Databehandleravtale

Innhold

DATABEHANDLERAVTALE I SAMSVAR MED GDPR ARTIKKEL 28

PARTER

Databehandleravtale mellom

<Kunde.Navn>, <Kunde.Postadresse>, <Kunde.Postnr>, <Kunde.Poststed> – **den behandlingsansvarlige** – heretter kalt den behandlingsansvarlige – og

<Firma.Navn> – **databehandleren** – heretter kalt databehandleren –.

Personvernkontaktinformasjon hos behandlingsansvarlig: *<Oppdragsavtale.Kontakt.Epost>*.

Personvernkontaktinformasjon hos databehandler: *hwingsternes@ecit.no*.

Den behandlingsansvarlige skal ha rettighetene og forpliktelsene som «behandlingsansvarlig» etter denne databehandleravtalen også når han fungerer som «databehandlen» etter personvernlovgivningen, og databehandleren skal ha rettighetene og forpliktelsene som «databehandler» også når han fungerer som «underleverandør» etter personvernlovgivningen.

1. AVTALENS HENSIKT OG VARIGHET

1.1 Hensikt

Hensikten med bestillingen eller avtalen følger av den primære serviceavtalen mellom behandlingsansvarlig og databehandler datert <Oppdragsavtale.Dato>, som er nevnt her (heretter kalt serviceavtale).

1.2 Varighet

Denne databehandleravtalens varighet tilsvarer serviceavtalens varighet.

2. SPESIFIKASJON AV AVTALENS ENKELTHETER

2.1 Den tiltenkte databehandlingens art og formål

Art og formål med databehandlerens behandling av personopplysninger for den behandlingsansvarlige er presist fastsatt i serviceavtalen. Det presiseres at formålet blant annet omfatter databehandlerens opplæring av personell og testing av systemer som brukes i forbindelse med leveringen av tjenester etter serviceavtalen.

Formålet med denne databehandleravtalen er å fastsette vilkårene for databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige i samsvar med kravene i de lover og forskrifter som gjelder for behandling av personopplysninger (heretter kalt **personvernlovgivning**), herunder EUs generelle personvernforordning (**GDPR**).

For alle spørsmål som ikke er regulert i databehandleravtalen, gjelder de relevante vilkårene i serviceavtalen. Ved konflikt mellom vilkårene i serviceavtalen og vilkårene i denne databehandleravtalen skal de relevante vilkårene i denne databehandleravtalen gjelde når annet

ikke uttrykkelig er angitt. Termer som brukes i denne databehandleravtalen, skal tolkes i samsvar med tilsvarende termer i personvernlovgivningen når annet ikke er angitt i databehandler- eller serviceavtalen.

3. KATEGORIER AV PERSONOPPLYSNINGER

Formålet med Regnskapsforetakets Behandling av Personopplysninger er å gjennomføre regnskapsoppdraget i samsvar med Oppdragsavtalen, herunder Standard leveransevilkår.

I **vedlegg 1** i dette dokumentet beskrives de konkrete formålene med Behandlingene, samt de kategorier Personopplysninger og Registrerte som omfattes.

Databehandleravtalen gjelder ikke for Behandling av Personopplysninger som utføres for Regnskapsforetakets egne formål. Dette omfatter også Behandlinger som er nødvendige for å oppfylle plikter som Regnskapsforetaket er pålagt gjennom lov. For slike Behandlinger er Regnskapsforetaket selv Behandlingsansvarlig.

4. DEN BEHANDLINGSANSVARLIGES ANSVAR

Den behandlingsansvarlige skal

(a) behandle personopplysningene i samsvar med personvernlovgivningen og god databehandlingspraksis

(b) gi dokumenterte instruksjoner til databehandleren om behandlingen av personopplysninger til enhver tid i skriftlig form

(c) umiddelbart bekrefte muntlig gitte instruksjoner (i det minste i tekstform)

(d) til enhver tid ha kontroll og myndighet over personopplysningene underlagt denne databehandleravtalen

(e) til enhver tid ha eiendomsrett, immaterialrettigheter og andre rettigheter til personopplysninger underlagt denne databehandleravtalen, når annet ikke er avtalt eller påkrevd etter bindende lovgivning.

5. DATABEHANDLERENS ANSVAR

5.1 Generelle forpliktelser

Databehandleren skal sikre at følgende krav oppfylles:

(a) Utnevnelse av ansvarlig person for personvern hvis det er påkrevd etter personvernlovgivningen.

(b) Behandling av personopplysninger bare på dokumenterte instruksjoner fra den behandlingsansvarlige, når annet ikke er påkrevd etter EUs regelverk eller nasjonal lovgivning i et EØS-land som databehandleren er underlagt. I så fall skal databehandleren underrette den behandlingsansvarlige om dette lovkravet før behandling, med mindre slik informasjon er forbudt ved lov av hensyn til viktige samfunnsinteresser. Databehandleren skal umiddelbart informere den behandlingsansvarlige hvis en instruksjon etter den behandlingsansvarliges mening krenker personvernlovgivningen.

(c) Konfidensialitet i samsvar med GDPR artikkel 28 nr. 3 annet punktum bokstav b), artikkel 29 og artikkel 32 nr. 4.

Databehandleren overlater behandling av personopplysninger beskrevet i denne databehandleravtalen bare til ansatte som er pålagt taushetsplikt og er kjent med de personvernbestemmelsene som er relevante for deres arbeid. Databehandleren, og enhver som opptrer under databehandlerens myndighet med tilgang til personopplysninger, skal ikke behandle disse opplysningene med mindre det skjer på instruks fra den behandlingsansvarlige, noe som omfatter fullmaktene gitt i denne databehandlingsavtalen, med mindre det er påkrevd ved lov.

(d) Gjennomføring og overholdelse av alle nødvendige tekniske og organisatoriske tiltak i samsvar med GDPR artikkel 28 nr. 3 bokstav c) og artikkel 32 [mer informasjon finnes i **vedlegg 2** til denne databehandleravtalen].

(e) Den behandlingsansvarlige og databehandleren skal på forespørsel samarbeide med tilsynsmyndigheten når tilsynsmyndigheten utfører sine oppgaver.

(f) Databehandleren skal regelmessig følge opp de interne prosessene og de tekniske og organisatoriske tiltakene for å sikre at behandling innenfor databehandlerens ansvarsområde er i samsvar med kravene i gjeldende personvernlovgivning og vernet av den registrertes rettigheter.

5.2 Opplysnings- og rapporteringsplikt

Den behandlingsansvarlige skal underrettes av databehandleren uten unødig opphold om alle inspeksjoner og tiltak som tilsynsmyndigheten har gjennomført, i den grad de har forbindelse med denne databehandleravtalen. Dette gjelder også i den grad databehandleren er under granskning eller er part i en granskning utført av en vedkommende myndighet i forbindelse med overtredelser av sivil- eller strafferett eller forvaltningsregel eller -reglement vedrørende behandling av personopplysninger i forbindelse med behandlingen etter denne databehandleravtalen.

5.3 Hjelp og kommunikasjon

I den grad det er påkrevd etter personvernlovgivningen skal databehandleren hjelpe den behandlingsansvarlige med å overholde forpliktelsene vedrørende sikkerheten for personopplysninger, rapporteringskrav for brudd på personopplysningssikkerheten, vurderinger av personvernkonsekvenser, tidligere konsultasjoner og registrertes rettigheter nevnt i GDPR artikkel 32–36 og kapittel III. Dette omfatter følgende:

(a) Hjelpe den behandlingsansvarlige med å sikre gjennomføring av egnede tekniske og organisatoriske tiltak for å oppnå et tilstrekkelig sikkerhetsnivå i forhold til behandlingens risiko idet det tas hensyn til det tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.

(b) Hjelpe med varsling om brudd på personopplysningssikkerheten, herunder ved å rapportere et brudd på personopplysningssikkerheten til den behandlingsansvarlige uten unødig opphold etter å ha bli gjort oppmerksom på bruddet.

(c) Bistå den behandlingsansvarlige i forbindelse med den behandlingsansvarliges plikt til å gi informasjon ved brudd på personopplysningssikkerheten til den berørte registrerte, og gi den behandlingsansvarlige relevant informasjon i denne forbindelse.

(d) Støtte den behandlingsansvarlige i forbindelse med vurdering av personvernkonsekvenser.

(e) Støtte den behandlingsansvarlige i forbindelse med tidligere konsultasjon av tilsynsmyndigheten.

(f) Hvis en registrert eller tilsynsmyndigheten kommer med en anmodning vedrørende personopplysninger (f.eks. retting, sletting eller endring), skal databehandleren uten unødig opphold underrette den behandlingsansvarlige om alle slike anmodninger før eventuelle tiltak, eller etterpå så snart som mulig hvis umiddelbar respons er påkrevd etter loven. Databehandleren kan håndtere anmodninger bare på vegne av den behandlingsansvarlige på den behandlingsansvarliges instruks i skriftlig form eller hvis det er lovpålagt.

Databehandleren kan kreve godtgjørelse for all hjelp som ikke er tatt med i beskrivelsen av tjenestene i den primære serviceavtalen mellom behandlingsansvarlig og databehandler, og som ikke kan tilskrives unnlatelser fra databehandlerens side. Hvis databehandleren har til hensikt å kreve godtgjørelse, skal databehandleren underrette den behandlingsansvarlige før hjelpen gis.

6. OVERFØRING AV PERSONOPPLYSNINGER

Databehandleren skal ikke overføre personopplysninger til land utenfor EU eller EØS («tredjeland») med mindre den behandlingsansvarlige uttrykkelig har krevd eller godtatt at dette gjøres.

Når en dataoverføring skjer til tredjeland, skal databehandleren sikre at slik overføring er i samsvar med personvernlovgivningen, herunder GDPR kapittel V, denne databehandleravtalen og den behandlingsansvarliges instruksjoner. Hvis overføringen ikke overholder relevante vilkår, skal databehandleren umiddelbart stoppe overføringen av personopplysninger til tredjeland og returnere personopplysningene til opprinnelseslandet.

7. BRUK AV UNDERLEVERANDØRER

(a) Bruk av underleverandører etter denne avtalen skal forstås som tjenester som er direkte knyttet til levering av hovedtjenesten. Dette omfatter ikke tilhørende tjenester, for eksempel telekommunikasjonstjenester, post-/transporttjenester, vedlikeholds- og brukerstøttetjenester samt andre tiltak for å ivareta konfidensialiteten, tilgjengeligheten, integriteten og robustheten til databehandlingsutstyrets maskinvare og programvare.

(b) Ved bruk av underleverandører skal databehandleren utarbeide egnede og juridisk bindende kontrakter i samsvar med GDPR artikkel 28 nr. 4 og iverksette egnede inspeksjonstiltak for å sikre og beskytte den behandlingsansvarliges opplysninger.

(c) Den behandlingsansvarlige gir med dette databehandleren generell tillatelse til å bruke underleverandører. Databehandleren skal, før bruk eller bytte av underleverandør, underrette behandlingsansvarlig skriftlig minst tre uker i forveien.

Den behandlingsansvarlige skal kunne protestere på eventuelle endringer i eksisterende eller ny underleverandør som databehandleren meddeler, bare av vesentlig viktige årsaker i forbindelse med behandlingen av personopplysninger innen to uker etter databehandlerens skriftlige underrettelse. Hvis den behandlingsansvarlige ikke protesterer innen denne tidsrammen, skal den behandlingsansvarlige anses for å ha godtatt en slik endring. Hvis den behandlingsansvarlige protesterer på endringen, skal partene forhandle i god tro for å finne en løsning omgående.

(d) Liste over underleverandører er vedlagt som **vedlegg 3** til denne databehandleravtalen og oppdateres av databehandleren ved eventuelle endringer.

(e) Overføringen av personopplysninger fra databehandleren til underleverandøren og underleverandørens start av behandlingen av opplysninger skal utføres først etter at alle krav er oppfylt.

(f) Hvis underleverandøren tilbyr den avtalte tjenesten utenfor EU/EØS, skal databehandleren sikre at personvernlovgivningen overholdes ved egnede tiltak.

(g) Hvis en underleverandør ikke oppfyller sine personvernforpliktelser, skal databehandleren holdes fullt ut ansvarlig overfor den behandlingsansvarlige for oppfyllelsen av underleverandørens forpliktelser.

8. INSPEKSJONER OG REVISJONER

(a) Den behandlingsansvarlige har etter samråd med databehandleren rett til å gjennomføre inspeksjoner eller få dem utført av en revisor som skal utpekes i hvert enkelt tilfelle. Inspeksjonene må utføres i den ordinære kontortiden, og databehandleren kan kreve at den eller de personene som utfører revisjonen, er underlagt en avtale om taushetsplikt.

Den behandlingsansvarlige skal gi skriftlig varsel til databehandleren tre (3) uker før eventuell revisjon.

(b) Databehandleren skal sikre at den behandlingsansvarlige kan verifisere at databehandlerens forpliktelser er overholdt i samsvar med GDPR artikkel 28. Databehandleren forplikter seg til å gi den behandlingsansvarlige nødvendig informasjon på forespørsel og særlig dokumentere gjennomføringen av de tekniske og organisatoriske tiltakene.

(c) Bevis på slike tiltak, som ikke bare vedrører den bestemte bestillingen eller databehandleravtalen, kan fremlegges ved nåværende revisors sertifikater, rapporter eller utdrag fra rapporter fra uavhengige organer (f.eks. revisor, personvernombud, IT-sikkerhetsavdeling, personvernrevisor, kvalitetsrevisor).

(d) Databehandleren kan kreve godtgjørelse for revisjoner og inspeksjoner som ikke er tatt med i beskrivelsen av tjenestene i den primære serviceavtalen mellom behandlingsansvarlig og databehandler, og som ikke kan tilskrives unnlatelser fra databehandlerens side.

9. SLETTING OG RETUR AV PERSONOPPLYSNINGER

(a) Kopier eller gjenparter av opplysningene skal aldri opprettes uten instruksjoner fra den behandlingsansvarlige, herunder instruksjonene i denne databehandleravtalen, med unntak av sikkerhetskopier i den grad de er nødvendige for å sikre ryddig databehandling samt opplysninger som kreves for å oppfylle krav i henhold til forskrift til lagring av opplysninger.

(b) Etter at det avtalte arbeidet er avsluttet, eller tidligere på forespørsel fra den behandlingsansvarlige, senest ved serviceavtalens opphør, skal databehandleren returnere til den behandlingsansvarlige eller – med forbehold om forutgående samtykke – tilintetgjøre alle dokumenter, resultater av behandlingen og bruken og datasett knyttet til avtalen som databehandleren har fått i sin besittelse, på en måte som beskytter personvernet. Det samme gjelder for alt tilknyttet test- eller avfallsmateriale samt redundant og forkastet materiale. Loggen for tilintetgjøring eller sletting skal legges frem på forespørsel.

(c) Den behandlingsansvarlige har rett til å velge mellom og er ansvarlig for slettingen eller returen av personopplysninger. Databehandleren skal følge den behandlingsansvarliges instruksjoner om dette, med mindre EUs regelverk eller nasjonal lovgivning i et EØS-land krever at personopplysningene lagres.

(d) Dokumentasjon som brukes til å godtgjøre ryddig behandling av opplysninger i samsvar med bestillingen eller databehandleravtalen, skal lagres av databehandleren utover avtalens varighet i samsvar med respektive lagringstider. Databehandleren kan overlevere slik dokumentasjon til den behandlingsansvarlige når avtalens varighet er opphørt for å frita databehandleren for denne avtalefestede forpliktelsen.

10. UNDERSKRIFTER

Elektronisk signatur

Vedlegg
Vedlegg 1, Kategorier Personopplysninger og behandlingsformål
Vedlegg 2, Tekniske og organisatoriske tiltak
Vedlegg 3, Liste over underleverandører

VEDLEGG 1 KATEGORIER PERSONOPPLYSNINGER OG BEHANDLINGSFORMÅL

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.
Adresse privat	Kommunikasjon.
Adresse arbeidssted	Offentlig og intern rapportering.
Statsborgerskap	A-melding og sikre korrekte ytelser og trekk.
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.

Personopplysning	Formål med opplysningen
Skattetrekksopplysninger	Sikre korrekt skattetrekk.
Forsikringsforhold, herunder dekningsomfang og nødvendige helseopplysninger (egenerklæringer mv)	Sikre korrekt forsikringsdekning etter avtale mellom 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.
Eierandeler i selskap	Aksjonærregstermeldinger
Rolle i selskap	Sikre korrekte ytelser og trekk. Interne rapporteringsformål. A-melding. Sikre korrekte opplysninger i årsregnskapet.
Vilkår i aksjonæravtaler	Sikre korrekt behandling aksjonærer i mellom.
Eiendeler i samboerskap	Sikre korrekt innberetning av skattemessige formål.
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.

Kategorier av registrerte vil kunne inkludere:

- Ansatte, vikarer eller midlertidig ansatte hos Kunden
- Personlige kunder hos Kunden
- Eiere av Kundens virksomhet
- Styremedlemmer hos Kunden

VEDLEGG 2, TEKNISKE OG ORGANISATORISKE TILTAK

1. KONFIDENSIALITET (GDPR ARTIKKEL 32 NR. 1 BOKSTAV B))

1.1 Fysisk tilgangskontroll

Fastsatte tiltak for å unngå ulovlig fysisk tilgang til produksjonslokaler og kontorer er på plass:

- Adgangs-/magnetkort, nøkkeltilgangsregulering, elektroniske døråpnere (avhengig av sted).
- På noen steder også alarmsystem, fasilitetssikkerhetstjenester og/eller sikkerhetspersonell og overvåkingskamera i adgangsområder.
- Adgangsbestemmelser for ikke-autoriserte ansatte eller eksterne personer, f.eks. vedlikeholdsteknikere, renholdspersonell, besøkende.

Alle ansatte har undertegnet konfidensialitetserklæringer.

1.2 Elektronisk adgangskontroll

Fastsatte tiltak for å unngå uautorisert bruk av databehandlings- og datalagringssystemer ved egnede tiltak:

- Prosessen for brukernavnadministrasjon er dokumentert og etablert. Autentiseringsinformasjonen leveres trygt til brukeren. Hver autorisert person har et individuelt passord.
- Fastsatte tiltak for å unngå uautorisert bruk av IT-systemer: Brukernavn, passordbeskyttelse, låst skjerm med passordbeskyttelse.
- Brukerkontoer deaktiveres uten unødig forsinkelse etter at brukeren har forlatt selskapet (f.eks. ved oppsigelse av arbeidsavtale).
- Harmonisert endring av brukerkontoer etter at brukeren er flyttet til et annet arbeidsfelt.

1.3 Intern adgangskontroll (tillatelser for brukernes rett til innsyn i og endring av data)

Tiltak på plass:

- Terminalservertilgang krever fysisk datamaskin i nettverk med brukernavn og passord. Dette gir tilgang til stasjonære «systemen» som på sin side har et eget brukernavn og passord. Utenfor terminalserver er MFA aktivert.
- Tilgang utenfor kontor krever forhåndsautorisering via fjerntilgangsportal. Dette gir tilgang til stasjonære «systemen» som på sin side har et eget brukernavn og passord.
- Systemadministrator per app tilordner brukernavn og passord etter tilordninger fra brukerens leder.
- I tillegg til autoriserte brukere har bare et begrenset antall IT-personell tilgang til produksjonssystemer.

1.4 Arbeid på hjemmekontor

Databehandleren kan utvide arbeidsstedet til den ansattes private bolig. Derfor er de ansattes behandling av personopplysninger omfattet av databehandling også tillatt på hjemmekontor.

Tiltak for å sikre personopplysninger i forbindelse med hjemmekontor:

- Selskapets retningslinjer for arbeid på hjemmekontor.
- Grunnleggende beskyttelsesnivå for tiltakene på hjemmekontor vil være det samme som i selskapets lokaler.
- Nødvendige endringer i de tekniske og organisatoriske tiltakene for hjemmekontor vil bli bestemt ved gjensidig avtale mellom den behandlingsansvarlige og databehandleren.
- Ansatte er tilstrekkelig opplært i forbindelse med risiko og riktig atferd ved arbeid på hjemmekontor.
- Inspeksjoner på hjemmekontoret utført ad hoc av databehandlerens personvernleder/-ombud og bare i særlige tilfeller når dette er tillatt ved lov.

1.5 Ingen uautorisert avlesning, kopiering, endring eller sletting av opplysninger i systemet

Tiltak for å sikre dette:

- Opprettelse av brukerkontoer er underlagt en godkjenningsprosess (fire øyne-prinsippet).
- Tilgangsrettigheter tilordnes bare ved behov. Bare de ansatte som har et behov i forbindelse med jobben, har tilgang til systemene og opplysningene.
- Brukere i hvert system har bare tilgang til kunder de skal arbeide med, så sant det er mulig med et slikt skille.
- Begrenset tilgang til databaser. Bare IT-bestillere kan be om tilgang til databaser og infrastruktur.
- Det er fastsatt frister for å deaktivere og slette brukerkontoer.

1.6 Atskillelseskontroll

Atskilt behandling av opplysninger, som samles inn for forskjellige formål, er sikret ved at

- databaser er i et redundant miljø / en redundant klynge (dette kan variere for forskjellige skyleverandører)
- alle endringer i opplysninger må gjøres i systemet (ingen endringer direkte i databaser) og systemet selv tilbyr logging og sporbarhet
- fastsatte tiltak for å sikre databehandling atskilt etter forskjellige formål og forskjellige avtalepartnere (flerklientskapasitet, atskillelse av test-/produksjonssystemer)

1.7 Pseudonymisering (GDPR artikkel 32 nr. 1 bokstav a), GDPR artikkel 25 nr. 1)

I den grad det er relevant og teknisk mulig for den gjeldende behandlingen, skal behandlingen av personopplysninger utføres slik at opplysningene ikke kan knyttes til en spesifikk registrert uten bruk av mer informasjon, forutsatt at denne tilleggsinformasjonen lagres separat.

De appene som brukes til behandlingen, er konfigurert og følger innstillinger for innebygd personvern og anbefalinger fra programvareleverandøren.

2. INTEGRITET (GDPR ARTIKKEL 32 NR. 1 BOKSTAV B))

2.1 Dataoverføringskontroll

Tiltak for å unngå uautorisert avlesning, kopiering, endring eller sletting av opplysninger med elektronisk overføring eller transport:

- Benyttede datatilkoblinger er SFTP, FTP med VPN, Internett/nett med HTTPS, kryptering av e-poster (avhengig av kundekrav).
- IPSec-kryptering er konfigurert for sted-til-sted-VPN-tilkoblinger til kunde; kryptering for apper er definert per app.
- Funksjonell tildeling av involvert maskinvare, registrering og analyse av systembruk.
- Sletting/kassering av datamedium før gjenbruk/deling (papir: personvernbeholder, dokumentmakuleringsmaskin, eksternt kasseringsselskap; magnetisk datamedium: fysisk kassering).

2.2 Dataangivelseskontroll

Brukeraktiviteter (angi, endre, slette personopplysninger) logges i appen. De appene som brukes til behandlingen, er konfigurert og følger innstillinger for innebygd personvern og anbefalinger fra programvareleverandøren.

3. TILGJENGELIGHET OG ROBUSTHET (GDPR ARTIKKEL 32 NR. 1 BOKSTAV B))

3.1 Tilgjengelighetskontroll

Tiltak for å hindre utilsiktet eller forsettlig tilintetgjøring eller tap av opplysninger:

- Sikkerhetstiltak i datasentre (virusbeskyttelse, brannmur, nettverksegmentering, innholdsfilter/proxy, avbruddsfri strømforsyning (UPS), speiling, brannvern, klimaanlegg).
- Rutiner for sikkerhetskopiering og gjenoppretting av data er på plass og testes regelmessig.
- Terminalservermiljøet har høy tilgjengelighet. I perioder med høy aktivitet kan beredskap og økt fokus på tilgjengelighet økes hvis partene samtykker til dette.

3.2 Hurtig gjenoppretting (GDPR artikkel 32 nr. 1 bokstav c))

Potensielt berørte IT-systemer og programvare er identifisert.

4. PROSEDYRER FOR REGELMESSIG TESTING, VURDERING OG EVALUERING (GDPR ARTIKKEL 32 NR. 1 BOKSTAV D), GDPR ARTIKKEL 25 NR. 1)

Fastsatte tiltak:

- Teknologiprinsipper for trygg systemutvikling er fastsatt og gjennomført.
- Atskillelse av utviklings-, test- og produksjonssystemer i størst mulig grad.
- Det er i høy grad unngått å bruke produksjonsdata for testformål.

VEDLEGG 3, LISTE OVER GODKJENTE UNDERLEVERANDØRER

Status:17.11.2025

Dette Vedlegget er en del av Databehandleravtalen og oppdateres av Databehandleren

Benyttes	Land	Navn og Org.nr.	Adresse	Behandlings sted	Type tjeneste
Systemer/underleverandører					
x	Norge	ECIT F&A Holding AS, 921862873	Rolfsbuktveien 2 1364 FORNEBU	EU/EØS	Årsoppgjørssystem, oppslagsverk, rapporteringssystem, Tripletex, Visma Software, Power Office, 24SevenOffice og tilsvarende
x	Norge	ECIT F&A Software AS, 930816639	Rolfsbuktsveien 2 1364 FORNEBU	EU/EØS, USA	KYC/AML system
x	Norge	ECIT Solutions AS, 921064802	Bjørnstjerne Bjørnsons gate 110 3044 DRAMMEN	EU/EØS	Nettverk og skrivere
	Norge	ECIT Digital AS, 955466330	Stadionveien 4 7898 LIMINGEN	EU/EØS	Dokumentsenter
x	Norge	ECIT Veny AS, 928173992	Espehaugen 32 5258 BLOMSTERDALEN	EU/EØS	Integrasjoner
Nearshoring sett x om benyttes	Litauen	Norian UAB	Konstitucijos pr. 21c, Quadrum North	EU/EØS	Lønn og regnskapstjenester
Marker på de kunder der dette benyttes	Norge	ECIT Norian AS, 879906792	Stortingsgata 2, 0158 OSLO	EU/EØS	Underleverandør
	Norge	Catacloud Services AS, 931102095	Rolfsbuktveien 2 1364 FORNEBU	EU/EØS	Regnskapssystem
	Norge	Adato AS	Rolfsbuktveien 2 1364 FORNEBU	EU/EØS	Lønnssystemer, Intect og Nettlønn

	Norge	Uni Micro AS, 925141623	Mo 3, 5729 MODA-LEN	EU/EØS	Regnskapssystem
	Norge	Siffer Systemer AS	Stortingsgata 28, 0161 OSLO	EU/EØS	Regnskapssystem
	Norge	Smartbob AS, 920411584	Inkognitogata 33A 0256 OSLO	EU/EØS	Prisolve rapporterig