Databehandlingstillägg, leverantörer, Language Solutions (bilaga 3)

Detta databehandlingstillägg **(”tillägg”)** har ingåtts mellan

_____

(”Leverantör”/”underleverantör”)

och

Semantix **(”beställare”/”personuppgiftsbiträde”)**, dvs. de företag som anges i leverantörsavtalet, eller ett annat företag som ingår i Semantix-koncernen (”Semantix”) i enlighet med inköpsordern.

Leverantören och beställaren godkänner att beställaren ibland kan be leverantören att utföra tjänster som innefattar personuppgifter. Dessa personuppgifter omfattas av dataskyddslagstiftning, vilken kräver att leverantören och beställaren behandlar personuppgifter på ett säkert och konfidentiellt sätt och i enlighet med gällande dataskyddslagstiftning.

Leverantören och beställaren enas, med beaktande av de ömsesidiga skyldigheter som beskrivs häri, om följande.

1. Definitioner

I detta tillägg ska följande begrepp ha nedan angivna innebörder:

”Personuppgiftsansvarig” avser den juridiska person som bestämmer ändamål och metoder för behandlingen av personuppgifter. Personuppgiftsansvarig är Semantix kund.

”Personuppgiftsbiträde” avser den juridiska person som behandlar personuppgifter för den personuppgiftsansvariges räkning.

”Registrerad person” avser en identifierad eller identifierbar fysisk person, dvs. en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för den registrerades fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.

”Tredje part” avser en fysisk eller juridisk person, myndighet, institution eller annat organ som inte är den registrerade personen, personuppgiftsansvarig, personuppgiftsbiträde eller personer som, på uppdrag av den personuppgiftsansvarige eller personuppgiftsbiträdet, har befogenhet att behandla personuppgifter.

”Lagar” avser tillämpliga lagar avseende dataskydd, sekretess och säkerhet, inklusive utan begränsning Europaparlamentets och rådets allmänna dataskyddsförordning (EU) 2016/679 och alla ändringar, ersättningar eller förnyanden av den, samt andra tillämpliga bindande direktiv, lagar, föreskrifter och beslut om dataskydd, sekretess och datasäkerhet vid behandling av personuppgifter enligt avtalet.

"Tredjeland" avser alla länder utanför EES eller utanför något annat land med dataskyddslagar som begränsar överföringen av personuppgifter till vissa länder.

"Standardavtalsklausuler" avser de standardavtalsklausuler som bifogas till EU-kommissionens genomförandebeslut (EU) 2021/914 av den 4 juni 2021 om standardavtalsklausuler för överföring av personuppgifter till tredjeländer i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 och alla ändringar, ersättningar eller förnyanden av denna som införts av EU-kommissionen.

"Personuppgifter" avser all information om en registrerad person som skickas till leverantören, som leverantören får åtkomst till eller som på annat sätt behandlas av leverantören för beställarens räkning i samband med tjänsterna.

"Personuppgiftsincident" avser säkerhetsincidenter som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till personuppgifter som överförs, lagras eller på annat sätt behandlas.

"Behandling" avser alla åtgärder där leverantören, dess dotterbolag eller underleverantörer behandlar personuppgifter, t.ex. insamling, inspelning, lagring, sammanslagning, organisering, ändring, beräkning, analys, användning, röjande genom överföring, spridning, radering eller borttagning.

"Tjänster" avser de tjänster och andra aktiviteter som leverantören tillhandahåller eller utför eller som utförs på uppdrag av leverantören för beställaren i enlighet med leverantörsavtalet.

"Tekniska och organisatoriska säkerhetsåtgärder" avser de åtgärder som syftar till att skydda personuppgifter mot oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter, särskilt när behandlingen innefattar överföring av uppgifter över ett nätverk, och mot andra olagliga former av behandling.

"EES" avser Europeiska ekonomiska samarbetsområdet.

"GDPR" avser den allmänna dataskyddsförordningen (EU) 2016/679.

"Leverantörsavtal" avser det specifika leverantörsavtal som upprättats mellan beställaren (eller ett av beställarens dotterbolag) och leverantören, tillsammans med efterföljande inköpsorder, arbetsorder eller arbetsbeskrivning, i samband med tjänster som ska utföras av leverantören på uppdrag av beställaren, en filial eller ett dotterbolag till beställaren.

"Begränsad överföring" avser

- vidarebefordran av personuppgifter från leverantören till en underleverantör, eller mellan två av leverantörens företag; eller
- i de fall en sådan överföring, i varje enskilt fall, är otillåten enligt dataskyddslagstiftningen eftersom det skydd som överförda personuppgifter ska ha i enlighet med detta tillägg saknas.

2. Behandling av personuppgifter

Parterna bekräftar att beställaren är personuppgiftsbiträde och leverantören är underleverantör för ändamålen med det här tillägget. I detta tillägg anges de krav som gäller avseende personuppgifter som behandlas av leverantören eller i leverantörens system i samband med att tjänsterna tillhandahålls.

I bilaga 1 till detta tillägg beskrivs, för parternas vetskap, vilka personuppgifter som ska behandlas av leverantören enligt detta tillägg, i enlighet med vad som krävs enligt artikel 28.3 och 28.4 i den allmänna dataskyddsförordningen. Beställaren ska informera leverantören i de fall bilagan behöver ändras för att återspegla beställarens faktiska användning av tjänsterna. Leverantören ska endast behandla personuppgifter i enlighet med instruktioner från beställaren för den personuppgiftsansvariges räkning, såvida inte behandling krävs enligt tillämplig lagstiftning som leverantören omfattas av. I sådana fall ska leverantören, i den omfattning det är tillåtet enligt lag, informera beställaren om det rättsliga kravet innan uppgifterna behandlas.

Leverantören ska

- följa alla tillämpliga dataskyddslagar när personuppgifter behandlas.
- följa skriftliga instruktioner från beställaren eller dataskyddsmyndigheter som leverantören erhåller, t.ex. om hantering, skydd och kryptering av personuppgifter.
- bistå beställaren, på beställarens rimliga begäran, med konsekvensbedömningar av behandlingen av personuppgifter och med att rådgöra tillsynsmyndigheterna före behandlingen, i de fall konsekvensbedömningen indikerar en hög risk.

Om leverantören anser sig inte ha fått tillräckliga instruktioner eller tillräcklig annan information om hur personuppgifter ska behandlas för beställarens räkning, ska leverantören se till att sådana instruktioner eller sådan information inhämtas från beställaren.

I bilaga 1 till detta tillägg finns information om behandlingen av personuppgifter i enlighet med artikel 28.3 och 28.4 i den allmänna dataskyddsförordningen (och, i vissa fall, motsvarande krav i andra dataskyddslagar). Beställaren kan komma att införa rimliga ändringar av bilaga 1 som beställaren anser är nödvändiga genom att skriftligen meddela leverantören.

3. Anlita underleverantör

Leverantören har inte rätt att anlita eller använda underleverantörer för att behandla personuppgifter som tillhandahålls av beställaren.

4. Radera eller återlämna personuppgifter

Leverantören ska, inom 90 dagar efter att en tjänst som innefattar behandling av personuppgifter levereras, på ett säkert sätt radera alla kopior av personuppgifter som mottagits från beställaren.

Leverantören ska säkerställa att personuppgifter behandlas konfidentiellt och att personuppgifterna endast behandlas utifrån vad som är nödvändigt för de ändamål som beskrivs i tillämpliga lagar.

5. Röjande av personuppgifter

Leverantören ska omedelbart meddela beställaren om förfrågningar från myndigheter om åtkomst till beställarens personuppgifter, såvida inte sådant meddelande är förbjudet enligt tillämplig lag. Leverantören får inte svara på en sådan förfrågan utan att ha fått ett skriftligt godkännande från beställaren i förväg.

6. Överföring av personuppgifter

Leverantören får inte överföra till eller behandla personuppgifter i ett tredjeland utan skriftligt godkännande från beställaren. Om beställaren godkänner en sådan överföring ska leverantören vidta alla nödvändiga åtgärder (inklusive, men inte begränsat till, det som anges i standardavtalsklausulerna) för att säkerställa att överföringen sker i enlighet med tillämplig dataskyddslagstiftning, och åtminstone i enlighet med EU:s dataskyddslagstiftning.

Om beställaren godkänner en överföring till leverantören, går beställaren respektive beställarens dotterbolag (i rollen som ”uppgiftsutförare”) och leverantören (som ”uppgiftsinförare”) upp i modul tre i standardavtalsklausulerna med avseende på överföringen från beställaren eller beställarens dotterbolag till leverantören i enlighet med den allmänna dataskyddsförordningen.

Leverantören får inte utföra någon begränsad överföring.

7. Säkerhet

Semantix (beställaren) garanterar en miniminivå av säkerhet för alla sina kunder. Beställaren måste, för att följa lagen, kräva åtminstone samma säkerhetsnivå från leverantören. Leverantören ska alltid införa och underhålla lämpliga organisatoriska och tekniska åtgärder för att skydda personuppgifterna, så att all behandling sker i enlighet med lagstiftningen och beställarens skriftliga instruktioner. Säkerhetskraven beskrivs mer ingående i bilaga 1.

8. Rätt till granskning

Beställaren kan begära en granskning av leverantörens säkerhetsdokumentation och/eller en skriftlig rapport om egna bedömningar från leverantören. Detta är den vanligaste formen av granskning.

Beställaren (eller en oberoende tredje part för dennes räkning) kan granska leverantörens och dess underleverantörers behandlingsaktiviteter i enlighet med den godkända granskningsplanen efter skriftligt meddelande tolv (12) arbetsdagar i förväg. Om en granskning visar att tjänsterna inte uppfyller bestämmelserna i detta tillägg, leverantörsavtalet eller lagstiftningen ska leverantören vidta alla nödvändiga åtgärder på egen bekostnad för att säkerställa att tjänsterna uppfyller tillämpliga bestämmelser. Beställaren ska ha rätt att kontrollera efterlevnaden genom en ytterligare granskning när som helst efter att korrigerande åtgärder har införts.

Beställaren står för kostnaderna för granskningarna.

Leverantören ska följa alla beslut från Integritetsskyddsmyndigheten eller annan behörig myndighet i fråga om personuppgifter som behandlas på uppdrag av beställaren. Leverantören ska även tillåta behöriga myndigheter att genomföra tillsyn över den behandling som äger rum.

9. Personuppgiftsincident

Vid en personuppgiftsincident, eller annat hot om verkställighetsförfaranden mot leverantören med avseende på behandlingen av personuppgifter, ska leverantören meddela beställaren skriftligen så snart som leverantören får kännedom om detta, och under inga omständigheter senare än inom tjugofyra (24) timmar.

- Leverantören ska, med beställarens i förväg givna godkännande, se till att snabbt lösa problemet och förhindra ytterligare förluster.
- Leverantören ska även, om nödvändigt, meddela enskilda personer eller myndigheter om uppgifterna i enlighet med lagen.
- Leverantören ska också, efter begäran från beställaren, tillhandahålla lämpligt stöd till enskilda personer.

10. Den registrerades rättigheter

Om beställaren, för att efterleva lagen, begär något av följande, ska leverantören, till en rimlig kostnad som baseras på leverantörens faktiska arbete:

- utan dröjsmål tillhandahålla en kopia av de registrerade personernas personuppgifter i ett tydligt och läsbart format till beställaren
- utan dröjsmål korrigera, förhindra åtkomst till eller radera de registrerades personuppgifter
- utan dröjsmål förse köparen med sådan information om behandlingen av personuppgifter enligt bilagan som beställaren rimligen kan begära
- tillhandahålla registrerade personer, vars personuppgifter behandlas, med sådan information om behandlingen som beställaren rimligen kan begära.

Om en myndighet eller tredje part begär ut information som anges i avsnittet ovan, ska leverantören utan dröjsmål informera beställaren om denna begäran. Leverantören och beställaren ska i samråd komma överens om hur de ska gå vidare på ett lämpligt sätt.

11. Skadeersättning

Parterna ska bära ansvar i enlighet med tillämplig dataskyddslagstiftning.

12. Allmänna villkor

Detta tillägg ska fortsätta att gälla så länge som leverantörsavtalet är giltigt och under erforderlig tid efteråt för att aktiviteterna ska kunna slutföras när avtalet har sagts upp eller löpt ut. I den omfattning som personuppgifter behandlas av eller för leverantören, oavsett skäl, efter att avtalet har sagts upp eller löpt ut, ska tillägget fortsätta gälla för sådan behandling så länge som behandlingen pågår.

Om leverantören bryter mot sina skyldigheter enligt detta tillägg anses det vara ett allvarligt avtalsbrott.

Skyldigheter som på grund av sina egenskaper ska fortsätta vara giltiga när avtalet har sagts upp eller löpt ut, ska även fortsatt vara giltiga.

13. Övrigt

Om villkoren i tillägget respektive leverantörsavtalet skiljer sig åt, ska villkoren i detta tillägg gälla. Alla ändringar av detta tillägg ska godkännas skriftligen av båda parter.

Alla ändringar, undantag och modifieringar av detta tillägg är endast bindande om de har skett skriftligen. Om någon bestämmelse i detta tillägg är ogiltig eller ogenomförbar, ska återstoden av avtalet fortsätta gälla. Den ogiltiga eller ogenomförbara bestämmelsen ska antingen (i) ändras efter behov för att se till att den är giltig och genomförbar, samtidigt som parternas

avsikter bevaras så långt som möjligt eller, om det inte är möjligt, (ii) tolkas på ett sätt som om den ogiltiga eller ogenomförbara delen aldrig hade ingått i avtalet.

Detta avtal träder i kraft när det undertecknats av parterna. Om villkoren i avtalet och standardavtalsklausulerna skiljer sig åt, ska villkoren i det sistnämnda gälla.

Detta dokument undertecknas digitalt. Den person som skriver under detta tillägg för leverantörens räkning garanterar att denne har rätt och befogenhet att underteckna detta tillägg och förbinda leverantören att fullgöra de skyldigheter som anges häri.

Bilaga 1: Beskrivning av behandling och säkerhetsåtgärder

Denna bilaga innehåller information om behandling av personuppgifter i enlighet med artikel 28.3 och 28.4 i den allmänna dataskyddsförordningen.

Föremålet för behandlingen och behandlingens varaktighet

De aktiviteter som är relevanta för de uppgifter som överförs i enlighet med dessa bestämmelser ska vara de som anges i leverantörsavtalet och i relaterade inköpsorder och beror på vilken av tjänsterna som beställaren efterfrågar.

Varaktigheten för behandlingen anges i inköpsordern där tjänsternas omfattning anges.

Behandlingens art och ändamål

Behandlingens art och ändamål är att tillhandahålla de tjänster som anges i leverantörsavtalet och relaterade inköpsorder, såsom beskrivs ovan. Leverantören kommer att översätta personuppgifter som finns i dokument som beställarens kunder anlitar beställaren för att översätta, inklusive, men inte begränsat till, personalrelaterade dokument, juridiska dokument, medicinska dokument samt affärsrelaterade och driftsrelaterade dokument.

Kategorier av registrerade som personuppgifterna avser

De kategorier av registrerade som personuppgifterna avser innefattar, men är inte begränsade till: beställarens kunder (och andra tredje parter), anställda, leverantörer, klienter (och deras anställda, kunder, patienter eller slutanvändare) samt studiedeltagare.

Typer av personuppgifter som ska behandlas

De typer av personuppgifter som ska behandlas innefattar, men är inte begränsade till: namn, adresser, kontaktuppgifter, födelsedatum, civilstånd, antal anhöriga, nationalitet, hälsostatus och -uppgifter, biometriska uppgifter, sexuell läggning, religiös övertygelse, politiska åsikter, ras, kön, etniskt ursprung, genetiska uppgifter, personalrelaterade uppgifter, fritidsintressen, yrken, uppgifter om användarmönster, loggdata och loggfiler, enkätuppgifter, video- och fotoinformation, försäkringsuppgifter, betalningsuppgifter, kontonummer och/eller andra uppgifter som avser en identifierbar fysisk person.

Särskilda kategorier av personuppgifter (i tillämpliga fall)

Överförda personuppgifter kan utgöra följande särskilda kategorier (ange vilka): de potentiella kategorier av personuppgifter som överförs är obegränsade, men kan omfatta ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Underleverantörens skyldigheter och rättigheter

De skyldigheter och rättigheter som gäller för underleverantören, som agerar på uppdrag av personuppgiftsbiträdet, anges i avtalet.

Tekniska och organisatoriska åtgärder

Tekniska skyddsåtgärder ska omfatta alla tekniska säkerhetsåtgärder som definieras av leverantören, i enlighet med rekommendationerna i ISO/IEC 27000-serien (eller motsvarande) och anpassade till en lämplig nivå, med hänsyn till hur känsliga personuppgifterna är, de särskilda risker som förekommer, befintliga tekniska möjligheter och kostnaderna för att införa åtgärderna. Leverantören ska begränsa tillgången till personuppgifterna till behörig personal som har erforderlig utbildning och ett väl definierat behov och som är bundna att följa

tillämpliga sekretessförpliktelser. Leverantören ska även, genom tekniska och organisatoriska åtgärder, säkerställa att beställarens personuppgifter inte behandlas för andra ändamål (t.ex. för andra kunder till leverantören) och att personuppgifterna behandlas separat från uppgifter som rör andra kunder till leverantören.

Leverantören försäkrar att vidta, när tjänsterna utförs i enlighet med tillägget, alla nödvändiga försiktighetsåtgärder för att förhindra förlust och ändring av personuppgifter, obehörig åtkomst till beställarens IT-miljö, införande av virus i köparens system och otillbörlig åtkomst till beställarens IT-miljö och konfidentiella uppgifter om beställaren.