Tillegg om databehandling, leverandører, Language Solutions (vedlegg 3)

Dette tillegget om databehandling (**«tillegget»**) er inngått mellom:

_____

(«leverandør» / «underleverandør»)

og

Semantix (**«kjøper»/«databehandler»**), altså selskapene som er oppført i leverandøravtalen, eller andre selskaper som er en del av Semantix-konsernets selskaper («Semantix»), og som av og til er inkludert i innkjøpsordre.

Leverandøren og kjøperen samtykker i at kjøperen fra tid til annen kan be leverandøren om å utføre tjenester som inkluderer personopplysninger. Personopplysningene er underlagt personvernlover som krever at både leverandøren og kjøperen behandler personopplysninger på en sikker og konfidensiell måte i samsvar med alle personvernlover.

Derfor har leverandøren og kjøperen avtalt følgende.

1. Definisjoner

I dette tillegget skal disse begrepene ha den betydningen som er angitt her:

«Behandlingsansvarlig» er den enheten som bestemmer formålet med behandling av personopplysninger samt hvordan de skal behandles. Behandlingsansvarlig er Semantix' kunde.

«Databehandler» er enheten som behandler personopplysninger på vegne av behandlingsansvarlig.

«Den registrerte» er en person som er eller kan bli identifisert, altså en person som kan identifiseres, direkte eller indirekte, spesielt ved å henvise til et ID-nummer eller til én eller flere faktorer som er spesifikke for vedkommendes fysiske, fysiologiske, mentale, økonomiske, kulturelle eller sosiale identitet.

«Tredjepart» er en person eller et selskap, en offentlig myndighet, et byrå eller en annen enhet enn den registrerte, behandlingsansvarlig, databehandler og personer som behandlingsansvarlig eller databehandler har gitt tillatelse til å behandle personopplysninger.

«Lover» er gjeldende lover om personopplysninger, personvern og sikkerhet, inkludert, men ikke begrenset til EUs personvernforordning 2016/679 og eventuelle tillegg, erstatninger eller fornyelser av denne, samt andre gjeldende bindende forskrifter, lover, forordninger og domsavsigelser om personopplysninger, personvern eller data, som gjelder ved behandling av personopplysninger basert på avtalen.

«Tredjeland» er land utenfor EØS eller andre land med personvernlovgivning som begrenser overføring av personopplysninger til enkelte land.

«Modellklausuler» er standard kontraktsklausuler som er vedlagt EU-kommisjonens implementeringsbeslutning 2021/914 av 4. juni 2021 om overføring av personopplysninger til tredjeland i henhold til forordning (EU) 2016/679 og eventuelle tillegg, erstatninger eller fornyinger av denne utført av EU-kommisjonen.

«Personopplysninger» er informasjon om den registrerte, som sendes til leverandøren, som leverandøren får tilgang til eller som leverandøren på andre måter behandler på vegne av kjøperen i henhold til tjenestene.

«Brudd på personvernet» er sikkerhetsbrudd som fører til utilsiktet eller ulovlig sletting, tap, endring, utlevering av eller tilgang til personopplysninger som overføres, lagres eller behandles på andre måter.

«Behandling» er enhver operasjon der leverandøren eller dennes underleverandører behandler personopplysninger, for eksempel innsamling, registrering, lagring, kombinering, organisering, endring, beregning, analyse, bruk, utlevering ved overføring, formidling eller sletting.

«Tjenester» er tjenestene og andre aktiviteter som leveres til eller utføres av eller på vegne av leverandøren for kjøperen i henhold leverandøravtalen.

«Tekniske og organisatoriske sikkerhetstiltak» er tiltak som beskytter personopplysninger mot utilsiktet eller ulovlig destruksjon eller utilsiktet tap, endring, uautorisert utlevering eller tilgang, særlig når behandlingen inkluderer overføring av data over et nettverk, samt mot alle andre ulovlige former for behandling.

«EØS» er det europeiske økonomiske samarbeidsområdet.

«GDPR (General Data Protection Regulation)» er EUs personvernforordning 2016/679.

«Leverandøravtale» er leverandøravtalen som er inngått mellom kjøperen (eller et datterselskap av denne) og leverandøren, sammen med eventuelle påfølgende innkjøpsordre, arbeidsordre eller arbeidserklæringer som er avtalt i forbindelse med tjenesten som leverandøren skal utføre for kjøperen eller en samarbeidspartner eller et datterselskap av denne.

«Begrenset overføring» betyr:

- en overføring av personopplysninger fra leverandøren til en underleverandør, eller mellom to virksomheter hos leverandøren
- tilfeller der slik overføring er forbudt i henhold til personvernlovgivningen hvis de ikke beskyttes som beskrevet i dette tillegget

2. Behandling av personopplysninger

Partene samtykker i at i forbindelse med dette tillegget er kjøperen databehandleren, og leverandøren er underleverandør for personopplysningene. Dette tillegget beskriver kravene for personopplysninger som behandles av leverandøren eller via leverandørens systemer i forbindelse med levering av tjenestene.

Vedlegg 1 beskriver partenes forståelse av personopplysningene som leverandøren skal behandle, i henhold til dette tillegget, som beskrevet i artiklene 28(3) og 28(4) i GDPR. Kjøperen skal informere leverandøren om endringer i vedlegg for å gjenspeile kjøperens faktiske bruk av tjenestene. Leverandøren skal ikke behandle personopplysninger med mindre leverandøren ber

om det på vegne av behandlingsansvarlig, bortsett fra hvis behandlingen er påkrevd av gjeldende lovgivning som leverandøren er underlagt. I slike situasjoner skal leverandøren i den grad lovgivningen tillater det, informere kjøperen om det juridiske kravet før personopplysningene behandles.

Leverandøren skal:

- overholde all relevant personvernlovgivning ved behandling av personopplysningene
- overholde skriftlige instruksjoner fra kjøperen eller tilsynsmyndigheten til leverandøren, for eksempel om behandling, beskyttelse og kryptering av personopplysninger
- bistå kjøperen når kjøperen ber om det, for å gjennomføre konsekvensutredninger for behandlingsaktiviteter og ved å konsultere tilsynsmyndigheten før behandling når konsekvensutredningen viser høy risiko

Hvis leverandøren mener at leverandøren ikke har tilstrekkelig informasjon eller annen informasjon når det gjelder hvordan behandling av personopplysninger på vegne av kjøperen skal gjøres, skal leverandøren sikre at slike instruksjoner eller slik informasjon innhentes fra kjøperen.

Vedlegg 1 til dette tillegget beskriver informasjon om behandling av personopplysninger i henhold til artiklene 28(3) og 28(4) i GDPR (og eventuelt tilsvarende krav i annen personvernlovgivning). Kjøperen kan foreta rimelige endringer i vedlegg 1 ved å varsle leverandøren om dette skriftlig innen rimelig tid.

3. Underleverandører

Leverandøren kan ikke utnevne, engasjere eller bruke ytterligere underleverandører til å behandle personopplysninger fra kjøperen.

4. Sletting eller retur av personopplysninger

Innen 90 dager etter å ha levert tjenester som inkluderer behandling av personopplysninger, skal leverandøren slette alle kopier av personopplysninger som leverandøren har fått fra kjøperen.

Leverandøren skal sikre at alle personopplysninger behandles konfidensielt, og at slike personopplysninger bare behandles når det er nødvendig for formålene som er beskrevet i den gjeldende lovgivningen.

5. Utlevering av data

Leverandøren skal varsle kjøperen umiddelbart om forespørsler fra offentlige myndigheter vedrørende tilgang til kjøperens personopplysninger, med mindre slik varsling er forbudt i henhold til gjeldende lovgivning. Leverandøren skal ikke svare på slike forespørsler uten å ha innhentet skriftlig tillatelse fra kjøperen først.

6. Overføring av personopplysninger

Leverandøren skal ikke overføre personopplysninger til tredjeland eller behandle personopplysninger i tredjeland uten å ha innhentet skriftlig tillatelse fra leverandøren. Hvis kjøperen godkjenner en slik overføring, skal leverandøren iverksette alle nødvendige tiltak (inkludert, men ikke begrenset til standard kontraktsklausuler) for å sikre at overføringen

utføres i henhold til all gjeldende personvernlovgivning, inkludert minimum EUs personvernlovgivning.

Hvis kjøperen godkjenner overføring til leverandøren, inngår kjøperen og kjøperens tilknyttede selskaper («dataeksportør» hver for seg) og leverandøren («dataimportør») en modul 3 standard kontraktsklausul for overføringen fra kjøperen eller kjøperens tilknyttede selskaper til leverandøren, underlagt GDPR.

Leverandøren skal ikke utføre begrenset overføring.

7. Sikkerhet

Semantix (kjøper) garanterer et minimumsnivå for sikkerheten til alle kundene. For å overholde lovgivningen må kjøperen kreve minimum samme sikkerhetsnivå fra leverandøren. Leverandøren skal alltid implementere og vedlikeholde egnede organisatoriske og tekniske tiltak for å beskytte personopplysningene, slik at all behandling utføres i henhold til lovgivningen og kjøperens skriftlige instruksjoner. Sikkerhetskravene beskrives ytterligere i vedlegg 1.

8. Rett til revisjon

Kjøperen kan be om revisjon av leverandørens sikkerhetsdokumentasjon og/eller en skriftlig rapport om leverandørens egenvurdering. Dette er den vanligste formen for revisjon.

Kjøperen (eller uavhengig tredjepart på vegne av kjøperen) kan revidere leverandørens og underleverandørenes behandlingsaktivitet i henhold til vedtatt revisjonsplan, forutsatt at det gis skriftlig varsel om dette tolv (12) dager i forveien. Hvis en revisjon avdekker at tjenestene ikke overholder dette vedlegget, leverandøravtalen eller lovene, skal leverandøren iverksette alle nødvendige tiltak, og selv dekke kostnadene, for å sikre at tjenestene overholder de gjeldende bestemmelsene. Kjøperen har rett til å kontrollere overholdelsen ved å gjennomføre en ny revisjon når som helst etter at tiltakene ble iverksatt.

Kjøperen skal dekke kostnadene for revisjonene.

Leverandøren skal overholde alle beslutninger fra tilsynsmyndigheten eller annen relevant myndighet i forbindelse med personopplysningene som behandles på vegne av kjøperen. Leverandøren skal også la aktuell myndighet gjennomføre kontroll av behandlingen.

9. Brudd på personvernet

Ved brudd på personvernet eller annen truende håndhevelse mot leverandøren i forbindelse med behandling av personopplysninger, skal leverandøren varsle kjøperen skriftlig og umiddelbart etter at bruddet ble avdekket, senest innen 24 timer.

- Med godkjenning fra kjøperen skal leverandøren arbeide for å løse problemet raskt og forhindre ytterligere tap.
- Leverandøren skal også varsle enkeltpersoner eller offentlige myndigheter, og varslene skal inneholde den lovpålagte informasjonen.
- Når kjøperen ber om det, skal leverandøren også gi nødvendig støtte til enkeltpersoner.

10. Den registrertes rettigheter

Hvis kjøperen ber om det for å overholde lovgivningen, skal leverandøren – til en rimelig pris – basert på leverandørens arbeid:

- umiddelbart gi kjøperen en kopi av enkeltpersoners personopplysninger i en lett lesbar form
- umiddelbart rette, blokkere eller slette enkeltpersoners personopplysninger
- umiddelbart gi kjøperen slik informasjon om behandlingen av personopplysninger i henhold til tillegget, som kjøperen med rimelighet kan be om
- gi de registrerte den informasjonen om behandlingen som kjøperen med rimelighet kan be om

Hvis en offentlig myndighet eller tredjepart ber om slik informasjon som følger av avsnittet over, skal leverandøren umiddelbart varsle kjøperen om forespørselen, og leverandøren og kjøperen skal sammen avtale egnet måte å gå videre på.

11. Skadesløsholdelse

Partene kan holdes ansvarlig i henhold til gjeldende personvernlovgivning.

12. Generelle vilkår

Dette vedlegget gjelder så lenge leverandøravtalen gjelder, og deretter så lenge det er nødvendig for at aktivitetene skal kunne fullføres når avtalen sies opp eller utløper. I den grad personopplysninger behandles av eller for leverandøren, uansett grunn, gjelder dette vedlegget fortsatt for slik behandling etter at leverandøravtalen er sagt opp eller utløpt, og så lenge slik behandling utføres.

Hvis leverandøren misligholder forpliktelsene i dette tillegget, anses det som et brudd på leverandøravtalen.

Forpliktelser som av natur skal gjelde etter at leverandøravtalen sies opp eller utløper, skal videreføres.

13. Annet

Ved avvik mellom vilkårene i dette vedlegget og i leverandøravtalen, er det vilkårene i dette vedlegget som gjelder. Endringer av dette vedlegget skal avtales skriftlig mellom partene.

Eventuelle endringer, fraskrivelser eller modifiseringer av dette tillegget gjelder bare hvis de gjøres skriftlig. Hvis noen av bestemmelsene i dette tillegget ikke er gyldige eller ikke kan håndheves, skal resten av avtalen fortsatt gjelde. Bestemmelsen som ikke er gyldig eller ikke kan håndheves, skal enten (i) endres etter behov for å sikre at den er gyldig og kan håndheves, samtidig som partenes intensjoner beholdes i så stor grad som mulig, eller hvis det ikke er mulig, (ii) tolkes som at delen som er ugyldig eller ikke kan håndheves, aldri har vært en del av avtalen.

Denne avtalen trer i kraft når partene har signert den. Ved avvik mellom vilkårene i denne avtalen og vilkårene i standard kontraktsklausuler, er det sistnevnte som har forrang.

Dette dokumentet signeres digitalt. Personen som signerer dette tillegget på vegne av leverandøren, bekrefter å ha rettigheter og myndighet til å gjøre det, og til å binde leverandøren til forpliktelsene som er angitt her.

Vedlegg 1: Beskrivelse av behandling og sikkerhetstiltak

Dette vedlegget inneholder enkelte opplysninger om behandling av personopplysninger i henhold til artiklene 28(3) og 28(4) i GDPR.

Innhold og varighet for behandlingen av personopplysninger

Innholdet som handler om aktiviteter knyttet til overføring av personopplysninger i disse klausulene, skal være som angitt i leverandøravtalen og i aktuelle innkjøpsordre, og det avhenger av hvilke tjenester kjøperen velger.

Behandlingens varighet er definert i innkjøpsordren som beskriver omfanget av tjenestene.

Art og formål med behandlingen av personopplysninger

Behandlingens art og formål er å levere tjenestene som fremgår av leverandøravtalen og eventuelle aktuelle innkjøpsordre, som oppsummert tidligere. Leverandøren skal oversette personopplysninger i dokumenter som kjøperens kunder overfører til kjøperen for oversettelse, inkludert, men ikke begrenset til HR-dokumenter, juridiske dokumenter, medisinske dokumenter og forretnings- og driftsdokumenter.

Kategoriene for registrerte som personopplysningene handler om

Kategoriene for registrerte som personopplysningene handler om, inkluderer, men er ikke begrenset til kjøperens kunders (og andre tredjeparters) ansatte, underleverandører, kunder (og deres ansatte, kunder, pasienter eller sluttbrukere) samt studiedeltakere.

Typer personopplysninger som behandles

De typene personopplysninger som behandles, inkluderer, men er ikke begrenset til navn, adresser, kontaktinformasjon, fødselsdato, sivilstatus, antall pårørende, nasjonalitet, helsestatus og -data, biometriske opplysninger, seksuell legning, religion eller politisk tro, rase, kjønn, etnisk bakgrunn, genetiske opplysninger, HR-opplysninger, hobbyer, yrker, opplysninger om brukeres atferd, loggdata og loggfiler, undersøkelsesdata, video- og fotoinformasjon, forsikringsopplysninger, betalingsinformasjon, kontonumre og/eller andre personopplysninger.

Sensitive personopplysninger (hvis det er aktuelt)

Personopplysningene som overføres, gjelder følgende sensitive personopplysninger (vennligst spesifiser): det er ingen begrensning for de potensielle kategoriene av opplysninger som overføres, og de kan inkludere rasemessig eller etnisk opprinnelse, politiske meninger, religiøs eller filosofisk tro eller fagforeningsmedlemskap, og behandlingen av genetiske opplysninger, biometriske opplysninger for å identifisere enkeltpersoner, opplysninger om helse eller opplysninger om enkeltpersoners seksualitet eller seksuelle legning.

Underleverandørens rettigheter og forpliktelser

Underleverandørens rettigheter og forpliktelser når underleverandøren opptrer på vegne av databehandleren, fremgår av avtalen.

Tekniske og organisatoriske tiltak

Tekniske sikkerhetstiltak skal inkludere alle tekniske sikkerhetskontroller som definert av leverandøren, i henhold til anbefalingene som definert i ISO/IEC 27000, som tilpasses til et egnet nivå, med hensyn til hvor sensitive personopplysningene er, de konkrete risikoene som finnes, tekniske muligheter samt kostnadene for å utføre tiltakene. Leverandøren skal begrense tilgang til personopplysningene til godkjent personell med egnet opplæring og godt definert «need to know»-grunnlag, og som er underlagt egnet taushetsplikt. Leverandøren skal også bruke tekniske og organisatoriske tiltak til å sikre at kjøperens personopplysninger ikke

behandles for andre formål (for eksempel for forskjellige kunder av leverandøren) og at personopplysningene behandles separat fra data fra leverandørens andre kunder.

Ved gjennomføring av tjenestene i henhold til avtalen skal leverandøren sikre at alle nødvendige forholdsregler blir iverksatt for å forhindre tap og endring av data, for å forhindre uautorisert tilgang til kjøperens IT-miljø, for å forhindre at det overføres virus til kjøperens systemer og for å forhindre uriktig tilgang til kjøperens IT-miljø og konfidensiell informasjon om kjøperen.