DATABEHANDLERAVTALE

I henhold til EUs personvernforordning av 27. april 2016, personopplysningsloven §13, jf. §15 og personopplysningsforskriftens kapittel 2.

Mellom

_____

behandlingsansvarlig

og

_____

Tidsbanken AS
Databehandler

1. Avtalens formål

Avtalens formål er å regulere rettigheter og plikter etter EUs personvernforordning av 27. april 2016, samt etter lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) og forskrift av 15. desember 2000 nr. 1265 (personopplysningsforskriften). Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller deles med uberettiget part.

Avtalen regulerer databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse. Personopplysningene er knyttet til den behandlingsansvarliges ansatte eller oppdragstakere.

2. Om behandlingen av personopplysninger

2.1 Om systemene Tidsbanken leverer

Tidsbanken AS leverer et system for elektronisk timeregistrering og bemanningsplanlegging. Systemet har i tillegg moduler for avviksbehandling, kvalitetssikring, flyt, kjørebok, gjestebok, CRM- og prosjekthåndtering. Databehandleravtalen vedrører hovedsakelig den delen av programmet som omfatter timeregistrering og bemanningsplanlegging, samt kjørebok dersom det er kjøpt tilgang til denne modulen.

2.2 Personopplysninger som behandles

Tidsbanken AS timeregistreringssystem registrerer løpende inn- og ut-tidspunkt etter hvert som brukerne stempler inn-/ut fra systemet. Arbeidstid beregnes etter oppsatt regelverk. Regelverk settes opp etter avtale med den behandlingsansvarlige, eller av behandlingsansvarlig selv. Det vil være mulig å slutte seg til hvem som har registrert den enkelte timelinje i systemet, enten fordi navnet på den ansatte er registrert i systemet, eller basert på annen informasjon hos behandlingsansvarlig.

Det er ikke nødvendig med navn på den enkelte ansatte, men dette kan være hensiktsmessig i de fleste tilfeller. Ved eventuell anonymisering av ansattkontoene må behandlingsansvarlig holde løpende oversikt over hvilken ansatt den enkelte Tidsbanken konto tilhører.

Personopplysninger som kan importeres eller registreres manuelt i systemet er:

- Fornavn og etternavn på ansatt
- Ansattnummer og identifikator
- Adresse, kommunenummer, telefon- og mobiltelefonnummer på ansatt
- Epostadresse
- Fødselsdato og personnummer
- Navn og telefonnummer på pårørende
- Tittel/stilling
- Bankkonto/lønnskonto
- Ansatt dato
- Timelønn
- Avdelingstilhørighet
- Disponible feriedager
- Timelister
- Vaktlister
- Arbeidsoppgaver
- GPS koordinater / kjørebok

Merk: Bare Ansattnummer, Fornavn og Etternavn er påkrevd, men også disse kan anonymiseres ved behov. Hvilke opplysninger som skal registreres er overlatt til behandlingsansvarlig.

Løpende vil systemet registrere ansattnummer, inn klokkeslett og ut klokkeslett for hver registrering, samt koble dette opp mot riktig lønnsart og beregne antall timer for hver enkelt registrering iht. det oppsettet som er lagt inn. Dette er et minimum av hva som er påkrevd for å kunne beregne arbeidstiden elektronisk.

Tidsbanken har ikke adgang til å behandle personopplysninger på vegne av behandlingsansvarlig ut over det som her er nevnt eller etter skriftlig melding fra eller avtale med behandlingsansvarlig.

2.3 Tidsbankens behandling av data

Tidsbanken AS skal sørge for å drifte og administrere systemet på vegne av behandlingsansvarlig. Tidsbanken AS skal ivareta nødvendig systemsikkerhet, og påse at ingen får uberettiget tilgang til systemet. Data lagres i samsvar med gjeldende lover og forskrifter for personvern.

Tidsbanken sine ansatte har generell taushetsplikt, og er bundet av taushetsavtale/personvernerklæring. Det er kun ansatte hos Tidsbanken AS som arbeider med drift og brukerstøtte av systemet som har tilgang til å se personopplysninger.

Databehandleren, samt eventuelle underleverandører, er forpliktet til utelukkende å behandle personopplysninger i overensstemmelse med instrukser ustedt av behandlingsansvarlig. Denne forpliktelse gelder for alle former for behandling, som databehandleren og dennes underleverandører foretar på vegne av den dataansvarlige.

Tidsbanken AS vil ikke selv benytte noen opplysninger i systemet for formål annet enn å oppfylle den avtale som er gjort med behandlingsansvarlige, samt som grunnlag for fakturering.

All trafikk er automatisk kryptert mellom bruker og system. Data lagres sikkert hos ekstern leverandør i Nord Europa.

2.4 Tilgang for behandlingsansvarlig

Systemet Tidsbanken stilles til rådighet for behandlingsansvarlig ved passord beskyttet internettbasert tilgang. Det er Tidsbanken AS som administrerer de ulike kundenes tilgang til systemet, men det er i hovedsak behandlingsansvarlig selv som styrer hvilken tilgang de ulike ansatte skal ha til kundens kundekonto. Tidsbanken AS kan også regulere graden av tilgang basert på avtale med behandlingsansvarlig.

Tidsbanken skal sette opp nødvendige tilganger til systemet, slik at behandlingsansvarlig kan benytte dette til sitt formål. Behandlingsansvarlig må selv ta stilling til hvilke personer hos behandlingsansvarlig som trenger tilgang, og hvilken tilgang den enkelte har behov for. Behandlingsansvarlige kan selv administrere denne tilgangen alene eller i samråd med databehandler.

Alle brukere hos behandlingsansvarlig har som standard lesetilgang til egne opplysninger, og i hvilken grad de skal ha skrivetilgang til egne opplysninger styres av behandlingsansvarlig.

Tidsbanken tilbyr generelle anbefalinger for å sikre data på våre supportsider.

2.5 Utlevering av personopplysninger

Utlevering av opplysninger fra systemet er regulert av «Lisens og brukeravtale for Tidsbanken». Med unntak av behandlingsansvarlig selv vil ikke Tidsbanken AS utlevere personopplysninger til andre enn politiet, mot gyldig rettskjennelse.

Tidsbanken sine ansatte har generell taushetsplikt, og er bundet av taushetsavtale/personvernerklæring. Det er kun ansatte hos Tidsbanken AS som arbeider med drift og brukerstøtte av systemet som har tilgang til å se personopplysninger.

Tidsbanken AS vil ikke selv benytte noen opplysninger i systemet for formål annet enn å oppfylle den avtale som er gjort med behandlingsansvarlige, samt som grunnlag for fakturering.

3. Databehandlers plikter

Databehandler skal følge de rutiner og instrukser for behandlingen som behandlingsansvarlig til enhver tid har bestemt skal gjelde. Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand i dette.

Databehandler vil også bistå behandlingsansvarlig med å oppfylle plikten til å svare de registrerte på anmodninger som inngis etter EUs personvernforordning, særlig etter art. 15 – 20.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

4. Bruk av annen databehandler

Databehandleren skal ikke benytte seg av underdatabehandlere lokalisert utenfor EU/EØS uten forutgående skriftlig varsel til behandlingsansvarlig minst 30 dager før den planlagte dataoverføringen finner sted. Behandlingsansvarlig har rett til å motsette seg en slik bruk av underdatabehandlere. Ved bruk av underdatabehandlere innenfor EU/EØS, påtar databehandleren seg ansvaret for å sikre at underdatabehandleren opprettholder et tilsvarende eller høyere nivå av datasikkerhet og personvern som avtalt med behandlingsansvarlig.

Tidsbanken timeregistreringssystem og tilhørende produkter er utviklet av Tidsbanken AS i Bergen, Norge. Data lagres trygt hos underleverandører av skytjenester, som leverer høy grad av sikkerhet. Databehandler skal ha rett til å benytte underleverandører. Databehandler skal gjøre underleverandører kjent med databehandlers avtalemessige og lovmessige forpliktelser. Alle underleverandører skal oppfylle disse forpliktelsene.

5. Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak, som stilles etter EUs personvernforordning, personopplysningsloven og personopplysningsforskriften, herunder særlig personopplysningslovens §§ 13-15 med forskrifter. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på behandlingsansvarliges forespørsel.

Brudd på personopplysningssikkerheten (EUs personvernforordning art 33) skal meldes til behandlingsansvarlig (jmfr EUs personvernforordning art 33 nr 2). Databehandleren er forpliktet til å informere den behandlingsansvarlige om ethvert potensielt brudd på personopplysninger uten ugrunnet opphold. Varselet skal gis straks etter at databehandleren ble kjent med bruddet, for å muliggjøre rask og effektiv håndtering i samsvar med gjeldende personopplysningslov.

Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet. Databehandler vil utforme meldingen til Datatilsynet om ønskelig.

6. Brudd på regelverk

Dersom Tidsbanken bryter avtalens regler om personopplysningssikkerhet, bindende instruks fra behandlingsansvarlig eller regler i personopplysningsloven, kan behandlingsansvarlig pålegge Tidsbanken å stoppe den videre behandling av personopplysninger med øyeblikkelig virkning.

7. Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig.

Oppsigelse av denne avtalen følger vilkårene for oppsigelse av avtalen i «Lisens og bruksavtale for Tidsbanken».

8. Ved opphør

Ved opphør av avtalen må behandlingsansvarlig selv hente ut nødvendig dokumentasjon de vil trenge i forbindelse med timebehandlingen før avtalen termineres. Disse data lagres da hos behandlingsansvarlige, som selv påtar seg det totale ansvar for datasikkerheten.

Dersom en ønsker kan databehandlere inngå en datalagringsavtale, som forlengelse av eksisterende avtale, hvor Tidsbanken tar vare på databasen, og databehandler vil ha tilgang til å logge på og ta ut data ved behov inntil datalagringsavtalen sies opp og avsluttes.

Tidsbanken kan og mot vederlag være behjelpelig til å hente ut data fra systemet til lagring i ulike formater. Et slikt ønske må meldes Tidsbanken senest 14 dager etter at avtaleperiode er utløpt.

Ved endelig opphør av denne avtale plikter databehandler å slette på en forsvarlig måte alle personopplysninger som er mottatt på vegne av den behandlingsansvarlige og som omfattes av denne avtalen. Dette gjelder også eventuelle sikkerhetskopier. Databehandler plikter ikke å slette opplysninger som han er pliktig til å lagre etter lov eller som han etter personopplysningsloven har adgang til å lagre etter at avtalen med behandlingsansvarlig er opphørt.

9. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Bergen tingrett som verneting. Dette gjelder også etter opphør av avtalen.

***

Denne avtalen er i 2 – to eksemplarer, hvorav partene har hvert sitt.

Sted og dato

Behandlingsansvarlig	Databehandler
_____	_____
(Underskrift)	(Underskrift)

Bilag A: Kontaktinformasjon
Bilag B: Tiltak

Kontaktinformasjon

Hos Behandlingsansvarlig	Hos Databehandlere
Sikkerhetsbrudd meldes:	
Telefon: _____	Telefon: 55 27 37 00
E-post: _____	E-post: support@tidsbanken.no
Andre henvendelser:	Andre henvendelser:
Navn: _____	Navn: _____
Stilling: _____	Stilling: _____
Telefon: _____	Telefon: _____
E-post: _____	E-post: _____

Databehandleravtalen vår er gjennomgått av en advokat og skal være tilstrekkelig dekkende for vår plattform og systemet vi leverer. Dokumentasjon om våre systemer for øvrig, ligger åpent tilgjengelig på vårt supportsenter.

Vi har en egen info-artikkel knyttet til GDPR som gir svar på spørsmål omkring GDPR i Tidsbanken.

Den artikkelen finner dere her: GDPR i Tidsbanken (https://tidsbanken.net/support/case.asp?ID=630)

Tidsbanken programvare, egne og kundenes data ligger lagret i skyen. Sky-leverandør er Microsoft Ireland Operations LTD. «Microsoft Azure», som vi bruker til skylaging av vår programvare er et amerikansk selskap med datterselskap i Irland, og serverlokasjon i Norge. Vi lager dataene tilknyttet Tidsbanken på europeiske servere, og fortrinnsvis i Norge der vi finner det forenlig med trygg drift. Selskapet betjener skylagring for systemet, men har ikke direkte tilgang til hverken våre eller kundenes databaser.

Diverse tiltak knyttet til personvern og sikkerhet med tanke på GDPR:

- **Pseudonymiseringstiltak**

  Vår databehandleravtale inneholder en liste over hvilke persondata som kan lagres i Tidsbanken, men hvilke av disse data som faktisk lagres, er helt opp til kundene våre.

  Fra et systemperspektiv er det ingenting i veien for å fjerne identifiserende informasjon fra datasettet og kun bruke unike identifikatorer i stedet.

  All den tid kundene våre benytter Tidsbanken til å ivareta krav som stilles i arbeidsmiljøloven og i bokføringsloven, så kan det for mange være nødvendig med minimum ansattnummer, navn og etternavn i datasettet.

- **Krypteringstiltak**

  Alle personopplysninger lagres trygt hos vår underleverandør sine datasentre. All overføring av data fra disse datasentrene gjøres over krypterte linjer og er beskyttet bak vårt tilgangssystem.

- **Tiltak for å sikre personoppysningens fortrolighet (konfendensialitet)**

  Alle data i Tidsbanken er beskyttet bak tilgangssystemet vårt og hver enkelt kundedatabase har sin egen pålogging, så vel som her enkelt ansattbruker. Autentiseringssystemet vårt har sin egen midlertidige lagring som separat fra alt annet i systemet, der informasjon om innlogget bruker lever i korte perioder. Så snart brukerinformasjonen er utgått, må den autentiseres på nytt. Dette skjer ofte i «bakgrunnen», men sørger for at vi har mulighet til å f.eks. invalidere muligheten til å kjapt endre tilgangsnivå for brukere, og «kaste ut» ansatte som ikke lenger er i bedriften. I tillegg sender vi aldri ukryptert sensitiv informasjon mellom våre system, og er sterkt beskyttet mot alle former for MITM-angrep på auth tokens og lignende.

  Alle ansatte i Tidsbanken har taushetsplikt og mottar opplæring i datasikkerhet, og hvordan personopplysninger skal håndteres på en sikker måte. Rutiner knyttet til dette er også beskrevet og praktiseres gjennom vårt internkontrollsystem.

- **Tiltak for å sikre robusthet i behandlingssystemene og -tjenestene**

  Siden systemet vårt er veldig bredt distribuert (mange tjenester som kjører på separate maskiner i skyen), vil selv en krisesituasjon med stor sannsynlighet kun påvirke en, eller et mindre antall tjenester. Det er en rekke personer fra forskjellige avdelinger i bedriften vår som har autoritet til å melde alarm, og et utvalg erfarne utviklere inngår i en bakvakt med responstid på maksimalt 30 minutt. Dersom vedkommende ikke har det som trengs av kompetanse for det spesifikke problemet, er det fritt fram for å dra med seg flere på problemløsningen.

  Tidsbanken er sky-basert, og alle tjenestene våre er bygd for å kunne skaleres både opp/ned (spesifikasjoner på maskinvaren som kjører tjenestene) og ut/inn (endre antall maskiner som kjører tjenestene) etter behov. En ekstremt nyttig bivirkning av dette er at vi i praksis kan bytte ut absolutt all maskinvare som kjører de forskjellige tjenestene våre i løpet av minutter. Dette er noe vi gjør for enkelte tjenester i tilfeller der en eller flere maskiner ikke oppfører seg som de skal. Når det gjelder kunder sin data, har vi 1 måned backup tilgjengelig for alle databaser (pr. kunde), slik at en når som helst kan rulle tilbake til et tidspunkt opp til 1 måned tilbake i tid. Utover det går kopiene tilbake et år, men med lengre intervall.

  Vi har rutiner på plass for å holde systemet oppdatert og erstatter regelmessig gamle teknologier med nye, samt for foretagelse av sårbarhetsskanninger av systemet.

  Ved hver minste endring i funksjonalitet i systemet vårt, må endringen både gjennom et såkalt "code review" der en eller flere (varierer basert på hvor kritisk tjenesten er) utviklere leser gjennom koden som har blitt skrevet, og gjennomfører testing. Hvilken testing som blir gjort vil variere, men et minimum er funksjonstesting der ansatte utenfor utviklingsavdelingen manuelt går gjennom tjenesten som det jobbes på, og alle andre tjenester som potensielt kan påvirkes. Det er også vanlig at det blir gjort en eller flere former for automatisert testing der funksjonalitet blir testet av programvare.

- **Tiltak for fysisk sikring av lokaler hvor data skal behandles**

  Lokaler hvor ansatte i Tidsbanken behandler data er fysisk sikret i flere ledd, i tillegg har vi internkontrollrutiner på plass knyttet til å begrense adgang til våre ansattes utstyr på arbeidsplassen.

- **Bruk av testdata**

  Tidsbanken bruker såkalte «cookies» til å styre innloggingen og samle logging til bruk i feilsøk.

  Denne loggingen inneholder ikke persondata, og det er også anonyme data – det vil derfor ikke ha noe påvirkning på GDPR. Til testing bruker vi fiktive datasett.

Andre datasikkerhetstiltak

Vi kan ikke gå for mye i detalj her, da dette potensielt ville kunne blitt et sikkerhetsbrudd i seg selv.

Tidsbanken tar sikkerhet på alvor. Vi har et eget sikkerhetsråd bestående av 4 personer fra ledelsen, og av andre ved behov. Disse jobber daglig med sikkerhetsforbedrende tiltak. Det gjelder generell datasikkerhet i selskapet Tidsbanken AS, og i produktet. Vår utviklingsavdeling arbeider med kontinuerlig forbedring og har en langtidsplan for å bli kvitt gammel kode, og gjøre systemet enda mer robust for fremtiden.

Tidsbanken tar i bruk moderne rammeverk med innebygde sikkerhetsmekanismer som beskytter mot angrep som bl.a. SQLinjection. Alle tjenestene våre er bak «load balances» med innebygd beskyttelse mot bla.. DDoS-angrep. Alle kundene våre har data i sine egne databaser, slik at evnt. brudd rettet mot en enkelt kunde ikke vil føre til lekkasje av data for andre kunder.

---------- Slutt ----------