

Databehandleravtale

mellom

Behandlingsansvarlig:	Bergen kommune
Organisasjonsnr:	964 338 531
Etablert i:	Norge
Databehandler:	Visma Enterprise AS
Organisasjonsnummer:	982 410 339
Etablert i:	Norge
Databehandlerens kontaktinformasjon for generelle henvendelser (navn, rolle, kontaktdetaljer):	GDPR.VE@visma.com

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 avtaler om levering av tjenester (Tjenesteavtale) mellom partene.

Definisjoner

Definisjonene av personopplysning, særlige kategorier av personopplysning, behandling av personopplysning, den registrerte, behandlingsansvarlig og databehandler skal forstås slik de brukes og tolkes i henhold til gjeldende personvernlovgivning, inkludert lov om behandling av personopplysninger av 15. juni 2018 nr. 38 og personvernforordningen Europaparlaments- og rådsforordning (EU) 2016/679 (GDPR) av 27. april 2016.

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 tidligere avtaler som omhandler personvern inngått mellom partene.

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 Databehandlerens 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, eller at behandling strider mot instruksjonene som angitt over, skal Databehandleren melde dette til Behandlingsansvarlige.

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

Databehandleren skal sikre konfidensialitet, integritet og tilgjengelighet til personopplysningene i henhold til de regulatoriske krav som gjelder for Databehandlere. 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 den 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. Pliktenes omfang avgrenses av formen for behandling av personopplysninger og hvilken informasjon som er tilgjengelig for Databehandler.

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

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 og skal blant annet sikres gjennom å inngå taushetserklæringer.

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

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 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. Ansvar for slike integrasjoner med tredjepart påhviler utelukkende Behandlingsansvarlig.

Behandlingsansvarliges plikter

Ved å signere Databehandleravtalen bekrefter Behandlingsansvarlig:

- 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, korrekte og tilstrekkelige.
- At forpliktelsen til å formidle relevant informasjon til registrerte eller myndigheter vedrørende behandlingen av personopplysninger er oppfylt.
- At sensitive personopplysninger kun vil bli behandlet som en del av Tjenesteavtalen der dette er uttrykkelig avtalt i Vedlegg A til Databehandleravtalen.

Bruk av underleverandører og overføring av personopplysninger

Som en del av leveransen under Tjenesteavtale vil Databehandleren bruke underleverandører og Behandlingsansvarlig gir sitt generelle samtykke til dette. Slike underleverandører kan være andre selskaper i Visma-konsernet eller eksterne tredjeparter. Databehandleren har plikt til å påse at underleverandører påtar seg tilsvarende forpliktelser som de som følger av denne Databehandleravtalen.

Oversikt over underleverandører med tilgang til personopplysninger fremgår på Visma Trust Center med besøksadresse: <https://www.visma.com/trust-centre/transparency/>. I tillegg kan Behandlingsansvarlig ta kontakt med Databehandler for mer detaljert informasjon om underleverandører.

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 Behandlingsansvarlig, herunder ved å gjøre bruk av EU standardavtaler.

Behandlingsansvarlig vil bli varslet før Databehandleren endrer underleverandør som behandler personopplysninger. Dersom Behandlingsansvarlig kommer med innsigelser til underleverandører i denne forbindelse skal partene tilgjengeliggjøre og gjennomgå informasjon og dokumentasjon om underleverandøren som påviser dens etterlevelse av personvernlovgivningen.

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.

Rett til tilsyn

Behandlingsansvarlig kan revidere Databehandler sin etterlevelse av denne Databehandleravtalen som hovedregel 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 forslagetets omfang, varighet og oppstart. Hvis tredjeparter skal gjennomføre tilsynet, skal dette som hovedregel avtales mellom partene. Hvis Databehandlers behandling av personopplysninger skjer i et "multitenant" miljø eller lignende, aksepterer Behandlingsansvarlig likevel at tilsynet gjennomføres av en tredjepart, som hovedregel utpekt av Databehandler, i den utstrekning dette er nødvendig av hensynet til sikkerheten.

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. Hver av partene bærer egne kostnader i forbindelse med årlig tilsyn. Dersom Behandlingsansvarlige ber om mer tilsyn, eller mer assistanse enn det som tilbys av Databehandler for å oppfylle kravene til rollen som Databehandler, kan Databehandleren kreve betaling for denne tilleggstjenesten i henhold til avtale mellom partene.

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 eventuell bistand fra Behandlingsansvarlig med dette arbeidet kompenseres basert på; i) kompleksiteten ved forespørselen og ii) betaling for medgått tid.

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

Endringer og ugyldighet

Eventuelle 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.

Ansvar

Begge parter har et individuelt ansvar etter gjeldende personvernlovgivning i forhold til de

personopplysningene de behandler og skal holdes selvstendig ansvarlig for å betale alle bøter og erstatning som ilegges den respektive part av myndigheter eller domstoler i henhold til GDPR. Øvrig ansvar reguleres av den Tjenesteavtale som foreligger mellom partene.

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:	Leif Arne Brandsæter
Tid og sted:	Oslo 21.12.2018 / 09.09.2020

Bekrefter epost til Os kommune v/ Simen Soltvedt fra Visma v/Liv Jorunn Wøien, 16.08.2018:

1. I nest nedste avsnitt på side to er det ikkje konkretisert kva Visma meiner med "ugrunnet opphold". Det kan vere fornuftig å fastsette, for eksempel maksimalt 36 timer.

SVAR: Ikkje akseptert. Visma inngår ingen harde tidsfristar i våre databehandlaravtalar då dette skapar meir forvirring enn klarhet. "Uten ugrunnet opphold" er raskare enn "innen 24 timer".

2. Punktet som gjeld bruk av underleverandører og overføring av personopplysningar er ikkje heldig. Det gjelder for det første om Visma skifter underleverandør. Då skal vi bli varsla, men det står ingenting om at vi har rett til å nekte skiftet, evt. at det gir oss mulighet for å seie opp avtalen. Slik rett har behandlingsansvarlig. I standenfor legges det opp til drøftelse og gjennomgang av informasjon, se nederste avsnitt.

SVAR: Vi kan ikkje akseptere å gje ein kunde vetorett på å seie nei til ein ny underleverandør, på vegne av alle andre kundar, noko som vil kunne medføre ei dårligare tjeneste. Merk at Visma har ingen interesse i å velge ein underleverandør som ikkje oppfyller krav i lov, kontrakt og databehandlaravtale - det vil raskt føre oss ut av markedet med produktet.

3. Noko av det samme gjeld om opplysningar skal bli overført til utanfor EU/EØS. Det skal bare skje på instruksar frå behandlingsansvarlig. I tredje avsnitt står det ingenting om denne retten.

SVAR: Vår variant med generell tillatelse er også ok ihht GDPR. Dersom dette er no-go frå dykkar side må vi forhandle spesielt om det. Viser for øvrig til siste del av svaret på punktet over.

4. Videre er retten til tilsyn noko begrensa. Den kan som hovedregel bare skje ein gong i året (side 4).

SVAR: Ja, som hovedregel. Dersom det skjer brudd på avtalen / mistanke om mislighold vil det sjølvsagt vere mogleg å gjennomføre tilsyn. Det vil ikkje vere i tråd med Visma sitt ynskje om eit godt kundeforhold å skulle nekte slikt tilsyn.

5. Det er vidare krav om ein tredjepart som er utpekt av databehandler dersom det er et «multitenant» miljø eller lignende.

SVAR: Ja, slik må det vere av to grunnar. Vi kan ikkje gje ein kunde potensielt innsyn i andre kunders data og dessuten har vi som mål å kunne nyttiggjere oss av evt eksisterande revisjonsrapportar/underlag.

6. Det er heller ikke noen punkt som gjelder mislighold og pålegg om stans.

SVAR: Alle tjenesteavtaler har reguleringar på hva som skal gjelde som oppsigelsesgrunn. Vesentlig mislighold er ein slik grunn, også innanfor personvern.

Visma Gat Ressursstyring (VGR) - DPA Appendix A + B

Last updated: 25.02.2020 LJW

Vedlegg A - Kategorier av registrerte og personopplysninger

VGR leveres som en on-premise løsning installert i kundens nettverk eller via kundens driftspartner. Databehandleravtalen med Visma er opprettet fordi Visma via support og/eller konsulentoppdrag vil kunne få sporadisk tilgang til persondata enten ved pålogging hos kunden eller via database-kopier i leverandørens nettverk.

1. Kategorier av registrerte og personopplysninger

- a. Kategorier av registrerte personer som produktet samler inn personopplysninger om:
 - i. Ansatte, vikarer og eksternt innleide personer hos kunden som skal planlegges i forhold til arbeidstid og oppgaver.
 - ii. Ledere hos kunden som skal planlegge arbeidstid og oppgaver for sin avdeling.
 - iii. Systemforvaltere hos kunden som skal sette opp og drifte den funksjonelle løsningen i kundens organisasjon.

- b. Kategorier av personopplysninger
 - i. Kontaktinformasjon som navn, initialer, adresse, telefon, epostadresser, fødselsdato, kjønn, pårørende informasjon etc.
Opsjonelt pr kunde: fødsels- og personnummer, bilde og bankkontonummer.
 - ii. Jobbrelatert stillingsinformasjon som ansattnummer, stillingsprosent, avdeling, fra- og tildato for stillingen, stillingskode/ kategori, tittel, ansettelsesforhold, regelsett, uketimetall etc.
Opsjonelt pr. kunde: Årslønn og fagforeningstilhørighet.
 - iii. Arbeidstid relatert informasjon om når (dato/tid) personen skal jobbe / har jobbet / ønsker å jobbe / er tilgjengelig for ekstrajobb, på hvilken avdeling og med hvilke oppgaver/ gjøremål, inklusive alle avvik fra opprinnelig planlagt arbeidstid med tilhørende timelister/ lønnstransaksjoner (antall timer med lønnart, ingen beløp) og eventuelle brudd på arbeidsmiljøloven etc.
 - iv. Fravær med fraværskode, fra- og tildato (evt. fra- og tilklokken på enkeltvakter) og fraværsprosent.
Opsjonelt pr. kunde: Oppfølging av IA fravær.
Opsjonelt pr. kunde: Data fra digitale sykemeldinger via integrasjon med Altinn.
 - v. Akkumulatorer for saldo på feriebank, avspaseringstimer, fleksitid etc.
 - vi. Dispensasjoner fra arbeidsmiljøloven
 - vii. Opsjonelt pr. kunde: Logg over all elektronisk kommunikasjon med den ansatte via løsningen, inkl. forespørsler, SMS og epost.
 - viii. Opsjonelt pr. kunde: Opparbeidet kompetanse og kundens egendefinerte ekstrarfelter pr. ansatt
 - ix. Opsjonelt pr. kunde: Timeføring på ulike prosjekter.
 - x. Opsjonelt pr. kunde: Spørreundersøkelser og resultater av disse.
 - xi. Opsjonelt pr. kunde: Ansatte sine barn
 - xii. Opsjonelt pr. kunde: dokumenter som arbeidsgiver mener er relevante for lagring i VGR.

- xiii. Opsjonelt pr kunde: Analysegrunnlag for arbeidstid og fravær i forhold til kundens bemanningsbehov.

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		X
at en person har vært eller er siktet/dømt for kriminalitet		X
helseopplysninger	X	
seksuell orientering		X
Fagforeningsmedlemskap	X	
genetisk eller biometrisk data		X

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	Bistår databehandler med
Visma IT & Communications	EU / EØS	Gjelder ikke innen EU	Intern-IT
Visma Labs	EU / EØS	Gjelder ikke innen EU	Support og konsulentoppdrag
Salesforce.com	EU (France, Germany)	EU Standard Contractual Clauses	Support - tool

Følgende underdatabehandlere kan i tillegg være aktuelle dersom kunden velger å ta i bruk / inngå tilleggsavtale om ulike tilleggsmoduler i løsningen:

Navn	Land	Overføringsgrunnlag hvis underleverandør er lokalisert utenfor EU	Bistår databehandler med
Business Analyze AS Org. nr. 984 589 379	Norway	Gjelder ikke innen EU	Leverer tilleggsmodul for analyse av data som en opsjon til VGR. Bistår Visma med support og har ingen direkte tilgang til personlige data hos kunden.
SINTEF AS Org. nr. 919 303 808	Norway	Gjelder ikke innen EU	Leverer tilleggsmodul for turnusgenerator som en opsjon til VGR. Bistår Visma med support og har ingen direkte tilgang til personlige data hos kunden.
Link Mobility AS Org. nr. 992 434 643	Norway	Gjelder ikke innen EU	Leverer tilleggsmodul for å sende og/eller motta SMS meldinger som en opsjon til VGR. Mottar all SMS fra VGR og videreformidler via egen gateway til ulike teleoperatører som igjen leverer meldingene til sine mobilabonnenter. Mottar eventuelle SMS svar fra mobilabonnementene og videreformidler til kundens mottakstjeneste for 2-veis SMS i VGR basert på kodeord i svarmeldingene.
Visma Labs	EU / EØS	Gjelder ikke innen EU	BSB Team i Visma Labs: Leverer tilleggsmodul for å hente digitale sykmeldinger fra Altinn som en opsjon til VGR.
Google LLC	USA	EU Standard Contractual Clauses, Privacy Shield	For MinGat kan kunden velge å slå på logging av anonymisert

			<p>brukerstatistikk og feilmeldinger til Google Analytics.</p> <p>For appen GatGo kan kunden velge å slå på logging av anonymisert brukerstatistikk og feilmeldinger til Google Firebase.</p> <p>Disse valgene gjør at feilsituasjoner logges og det muliggjør datadrevet utvikling og bedre tjenester.</p> <p>Brukers IP-adresse behandles og Google Analytics/Firebase er satt opp slik at den blir anonymisert av Google, ingen andre persondata enn anonymisert IP adresse vil logges.</p>
<p>NB! Underleverandørene har på samme måte som Visma Enterprise AS ingen direkte datatilgang til persondata siden løsningen er installert lokalt / on-premise hos kunden.</p>			

Visma barnevern Familia og Mobilt barnevern - DPA Appendix A + B

Last updated: 25.02.2020 LJW

Vedlegg A - Kategorier av registrerte og personopplysninger

Visma Barnevern Familia leveres som en on-premiss løsning installert i kundens nettverk eller via kundens driftspartner.

Databehandleravtalen med Visma er opprettet fordi Visma via support og/eller konsulentoppdrag vil kunne få sporadisk tilgang til persondata enten ved pålogging hos kunden eller via database-kopier i leverandørens nettverk.

1. Kategorier av registrerte og personopplysninger

- a. Kategorier av registrerte personer som produktet samler inn personopplysninger om:
 - i. Ansatte og ledere i tjenesten hos kunden.
 - ii. Oppdragstakere oa. ansatt i tjenesten og kunden
 - iii. Klienter med familie og kontaktpersoner etc.
 - iv. Systemforvaltere hos kunden som skal sette opp og drifte den funksjonelle løsningen i kundens organisasjon.

- b. Kategorier av personopplysninger
 - i. Kontaktinformasjon som navn, initialer, adresse, telefon, epostadresser, fødsels- og personnummer, kjønn, pårørende informasjon etc.
 - ii. Jobbrelatert stillingsinformasjon som ansattnummer, stillingsident, fra- og tildato for stillingen, tittel etc.
 - iii. Klientinformasjon som selv kan defineres av kunden (klientgruppe etc)
 - iv. Merknadsfelt felt hvor kunden selv definerer innholdet

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	X (vil kunne forekomme i dokumenter)	
at en person har vært eller er siktet/dømt for kriminalitet	X (vil kunne forekomme i dokumenter)	
helseopplysninger	X (vil kunne forekomme i dokumenter)	
seksuell orientering	X (vil kunne forekomme i dokumenter)	
Fagforeningsmedlemskap		X
genetisk eller biometrisk data		X

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	Bistår databehandler med
Visma Labs	EU/EØS	Gjelder ikke innen EU	Support og konsulenttjenester
Visma IT & Communications	EU/EØS	Gjelder ikke innen EU	Intern IT
Salesforce.com	EU (France, Germany)	EU Standard Contractual Clauses	Support - tool

NB! Underleverandørene har på samme måte som Visma ingen direkte datatilgang til persondata siden løsningen er installert lokalt / on-premiss hos kunden.

Aktuelt kun for tilleggsmodulen **Visma Mobilt Barnevern** - som benyttes for å levere Visma Barnevern Familia som en mobil løsning:

Navn	Land	Overføringsgrunnlag hvis underleverandør er lokalisert utenfor EU	Assisting the Processor with
Link Mobility AS 992 434 643	Norge	Gjelder ikke innen EU	Sender PIN-kode på sms i forbindelse med pålogging

Visma Flyt Sikker Sak - DPA Appendix A + B

Last updated: 25.02.2020 LJW

Dette dokumentet gjelder også Visma Link for de kunder som bruker løsningen som meldingsformidler i forbindelse med Visma Flyt Sikker Sak. De samme opplysninger som behandles i Visma Flyt Sikker Sak behandles også i Visma Link i de tilfeller der begge løsninger brukes.

Vedlegg A - Kategorier av registrerte og personopplysninger

1. Kategorier av registrerte og personopplysninger

- a. Kategorier av registrerte personer som produktet samler inn personopplysninger om:
 - i. Ansatte i tjenesten hos kunden.
 - ii. Personer (tjenestemottakere) med familie (pårørende etc.).
 - iii. Andre kontaktpersoner

- b. Kategorier av personopplysninger
 - i. Kontaktinformasjon som navn, initialer, adresse, telefon, epostadresser, fødsels- og personnummer, kjønn, pårørende informasjon etc.
 - ii. Jobbrelatert stillingsinformasjon som ansattnummer, stillingsprosent, avdeling, fra- og tildato for stillingen, tittel etc.
 - iii. Egendefinerte fritekstfelt hvor kunden selv velger informasjon som legges inn
 - iv. Logg over all elektronisk kommunikasjon
 - v. Logg over endringer og oppslag 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	X (vil kunne forekomme i dokumenter)	
at en person har vært eller er siktet/dømt for kriminalitet	X (vil kunne forekomme i dokumenter)	
helseopplysninger	X (vil kunne forekomme i dokumenter)	
seksuell orientering	X (vil kunne forekomme i dokumenter)	
Fagforeningsmedlemskap		X
genetisk eller biometrisk data		X

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	Bistår databehandler med
Link Mobility AS 992 434 643	Oslo, Norway	Gjelder ikke innen EU	Tilleggsmodul / opsjon for å sende og/eller motta SMS varsler
Visma Labs	EU/EØS	Gjelder ikke innen EU	Support og konsulenttjenester
Visma IT & Communications	EU/EØS	Gjelder ikke innen EU	Drift av IT-miljø inkludert lagring
Amazon Web Services	EU (Ireland)	EU Standard Contractual Clauses	Logon via Visma Connect, implementeres i 2020.
Salesforce.com	EU (France, Germany)	EU Standard Contractual Clauses	Support - tool

Visma Omsorg HsPro - DPA Appendix A + B

Last updated: 25.02.2020 LJW

Vedlegg A - Kategorier av registrerte og personopplysninger

Visma Omsorg HsPro (HsPro) leveres som en on-premise løsning installert i kundens nettverk eller via kundens driftspartner.

Databehandleravtalen med Visma er opprettet fordi Visma via support og/eller konsulentoppdrag vil kunne få sporadisk tilgang til persondata enten ved pålogging hos kunden eller via database-kopier i leverandørens nettverk.

1. Kategorier av registrerte og personopplysninger

- a. Kategorier av registrerte personer som produktet samler inn personopplysninger om:
 - i. Ansatte og ledere i tjenesten hos kunden.
 - ii. Klienter / pasienter med kontaktpersoner (pårørende, relasjoner, fastlege etc)
 - iii. Systemforvaltere hos kunden som skal sette opp og drifte den funksjonelle løsningen i kundens organisasjon.

- b. Kategorier av personopplysninger
 - i. Informasjon om den ansatte som navn, initialer, telefon, organisatorisk tilhørighet, stilling, fagkode (eks. jordmor jfr VOLVEN), stillingstype, ansettelsesperiode, felt for jobb mobil, rolle, begrunnelse etc.
 - ii. Informasjon om klient som navn, fødsels- og personnummer, kjønn, adresse, evt. hemmelig adresse, kommune, telefon, relasjoner (pårørende, fastlege), demografi (språk, nasjonalitet, fødeland etc)
 - iii. Medisinsk informasjon om klienten som medisin, diagnose, vaksinasjon, percentiler, CAVE, viktig merknad, helseundersøkelse, fortløpende journal etc.
 - iv. Elektronisk kommunikasjon mellom helsestasjon og fastlege, sykehus, etc.
 - v. Logg over all elektronisk kommunikasjon 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 Behandlingsansvarlig behandle følgende sensitive personopplysninger:	Yes	No
rase, etnisitet, politisk eller filosofisk tilhørighet eller religion	X Kan forekomme i journalnotat	
at en person har vært eller er siktet/dømt for kriminalitet		X
helseopplysninger	X	
seksuell orientering	X Kan forekomme i journalnotat	
Fagforeningsmedlemskap		X
genetisk eller biometrisk data		X

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	Bistår databehandler med
Visma Labs	EU/EØS	Gjelder ikke innen EU	Support og konsulenttjenester
Visma IT & Communications	EU/EØS	Gjelder ikke innen EU	Intern IT
Link Mobility AS Org. nr. 992 434 643	Oslo, Norway	Gjelder ikke innen EU	Tilleggsmodul / opsjon for å sende og/eller motta SMS meldinger via HsPro.
Salesforce.com	EU (France, Germany)	EU Standard Contractual Clauses	Support - tool
NB! Underleverandørene har på samme måte som Visma ingen direkte datatilgang til persondata siden løsningen er installert lokalt / on-premise hos kunden.			

Visma Omsorg Profil - DPA Appendix A + B

Last updated: 25.02.2020 (LJW)

Dette dokumentet gjelder også Visma Link for de kunder som bruker løsningen i forbindelse med Visma Omsorg Profil. De samme opplysninger som behandles i Visma Omsorg Profil behandles også i Visma Link i de tilfeller der begge løsninger brukes.

Vedlegg A - Kategorier av registrerte og personopplysninger

Visma Omsorg Profil leveres som en on-premise løsning installert i kundens nettverk eller via kundens driftspartner, og i utgangspunktet er da kunden både behandlingsansvarlig og databehandler.

Databehandleravtalen med Visma er opprettet fordi Visma via support og/eller konsulentoppdrag vil kunne få sporadisk tilgang til persondata enten ved pålogging hos kunden eller via scrambled database-kopier i leverandørens nettverk.

1. Kategorier av registrerte og personopplysninger

- a. Kategorier av registrerte personer som produktet samler inn personopplysninger om:
 - i. Ansatte i tjenesten hos kunden.
 - ii. Klienter med kontaktpersoner (pårørende, relasjoner, fastlege etc)
 - iii. Systemforvaltere hos kunden som skal sette opp og drifte den funksjonelle løsningen i kundens organisasjon.

- b. Kategorier av personopplysninger
 - i. Informasjon om den ansatte som navn, initialer, adresse, telefon, fødsels- og personnummer, kjønn, organisatorisk tilhørighet, stilling, ansettelsesforhold, fravær, turnusplan, vaktplan, arbeidslister etc.
 - ii. Informasjon om klient som navn, fødsels- og personnummer, adresse, telefon, sivilstatus, fødested, nasjonalitet, språk, nåværende og tidligere yrke, umyndiggjort, kontaktpersoner (nærmeste pårørende, relasjoner, fastlege etc), organisatorisk tilhørighet etc
 - iii. Post- og saksbehandling, arkiv, SvarUt etc.
 - iv. Medisinsk informasjon som tjenester, diagnoser, medisiner, cave, allergier, tiltaksplaner, prøvesvar, målinger, IPLOS, Bruk av tvang, tekniske hjelpemidler etc.
 - v. Dagsenteropphold, Institusjonsopphold, Boligtilknytning etc
 - vi. Elektronisk kommunikasjon mellom Pleie- og Omsorg og fastlege, sykehus, helsenorge. etc.
 - i. Logg over all elektronisk kommunikasjon etc.
 - vii. Innbyggerdialog mellom Pleie- og Omsorg og klient/pårørende
 - viii. Egenbetaling, fakturagrunnlag, vederlagsberegning (inntekter og fradrag), inntektsopplysninger, meldinger til/fra NAV, pasientregnskap 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 Behandlingsansvarlig behandle følgende sensitive personopplysninger:	Yes	No
rase, etnisitet, politisk eller filosofisk tilhørighet eller religion	X Kan forekomme i journalnotat	
at en person har vært eller er siktet/dømt for kriminalitet	X Kan forekomme i journalnotat	
helseopplysninger	X	
seksuell orientering	X Kan forekomme i journalnotat	
Fagforeningsmedlemskap		X
genetisk eller biometrisk data		X

Vedlegg B - Oversikt underleverandører

NB! Underleverandørene har på samme måte som Visma ingen direkte datatilgang til persondata siden løsningen er installert lokalt / on-premise hos kunden.

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

Navn	Land	Overføringsgrunnlag hvis underleverandør er lokalisert utenfor EU	Bistår databehandler med
Visma Labs	EU/EØS	Gjelder ikke innen EU	Support og konsulenttjenester
Visma IT & Communications	EU/EØS	Gjelder ikke innen EU	Intern IT
Link Mobility AS Org. nr. 992 434 643	Norge	Gjelder ikke innen EU	Tilleggsmodul / opsjon for å sende og/eller motta SMS meldinger.
Salesforce.com	EU (France, Germany)	EU Standard Contractual Clauses	Support - tool

NB! Underleverandørene har på samme måde som Visma ingen direkte datatilgang til persondata siden løsningen er installeret lokalt / on-premise hos kunden.

Visma Samhandling Arkiv - DPA Appendix A + B

Last updated: 25.02.2020 LJW

Vedlegg A - Kategorier av registrerte og personopplysninger

Visma Samhandling Arkiv (VSA) leveres som en on-premise løsning installert i kundens nettverk eller via kundens driftspartner.

Databehandleravtalen med Visma er opprettet fordi Visma via support og/eller konsulentoppdrag vil kunne få sporadisk tilgang til persondata enten ved pålogging hos kunden eller via database-kopier overført til leverandørens nettverk.

1. Kategorier av registrerte og personopplysninger

- a. Kategorier av registrerte personer som produktet samler inn personopplysninger om:
 - i. Ansatte i tjenesten hos kunden.
 - ii. Personer (tjenestemottakere) som registreres i Visma sine fagsystem og som det arkiveres opplysninger om.
- b. Kategorier av personopplysninger
 - i. Kontaktinformasjon som navn og internt løpenr/id fra Visma sine fagsystem samt informasjon om korrespondanseparter som beskrevet i Noark5-standarden.
 - ii. Ansattrelatert stillingsinformasjon som brukerid, navn, tlfnr, epostadresse, og fra - til dato med tilgang til løsningen, samt hvilke tilganger den ansatte har i løsningen etc.
 - iii. Bruk av løsningen logges

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 Behandlingsansvarlig behandle følgende sensitive personopplysninger:	Yes	No
rase, etnisitet, politisk eller filosofisk tilhørighet eller religion	(x)	X
at en person har vært eller er siktet/dømt for kriminalitet	(x)	X
helseopplysninger	(x)	X
seksuell orientering	(x)	X
Fagforeningsmedlemskap	(x)	X
genetisk eller biometrisk data	(x)	X

Kommentarer til avmerking i kolonne Yes:

Sensitive personopplysninger blir ikke lagret i form av egne metadata (datafelt), men det kan forekomme sensitive personopplysninger i form av innhold i dokument som arkiveres.

Visma Samhandling Arkiv mottar dokumenter og journalnotater fra Visma sine fagløsninger som driftes i sikret sone, og dermed bør også arkivkjernen driftes i sikret sone. Innhold i den arkiverte informasjonen kan ha sensitivt innhold på lik linje med andre fagløsninger det arkiveres fra. Ingen opplysninger oppstår i Visma Samhandling Arkiv.

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	Tilleggsfunksjon
Visma Labs	EU/EØS	Gjelder ikke innen EU	Support og konsulenttjenester
Visma IT & Communications	EU/EØS	Gjelder ikke innen EU	Intern IT
Salesforce.com	EU (France, Germany)	EU Standard Contractual Clauses	Support - tool
NB! Underleverandørene har på samme måte som Visma ingen direkte datatilgang til persondata siden løsningen er installert lokalt / on-premise hos kunden.			

Visma Samhandling Link - Vedlegg A + B

Last updated: 14.04.2020 (ML / BK)

Dette dokumentet gjelder Visma Samhandling Link i de tilfeller der løsningen IKKE selges sammen med Visma Omsorg Profil, Visma Omsorg HsPro eller Visma Flyt-produkter. I de tilfeller hvor Visma Samhandling Link er en del av nevnte leveranser er det vedlegg A+B for de aktuelle produkter som er gjeldende.

Vedlegg A - Kategorier av personer og personopplysninger

Visma Samhandling Link leveres som en on-premise løsning installert i kundens nettverk eller via kundens driftspartner. Visma Samhandling Link er en meldingstjener og integrasjons-software hvis viktigste formål er å sørge for sikker meldingsflyt via standardiserte meldingsprotokoller.

Databehandleravtalen med Visma er opprettet fordi Visma via support og/eller konsulentoppdrag vil kunne få sporadisk tilgang til persondata enten ved pålogging hos kunden eller via scrambled database-kopier i leverandørens nettverk.

Det er kunden som bestemmer hvilke dataløsninger Visma Samhandling Link skal knyttes opp mot, og dermed også hvilke data som formidles gjennom tjeneren. Tabellene nedenfor er bare eksempler på utfylling, og må oppdateres av kunden (behandlingsansvarlig)

1. Kategorier av personer og personopplysninger som behandles i Visma Samhandling Link i henhold til databehandleravtalen.
 - a. Kategorier av registrerte personer som produktet samler inn personopplysninger om:
 - i. Pasienter
 - ii. Ansatte i fylket/kommunen
 - iii. Vikarer/eksternt innleide
 - iv. Etc.
 - b. Kategorier av personopplysninger:
 - i. Navn
 - ii. Stilling
 - iii. Telefon
 - iv. Epost
 - v. Adresse
 - vi. Etc.

1. Særlige kategorier av personopplysninger (sensitive personopplysninger)

Denne delen er bare relevant hvis databehandler, som del av tjenesteavtalen med behandlingsansvarlig, skal behandle sensitive personopplysninger som angitt under:

Databehandler skal på vegne av Behandlingsansvarlig behandle følgende sensitive personopplysninger:	Ja	Nei
Rase, etnisitet, eller filosofisk tilhørighet eller religion		x
Politisk tilhørighet		x
At en person har vært eller er siktet/dømt for kriminalitet		x

Helseopplysninger	x	
Seksuell orientering		x
Fagforeningsmedlemskap		x
Genetisk eller biometrisk data		x

Appendix B - Overview of approved subcontractors

Approved subcontractors with access to the Processor's (Controller's) Personal Data:

Navn	Land	Overføringsgrunnlag hvis underleverandør er lokalisert utenfor EU	Bistår databehandler med
Visma Labs	EU/EØS	Gjelder ikke innen EU	Support og konsulenttjenester
Visma IT & Communications	EU/EØS	Gjelder ikke innen EU	Intern IT
Salesforce.com	EU (France, Germany)	EU Standard Contractual Clauses	Support - tool
NB! Underleverandørene har på samme måte som Visma ingen direkte datatilgang til persondata siden løsningen er installert lokalt / on-premise hos kunden.			

Visma Voksenopplæring - DPA Appendix A + B

Last updated: 25.02.2020 LJW

Vedlegg A - Kategorier av registrerte og personopplysninger

Visma Voksenopplæring leveres som en on-premise løsning installert i kundens nettverk eller via kundens driftspartner.

Databehandleravtalen med Visma er opprettet fordi Visma via support og/eller konsulentoppdrag vil kunne få sporadisk tilgang til persondata enten ved pålogging hos kunden eller via database-kopier overført til leverandørens nettverk.

1. Kategorier av registrerte og personopplysninger

- a. Kategorier av registrerte personer som produktet samler inn personopplysninger om:
 - i. Ansatte i tjenesten hos kunden.
 - ii. Personer som er deltakere i introduksjonsprogrammet ihht. Lov om introduksjonsordning og norskopplæring, med familieopplysninger inkl. barn, og øvrige kontaktpersoner (pårørende, relasjoner, fastlege etc).
I tillegg elever uten rett og plikt og som betaler for sin undervisning. Disse vil kreve samtykkeerklæring for at behandlingen skal være lovlig.
- b. Kategorier av personopplysninger
 - i. Kontaktinformasjon som navn, adresse, telefon, epostadresser, DUFnr, fødsels- og personnummer, alternativt D-nummer, kjønn, pårørende informasjon etc.
 - ii. Ansattrelatert stillingsinformasjon som brukerid, navn, tlfnr, epostadresse og om aktiv eller ikke, samt hvilken tilgang den ansatte har i løsningen etc.
 - iii. Ansatte sin bruk av løsningen logges
- c. Behandling av personopplysninger
 1. Tilknyttet personopplysninger for personer/deltakere som registreres inn i løsningen behandles opplysninger i form av:
 - a. inngående og utgående korrespondanse (dokumenter) - herunder vedtak
 - b. journalnotat som loggfører informasjon som ikke ligger i korrespondanse
 - c. kartlegging av kompetanse som grunnlag for CV
 - d. fravær og dermed oppmøte til undervisning
 - e. nivå av kompetanse
 - f. for deltakere som følger grunnskoleundervisning som del av introduksjonsprogrammet, registreres karakterer
 - g. ansatte blir lagret som saksbehandlere på de enkelte hendelsene som registreres i løsningen

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 Behandlingsansvarlig behandle følgende sensitive personopplysninger:	Yes	No
rase, etnisitet, politisk eller filosofisk tilhørighet eller religion	(x)	X
at en person har vært eller er siktet/dømt for kriminalitet	(x)	X
helseopplysninger	(x)	X
seksuell orientering	(x)	X
Fagforeningsmedlemskap	(x)	X
genetisk eller biometrisk data	(x)	X

Kommentarer til avmerking i kolonne Yes:

Sensitive personopplysninger blir ikke registrert i form av egne metadata (datafelt), men det kan forekomme sensitive personopplysninger i form av fritekst i journalnotat og/eller dokument i postjournal. Indikasjon på sensitive personopplysninger kan også forekomme i form av kodeverk som Behandlingsansvarlig selv legger inn og benytter i løsningen.

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	Bistår databehandler med
Link Mobility AS 992 434 643	Norge	Gjelder ikke innen EU	Sende SMS meldinger
Visma Labs	EU/EØS	Gjelder ikke innen EU	Support og konsulenttjenester
Visma IT & Communications	EU/EØS	Gjelder ikke innen EU	Intern IT
Salesforce.com	EU (France, Germany)	EU Standard Contractual Clauses	Support - tool
NB! Underleverandørene har på samme måte som Visma ingen direkte datatilgang til persondata siden løsningen er installert lokalt / on-premise hos kunden.			

