

ADDSECURES BEHANDLING AV PERSONOPPLYSNINGER

For den behandlingen av personopplysninger som AddSecure utfører på vegne av kundene sine, er AddSecure databehandler for kunden. Hvis du er kontaktperson for en av AddSecures kunder, er det arbeidsgiveren din som har ansvaret for personopplysningene dine. AddSecure har ansvar for å påse at personopplysningene dine er sikre når vi behandler dem. De forpliktelsene AddSecure har som databehandler er regulert i hovedavtalen og AddSecures generelle databehandleravtale, som ligger som vedlegg til hovedavtalen med mindre kunden har valgt å inngå en egen databehandleravtale. AddSecures personvernerklæring og generelle databehandleravtale er publisert på bedriftens nettsted.

ADDSECURE SOM DATABEHANDLER

Som en del av AddSecures tilbud inngår ulike nettbaserte tjenester, for eksempel AddView, SafeView, SecureApps, Telecall og ulike partnernettsider, heretter kalt «**Tjenestene**». I tjenestene er AddSecure databehandler og har derfor ansvar for blant annet de tekniske og organisatoriske sikkerhetstiltakene. AddSecure sørger også for at lagringen av, og tilgangen til personopplysningene gjøres på en sikker måte og basert på den nyeste utviklingen, kostnadene for gjennomføring og behandlingens art, omfang, sammenheng og formål, samt risikoene for den registrertes rettigheter og friheter, risikoer som har varierende sannsynlighetsgrad og alvorlighetsgrad.

Kunden er behandlingsansvarlig for opplysninger i tjenestene. Med kunden menes den kunden som er registrert som mottaker av AddSecures faktura for tjenestene. AddSecure behandler personopplysninger på vegne av kunden.

DETTE MÅ DERE TENKE PÅ SOM BEHANDLINGSANSVARLIG

Ansvaret for personopplysninger er regulert i personvernforordningen. Som behandlingsansvarlig må bedriften som er kunde hos AddSecure, blant annet ha kontroll over hvilken type opplysninger dere behandler, hva formålet for behandlingen er, hvor lenge opplysningene skal lagres samt hvilket rettslig grunnlag dere har for behandlingen. Det kan også hende at dere må innhente samtykke fra den registrerte. Du finner mer informasjon om den behandlingsansvarliges ansvar hos Datatilsynet: <https://www.datatilsynet.no/>.

GENERELT DATABEHANDLERAVTALE

1. PARTER

AddSecure Group ("AddSecure") består av selskapene:

- AddSecure AB (Sweden) SE5565272001
- AddSecure AG (Switzerland), CH02030377837
- AddSecure AS (Norway) NO976145178
- AddSecure Ltd (England), GB03593453
- AddSecure Oy (Finland), FI28410722
- AddSecure Smart Grids AB (Sweden), SE5590442314
- Contal Security AB (Sweden), SE5564684123

Mellom Kunde (i Hovedavtale) angitt nedenfor som "Behandlingsansvarlig" og AddSecure angitt nedenfor som "Databehandleren" har følgende Databehandleravtale blitt inkludert som en del av Hovedavtale.

2. FORMÅL

2.1

Formålet med denne databehandleravtalen for personopplysninger er å sikre at databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig, kun skjer i tråd med den behandlingsansvarliges instruks, i samsvar med denne databehandleravtalen og i tråd med kravene som fremgår av artikkel 28 i Personvernforordningen (Europaparlaments- og rådsforordning (EU) 2016/679).

2.2

Emnet for behandling av personopplysninger i henhold til denne avtalen er personopplysninger knyttet til systemer og tjenester som omfattes av Hovedavtalen.

Behandlingen kommer til å fortsette så lenge hovedavtalen er gyldig, og kan skje på ulike måter som for eksempel innsamling, registrering, organisering, strukturering, oppbevaring, bearbeiding, endring, uthenting, lesing, bruk, utlevering, formidling eller på annen måte tilgjengeliggjøring, justering, sammenstilling, begrensning, sletting eller ødeleggelse av personopplysninger.

Behandlingen gjelder alle typer personopplysninger som Databehandleren får tilgang til for å kunne oppfylle sine forpliktelser i henhold til Hovedavtalen.

3. DEFINISJONER

Denne databehandleravtalen skal tolkes i samsvar med, og med definisjoner from fremgår av artikkel 4 i personvernforordningen.

4. BEHANDLINGSANSVARLIG

Behandlingsansvarlig plikter å overholde personvernforordningen, når det gjelder behandling av personopplysninger og bruk av databehandlere. Behandlingsansvarlig har rett til å kontrollere behandlingen av personopplysninger som utføres av databehandleren, og skal gi databehandleren dokumenterte instruksjoner som er nødvendige når denne skal behandle opplysninger.

5. DATABEHANDLERENS ANSVAR

Databehandleren påtar seg å kun behandle personopplysninger i samsvar med dokumentert instruks fra behandlingsansvarlig, samt i tråd med denne databehandleravtalen og hovedavtalen.

5.1

Ved behandling av personopplysninger plikter databehandleren å overholde gjeldende lov, særlig personvernforordningen. I tillegg plikter databehandleren å overholde forskrifter, beslutninger og anbefalinger som er kunngjort eller formidlet av Datatilsynet eller relevante EU-organer, med hensyn til akseptabel håndtering av personopplysninger.

5.2

Ved å undertegne denne avtalen bekrefter databehandleren at nødvendige tekniske og organisatoriske sikkerhetstiltak er implementert for å beskytte personopplysningene, slik at behandlingen av disse skjer i tråd med kravene i personvernforordningen og ivaretar de registrerte personenes rettigheter.

5.3

Databehandleren skal etter instruks fra behandlingsansvarlig korrigere, slette eller overføre feilaktige, ufullstendige, unøyaktige eller utdaterte personopplysninger uten unødig forsinkelse.

6. SIKKERHETSTILTAK

Databehandleren skal iverksette, implementere og opprettholde hensiktsmessige tekniske og organisatoriske sikkerhetstiltak for å verne personopplysningene.

6.1

Sikkerhetstiltakene databehandleren iverksetter, skal sikre det beskyttelsesnivået som kreves av gjeldende lov og personvernforordningen (når denne trer i kraft), og som ellers er hensiktsmessig med hensyn til tekniske muligheter, implementeringskostnader, særskilte risikoer knyttet til behandlingen av opplysningene samt i hvilken grad personopplysningene som behandles, er eller kan anses som sensitive.

6.2

Databehandleren er ansvarlig for å sikre at dennes virksomhet drives på en måte som også ellers sikrer tilstrekkelig personvern og informasjonssikkerhet.

6.3

Databehandleren skal sørge for at ansatte, konsulenter og andre personer som databehandleren er ansvarlig for, og som behandler eller har tilgang til personopplysninger, er bundet av en dertil egnet konfidensialitetsforpliktelse, og at disse er informert om at behandlingen av personopplysninger skal skje i samsvar med instruks fra behandlingsansvarlig.

6.4

Ved implementering av tekniske og organisatoriske sikkerhetstiltak skal databehandleren ta i betraktning den nyeste utviklingen, implementeringskostnader, arten av behandlingen av personopplysninger, omfang, sammenheng og formål, herunder risikoer for fysiske personers rettigheter og friheter med varierende alvorlighetsgrad og sannsynlighet, for å sikre et sikkerhetsnivå i samsvar med de aktuelle risikoene.

6.5

Databehandlerens implementering av sikkerhetstiltak skal omfatte, der dette er hensiktsmessig, pseudonymisering og kryptering av personopplysninger, muligheten til å fortløpende sikre konfidensialiteten, integriteten, tilgjengeligheten og robustheten til systemene og tjenestene for behandling av personopplysninger samt muligheten til å gjenopprette tilgjengeligheten av og tilgangen til personopplysningene innen rimelig tid hvis det forekommer fysiske eller tekniske sikkerhetshendelser, samt prosedyrer for regelmessig testing, undersøkelser og evaluering av hvor effektive sikkerhetstiltakene er.

6.6

Ved vurdering av sikkerhetstiltakenes egnethet skal man særlig vurdere risikoen for utilsiktet eller ulovlig ødeleggelse av, tap av, endring i eller uautorisert tilgang til personopplysninger.

7. SIKKERHETSHENDELSER

Ved mistenkte eller påviste sikkerhetshendelser, som uautorisert tilgang til, ødeleggelse av, endring i eller annen ikke-autorisert påvirkning av personopplysningene, skal databehandleren umiddelbart undersøke det aktuelle tilfellet, iverksette hensiktsmessige tiltak for å avhjelpe situasjonen og for å forhindre gjentakelse, samt gi behandlingsansvarlig en utførlig hendelsesrapport, hvis ikke databehandleren kan vise at det ikke er fare for at de registrertes rettigheter og friheter krenkes som følge av sikkerhetshendelsen.

7.1

Hendelsesrapporter skal inneholde en beskrivelse av hendelsens art, kategorier av registrerte personer samt det omtrentlige antallet registrerte som er berørt av hendelsen, samt kategorier av og det

omtrentlige antallet personopplysninger som er berørt, en beskrivelse av sannsynlige konsekvenser av hendelsen samt en handlingsplan, herunder eventuelle tiltak for å redusere eventuelle negative konsekvenser. I tillegg skal hendelsesrapporten inneholde kontaktopplysninger til personvernombudet eller andre kontaktpunkter for mer informasjon om hendelsen.

8. UNDERLEVERANDØRER (UNDERBEHANDLERE)

Databehandleren som behandler personlige opplysninger, har rett til å outsource behandlingen av personopplysninger til underbehandlere i og utenfor EU-/EØS-området. Databehandleren godkjenner herved at behandlingen av personopplysninger kan utføres av underbehandlere som vanligvis brukes i bransjen, til å utføre behandlingen av personopplysninger helt eller delvis, uten skriftlig forhåndssamtykke til dette fra behandlingsansvarlig. Databehandleren må sikre at underbehandlerne er bundet av skriftlige avtaler som gir minimum samme grad av beskyttelse av personopplysninger som forpliktelsene i henhold til denne databehandleravtalen. Hvis noen av underbehandlerne ikke oppfyller sine forpliktelser i tråd med det ovennevnte, er databehandleren ansvarlig for denne manglende oppfyllelsen av forpliktelser på vegne av underbehandlerne.

Databehandleren skal informere behandlingsansvarlig om eventuelle intensjoner om å erstatte eller engasjere nye underbehandlere, med unntak av underbehandlere som vanligvis brukes i bransjen. Denne informasjonen skal inneholde navnet på de aktuelle underbehandlerne samt den geografiske posisjonen for stedet behandlingen av personopplysninger gjennomføres på. Behandlingsansvarlig har rett til å sende inn en skriftlig innsigelse mot erstatningen eller engasjementet av slike nye underbehandlere innen fjorten dager fra vedkommende mottok varsel om dette. Dersom databehandleren, til tross for innsigelser fra databehandleren, fortsatt skulle ønske å erstatte eller engasjere en ny underbehandler, skal behandlingsansvarlig ha rett til å si opp avtalen i henhold til punkt 12.

9. INNSYN

For å sikre at hensiktsmessig sikkerhetsnivå opprettholdes, samt at denne databehandleravtalen overholdes, har behandlingsansvarlig rett til nødvendig innsyn i de delene av databehandlerens organisasjon og systemer som er knyttet til behandlingen av personopplysninger.

10. SKADEANSVAR

Dersom det forekommer skade for behandlingsansvarlig som skyldes at databehandleren behandler personopplysninger i strid med vilkårene i denne databehandleravtalen eller instruks fra behandlingsansvarlig, eller annen unnlattelse fra databehandlerens side, skal disse skadene erstattes av databehandleren.

11. AVTALENS OVERDRAGELSE

Overdragelse av denne databehandleravtalen kan kun skje i forbindelse med overdragelse av hovedavtalen.

12. AVTALENS VARIGHET

Denne avtalen er gyldig fra startdato for hovedavtale og så lenge databehandleren oppbevarer eller på annen måte utfører behandling av personopplysninger på vegne av behandlingsansvarlig.

12.1

Ved opphør av databehandleravtalen skal databehandleren, i samsvar med instruks fra behandlingsansvarlig, slette eller returnere alle data som inneholder personopplysninger, fra samtlige medier der personopplysningene har vært lagret eller oppbevart, og deretter slette samtlige eventuelle kopier eller backup av disse.

13. TVISTER OG GJELDENE LOV

Landet der behandlingsansvarlig er lokalisert, er det lands lover som gjelder for denne avtalen. Tvister som oppstår som følge av denne avtalen, skal avgjøres i samsvar med hovedavtalens bestemmelser om tvisteløsning.