TILLEGG FOR LISENSTJENESTER

Autronica Fire and Security AS

Gjeldende fra 22. desember 2020

TILLEGG IV - Databehandlings- og dataoverføringsavtale (DBA)

Denne databehandlings- og dataoverføringsavtalen («DBA-en») skal gjelde for bruk av portalen, programvaren og støttetjenestene som leveres i henhold til kontrakten med Autronica («kontrakten») fra og med ikrafttredelsesdatoen for denne, da denne er inngått mellom de nevnte partene, og der denne DBA-en er innlemmet ved henvisning. Autronica Fire and Security AS skal fungere som databehandler og kunden som behandlingsansvarlig.

Med unntak av det som uttrykkelig suppleres av denne DBA-en med hensyn til dennes gjenstand, skal vilkårene i kontrakten fortsette å være gjeldende med full kraft og virkning for kontraktens gjenstand og det som er anført i kontrakten.

1. DEFINISJONER

Definerte termer i denne DBA-en skal ha betydningen som er tilskrevet de aktuelle termene under punkt 1.2 (eller andre steder i denne DBA-en eller kontrakten), og dersom intet annet er anført, skal de ha sin vanlige og alminnelig anvendte betydning.

Følgende definisjoner gjelder for denne DBA-en:

«Personvernlovgivning(en)» betyr gjeldende nasjonale, føderale, statlige og lokale lover knyttet til personvern, beskyttelse av personopplysninger og data, samt overføringer av personopplysninger eller data på tvers av landegrenser, herunder blant annet personvernforordningen («personvernforordningen») og enhver EU-lov eller forskrift som kan vedtas for å implementere eller erstatte personvernforordningen.

«Den registrerte» betyr en identifiserbar fysisk person som kan identifiseres direkte eller indirekte, særlig ved henvisning til identifiserende informasjon som navn, identifikasjonsnummer, posisjonsdata, online.identifikatorer eller en eller flere faktorer som er spesifikke for den fysiske, fysiologiske, genetiske, mentale, økonomiske, kulturelle eller sosiale identiteten til den fysiske personen.

«Hendelse» betyr enhver faktisk hendelse eller rimelig mistanke om hendelser med utilsiktet eller ulovlig tap, endring eller uautorisert eller utilsiktet avsløring av eller innsyn i personopplysningene.

«Personopplysninger» betyr enhver informasjon eller data som er gitt til Autronica eller dens underleverandører av behandlingsansvarlig eller dennes representanter, underleverandører eller kunder i forbindelse med kontrakten, som er tilknyttet en hvilken som helst identifisert eller identifiserbar fysisk person eller, i tilfelle eventuell motstrid med gjeldende lovgivning, som er underlagt personvernlovgivningen.

2. DENNE DBA-ENS GJENSTAND

Denne DBA-en gjelder utelukkende for vertstjenestene og administrasjonsaktivitetene som databehandleren leverer til behandlingsansvarlig i forbindelse med lagring av personopplysninger knyttet til portalen, samt relaterte tjenester som beskrevet i kontrakten.

En oversikt over kategoriene av personopplysninger, kategorier av registrerte og formålene personopplysningene behandles for, er anført i vedlegg 1 til denne DBA-en.

3. VARIGHET OG OPPSIGELSE

Denne DBA-en trer i kraft på ikrafttredelsesdatoen, og skal være gjeldende frem til kontrakten sies opp eller opphører.

Denne DBA-ens oppsigelse eller utløp skal ikke frita databehandleren fra dennes konfidensialitetsforpliktelser i henhold til punkt 6 i vedlegg II til kontrakten.

Databehandleren skal behandle personopplysninger frem til datoen kontrakten utløper eller sies opp, med mindre behandlingsansvarlig gir instruks om noe annet, eller frem til slike opplysninger returneres eller destrueres etter instruks fra behandlingsansvarlig, i henhold til punkt 12 i denne DBA-en. Den behandlingsansvarliges instruksjoner er, i den grad de fordrer ytterligere tjenester eller utgifter for databehandleren, underlagt ytterligere avgifter som skal forhandles bona fide mellom partene.

4. DATABEHANDLERENS OG DEN BEHANDLINGSANSVARLIGES FORPLIKTELSER

Begge parter skal overholde all gjeldende personvernlovgivning og umiddelbart varsle hverandre skriftlig hvis man mener at innsamlingen eller behandlingen av personopplysninger i henhold til denne DBA-en eller kontrakten er i strid med personvernlovgivningen

Databehandleren skal kun behandle personopplysninger på skriftlig instruks fra behandlingsansvarlig eller som angitt i kontrakten eller denne DBA-en, på en slik måte og i den grad det er hensiktsmessig som dette kreves for leveringen av tjenestene beskrevet i kontrakten, med unntak av det som kreves for å overholde en rettslig forpliktelse som databehandleren er underlagt.

Partene har inngått kontrakten for å dra nytte av databehandlerens ekspertise i å sikre og behandle personopplysningene for formålene som er anført i vedlegg 2. Databehandleren skal ha rett til å handle etter eget skjønn ved utvelgelse og bruk av midlene denne anser som nødvendig for å oppfylle disse formålene, underlagt kravene i denne DBA-en.

5. DEN BEHANDLINGSANSVARLIGES FORPLIKTELSER

Den behandlingsansvarlige skal:

a) garantere at den har alle nødvendige rettigheter til å formidle personopplysningene til databehandleren for at behandlingen skal kunne utføres i forbindelse med portalen, programvaren og relaterte tjenester. I den grad det kreves av gjeldende personvernlovgivning, er behandlingsansvarlig ansvarlig for å sikre at denne formidler slike personopplysninger til Autronica i henhold til et passende rettslig grunnlag som muliggjør lovlig behandling av personopplysningene, herunder innhenting av eventuelt påkrevd samtykke til behandlingen, og for å sørge for å opprettholde en løpende oversikt over slike samtykker. Dersom en registrert person trekker tilbake sitt samtykke til behandling av personopplysninger, har behandlingsansvarlig ansvaret for å opplyse databehandleren om dette

b) gi alle fysiske personer som den samler inn personopplysninger fra, informasjon om den relevante personvernerklæringen, basert på Autronicas personvernerklæring som vises i portalen

c) kreve at databehandleren sletter personopplysninger på anmodning fra behandlingsansvarlig

eller eventuelle registrerte personer som den har samlet inn personopplysninger om, med mindre databehandleren på annen måte plikter å fortsette å oppbevare personopplysningene i henhold til gjeldende lov, og

d) straks skriftlig varsle databehandleren hvis den mottar eller får vite om noen: (i) klage eller påstand som indikerer et brudd på personvernlovgivningen vedrørende personopplysningene; (ii) anmodning fra en eller flere personer om å få tilgang til, korrigere eller slette personopplysninger; (iii) henvendelser eller klager fra en eller flere personer i forbindelse med innsamling, behandling, bruk eller overføring av personopplysninger; og (iv) anmodning fra myndigheter, rettskjennelse, ransakingsordre eller annen rettslig, juridisk, administrativ eller myndighetspålagt prosess som medfører utlevering av personopplysninger (samlet kalt «personvernsaker»).

6. DATABEHANDLERENS FORPLIKTELSER

Databehandleren skal:

a) kun behandle personopplysninger, eller overføre personopplysninger til autoriserte tredjeparter, for å oppfylle sine forpliktelser i henhold til kontrakten og i samsvar med den behandlingsansvarliges instruksjoner eller det som er anført i denne databehandleravtalen, eller for å oppfylle sine juridiske forpliktelser

b) ikke dele, overføre, utlevere eller gi tilgang til personopplysninger til noen tredjepart, unntatt for å levere tilgang til portalen og for å levere tjenestene som omfattes av kontrakten, eller i henhold til gjeldende lov. Denne bestemmelsen utelukker ikke databehandleren fra å bruke underleverandører til å levere tjenestene, så lenge den sørger for at eventuelle personopplysninger som databehandleren deler, overfører, formidler eller gir innsyn i til tredjepart, behandles i samsvar med bestemmelsene i punkt 8 i denne DBA-en, og

c) iverksette kommersielt rimelige tiltak for å verifisere påliteligheten av databehandlerens ansatte, agenter, representanter, underleverandører, underleverandørers ansatte eller eventuelle andre personer databehandleren bruker (samlet kalt «databehandlerens personell») som har tilgang til personopplysninger, sørge for tilgang kun gis der det er nødvendig og sørge for at databehandlerens personell er forpliktet til å holde personopplysningene konfidensielle, for eksempel gjennom en konfidensialitetsavtale eller gjennom å anvende gjeldende lover eller forskrifter

7. ASSISTANSE FRA BEHANDLINGSANSVARLIG

Databehandleren skal:

a) i rimelig grad gi informasjon, bistand og samarbeid som behandlingsansvarlig fra tid til annen kan trenge for å bekrefte at databehandleren overholder gjeldende personvernlovgivning

b) bistå behandlingsansvarlig med egnede tekniske og organisatoriske tiltak, i den grad dette er mulig, for å oppfylle den behandlingsansvarliges plikt til å svare på henvendelser der registrerte personer vil utøve sine rettigheter i henhold til gjeldende personvernlovgivning

c) bistå behandlingsansvarlig i å sikre samsvar med og demonstrere tiltakene denne har truffet for å overholde forpliktelsene i henhold til punkt 10 (sikkerhetstiltak), en vurdering av personvernkonsekvenser samt forhåndsdrøftinger med tilsynsmyndigheten som kreves i henhold til personvernforordningens Artikkel 36 med hensyn til behandlingens art og informasjonen som er tilgjengelig for databehandleren, og

d) hvis databehandleren får vite om noen slik klage, anmodning, påstand eller forespørsel, skal denne gi behandlingsansvarlig assistanse og fullt ut samarbeide med behandlingsansvarlig om å undersøke saken, inkludert, men ikke begrenset til, å gi behandlingsansvarlig

all relevant informasjon, utarbeide et svar, implementere avhjelpende tiltak og/eller samarbeide i gjennomføringen av og forsvaret mot eventuelle krav, rettslige eller regulatoriske prosesser. Behandlingsansvarlig skal være ansvarlig for å kommunisere med personer om deres personopplysninger i forbindelse med slike personvernsaker, med mindre behandlingsansvarlig bemyndiger databehandleren til å gjøre dette på dennes vegne. Databehandleren skal gjøre kommersielt og juridisk rimelige anstrengelser for å begrense arten og omfanget av den påkrevde utleveringen til den minste mengden personopplysninger som er påkrevd for å overholde gjeldende lovgivning. Hvis gjeldende lovgivning ikke forhindrer det, skal databehandleren gi behandlingsansvarlig skriftlig forhåndsvarsel om alle slike personvernsaker som er tilstrekkelig til at behandlingsansvarlig kan bestride rettslige, juridiske, administrative eller andre myndighetspålagte prosesser.

Hvis noen del av slik nødvendig bistand innebærer tidsbruk og utgifter utover det som kreves for å levere tjenestene, skal databehandleren og behandlingsansvarlig forhandle bona fide om hva som skal være rimelig kompensasjon for databehandlerens tidsbruk og utgifter i denne forbindelse. Dersom partene ikke kan bli enige, skal tvisteløsningsbestemmelsene i kontrakten komme til anvendelse.

8. OUTSOURCING TIL SEKUNDÆRBEHANDLERE

Databehandleren skal ikke outsource noen av tjenestene eller annen behandling av personopplysninger til noen tredjepart uten å gi to ukers skriftlig forhåndsvarsel til behandlingsansvarlig. I løpet av denne perioden skal behandlingsansvarlig ha rett til innsigelse, men kun bona fide og der dette er berettiget. Databehandleren skal da ha 60 dager på seg til å velge en alternativ underleverandør. Databehandleren kan bytte underleverandør uten forhåndsvarsel i nødstilfeller, men skal da umiddelbart varsle behandlingsansvarlig om dette og gi behandlingsansvarlig anledning til å fremme innsigelser mot dette i en periode på to uker.

Uavhengig av det foregående samtykker behandlingsansvarlig til og godtar at databehandleren outsourcer vertstjenestene til en tredjeparts leverandør av vertstjenester, i den grad en hensiktsmessig avtale er inngått med den aktuelle underleverandøren; denne avtalen kan omfatte EUs standardavtalevilkår eller andre kontraktsordninger som anført i punkt 13.

Databehandleren skal påse at sekundærbehandleren er bundet av de samme forpliktelsene til databeskyttelse og personvern som databehandleren er underlagt i henhold til denne DBA-en, skal føre tilsyn med at dette overholdes og skal pålegge sine sekundærbehandlere en plikt til å implementere egnede tekniske og organisatoriske sikkerhetstiltak som gjør at behandlingen innfrir kravene i gjeldende personvernlovgivning.

Databehandleren skal i alle tilfeller være fullt ut ansvarlig for tjenesteytingen til slike sekundærbehandlere som ikke oppfyller sine forpliktelser i henhold til denne DBA-en med hensyn til tjenestene.

9. REVISJON OG TILSYN

På anmodning fra behandlingsansvarlig og med minst 30 dagers forhåndsvarsel til databehandleren skal databehandleren gi behandlingsansvarlig en detaljert revisjonsrapport som er utarbeidet av databehandleren eller en tredjepart utpekt av databehandleren, for å dokumentere overholdelse med bestemmelsene i denne kontrakten og denne DBA-en.

Dersom det foreligger alvorlig tvil om nøyaktigheten av en slik revisjonsrapport, skal behandlingsansvarlig ha rett til å utføre revisjoner (eller få en tredjepart som har inngått en konfidensialitetsavtale med databehandleren, til å utføre revisjoner), for egen regning, av databehandlerens retningslinjer, prosesser og dokumentasjon som er knyttet til personopplysninger, for å bekrefte hvorvidt databehandleren overholder sine forpliktelser i henhold til kontrakten og denne DBA-en. Databehandleren skal samarbeide i forbindelse med slike tilsyn.

10. SIKKERHETSTILTAK

Databehandleren skal implementere – med i henhold til teknikkens stand, typen personopplysninger, kostnadene ved implementering og behandlingens art, omfang, kontekst og formål samt risikoen for varierende sannsynlighet og alvorlighetsgrad for rettighetene og frihetene til de registrerte, uten at det berører øvrige sikkerhetsstandarder som partene har blitt enige om – egnede tekniske og organisatoriske tiltak for å ivareta et sikkerhetsnivå for behandlingen av personopplysninger som er i samsvar med aktuell risiko. Disse tiltakene er beskrevet nærmere i vedlegg 2.

Partene erkjenner at sikkerhetskravene er i stadig endring, og at effektiv sikkerhet krever hyppig evaluering og regelmessige forbedringer av utdaterte sikkerhetstiltak. Databehandleren skal derfor evaluere tiltakene som er iverksatt i samsvar med dette punkt 10 på løpende basis, og vil modifisere disse tiltakene for å sikre overholdelse av kravene i dette punktet. Partene skal forhandle bona fide om eventuelle kostnader for implementering av vesentlige endringer som kreves i henhold til spesifikke oppdaterte sikkerhetskrav som er angitt i gjeldende personvernlovgivning eller vedkommende datatilsynsmyndigheter.

11. INFORMASJONSFORPLIKTELSER OG HENDELSESHÅNDTERING

Dersom databehandleren blir oppmerksom på en hendelse som har innvirkning på behandlingen av personopplysningene som er underlagt denne DBA-en og kontrakten, skal databehandleren umiddelbart – og innen 48 timer der dette er mulig – varsle behandlingsansvarlig om den aktuelle hendelsen, og skal samarbeide med behandlingsansvarlig og etterleve dennes instrukser i forbindelse med hendelsen, unntatt der dette er forbudt ved lov eller der hendelsen omfatter opplysningene til flere behandlingsansvarlige. Hvis hendelsen involverer personopplysningene til flere behandlingsansvarlige, skal databehandleren treffe rimelige tiltak for å undersøke forholdet, informere de behandlingsansvarlige og utbedre problemet. Dersom databehandleren ikke er i stand til å varsle om forholdet innen 48 timer, skal denne gi behandlingsansvarlig en forklaring på forsinkelsen som behandlingsansvarlig skal kunne dele med lovgivende og rettshåndhevende myndigheter.

Databehandleren skal til enhver tid ha på plass skriftlige prosedyrer for hendelsesrespons.

Alle henvendelser og varsler til behandlingsansvarlig i henhold til dette punkt 11.2 skal rettes til den ansatte hos behandlingsansvarlig som har sine kontaktopplysninger oppført i punkt 14.4 av denne DBA-en, og skal inneholde følgende:

a) en beskrivelse av hendelsens art, herunder (når dette er mulig) kategoriene av og omtrentlig antall berørte registrerte personer samt kategoriene av og omtrentlig antall personopplysninger som er berørt

b) navn og kontaktinformasjon til databehandlerens personvernombud eller et annet kontaktpunkt som kan gi mer informasjon

c) en beskrivelse av de sannsynlige konsekvensene av hendelsen

d) en beskrivelse av tiltakene som er iverksatt eller foreslått iverksatt av databehandleren for å håndtere hendelsen, herunder (der det er aktuelt) eventuelle tiltak for å redusere mulige negative konsekvenser

12. RETUR ELLER SLETTING AV PERSONOPPLYSNINGER

Ved denne DBA-ens opphør eller på skriftlig anmodning fra behandlingsansvarlig skal databehandleren etter databehandlerens avgjørelse enten slette, ødelegge eller returnere alle personopplysninger til behandlingsansvarlig, og destruere eller returnere eventuelle eksisterende kopier, med unntak av situasjoner der (i) slike personopplysninger er nødvendige for databehandleren for å oppfylle sine forpliktelser i henhold til denne DBA-en og/eller kontrakten eller gjeldende lov, eller (ii) retur eller destruksjon av opplysningene er forbudt i henhold til gjeldende lov.

Databehandleren skal varsle alle tredjeparter som støtter databehandlerens behandling av personopplysningene om DBA-ens eventuelle opphør, og skal påse at alle slike tredjeparter enten destruerer eller returnerer de aktuelle personopplysningene.

13. OVERFØRING AV PERSONOPPLYSNINGER

Databehandleren skal ha rett til å overføre eller tillate overføring av personopplysninger til mottakere utenfor EØS eller Sveits, underlagt bestemmelsene i punkt 13.2 nedenfor. For å unngå tvil, gjelder det foregående mutatis mutandis å få tilgang og tillate tilgang til personopplysninger som er lagret i EØS eller Sveits, for en person som befinner seg utenfor dette området.

Før overføringen eller tilgangen igangsettes, skal databehandleren utarbeide og signere adekvate kontraktsmessige ordninger for overføringen av personopplysninger til behandlere i tredjeland som ikke tilbyr et tilstrekkelig beskyttelsesnivå med hensyn til de registrertes rettigheter og friheter.

Uavhengig av det foregående skal databehandleren utveksle slike personopplysninger med ethvert av sine tilknyttede selskaper, i samsvar med Autronicas bindende virksomhetsregler, som er innlemmet i Carrier Global Corporation-konsernet og tilgjengelig på https://www.corporate.carrier.com/legal/privacy-notice/ .

14. ANNET

Dersom det foreligger avvik mellom bestemmelsene i denne DBA-en og bestemmelsene i kontrakten, skal bestemmelsene i denne DBA-en ha forrang.

Denne DBA-en er underlagt lovene i Nederland. Eventuelle tvister som måtte oppstå med utgangspunkt i eller i forbindelse med denne DBA-en, skal utelukkende behandles av en stedlig kompetent domstol i Amsterdam.

Hvis personvernlovgivningen endres, skal begge parter samarbeide med hverandre om å gjøre eventuelle påkrevde endringer i denne DBA-en. Behandlingsansvarlig skal sørge for at alle tredjeparter gjør de samme eller sammenlignbare endringer.

Enhver henvendelse i forbindelse med denne DBA-en skal sendes til CarrierHQ_Compliance@carrier.com.

VEDLEGG 1. OVERSIKT OVER BEHANDLINGSAKTIVITETER

1. DEN/DE REGISTRERTE

Den behandlingsansvarliges ansatte eller innleid personell samt sluttbrukere.

2. KATEGORIER AV PERSONOPPLYSNINGER

Følgende personopplysninger kan behandles av databehandleren, avhengig av hvilke personopplysninger behandlingsansvarlig vil innlemme i portalen:

- Når det gjelder den behandlingsansvarliges ansatte eller innleid personell:
  - Påloggingsinformasjon
  - Fornavn og etternavn
  - E-postadresse
  - Rolle/funksjon

- Når det gjelder sluttbrukere:
  - Stedsnavn
  - Boligadresse
  - Telefonnummer

3. BEHANDLINGSOPERASJONER

Personopplysningene nevnt ovenfor vil være gjenstand for følgende grunnleggende behandlingsaktiviteter:

- Databehandling, nettverk, lagring og innholdslevering.
- Teknisk støtte til portalen og relaterte produkter og tjenester, som beskrevet i kontrakten.

VEDLEGG 2. SIKKERHETSTILTAK

1. DATABEHANDLERENS ANSVAR

Databehandleren skal opprettholde et informasjonssikkerhetsprogram i samarbeid med underleverandøren sin, der det er aktuelt, som er designet med tanke på følgende:

1.1. sikre de registrertes personopplysninger mot utilsiktet eller ulovlig tap, innsyn eller avsløring

1.2. å identifisere interne risikoer for sikkerheten og uautorisert tilgang til nettverket som støtter vertstjenestene for portalen, programvaren eller de eksterne tjenestene, der disse risikoene med rimelighet kan forutses

1.3. å minimere sikkerhetsrisikoer, blant annet gjennom risikovurderinger og regelmessig testing

1.4. å sikre et tilstrekkelig beskyttelsesnivå med hensyn til personopplysningenes integritet, konfidensialitet og tilgjengelighet

2. FYSISKE TILGANGSKONTROLLER OG SIKKERHETSBESKYTTELSE

2.1. Fysiske sperringer skal være på plass for å hindre uautorisert tilgang til lokalene der personopplysningene lagres. For å kunne passere disse sperringene kreves det enten validering av tilgangskontroll eller validering av sikkerhetspersonell.

2.2. Alle tilgangspunkter til fasilitetene (med unntak av hovedinngangen) holdes låst og overvåkes med videoovervåkningskameraer. Fasilitetene er sikret med elektroniske systemer for inntrengningsdeteksjon, slik at eventuell uautorisert tilgang kan oppdages. Tilgangen til databehandlerens personell overvåkes og logges i sikkerhetssystemene.

2.3. Databehandlerens eventuelle underleverandører som leverer vertstjenestene er sertifisert i henhold til ISO 27001-standarden. Databehandleren skal minst en gang årlig evaluere underleverandørens overholdelse av vilkårene for denne sertifiseringen.

3. TILGANG OG INNSYN FOR DATABEHANDLERENS PERSONELL

3.1. Databehandleren skal kun gi innsyn i personopplysninger til de ansatte og innleid personell som har et legitimt tjenstlig behov for dette. Slikt personell hos databehandleren er pålagt taushetsplikt eller er underlagt en annen relevant lovfestet taushetsplikt.