehandleravtalens punkt 10.

Databehandleren bruker følgende underdatabehandlere:

<b>Underdatabehandler</b>	<b>CVR/VAT</b>	<b>Beskrivelse</b>
Bambora Online A/S	28855060	Betaling med kredittkort
Geomatic	28862245	Telefonnummer søk
GlobalConnect A/S	26759722	Hosting
Link Mobility A/S	30077520	SMS-levering av engangskoder og meldinger
Saint-Gobain A/S	81822514	Login info fra Brødrene Dahl
SendGrid, Inc.	USA	Sending av utgående e-post fra Xena
Sproom Solutions A/S	37498009	Elektroniske fakturaer
Zitcom A/S	29412006	Hosting selskap

### **Lokasjoner for oppbevaring av personopplysninger**

Data oppbevares på servere i EU/EEA.

### **Spesielle dokumentasjonskrav**

#### ***Ved bruk av Cloud & Hosting gjelder følgende:***

Databehandleren får én gang om året utarbeidet revisjonserklæringer av typene ISAE 3402 type 2 og ISAE 3000 type 2 eller lignende med utgangspunkt i en risikovurdering foretatt med ISO 27002 som referanseramme.

Erklæringen ISAE 3402 type 2 omfatter Databehandlerens interne kontormiljø på OS og database nivåa, men ikke omfattende applikasjoner, som inngår i Databehandlerens datasentre. ISAE 3000 type 2 vedrører kontroller for behandlingssikkerhet i relasjon til persondata.

Databehandleren må gjøre bruk av en annen type erklæring enn den nåværende, såfremt den dekker de samme IT-sikkerhetsmessige forhold uten forutgående spesifikk godkjennelse fra den Dataansvarlige.

Databehandleren skal underrette den Dataansvarlige om eventuelle planlagte endringer vedrørende endringer av erklæringstyper senest 14 dager forut for det planlagte oppstartstidspunktet for anvendelsen av annen type erklæring.

Databehandleren er berettiget til et vederlag for denne dokumentasjon. Den Dataansvarlige dekker alle kostnader forbundet med utarbeidelse og innhenting av slik dokumentasjon.

## **Bilag 2: Endring av mottaker hos den Dataansvarlige**

Databehandleren sender ut underleverandørers standardvilkår til den Dataansvarlige til den e-postadressen hos den Dataansvarlige som denne Databehandleravtalen er sendt til.

Den Dataansvarlige skal straks melde fra til Databehandleren, dersom underleverandørers standardvilkår skal sendes til en annen e-postadresse.

Når den Dataansvarlige mottar slike standardvilkår, skal den Dataansvarlige uten unødig opphold melde fra om Dataansvarlig gir samtykke til at disse standardvilkårene finner anvendelse som beskrevet i Databehandleravtalens punkt 11.