18. mai 2018

Databehandleravtale

GDPR

mellom

Kunde av NettLønn

Organisasjonsnummer: xxx xxx xxx

Adresse

Postnummer Sted

(Behandlingsansvarlig, forkortet «BA»)

og

NettLønn (Adato AS)

Organisasjonsnummer: 995 221 608

Kjelsåsveien 114, Postboks 5

0411 Oslo

(Databehandler, forkortet «DB»)

(Behandlingsansvarlig og Databehandler blir kollektivt referert til som “Partene” og individuelt som “Part”)

1 Innholdsfortegnelse

2 Vedlegg til Databehandleravtalen

3 Bakgrunn og formål

3.1 Partene har inngått avtale som innebærer at Databehandler skal utføre spesifiserte tjenester for Behandlingsansvarlig. De spesifiserte tjenestene (leveransebeskrivelse) fremkommer av Vedlegg 1 til denne avtalen.

3.2 Denne avtalen med tilhørende vedlegg («Databehandleravtalen») innebærer at Databehandler skal behandle personopplysninger på vegne av Behandlingsansvarlig.

3.3 Databehandleravtalens formål er å regulere Databehandlers behandlingen av Behandlingsansvarliges personopplysninger, og sikre at Databehandler oppfyller kravene i gjeldende personvernlovgivning, herunder særlig:

- Lov om behandling av personopplysninger (personopplysningsloven).
- Generell personvernforordning («General Data Protection Regulation») (Europaparlaments- og rådsforordning (EU) 2016/679 av 27. April 2016).

4 Omfang

4.1 Databehandler er autorisert av Behandlingsansvarlig til å behandle personopplysninger på vegne av Behandlingsansvarlig i henhold til bestemmelsene i Databehandleravtalen.

4.2 Databehandler skal kun behandle personopplysninger i henhold til instruks gitt i denne Databehandleravtalen.

4.3 Alle personopplysninger som Databehandler behandler på vegne av Databehandler i henhold til denne avtalen, vil samlet omtales som «personopplysningene».

4.4 Med mindre annet er spesifisert i Databehandleravtalen, kan Databehandler benytte alle relevante tekniske hjelpemidler.

5 Varighet

5.1 Databehandleravtalen er gyldig inntil enten; a) leveranseomfanget i avtalen er fullført, eller b) avtalen sies opp.

6 Databehandlers plikter

6.1 Tekniske- og organisatoriske informasjonssikkerhetstiltak

6.1.1 Databehandler er ansvarlig for å implementere nødvendige; a) tekniske- og b) organisatoriske informasjonssikkerhetstiltak for sikker behandling av personopplysningene, og på en slik måte at en oppfyller kravene i gjeldende personvernlovgivning.

6.1.2 I tillegg skal Databehandler implementere de; a) tekniske- og b) organisatoriske informasjonssikkerhetstiltakene som er spesifisert i Vedlegg 2.

6.1.3 Partene er enige om at alle tekniske- og organisatoriske informasjonssikkerhetstiltak spesifisert i Vedlegg 2 er tilstrekkelig på plass ved dato for Databehandleravtalens oppstart, om ikke annet er spesifisert i Databehandleravtalens Vedlegg 2.

6.2 Forhold rundt Databehandlers ansatte

6.2.1 Databehandler skal sikre at ansatte som er involvert i behandling av personopplysningene har inngått en konfidensialitetskontrakt eller på annen måte godtatt å overholde full konfidensialitet i arbeidet med personopplysningene.

6.3 Dokumentasjon om oppfyllelse av plikter

6.3.1 På skriftlig forespørsel skal Databehandler dokumentere, innen rimelig tid, at behandlingen av personopplysningene:

a) Møter forpliktelsene i Databehandleravtalen.
b) Møter de krav som gjeldende personvernlovgivning stiller i forbindelse med behandling av personopplysningene.

6.3.2 Det spesifiserte innhold i forpliktelsene under dette pkt. 6.3 er beskrevet i Vedlegg 3 til Databehandleravtalen.

6.4 Sikkerhetshendelser

6.4.1 Databehandler skal orientere Behandlingsansvarlig om alle sikkerhetshendelser (avvik) ved behandlingen av personopplysninger som potensielt kan føre til utilsiktet eller ulovlig sletting, forandring, deling eller uautorisert tilgang til personopplysninger.

6.4.2 Sikkerhetshendelser skal rapporteres til Behandlingsansvarlig uten forsinkelse. Det skal gjøres nødvendige tiltak i å påse og innhente bekreftelse om at Behandlingsansvarlig har mottatt og registrert denne informasjonen.

6.4.3 Ved sikkerhetshendelser rapportert til Behandlingsansvarlig, skal Behandlingsansvarlig uten forsinkelse informere den/de berørte registrerte.

6.5 Assistanse

6.5.1 Databehandler skal når det er nødvendig, og innenfor rimelige grenser, assistere i Behandlingsansvarlig sin utøvelse av sine plikter i forbindelse med behandlingen av personopplysninger omfattet av Databehandleravtalen, inkludert i forbindelse med:

a) Respondering ovenfor den registrerte vedrørende personvernrettigheter.
b) Sikkerhetshendelser.
c) Risikovurderinger.
d) I forbindelse med forhåndsdrøftelser med tilsynsmyndighet.

6.5.2 I tillegg skal Databehandler assistere i forbindelse med oppgaver spesifisert i Vedlegg 4.

6.5.3 Databehandler kan kreve betaling for medgått tid og utgifter i forbindelse med assistanse som beskrevet i dette pkt. 6.5 med mindre annet er spesifisert i Vedlegg 4.

7 Behandlingsansvarliges plikter

7.1 Behandlingsansvarliges plikter fremgår av Vedlegg 5.

8 Databehandlers underleverandører

8.1 Databehandler kan kun benytte underleverandører («Underdatabehandlere») i forbindelse med behandling av personopplysninger når dette er spesifisert i Vedlegg 6 i denne Databehandleravtalen.

8.2 Databehandler og Underdatabehandlere skal inngå skriftlig avtale som stiller samme krav til personvern for Underdatabehandlere som for Databehandler.

8.3 Underdatabehandlere skal utelukkende utføre tjenester slik de er formulert i instruks fra Behandlingsansvarlig.

8.4 Databehandler er direkte ansvarlig for Underdatabehandleres behandling av personopplysninger på samme måte som om Databehandler hadde utført behandlingen.

9 Overføring til 3. land og internasjonale organisasjoner

9.1 Databehandler kan kun overføre personopplysninger til tredjeland eller internasjonale organisasjoner i den grad det er spesifisert i;

a) Vedlegg 7 til denne Databehandleravtalen, eller i
b) Skriftlig instruks fra Behandlingsansvarlig.

9.2 Personopplysninger kan kun overføres hvis den til enhver tid gjeldende lovgivning tillater det.

10 Databehandling utenfor instruksene gitt av Behandlingsansvarlig

10.1 Databehandler kan behandle personopplysninger utenfor rammene av Behandlingsansvarliges instrukser i situasjoner der lovgivning som Databehandler er underlagt krever det.

10.2 Hvis personopplysninger behandles utenfor rammene av instruksene, skal Databehandler varsle Behandlingsansvarlig om årsaken samt innhente skriftlig godkjennelse før iverksettelse. I et slikt varsel skal Databehandler gi henvisning til det juridiske grunnlaget for behandlingen.

10.3 Varsling skal ikke finne sted dersom slikt varsel strider mot lovgivningen.

11 Force majeure

11.1 Hvis bestemmelser om force majeure er del av leveransebeskrivelsene i Vedlegg 1, så gjelder tilsvarende bestemmelser for Databehandleravtalen. Hvis ikke bestemmelser om force majeure er del av leveransebeskrivelsene i Vedlegg 1, gjelder bestemmelsene om force majeure i dette pkt. 11 i Databehandleravtalen.

11.2 Databehandler kan ikke holdes ansvarlig for situasjoner som normalt refereres til som force majeure, inklusive men ikke begrenset til, opprør, terrorisme, streiker, brann, naturkatastrofer, valutarestriksjoner, import- og eksportrestriksjoner, trafikkaos, feil ved energileveranser, feil i offentlige datasystemer og kommunikasjonssystemer, langtids sykefravær blant nøkkelpersoner, virus og påberopt force majeure fra underleverandører.

11.3 Force majeure kan kun påberopes for antall arbeidsdager som force majeure-situasjonen er til stede.

12 Konfidensialitet

12.1 Hvis bestemmelser om konfidensialitet er del av leveransebeskrivelsene i Vedlegg 1, så gjelder tilsvarende bestemmelser for Databehandleravtalen. Hvis ikke bestemmelser om konfidensialitet er del av leveransebeskrivelsene i Vedlegg 1, gjelder bestemmelsene i dette pkt. 12 for Databehandleravtalen.

12.2 Informasjon om innholdet i Databehandleravtalen, underliggende leveransebeskrivelse, samt informasjon om den andre Partens virksomhet som er angitt å være konfidensiell, eller som av sin natur eller på annen måte er å betrakte som konfidensiell, skal behandles konfidensielt. Dette gjelder for øvrig ikke informasjon som er offentlig kjent eller kommer til å bli offentlig kjent og dette ikke har noe med sikkerhetsbrudd å gjøre.

12.3 Personopplysninger skal alltid behandles konfidensielt.

13 Terminering og opphør

13.1 Ved brudd på denne databehandleravtale, kan Behandlingsansvarlig pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning, samt terminere avtalen.

13.2 Ved terminering/opphør av Databehandleravtalen skal Databehandler og eventuelle Underdatabehandlere returnere alle personopplysninger som har vært del av Databehandleravtalen, til Behandlingsansvarlig.

13.3 Behandlingsansvarlig kan også kreve alle personopplysninger overført til tredje part.

13.4 Databehandler er pliktig til å slette alle personopplysningene jf. pkt. 13.2 fra sine systemer, og skal på forespørsel fremlegge dokumentasjon på at dette er gjort.

13.5 Eventuelle øvrig forhold om behandling av personopplysninger i forbindelse med terminering og opphør jf. dette pkt. 13 kan være spesifisert i Vedlegg 1.

13.6 Sletting, stopping, overføring og annen behandling av personopplysninger jf. dette pkt. 13 kan bare skje når det er i tråd med gjeldende lovgivning.

14 Presedens

14.1 Hvis det skulle oppstå uoverensstemmelser mellom Databehandleravtalen og leveransebeskrivelsen til denne avtalen (Vedlegg 1), er det Databehandleravtalen som gjelder, med mindre annet er spesifisert i Databehandleravtalen.

15 Lovvalg og verneting

15.1 Denne Databehandleravtalen er underlagt norsk lov

15.1.1 Enhver tvist vedrørende Databehandleravtalen, eller som utspringer på bakgrunn av denne, skal i første instans søkes løst av Partene ved forhandling.

15.1.2 Såfremt forhandling ikke fører frem, skal en eventuell tvist innbringes for det verneting som er avtalt i øvrige avtaler knyttet til denne Databehandleravtalen (eksempelvis oppdragsavtale). Dersom dette ikke fremgår av tilknyttede avtaler, skal en eventuell tvist innbringes for det verneting som Behandlingsansvarlig har sitt hovedkontor om ikke annet avtales i Vedlegg 8 eller reguleres av lov.

16 Signaturer

Dato: 24.05.2018	**Sted: Oslo**
For Behandlingsansvarlig:	For Databehandler:
	KMS
Signatur	Signatur
	Kaj M. Solberg
Navn (i blokkbokstaver)	Navn (i blokkbokstaver)
	Daglig leder
Tittel (i blokkbokstaver)	Tittel (i blokkbokstaver)

Vedlegg 1

Leveransebeskrivelse

1 Leveransebeskrivelse

1.1 Leveransebeskrivelsen: NettLønn tilbyr bedrifter lønns- og personalsystem i skyen. Kunde av NettLønn har samtykket i brukeravtalen når kunden tok i bruk NettLønn.

2 Personopplysninger

2.1 Definisjoner:

2.1.1 **Personopplysninger:** opplysninger eller vurderinger som kan knyttes til den registrerte som enkeltperson, slik som for eksempel, men ikke begrenset til, navn, adresse, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilder, og fødselsnummer (både fødselsdato og personnummer).

2.1.2 **Sensitive personopplysninger:** slik som for eksempel, men ikke begrenset til: rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold og preferanser, medlemskap i fagforeninger, genetiske data, biometriske data (slik som fingeravtrykk, irismønster, høydemål, hodeform, osv.), samt adferdsmønstre, alvorlige sosiale problemer og andre rent private saker.

2.1.3 **Den registrerte:** Personen som opplysningene kan knyttes til.

2.1.4 **Behandling:** Med behandling av personopplysninger menes enhver bruk av personopplysninger, slik som for eksempel, men ikke begrenset til: registrering, sammenstilling, lagring, endring, sletting, overføring eller utlevering.

2.2 Typer personopplysninger relevante for leveransen, jf. punkt 1.1.

2.2.1 I forbindelse med utførelsen av leveransen beskrevet i dette Vedlegg 1, pkt. 1, kan Databehandler bl.a. komme i kontakt med og behandle følgende personopplysninger:

Personopplysning	Formål med opplysningen
For- og etternavn	Identifikasjon for korrekt utbetaling av lønn og godtgjørelser herunder reiseregninger og utlegg. Identifikasjon for hendelser relatert til arbeidsforholdet og identifikasjon ved annen pliktig offentlig innrapportering. Kommunikasjon (utsendelse av brev. Lette behandling av personopplysninger i ansattregisteret). Reise- og timeregistreringsmodulen vil benytte fornavn og etternavn.
Adresse privat	Kommunikasjon, leveranse
Adresse arbeidssted	Offentlig og intern rapportering.
Statsborgerskap	A-melding og sikre korrekte ytelser og trekk.

Personopplysning	Formål med opplysningen
Bostedsland	A-melding og sikre korrekte ytelser og trekk.
Telefonnummer (fast)	Kommunikasjon.
Telefonnummer (mobil)	Kommunikasjon.
E-postadresse	Kommunikasjon.
Fødselsdato / nummer	Identifikasjon for utbetaling av lønn og godtgjørelser herunder reiseregninger og utlegg, arbeidsforhold, annen pliktig offentlig innrapportering.
Kjønn	Statistikkformål for styrets årsberetning, intern rapportering mv.
Ansattnummer / ArbeidsforholdsID	A-melding. Intern identifikasjon og kategorisering for tilordning i avdeligsregnskap mv.
Kontonummer i bank	Sikre korrekt utbetaling av lønn og andre ytelser.
Sivilstatus	Sikre korrekte ytelser og trekk som påvirkes av sivilstatus.
Ektefelle, herunder navn og fødselsnummer	Sikre korrekt skattemessig innrapportering av lønnsforhold, formuesforhold mv.
Pårørendeinformasjon	Kommunikasjon med pårørende om særskilte forhold ved akutt sykdom, dødsfall mv.
Stillingsbetegnelse / yrkeskode	A-melding og sikre korrekt utbetaling lønn.
Stillingsnivå, herunder stillingsprosent og timer pr uke. Dato for siste endring.	A-melding og sikre korrekt utbetaling lønn.
Arbeidstidsordning	A-melding og sikre korrekt utbetaling lønn.
Yrkesopplysninger av betydning for lønns og arbeidsvilkår	A-melding og sikre korrekt utbetaling lønn.
Utdannelse og praksis, herunder lønnsansiennitet.	A-melding og sikre korrekte ytelser og trekk.
Medlemskap i fagforeninger og andre yrkesrelaterte foreninger.	Sikre korrekte ytelser og trekk.
Dekket av tariffavtale, herunder lønnstrinn	Sikre korrekte ytelser og trekk.
Lønns- og provisjonsopplysninger, herunder avlønningstype og siste dato for avlønning.	A-melding og sikre korrekt utbetaling lønn.
Pensjonsopplysninger	Sikre korrekt pensjonsinnbetaling og pensjonsytelse.
Skattetrekksopplysninger	Sikre korrekt skattetrekk.
Forsikringsforhold,	Sikre korrekt forsikringsdekning etter avtale mellom

Personopplysning	Formål med opplysningen
herunder dekningsomfang og nødvendige helseopplysninger (egenerklæringer mv)	arbeidsgiver og forsikringsselskap.
Fravær og permisjoner, herunder type og varighet.	Sikre korrekte ytelser og trekk. Offentlig innrapportering av sykepenger, permisjonsgodtgjørelse mv.
Ansettelses- og sluttdato, herunder start- og sluttdatoer ved fusjon og fisjon.	A-meldingen, lønnsberegninger og forsikringsordninger. Følge opp jubileum mv.
Sluttårsak, herunder oppsigelse og dødsfall.	Sikre korrekte ytelser og trekk. Statistiske formål.
Firmabil og andre naturalytelser	Sikre korrekt regnskapsrapportering og innberetning av fordel. Forsikringsdekningsformål.
Rolle i selskap	Sikre korrekte ytelser og trekk. Interne rapporteringsformål. A-melding. Sikre korrekte opplysninger i årsregnskapet.
Gjeld / fordringer overfor arbeidsgiver, herunder vilkår for mellomregningen.	Sikre korrekt inn- og utbetaling samt avregning av renter og gebyrer.
Informasjon i regnskapsdokumentasjon om ansattes atferdsmønster, herunder kjøp av varer og tjenester og bevegelsesmønster	Godtgjørelse av utlegg pådratt i næringsvirksomhet eller føring av private utgifter på privatkonto.

2.3 Kategorier av registrerte identifiserte eller identifiserbare personer som omfattes av Databehandleravtalen:

a) Klienter
b) Sluttkunder
c) Ansatte
d) Brukere av NettLønn

2.4 Sletting/tilbakelevering av personopplysninger

2.4.1 Når formålet med behandlingen av personopplysninger, jf. dette pkt. 2 er oppfylt, skal opplysningene tilbakeleveres og/eller slettes, jf. Databehandleravtalen pkt. 13. så fremt ikke annen lovgivning hindrer sletting.

Vedlegg 2

Krav til teknisk- og organisatorisk informasjonssikkerhetstiltak

1 Informasjonssikkerhetstiltak

1.1 Følgende spesifikke krav er gjort for å tilfredsstille sikkerheten til Databehandlers fysiske datasenter:

☒ Alarmsystem	☒ Bevegelsessensor
☒ Bygning er inngjerdet	☒ Videoovervåking
☒ Konfidensialitetsavtaler med leverandører	☒ Automatisert kontroll av tilganger
☒ Mottaks- og adgangskontroll (eks. ifm. varemottak, inspeksjoner ol.)	☒ Låsing av systemer med chipkort
☒ Låsing av systemer med brukernavn og passord	☒ Låsbare rom og områder

Beskrivelse av andre sikkerhetstiltak (hvis relevant):

1.2 Følgende særlige krav er møtt for virksomhetens tekniske sikkerhet.

1.2.1 Tilgangskontroll:

☒	Brukerkontoer er definert i it-systemer for å støtte virksomhetsfunksjonene til virksomheten.	☒	Listen over brukere i it-systemer blir periodisk undersøkt og oppdatert.
☒	Logiske tilgangsprivilegier er definert i it-systemer for begrense informasjonstilgang henhold til virksomhetens tilgangskontrollpolicy.	☒	Brukerrettigheter i it-systemer er begrenset til det vesentlige minimum slik at kun relevante brukere får utføre sine oppgaver.
☒	Begrenset brukerinnlogging til it-systemer etter flere mislykkede påloggingsforsøk. Dette ved å bruke auto-låsealternativer som tidsbegrensning før ny innlogging, sikkherhetskoder, eller til den er opplåst av virksomhetens systemadministrator.	☒	Beskyttelse av tilkobling til it-systemer fra trådløst nettverk ved bruk av autentisering fra brukerenheter, kryptering og innstilling av brukerbegrensninger.
N/A	Forbudt tilkobling til organisasjonssystemer fra trådløst nettverk.	N/A	Brukerbegrensninger og konfigurasjonskrav for tilkobling gjennom mobile enheter er implementert og dokumentert.

☒	Brukerne av systemet identifiseres og valideres unikt.	☒	Multifaktorautentisering for innlogging til kontoer med overdrevne privilegier på tvers av nettverket er implementert.
☒	Multifaktorautentisering for å koble eksternt til it-systemer er implementert.	☒	Organisasjonen håndhever passordspolitikken gjennom teknologi.
☒	Kryptert godkjenningsmekanisme er implementert.		

1.2.2 Forretningskontinuitet:

☒	Alternative sikkerhetskopierings- og databehandlingssted er etablert for å tillate full gjenoppretting på samme sikkerhetsnivå som hovedstedet.	☒	Fysisk og logisk adskillelse mellom hovedsted og sikkerhetskopieringssted er implementert for å unngå at begge steder blir angrepet samtidig.
☒	Sikkerhetsstedet er definert på en måte som støtter gjenopprettingsplanen.	☒	Forberedelse og sikkerhetskopiering av brukere, it-system og dokumentasjonsnivå.
☒	Verifisert sikkerhetskopi og pålitelighet.		
☒	Tidligere versjoner av systemkonfigurasjonen for å støtte tilbakeringing beholdes.		

1.2.3 Kryptering:

☒	Definisjon av bruksområder som krever kryptering og krypteringstype som kreves, er i samsvar med lover, retningslinjer, prosedyrer, forskrifter og forretningsforpliktelser.		
N/A	Implementerte krypteringsmekanismer på bærbare enheter (bærbare datamaskiner, mobiltelefoner, nettbrett, ol.).	☒	Krypteringsmekanismer basert på anerkjente krypteringsalgoritmer og nøkkelstørrelser som svarer til trusselpotensialet.

1.2.4 Bevissthet:

☐	Ansatte er forpliktet til organisasjonens krav til personvern- og informasjonssikkerhet.	☒	Taushetserklæring for alle ansatte i organisasjonen som går lengre enn deres ansettelse.

1.2.5 Enhetshåndtering:

☒	Enheter (maskin- og programvare) lagres sikkert.	☒	Definerte sletting- og/eller destruksjonsprosesser for utgåtte og/eller avhendbare enheter er implementert.

1.2.6 Nettverkssikkerhet:

☒	The Address Translation Service (DNS) leveres av pålitelig server og leverandør.	☒	Organisasjonens utgående / innkommende nettverkstrafikk overvåkes.
☒	Begrenset antall kommunikasjonskanaler utenfor systemet.	☒	Som standard er alle nettverkstrafikk- og «tillat manuelt»-unntaktsregler blokkert.
☒	Separate nettverksadresser (annet undernettverk) for å koble til ulike sikkerhetssoner.	☒	Implementerte mekanismer for å opprettholde integriteten og konfidensialiteten til nettverkstrafikken på offentlig medium.

1.2.7 Forhindring av ondsinnede koder og programvare

☒	Aktiverte verktøy og systemer ved eksterne kommunikasjonspunkter. Disse verktøyene skanner og oppdager ondsinnet kode/programvare i kommunikasjon med eksterne parter, e-post og surfing.	☒	Definerte prosedyrer for håndtering av stasjoner, servere eller nettverk infisert av ondsinnet kode/programvare.
☒	Implementerte verktøy for å oppdage og forhindre ondsinnet kode/programvare på endepunkter og servere i organisasjonen. Disse verktøyene kjører i en aktiv beskyttelsesmodus og periodiske skanninger utføres.	☒	Administrerer skadeforebyggingsverktøy i organisasjonen gjennom sentralt system. Skadeforebyggingsverktøy rapporterer mistenkelige hendelser og systemhendelseidentifikasjon (oppdatering av problemer, beskyttelsesinaktivitet, fjerning av komponenter, osv.).
☒	Automatisk oppdatering av alle systemer for å identifisere og forebygge ondsinnet kode i organisasjonen.	☒	Implementerte sikkerhetstiltak for å forhindre informasjonslekkasje ved overføring av informasjon til interne eller eksterne parter.
☒	Policy for å kontrollere, håndheve og overvåke installasjon av programvare på organisasjonens PC'er og enheter.		

1.2.8 Lagring og overvåkning

☒	Logginng omfatter som et minimum data om hendelsen, tidsstempel, kilde og mål for aktiviteten, brukeridentifikator, prosessidentifikator, suksess/feil, filnavn.	☒	Tilstrekkelig lagringsplass for lagring.
N/A	Opprett en varslingsmekanisme i tilfelle loggfeil.	☒	Beskyttet kontroll-logger fra uautorisert tilgang, endring eller sletting.

1.2.9 Sikring av mobile enheter (Ingen trådløse system i datasenteret):

N/A	Implementerte beskyttelsesmekanismer for å kontrollere tilgang til enhetene, for eksempel passord eller biometriske tiltak.	N/A	Implementert kryptering av sensitive data lagret på mobile enheter.
N/A	Implementert kryptering av sensitive data i innkommende og utgående kommunikasjon av mobile enheter.	N/A	Implementert sentralisert styringssystem, som styrer konfigurasjonen av mobile enheter og muliggjør ekstern sletting av data fra enheten.

1.2.10 Separasjon av miljøer

N/A	Begrenset bruk av sensitive produksjonsdata (kundedata eller data definert av organisasjonen som følsom) i ikke-produksjonsmiljøer hvis dataene ikke er beskyttet på samme nivå som i produksjonsmiljø.	N/A	Separate brukerrettigheter for ulike miljøer, og definere privilegier for hvert miljø.

Beskrivelse av andre sikkerhetstiltak (hvis relevant):

Ingen

Vedlegg 3

Dokumentasjon av oppfyllelse av plikter

1 Innledning

Som del av Databehandlers forpliktelser i henhold til Databehandleravtalen, må følgende punkter oppfylles:

1.1 Dokumentasjon om oppfyllelse av plikter

1.1.1 På skriftlig forespørsel skal Databehandler dokumentere at behandlingen av personopplysninger:

a) Møter forpliktelsene i Databehandleravtalen.
b) Møter de krav som gjeldende personvernlovgivning stiller i forbindelse med behandling av personopplysninger på vegne av Behandlingsansvarlig.

2 Innhenting av dokumentasjon til behandlingsansvarlig

2.1 På skriftlig forespørsel skal Databehandler oversende dokumentasjon til Behandlingsansvarlig som beskriver hvordan Databehandler leverer i henhold til leveransebeskrivelsen, inkludert, men ikke begrenset til, spesifiserte tekniske og organisatoriske sikkerhetstiltak og rutiner.

3 Kontroll

3.1 På skriftlig forespørsel skal Databehandler bidra til, og gi tilgang til, kontroll av hvordan Databehandler leverer i henhold til leveransebeskrivelsen.

3.2 Kontrollen skal utføres av en uavhengig tredjepart valgt av Behandlingsansvarlig og godkjent av Databehandler. Databehandler kan ikke nekte Behandlingsansvarliges valg av tredjepart uten saklig grunn. Den uavhengige tredjepart skal undertegne en generell konfidensialitetsavtale med Databehandler. Forespørsel om kontroll, jf. pkt. 3.1. skal gis med minimum **30** dagers varsel.

3.3 Databehandler har krav på å bli betalt for medgått tid og få dekket eventuelle utlegg og kostnader i forbindelse med oppfyllelse etter dette punkt 3, med mindre annet er angitt i Vedlegg 4.

4 Øvrige vilkår

4.1 Punktene over er ikke uttømmende og Databehandler er således forpliktet til å iverksette alle de tiltak som er nødvendig for å imøtekomme de krav som framgår av punkt 6 i Databehandleravtalen.

4.2 Databehandler er ikke forpliktet til å følge instruks eller anmodning fra Behandlingsansvarlig i henhold til dette Vedlegg 3 dersom instruksen eller anmodningen er i strid med personvernlovgivningen. Databehandler skal uten opphold varsle Behandlingsansvarlig dersom Databehandler mener at dette er tilfelle.

Vedlegg 4

Spesifikk assistanse

1 Assistanse

1.1 Partene er enige om at de følgende spesifiserte oppgavene skal utføres av Databehandler:

Oppgave og tjenester	Godtgjørelse
Bistå Behandlingsansvarlig med databehandlingsopplysninger for tredjeparter.	Databehandler har krav på medgått tid og påløpte utgifter
Respondering ovenfor den registrerte vedrørende personvernrettigheter.	Databehandler har krav på medgått tid og påløpte utgifter
Sikkerhetshendelser.	Databehandler har krav på medgått tid og påløpte utgifter
Risikovurderinger.	Databehandler har krav på medgått tid og påløpte utgifter
I forbindelse med forhåndsdrøftelser med tilsynsmyndighet.	Databehandler har krav på medgått tid og påløpte utgifter
Supportere Behandlingsansvarlig ved supporteringsbehov. Dette gjelder selv om ansatte og samarbeidspartnere av databehandler kan få tilgang til, samt slette, endre og legge til personopplysninger hos BA der dette er nødvendig for supporteringen.	Databehandler har krav på medgått tid og påløpte utgifter

Vedlegg 5

Behandlingsansvarliges plikter

1 Plikter

1.1 Behandlingsansvarlig er underlagt følgende plikter:

a) Databehandler er ikke underlagt andre plikter enn de som følger av personvernlovgivningen.

1.2 Øvrige vilkår:

Ingen

Vedlegg 6

Underdatabehandlere

1 Generelt

1.1 Databehandleravtalen gir med dette Databehandler en generell skriftlig tillatelse til å bruke Underdatabehandlere.

1.2 Ved opphør av eksisterende, eller bruk av ny Underdatabehandler, skal Databehandler skriftlig varsle Behandlingsansvarlig senest **30** dager før endringen iverksettes. Dette slik at Behandlingsansvarlig skal kunne vurdere og eventuelt motsette seg endringen.

1.3 Behandlingsansvarlig godtar ved inngåelsen av denne avtalen at Databehandler bruker følgende Underdatabehandlere:

a) WEBSPESIALISTEN AS, org.894 785 942, Fredrikke Qvams gate 19, 0172 Oslo
b) ECIT Labs Norge AS, org. 924 597 984, Hvamsvingen 7, 2013 Skjetten

1.4 Under punkt 1.3 del b) gis kun tillatelse i de tilfeller der Behandlingsansvarlig benytter seg av ECIT Labs Norge sine produkter og tjenester (Timer, Reise med fler)

2 Særlige vilkår

2.1 Behandlingsansvarlig kan ikke instruere Databehandler om bruk av bestemte Underdatabehandlere.

2.2 Databehandler kan komme med innsigelser til en Underdatabehandler dersom det er saklig begrunnet.

2.3 Varsling fra Databehandler til Behandlingsansvarlig om endring av Underdatabehandler jf. pkt. 1.2, skal skje skriftlig per e-post til: <**Behandlingsansvarliges e-post-adresse**>.

Vedlegg 7

Overføring til 3.land og internasjonale organisasjoner

1 Generelt

1.1 Behandlingsansvarlig godtar med dette at Databehandler overfører personopplysninger til organisasjoner i de følgende sikrede tredjeland:

a) Ikke relevant

1.2 Behandlingsansvarlig godtar med dette at Databehandler overfører personopplysninger til organisasjoner i de følgende usikrede tredjeland:

b) Ikke relevant

1.3 Personopplysninger skal utenom dette ikke behandles av Databehandler eller en Underdatabehandler i et land utenfor EU/EØS-området (et "Tredjeland") eller en internasjonal organisasjon med mindre det uttrykkelig er gitt tillatelse fra Behandlingsansvarlig. Databehandler skal varsle Behandlingsansvarlig om overføringen før den finner sted.

2 Særlige vilkår

2.1 Ingen

Vedlegg 8

Øvrige forhold

1 Øvrige vilkår/tilføyelser

1.1 LOVVALG OG TVISTELØSNING

1.2 (i) Avtalen og enhver tvist forbundet med den, er underlagt norsk rett.

1.3 (ii) Dersom det oppstår en tvist mellom Partene om gyldigheten, tolkningen eller gjennomføringen av Avtalen, og tvisten ikke kan løses ved forhandlinger, skal tvisten behandles gjennom voldgift i henhold til reglene i lov om voldgift av 14. mai 2004 nr. 25. Forhandlingene skal finne sted i Oslo. Voldgiftsforhandlingene, alle dokumenter fremlagt i denne sammenheng samt voldgiftsavgjørelsen skal være konfidensielle, og Partene skal inngå en særskilt konfidensialitetsavtale i forbindelse med at voldgiftsforhandlinger initieres.