Databehandleravtalen vår er gjennomgått av 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 beskriver flere av sakene over, den finner dere her: GDPR i Tidsbanken

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 isteden.
  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 våre underleverandørers datasentre.
  All overførsel av data fra disse datasentrene gjøres over krypterte linjer og er beskyttet bak vårt tilgangssystem.
- **Tiltak for å sikre personopplysningens fortrolighet (konfidensialitet)**
  Alle data i Tidsbanken er beskyttet bak tilgangssystemet vårt og hver enkelt kundedatabase har sin egen pålogging, så vel som hver enkelt ansattbruker.

  Autentiseringssystemet vårt har sin egne midlertidige lagring som er separat fra alt annet i systemet, der informasjon om innlogget bruker lever i korte perioder.
  Så snart brukerinformasjon er utgått, må det 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.

  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 behandles**
  Lokaler hvor ansatte i Tidsbanken behandler data er fysisk sikret i flere

ledd, i tillegg til at vi har internkontrollrutiner på plass knyttet til å begrense adgang til våre ansattes utstyr på arbeidsplassen.

- **Bruk av evt. 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 mer i detalj her, da dette potensielt kan bli et sikkerhetsbrudd i seg selv.

Tidsbanken tar i bruk moderne rammeverk med innebygde sikkerhetsmekanismer som beskytter mot angrep som bl.a. SQLinjection. Alle tjenestene våre er bak "load balancers" med innebygd beskyttelse mot bl.a. DDoS-angrep. En ting til er at kunder har sine data i hver sine databaser, slik at et evt. brudd rettet mot en enkelt kunde ikke vil føre til lekkasje av data for andre kunder.