

Parter enligt huvudavtal Hädanefter benämnda som "Personuppgiftsansvarig", "Personuppgiftsbiträdet" eller "Parten" och kollektivt som "Parterna".

Inledning

Båda Parterna bekräftar att de undertecknade har fullmakt att ingå detta personuppgiftsbiträdesavtal ("Avtal"). Detta Avtal kommer att ingå i och reglera Behandlingen av Personuppgifter i följande tjänsteavtal ("Tjänsteavtal") mellan Parterna:

- Avtal om hantering av inkommande leverantörsfakturor
- Avtal om hantering av utgående kundfakturor

Eller endast ett av ovanstående tjänsteområden enligt tjänsteavtal.

Definitioner

Definitionen av Personuppgifter, Särskilda kategorier av Personuppgifter (Känsliga Personuppgifter), Behandling av Personuppgifter, Registrerad, Personuppgiftsansvarig och Personuppgiftsbiträde är densamma som används i gällande dataskyddslagstiftning, inklusive den allmänna dataskyddsförordningen (EU) 2016/679 (GDPR), av den 27 april 2016.

Omfattning

Avtalet reglerar Personuppgiftsbiträdets Behandling av Personuppgifter på uppdrag av Personuppgiftsansvarig och beskriver hur Personuppgiftsbiträdet ska säkerställa dataskydd, genom tekniska och organisatoriska åtgärder enligt gällande dataskyddslagstiftning, inklusive dataskyddsförordningen.

Syftet med Personuppgiftsbiträdets Behandling av Personuppgifter på uppdrag av Personuppgiftsansvarig är att uppfylla Tjänsteavtal och detta Avtal.

Detta Avtal har företräde framför eventuella motstridiga bestämmelser om Behandling av Personuppgifter i Tjänsteavtal eller i andra tidigare avtal som ingåtts mellan Parterna.

Personuppgiftsbiträdets skyldigheter

Personuppgiftsbiträdet får endast Behandla Personuppgifter på uppdrag av och i enlighet med Personuppgiftsansvarigs

instruktioner. Genom att ingå detta Avtal instruerar Personuppgiftsansvarig Personuppgiftsbiträdet att Behandla Personuppgifter på följande sätt: i) endast i enlighet med gällande lag, ii) för att uppfylla alla förpliktelser enligt Tjänsteavtal, iii) som vidare specificerat genom Personuppgiftsansvarigs normala användning av Personuppgiftsbiträdets tjänster och iv) på så sätt som anges i detta Avtal.

Personuppgiftsbiträdet har ingen anledning att tro att det finns lagstiftning som förhindrar att Personuppgiftsbiträdet följer de ovan angivna instruktionerna. Personuppgiftsbiträdet ska, efter att ha blivit medveten om det, informera Personuppgiftsansvarig i de fall Personuppgiftsansvarigs instruktioner eller behandling, enligt Personuppgiftsbiträdet, strider mot gällande dataskyddslagstiftning.

De kategorier av Registrerade och Personuppgifter som omfattas av Behandling i detta Avtal framgår av Appendix A.

Personuppgiftsbiträdet ska säkerställa konfidentialitet, integritet och tillgänglighet av Personuppgifter enligt den dataskyddslagstiftning som gäller för Personuppgiftsbiträdet. Personuppgiftsbiträdet ska genomföra systematiska, organisatoriska och tekniska åtgärder för att säkerställa en rimlig säkerhetsnivå, med hänsyn tagen till den senaste tekniken och implementationskostnader i förhållande till den risk som Behandlingen innebär, och typen av Personuppgifter som ska skyddas.

Personuppgiftsbiträdet ska bistå Personuppgiftsansvarig med lämpliga tekniska och organisatoriska åtgärder, så långt det är möjligt med hänsyn tagen till typ av Behandling och den informationen som är tillgänglig för Personuppgiftsbiträdet, för att uppfylla Personuppgiftsansvarigs skyldigheter enligt gällande dataskyddslagstiftning avseende förfrågningar från Registrerade och allmänt dataskydd enligt dataskyddsförordningen artikel 32-36.

Om Personuppgiftsansvarig behöver information om säkerhetsåtgärder, dokumentation eller annan information om hur Personuppgiftsbiträdet Behandlar Personuppgifter, och sådana förfrågningar innebär mer information eller bistånd än den standard som tillhandahålls av Personuppgiftsbiträdet för att följa gällande dataskyddslagstiftning som Personuppgiftsbiträde, kan Personuppgiftsbiträdet debitera Personuppgiftsansvarig för sådana ytterligare tjänster.

Personuppgiftsbiträdet och dennes personal ska säkerställa konfidentialitet av Personuppgifter som Behandlas under detta Avtal. Detta villkor gäller även efter att Avtalet upphört att gälla.

Personuppgiftsbiträdet ska, genom att skyndsamt och utan onödigt dröjsmål meddela Personuppgiftsansvarig, göra det möjligt för Personuppgiftsansvarig att uppfylla de rättsliga krav som gäller för information till relevanta dataskyddsmyndigheter och Registrerade rörande personuppgiftsincidenter.

Vidare ska Personuppgiftsbiträdet, i den utsträckning det är praktiskt möjligt och lagligt, meddela Personuppgiftsansvarig om;

i) förfrågningar om utlämnande av Personuppgifter som erhållits från en Registrerad

ii) förfrågningar från myndigheter, exempelvis Polisen, om utlämnande av Personuppgifter

Personuppgiftsbiträdet får inte svara direkt på förfrågningar från Registrerade utan medgivande från

Personuppgiftsansvarig. Personuppgiftsbiträdet får inte delge innehåll som berörs av detta Avtal eller Tjänsteavtalet till myndigheter som Polisen, inklusive Personuppgifter, med undantag för vad som är lagstadgat, exempelvis genom domstolsbeslut eller liknande beslut.

Personuppgiftsbiträdet har inte ägarskap till eller kontroll över huruvida och hur Personuppgiftsansvarig väljer att använda sig av eventuella tredjepartsintegrationer via Personuppgiftsbiträdets API, via direkt databaskoppling eller liknande. Ansvar för sådana integrationer med tredje part åligger uteslutande Personuppgiftsansvarig.

Personuppgiftsansvarigs skyldigheter

Genom att underteckna detta Avtal bekräftar Personuppgiftsansvarig att:

- Personuppgiftsansvarig har rättslig grund att Behandla och utlämna de aktuella Personuppgifterna till Personuppgiftsbiträdet (inklusive eventuella underbiträden som Personuppgiftsbiträdet använder).
- Personuppgiftsansvarig är ansvarig för riktigheten, integriteten, innehållet, tillförlitligheten och lagenligheten av de Personuppgifter som lämnats till Personuppgiftsbiträdet.
- Personuppgiftsansvarig har uppfyllt alla obligatoriska krav och skyldigheter att anmäla hos eller få tillstånd från relevanta myndigheter för Behandlingen av Personuppgifter.
- Personuppgiftsansvarig har fullgjort sina skyldigheter att tillhandahålla relevant information till Registrerade avseende Behandling av Personuppgifter enligt obligatorisk dataskyddslagstiftning.
- Vid användning av de tjänster som tillhandahålls av Personuppgiftsbiträdet under Tjänsteavtal får Personuppgiftsansvarig inte överföra några Känsliga Personuppgifter till Personuppgiftsbiträdet utan uttrycklig överenskommelse om detta i Appendix A till detta Avtal.

Användande av underbiträden och överföring av data

Som en del av leveransen av tjänster till Personuppgiftsansvarig, enligt Tjänsteavtal och detta Avtal, kan Personuppgiftsbiträdet använda sig av underleverantörer i rollen underbiträde. Sådana underbiträden kan vara andra företag inom Visma-koncernen eller externa underleverantörer (tredje part) inom eller utanför EU. Personuppgiftsbiträdet ska säkerställa att underleverantörer genom avtal samtycker till att åta sig ansvar som motsvarar de skyldigheter som anges i detta Avtal.

En översikt över underleverantörer med tillgång till Personuppgifter finns i Appendix B. Personuppgiftsansvarig kan begära mer detaljerad information om underleverantörer.

Om underleverantörerna finns utanför EU ger Personuppgiftsansvarig behörighet till Personuppgiftsbiträdet för att säkerställa lämpliga rättsliga grunder för överföring av Personuppgifter utanför EU på Personuppgiftsansvarigs uppdrag, genom att införa EU-standardavtalsklausuler eller överföra Personuppgifter i enlighet med Privacy Shield.

Personuppgiftsansvarig ska underrättas innan ändringar sker rörande underleverantörer som Behandlar Personuppgifter så att den Personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar. Om Personuppgiftsansvarig gör invändningar mot ny underleverantör ska Personuppgiftsbiträdet och Personuppgiftsansvarig granska dokumentationen för underleverantörernas efterlevnad av GDPR för att säkerställa uppfyllandet av gällande dataskyddslagstiftning.

Genom att underteckna detta Avtal accepterar Personuppgiftsansvarig att Personuppgiftsbiträdet generellt använder sig av underleverantörer på så sätt som beskrivs ovan.

Säkerhet

Personuppgiftsbiträdet har åtagit sig att tillhandahålla en hög säkerhetsnivå i sina produkter och tjänster. Personuppgiftsbiträdet tillhandahåller säkerhetsnivån genom organisatoriska, tekniska och fysiska säkerhetsåtgärder, i enlighet med kraven på informations-säkerhet som beskrivs i dataskyddsförordningen artikel 32. Vidare syftar det interna dataskyddsramverk som utvecklats av Visma-koncernen till att skydda konfidentialitet, integritet, korrekthet och åtkomst av Personuppgifter. Följande åtgärder är av särskild betydelse i detta avseende:

- Klassificering av Personuppgifter för att säkerställa genomförandet av säkerhetsåtgärder som motsvarar riskbedömning.
- Utvärdering av användning av kryptering och pseudonymisering som riskreducerande faktorer.
- Begränsning av tillgång till Personuppgifter till de som behöver behörighet för att fullgöra skyldigheterna i detta Avtal eller Tjänsteavtal.
- Användande av system som upptäcker, återställer, förhindrar och rapporterar personuppgiftsincidenter.
- Genomförande av säkerhetsanalyser för att bedöma kvaliteten i nuvarande tekniska och organisatoriska åtgärder för att skydda Personuppgifter, med beaktande av kraven i gällande dataskyddslagstiftning.

Revisionsrättigheter

Personuppgiftsansvarig har rätt att genomföra årlig revision av Personuppgiftsbiträdets uppfyllande av villkoren i Avtalet. Om lagstiftningen kräver det kan Personuppgiftsansvarig begära revisioner oftare.

För att begära en revision måste Personuppgiftsansvarig lämna in en detaljerad revisionsplan till Personuppgiftsbiträdet minst fyra veckor före det föreslagna revisionsdatumet med en beskrivning av revisionens omfattning, varaktighet och startdatum. Om tredje part ska utföra revisionen, måste båda Parterna godkänna tredje part. Om Behandlingen sker i ett "multitenant" miljö, ger Personuppgiftsansvarig Personuppgiftsbiträdet befogenhet, att av säkerhetsskäl, bestämma att revisioner ska utföras av en neutral tredjepartsrevisor som Personuppgiftsbiträdet väljer.

Om det begärda revisionsområdet är upptaget i en ISAE-, ISO- eller liknande granskningsrapport som utförts av en kvalificerad tredjepartsrevisor inom de föregående tolv månaderna, och Personuppgiftsbiträdet bekräftar att det inte finns några kända väsentliga förändringar i de åtgärder som granskats, accepterar Personuppgiftsansvarig denna granskningsrapport istället för att begära en ny revision av åtgärder som redan granskats.

Under alla omständigheter måste revisioner utföras under vanliga öppettider vid den aktuella anläggningen, med förbehåll för Personuppgiftsbiträdets regler, och får inte störa Personuppgiftsbiträdets affärsverksamhet i väsentlig grad.

Personuppgiftsansvarig står för eventuella kostnader som uppstår i samband med begärda revisioner. Hjälp från Personuppgiftsbiträdet som överstiger standardtjänsten som tillhandahålls av Personuppgiftsbiträdet och/eller Visma-koncernen för att följa gällande dataskyddslagstiftning, kommer att debiteras.

Varaktighet och uppsägning

Detta Avtal är giltigt så länge som Personuppgiftsbiträdet Behandlar Personuppgifter på uppdrag av Personuppgiftsansvarig enligt gällande Tjänsteavtal. Avtalet upphör automatiskt när Tjänsteavtal upphör att gälla. När Avtalet upphör kommer Personuppgiftsbiträdet

att radera eller återlämna Personuppgifter som Behandlas på uppdrag av Personuppgiftsansvarig, i enlighet med gällande klausuler i respektive Tjänsteavtal. Om inte annat avtalats skriftligen ska kostnaden för sådana åtgärder baseras på; i) timtaxa för Personuppgiftsbitrådets tid och ii) komplexiteten i den begärda processen. Personuppgiftsbitrådet kan behålla Personuppgifter efter att Avtalet har upphört, i den utsträckning det krävs enligt lag, med samma typ av tekniska och organisatoriska säkerhetsåtgärder som beskrivs i detta Avtal.

Ändringar och tillägg

Ändringar i denna bilaga ska inkluderas i ett ny Appendix till denna Bilaga och undertecknas av båda Parter för att vara giltigt. Om några villkor i detta Avtal blir ogiltiga, ska detta inte påverka återstående villkor. Parterna ska ersätta eventuella ogiltiga villkor med villkor som återspeglar syftet med ogiltiga villkor.

Appendix A - Kategorier av Personuppgifter och Registrerade

1. Kategorier av Registrerade och Personuppgifter som omfattas av Behandling i detta Avtal
 - a. Kategorier av Registrerade
 - i. kunds avtalsansvariga i kontakt med leverantör
 - ii. kunds supportpersonal i kontakt med leverantör
 - iii. kunds kontaktpersoner i kontakt med leverantör
 - iv. Leverantörers referenspersoner
 - b. Kategorier av Personuppgifter
 - i. Kontaktuppgifter såsom namn, telefonnummer, e-postadress, etc.
 - ii. Information om anställning såsom befattning, företagsnamn, etc.
2. Kategorier av Känsliga Personuppgifter (särskilda kategorier av personuppgifter) som omfattas av Behandling i detta Avtal

Det här avsnittet är endast relevant om Personuppgiftsbitrådet ska Behandla Känsliga Personuppgifter (angivna nedan) på uppdrag av Personuppgiftsansvarig som en del av respektive Tjänsteavtal. För att Personuppgiftsbitrådet ska kunna Behandla sådan information på Personuppgiftsansvarigs uppdrag, måste Personuppgiftsansvarig ange aktuella typer av Känsliga Personuppgifter nedan. Personuppgiftsansvarig är också ansvarig för att informera Personuppgiftsbitrådet, och ange nedan, om det finns ytterligare typer av Känsliga Personuppgifter enligt gällande dataskyddslagstiftning.

Personuppgiftsbitrådet ska på Personuppgiftsansvarigs uppdrag, Behandla information om:	Ja	Nej
ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse,		X
att en person har misstänkts för, åtalats för eller dömts för brott,		X
hälsainformation,		X
en persons sexualliv eller sexuell läggning,		X
medlemskap i fackförening,		X
genetiska uppgifter eller biometriska uppgifter som entydigt identifierar en person		X

Ansvar

Parterna är överens om och erkänner att vardera Parten är skyldig att själv ansvara för och betala sådan administrativ sanktionsavgift som ålagts Parten enligt dataskyddsförordningen. Part är vidare skyldig att erlagga sådant skadestånd till Registrerade som Part av behörig domstol ålagts att betala direkt till Registrerade. Ansvaret mellan Parterna regleras av ansvarsbestämmelser i respektive Tjänsteavtal.

Tillämplig lag och jurisdiktion

Detta Avtal är underkastat tillämplig lag och den jurisdiktion som anges i respektive Tjänsteavtal mellan Parterna.

Tillämplig lag och jurisdiktion

Detta Avtal är underkastat tillämplig lag och den jurisdiktion som anges i respektive Tjänsteavtal mellan Parterna.

APPENDIX B - Översikt över nuvarande underleverantörer

Partner	Behandling	Plats	Personuppgifter som delas och varför
Addonomy LTD	Del i basproduktionen	EU	Adressuppgifter till mottagare samt ev. personuppgifter som finns i inskickade leverantörsfakturer eller andra underlag. Data som krävs för att kunna leverera avtalad tjänst.
Microsoft		EU (Azure)	Namn och e-post på de som registrerar sig i våra system. Data som krävs för att kunna leverera avtalad tjänst.
Zendesk	Support via mail/chat	EU eller USA (Privacy Shield)	Namn och epost på den som upprättade ärendet samt ev. personuppgifter i själva ärendet. Att kunna fullgöra avtalad tjänst. För hantering av support- och för utvecklings-ärenden samt för intern-kommunikation och dokumentation.
Telia	Telefoni	EU	Namn, Telefonnummer. Att kunna fullgöra avtalad tjänst. Hantering av support- och för utvecklings-ärenden samt för löpande kommunikation före, under och efter avtalsperiod.
Microsoft	Office med mailhantering	EU (Azure)	Namn, Mail, Telefonnummer. För hantering av brev, avtal, mail, kalkyler, presentationer.
Visma Financial Solutions	Kravhantering	EU	Personuppgifter till kravansvarig samt, ev personuppgifter på kundfakturan. Att kunna fullgöra avtalad tjänst.
Evry	Printtjänst	EU	Ev. personuppgifter på kundfakturer. Att kunna fullgöra avtalad tjänst. Utskrift, distribution kundfakturer på papper.
Auth0	Login/Password	EU eller USA (Privacy Shield)	Användarnamn på konton

I syfte att ta betalt för våra tjänster

Partner	Behandling	Plats	Personuppgifter som delas och varför
Creditsafe	Kredit-information	(EU/ESS)	Firmatecknare, Namn. Företags/kreditinformation inför/under pågående avtalsrelation.
PE Accounting	ERP	EU	Ev. personuppgifter på kundfakturor. Att kunna fullgöra avtalad tjänst. Utskrift, distribution kundfakturor på papper.
Adobe	Avtalshantering	EU eller USA (Privacy Shield)	Kontaktinformation till avtalsparten och andra kontakter som berörs av avtalet, samt ev. personuppgifter i själva avtalet. Används vid avtalssignering vid tecknande eller förlängning av

Övrigt

Partner	Behandling	Plats	Personuppgifter som delas och varför
Upsales	CRM	EU	Namn, titel, telefonnummer, adress och e-postadress för användare med behörighet CFO, CEO, CTO. För att säkerställa korrekt kommunikation med våra
Pixie	SMS	EU	Mobiltelefonnummer för att skicka SMS. Att kunna fullgöra avtalad tjänst. Används för att skicka SMS internt samt till våra användare.

I syfte att leverera beställda tjänster

Underbiträden i lila text berörs endast om tjänsteavtalet innefattar inkommande Leverantörsfakturor.

Underbiträden i blå text berörs endast om tjänsteavtalet innefattar utgående kundfakturor.

Underbiträden i svart text berörs av samtliga tjänsteavtal.