Personuppgiftsbiträdesavtal

Version 1.2.1 (200102)

Innehållsförteckning

PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679[1]

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	**Personuppgiftsbiträde**
	Online Partner AB
Organisationsnummer	**Organisationsnummer**
	556566-5527
Postadress	**Postadress**
	Västberga Allé 60 126 30 Hägersten
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	**Kontaktperson för administration av detta personuppgiftsbiträdesavtal**
Namn: E-post: Tfn:	Namn: Fredrik Linnander E-post: fredrik@onlinepartner.se Tfn: 08-420 004 44
Kontaktperson för parternas samarbete om dataskydd	**Kontaktperson för parternas samarbete om dataskydd**
Namn: E-post: Tfn:	Namn: Fredrik Hedström E-post: hedstrom@onlinepartner.se Tfn: 08-420 004 08

2. DEFINITIONER

Utöver de begrepp som definieras i löptext, i detta personuppgiftsbiträdesavtal, ska dessa definitioner oavsett om de används i plural eller singular, i bestämd eller obestämd form, ha nedanstående innebörd när de anges med versal som begynnelsebokstav.

[1] Allmänna dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbiträdets Behandling av Personuppgifter för Den personuppgiftsansvariges räkning.

Behandling	En åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
Dataskyddslagstiftning	Avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den Behandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning.
Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.
Instruktion	De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen.
Logg	Logg är resultatet av Loggning.
Loggning	Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt detta PUB-avtal och som kan knytas till en enskild fysisk person.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de Personuppgifter som överförts, lagrats eller på annat sätt Behandlats.
Registrerad	Fysisk person vars Personuppgifter Behandlas.
Tredje land	En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).

Underbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning.

3. BAKGRUND OCH SYFTE

3.1 Med detta Personuppgiftsbiträdesavtal jämte Instruktioner och en eventuell förteckning över Underbiträden (nedan gemensamt ”PUB-avtalet”) reglerar den Personuppgiftsansvarige Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad stadgas i artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679 (”Dataskyddsförordningen”).

3.2 När PUB-avtalet utgör ett av flera avtalsdokument inom ramen för ett annat avtal benämns det andra avtalet ”Huvudavtalet” i PUB-avtalet.

3.3 För det fall något av det som stadgas i punkterna 1, 16, 17, 18.2, 19–22 i PUB-avtalet regleras på annat sätt i Huvudavtalet ska Huvudavtalets reglering ha företräde.

3.4 Hänvisningar i PUB-avtalet till nationell eller unionsrättslig lagstiftning, avser vid var tid tillämpliga bestämmelser.

4. BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

4.1 Den Personuppgiftsansvarige utser härmed Personuppgiftsbiträdet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.

4.2 Den Personuppgiftsansvarige ska ge skriftliga Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.

4.3. Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och vid var tid gällande Instruktioner.

5. DEN PERSONUPPGIFTSANSVARIGES ANSVAR

5.1 Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta Instruktioner så att Personuppgiftsbiträdet och eventuellt Underbiträde kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Huvudavtal i förekommande fall.

5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt Dataskyddslagstiftningen.

5.3 Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

6. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och Instruktioner samt att följa Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda Personuppgifterna mot alla slag av Behandlingar som inte är förenliga med PUB-avtalet, Instruktioner och Dataskyddslagstiftningen.

6.3 Personuppgiftsbiträdet åtar sig att säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.

6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt artikel 32–36 i Dataskyddsförordningen fullgörs och svara på begäran om utövande av den Registrerades rättigheter i enlighet med Dataskyddsförordningen, kap. III, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.

6.5 För det fall att Personuppgiftsbiträdet finner att Instruktioner är otydliga, i strid med Dataskyddslagstiftningen eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande Instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgiftsansvarige, tillfälligt upphöra med Behandlingen och invänta nya Instruktioner.

6.6 För det fall att den Personuppgiftsansvarige förser Personuppgiftsbiträdet med nya eller ändrade Instruktioner ska Personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den Personuppgiftsansvarige huruvida genomförandet av de nya Instruktionerna föranleder förändrade kostnader för Personuppgiftsbiträdet.

7. SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Dataskyddslagstiftningen för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas.

7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.

7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den Personuppgiftsansvarige, efter parternas tecknande av PUB-avtalet, ska betraktas som nya Instruktioner enligt PUB-avtalet.

7.4 Personuppgiftbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbiträdets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.

7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt Logga åtkomst till Personuppgifterna enligt PUB-avtalet i den utsträckning det krävs enligt Instruktionen. Loggar får gallras först fem (5) år efter Loggningstillfället om inte annat anges i Instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med Dataskyddslagstiftningen.

7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa Behandlingens säkerhet.

8. SEKRETESS/TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, såvida inte annat avtalats.

8.2. Personuppgiftsbiträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen.

8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende Behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvarige eller agera för den Personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende Behandlingen.

8.4 Om den Registrerade, tillsynsmyndighet eller tredje man begär information från Personuppgiftsbiträdet vilken rör Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om saken. Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas.

Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

9. GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål som en del av sina garantier, enligt artikel 28.1 i Dataskyddsförordningen, på den Personuppgiftsansvariges begäran kunna redovisa vilka tekniska och organisatoriska säkerhetsåtgärder som används för att Behandlingen ska uppfylla kraven enligt PUB-avtalet och artikel 28.3.h i Dataskyddsförordningen.

9.2 Personuppgiftsbiträdet ska minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.

9.3 Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet), följa upp att Personuppgiftsbiträdet uppfyller PUB-avtalets, Instruktionernas och Dataskyddslagstiftningens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska Personuppgiftsbiträdets efterlevnad av PUB-avtalet, Instruktioner och Dataskyddslagstiftningen. Den Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.

9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkterna 9.2–9.3, rätt att erbjuda andra tillvägagångssätt för granskning av Behandlingen, exempelvis granskning genomförd av oberoende tredje part. Den Personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska Personuppgiftsbiträdet ge den Personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

9.5 Personuppgiftbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet.

9.6 Personuppgiftsbiträdet ska tillförsäkra den Personuppgiftsansvarige rättigheter gentemot Underbiträdet vilka motsvarar den Personuppgiftsansvariges samtliga rättigheter gentemot Personuppgiftsbiträdet enligt punkten 9 i PUB-avtalet.

10. HANTERING AV RÄTTELSER OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbiträdets felaktiga Behandling ska Personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom trettio (30) dagar, från det att Personuppgiftsbiträdet mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt

radering får Personuppgiftsbiträdet endast utföra Behandling av den aktuella Personuppgiften som ett led i processen för rättelse eller radering.

10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka kan väntas påverka Behandlingen, ska Personuppgiftsbiträdet skriftligt informera den Personuppgiftsansvarige om detta i enlighet med vad stadgas om meddelanden i punkten 19 i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

11. PERSONUPPGIFTSINCIDENTER

11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt artikel 32.1.c i Dataskyddsförordningen.

11.2 Personuppgiftbiträdet åtar sig att med beaktande av Behandlingens art, och den information som Personuppgiftsbiträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Personuppgiftbiträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörigs Behandling och/eller åtkomst till Personuppgifterna.

11.3 Vid Personuppgiftsincident, vilken Personuppgiftbiträdet fått vetskap om, ska Personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå, tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.

Beskrivningen ska redogöra för:

1. Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
2. de sannolika konsekvenserna av Personuppgiftsincidenten, och
3. åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftincidentens potentiella negativa effekter.

11.4 Om det inte är möjligt för Personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkten 11.3 i PUB-avtalet, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

12. UNDERBITRÄDE

12.1 Personuppgiftsbiträdet äger rätt att anlita den eller de Underbiträden som framgår av bilagd förteckning över Underbiträden.

12.2 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt avtal med Underbiträdet som reglerar Behandlingen som Underbiträdet utför å den Personuppgiftsansvariges vägnar samt att endast anlita Underbiträden som ger tillräckliga garantier för att genomföra lämpliga tekniska och organisatoriska åtgärder så att Behandlingen uppfyller kraven i Dataskyddsförordningen. I fråga om dataskydd ska avtalet ålägga Underbiträdet samma skyldigheter som åläggs Personuppgiftsbiträdet i detta PUB-avtal.

12.3 Personuppgiftsbiträdet ansvarar fullt ut för Underbiträdets Behandling gentemot den Personuppgiftsansvarige.

12.4 Personuppgiftsbiträdet äger rätt att anlita nya underbiträden och ersätta befintliga underbiträden.

12.5 När Personuppgiftsbiträdet avser att anlita ett nytt eller ersätta ett befintligt Underbiträde ska Personuppgiftsbiträdet säkerställa Underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

1. Underbiträdets namn, organisationsnummer och säte (adress och land),
2. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
3. var Personuppgifterna ska behandlas.

12.6 Den Personuppgiftsansvarige äger rätt att inom trettio (30) dagar från dag för meddelande enligt punkten 12.5 invända mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde och att, med anledning av sådan invändning, säga upp detta PUB-avtal att upphöra i enlighet med vad stadgas i PUB-avtalet, punkten 17.4.

12.7 När Personuppgiftsbiträdet upphör med att anlita Underbiträdet ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om att det upphör med att anlita Underbiträdet.

12.8 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det avtal som reglerar Behandling av Underbiträdets Behandling av Personuppgifter enligt punkten 12.2.

13. LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.

13.2 Personuppgiftsbiträdet äger endast rätt att överföra Personuppgifter till Tredje land för Behandling (t.ex. service, support, underhåll, utveckling, drift eller liknande hantering) om den Personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat Instruktioner för detta ändamål.

13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkten 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.

14. ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

14.1 Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-avtalet, Instruktioner och/eller tillämplig bestämmelse i Dataskyddslagstiftningen ska artikel i 82 i Dataskyddsförordningen tillämpas.

14.2 Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.

14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Oaktat vad sägs i Huvudavtalet gäller detta PUB-avtal, punkterna 14.1 och 14.2, före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser Behandlingen.

15. LAGVAL OCH TVISTLÖSNING

15.1 För detta avtal gäller svensk rätt. Eventuell tolkning eller tvist i anledning av PUB-avtalet, som parterna inte kan lösa på egen hand, ska avgöras av svensk allmän domstol.

16. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

16.1 PUB-avtalet gäller från och med den tidpunkt PUB-avtalet undertecknats av båda parter och tillsvidare. Parterna äger ömsesidig rätt att säga upp PUB-avtalet att upphöra med trettio (30) dagars varsel.

17. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

17.1 Endera part i PUB-avtalet äger rätt att påkalla omförhandling av PUB-avtalet om motpartens ägarförhållanden ändras väsentligt eller om tillämplig lagstiftning, eller tolkningen av den, ändras på ett för Behandlingen avgörande sätt. Påkallande av omförhandling enligt första meningen innebär inte att PUB-avtalet till någon del upphör att gälla utan endast att en omförhandling om PUB-avtalet ska påbörjas.

17.2 Tillägg till, och ändringar i, PUB-avtalet ska vara skriftliga och undertecknade av båda parter.

17.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet och/eller Instruktioner ska parten utan dröjsmål meddela motparten om agerandet. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt PUB-avtalet till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.

17.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde, enligt detta PUB-avtal, punkten 12.6, har den Personuppgiftsansvarige rätt att säga upp PUB-avtalet att upphöra med omedelbar verkan.

18. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

18.1 Vid uppsägning av PUB-avtalet ska den Personuppgiftsansvarige utan onödigt dröjsmål begära att Personuppgiftsbiträdet överlämnar samtliga Personuppgifter till den Personuppgiftsansvarige eller raderar dem, enligt dennes önskemål. Om Personuppgifterna överlämnas ska det ske i ett öppet och standardiserat format. Med samtliga Personuppgifter avses alla Personuppgifter vilka har omfattats av Behandlingen samt annan tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

18.2 Överlämning och radering enligt PUB-avtalet, punkten 18.1, ska vara utförda senast trettio (30) dagar räknat från den tidpunkt uppsägning gjorts enligt detta PUB-avtal, punkten 16.1.

18.3 Behandling som utförs av Personuppgiftsbiträdet efter den tidpunkt som stadgas i punkten 18.2 är att betrakta som en otillåten Behandling.

18.4 Bestämmelser om sekretess/tystnadsplikt i punkten 8 enligt detta PUB-avtal ska fortsätta gälla även om PUB-avtalet i övrigt upphör av gälla.

19. MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

19.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas till respektive parts kontaktperson för PUB-avtalet.

19.2 Meddelanden om parternas samarbete om dataskydd, gällande Behandlingen, ska skickas till respektive parts kontaktperson för parternas samarbete om dataskydd.

19.3 Meddelanden inom ramen för PUB-avtalet och Instruktioner ska skickas skriftligt. Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

20. KONTAKTPERSONER

20.1 Parterna ska utse var sin kontaktperson för PUB-avtalet.

20.2 Parterna ska utse var sin kontaktperson för parternas samarbete om dataskydd.

21. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

21.1 Varje part ansvarar för att de uppgifter som anges i punkten 1 i PUB-avtalet alltid är aktuella. Ändring av uppgifter i punkten 1 ska meddelas skriftligen enligt punkten 19.1 i PUB-avtalet.

22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt tecknande eller i pappersformat för tecknande med penna. Om PUB-avtalet tillhandahålls i digitalt format utgår punkter 22.2–22.3.

22.2 Den Personuppgiftsansvariges undertecknande av PUB-avtalet

Ort Datum

.....

Undertecknande

.....

Namnförtydligande

22.3 Personuppgiftsbiträdets undertecknande av PUB-avtalet

Ort Datum

Hägersten

.....

Undertecknande 

.....

Namnförtydligande **Fredrik Linnander**

Versionshantering

Version	Datum	Förändringar	Ansvarig
1.1	2018-12-19	10.1, 14.1, 18.2,	PR
1.2	2019-12-17	2, 3.1, 3.3, 5.1, 6.3, 6.4, 7.1, 8.2, 9.1, 9.2, 9.6, 10.1, 10.2, 11.4, 12, 13.3, 14.2, 14.3, 17.3, 17.4, 18.2, 18.3, 18.4, 21.1, 22.1	NE
1.2.1	2020-01-02	17.4	PR

Bilaga 1. Behandlingsbeskrivning

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även följa nedanstående Instruktion:

1. Ändamål, föremålet och arten
Systemet i sig är till för en säker provsituation, att genomföra prov digitalt men omöjliggöra fusk genom surf på webben och liknande.
2. Behandlingen omfattar följande typer av Personuppgifter
Följande kategorier kan förekomma i behandlingen av personuppgifter. 1. *Personuppgifter hänförliga till den Personuppgiftsansvariges personal, i huvudsak kontaktuppgifter;* *Namn, efternamn, E-postadress, Gruppmedlemskap, Publik IP-adress* 2. *Personuppgifter hänförliga till den Personuppgiftsansvariges elever, i huvudsak kontaktuppgifter; och* *Namn, efternamn, E-postadress, Gruppmedlemskap, Publik IP-adress*
3. Behandlingen omfattar kategorier av Registrerade
Kategorierna av registrerade inkluderar den Personuppgiftsansvariges: 1. *Personal;* 2. *Elever*
4. Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena
● *Gallringstiden för systemet ChromEx är 2 år.*
5. Ange särskilda tekniska och organisatoriska säkerhetsåtgärder vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena
Personuppgiftsbiträdet och ev. underbiträden ska, vidta tekniska, administrativa och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripande; 1. *pseudonymisering och kryptering av personuppgifter,* 2. *förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos informationssystemet samt e-tjänster,* 3. *förmågan att återställa tillgänglighet och tillgång till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, och* 4. *ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.*

6. Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem

Personuppgiftsbiträdet och Underbiträden ska ansvara för att,

- *det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en registrerad person,*
- *det av loggarna framgår vid vilken enhet åtgärderna vidtagits,*
- *det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,*
- *användarens och den registrerades identitet framgår av loggarna,*
- *systematiska och återkommande stickprovskontroller av loggarna görs, och*
- *kontroller av loggarna dokumenteras.*
- *Serverloggar sparas i 30 dagar. (Ex. användare X kallade på API Y)*
- *Auditloggar sparas i 400 dagar. (Ex. konto X gjorde operation Y i produkt Z)*

7. Lokalisering och överföring av Personuppgifter till Tredje land

Som en del av Personuppgiftsbiträdets fullgörande av tjänsterna som levereras enligt Tjänsteavtalet kan avidentifierade personuppgifter relaterade till supportärenden samt personuppgifter i form av kontaktuppgifter såsom namn, telefonnummer och e-postadress hänförliga till den Personuppgiftsansvariges personal komma att föras över till Personuppgiftsbiträdets underleverantör, se Bilaga 2.

- *Personuppgiftsbiträdet ska säkerställa att överföring till tredje land uppfyller dataskyddsförordningens krav. Se bilaga 3.*

8. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av biträdet/biträdena

Bilaga 3 och de skyddsåtgärder som där presenteras kommer att revideras och uppdateras när EDPB (European Data Protection Board) och/eller Datainspektionen presenterar riktlinjer för vilka säkerhetsåtgärder som ska vidtas i relation till EU-domstolens dom i mål nr C-311/18, "Schrems II".

Bilaga 2 - Underbiträdeslista för applikationen ChromEx

Underbiträde: Google Cloud Platform	**Kontaktinformation**: Privacy Help Center - Policies Help
Geografisk placering och avtal: Servrar inom EU/EES Frankfurt. (Kan komma att behandlas utomlands vid specifika tillfällen. Se Bilaga 3.) Our Cloud Data Privacy Commitments Google Cloud Platform: EU Model Contract Clauses	**Typ av tjänst:** Drift av databas och applikationer. (Molntjänst)
Används av följande tjänster: ChromEx Chrome-tillägg, ChromEx lärarpanel, ChromEx elevapp	**Data som behandlas:** Namn, e-postadresser, grupper, Publik IP-adress

Underbiträde: Google Fonts (Google Ireland Limited)	**Kontaktinformation**: Privacy Help Center - Policies Help
Geografisk placering och avtal: Irland (Kan komma att behandlas utomlands vid specifika tillfällen. Se Bilaga 3.) Privacy Policy – Privacy & Terms – Google	**Typ av tjänst:** **Distributionsnätverk av bl.a typsnitt** Enbart ett publikt IP-nummer används för att hantera statistik.Google fonts är en tjänst som är helt separerat från Google eller G Suite. Ingen användardata som finns i t.ex. Gmail eller andra tjänster som tillhandahålls av Google används av Google Fonts.
Används av följande tjänster: ChromEx Chrome-tillägg, ChromEx lärarpanel, ChromEx elevapp	**Data som behandlas:** Publik IP-adress

Underbiträden för applikationen ChromEx avseende specifika tjänster och avtal

Underbrität: Zendesk	**Kontaktinformation**: Zendesk's Global Privacy Counsel: Rachel Tobin, AGC, EMEA & Global Privacy Counsel, Zendesk International Ltd. 55 Charlemont Place, Saint Kevin's, Dublin, D02 F985 Ireland

	privacy@zendesk.com
Geografisk placering och avtal: EU, USA Privacy Policy Update on Privacy Shield Invalidation by the European Court of Justice	**Typ av tjänst:** Supportsystem för att hantera och besvara förfrågningar från kunder.
Används av följande tjänster: Support på Online Partner	**Data som behandlas:** Förnamn, Efternamn, E-postadress

Bilaga 3- Ytterligare skyddsåtgärder för att säkerställa standardavtalsklausuler (Standard Contract Clauses) vid överföring till tredje land avseende ChromEx

Utifrån domslutet den 16 juli 2020 "Schrems II" (Case C-311/18) gäller inte längre Privacy Shield som laglig grund för behandling av personuppgifter som överförs till USA. Företag som behöver överföra personuppgifter till USA måste numera ingå så kallade Standard Contractual Clauses samt lämpligen vidta ytterligare skyddsåtgärder. Detta dokument beskriver vilka ytterligare skyddsåtgärder vi som företag (Online Partner AB) vidtagit för att ytterligare skydda personuppgifter vid behandling i USA.

Detta dokument och skyddsåtgärder kommer att revideras och uppdateras när EDPB (European Data Protection Board) och/eller Datainspektionen presenterar riktlinjer för vilka säkerhetsåtgärder som ska vidtas.
(https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en)

Online Partner har noterat att följande tjänster och underbiträden innebär eller kan innebära överföring till USA. Online Partner har övervägt och analyserat för det fall applikationen ChromEx kan tillhandahållas utan nedanstående tjänster. Efter analys på marknaden och av tjänstens syfte och innehåll har det konstaterats att tjänsterna är nödvändiga för att kunna tillhandahålla ChromEx till våra kunder och användare. Online Partner har därför analyserat tjänsterna och vidtagit ytterligare skyddsåtgärder.

1 GENERELLA ORGANISATORISKA SÄKERHETSÅTGÄRDER PÅ ONLINE PARTNER

1.1 Kontohantering på Online Partner

Personal på Online Partner får vid tillträde av sin tjänst ett konto i G Suite som används som en SSO-tjänst gentemot alla andra applikationer som används i företaget. För att kunna logga in på sitt G Suite konto på Online Partner måste alla medarbetare använda den av företagets bestämda policy för tvåfaktorsinloggning. Utöver den specifika arbetstagaren är det endast en administratör som kan återställa ett konto för att komma åt personuppgifter. Denna administratör hanteras med ett no-reply konto som har en fysisk tvåfaktorsinloggning på ett USB inlåst på vår VD:s kontor.

1.2 Tillgång till användares persondata på Online Partner

På Online Partner arbetar vi efter premissen att enbart de personer som på grund av sina arbetsuppgifter har i uppdrag att hantera användares persondata har tillgång till personuppgifterna. Detta innebär att det endast är personal för varje specifik tjänst som

har tillgång till personuppgifterna. Personalen har sekretessåtaganden avseende de personuppgifter som behandlas.

1.3 **Fysiska enheter på företaget**

Alla enheter som används på Online Partner använder senaste säkerhetsuppdateringar samt kryptering av hårddisk. Tjänsterna som används är molnbaserade och skyddas utav ett extra lager med tvåfaktorsinloggning. Se “Kontohantering på Online Partner 1.1”

1.4 **Skalskydd på företaget**

Kontoret är beläget på andra och tredje våningsplan och nås endast från trapphuset och brandstege på baksidan. Ytterdörren till lokalen är av märket Dalloc och i stål, den är klassad enligt SSF Certifkat C95-337 Klass 2.

Dörren har två separata låsanordningar nattlås och dagslås, daglåset kan öppnas utifrån med nyckel och inifrån via vred alternativt elektronisk fjärröppning från majoriteten av arbetsrummen.

1.5 **Tillgång till användares persondata på Online Partner**

På Online Partner arbetar vi efter premissen att enbart de personer som på grund av sina arbetsuppgifter har i uppdrag att hantera användares persondata har tillgång till personuppgifterna. Detta innebär att det endast är personal för varje specifik tjänst som har tillgång till personuppgifterna. Personalen har sekretessåtaganden avseende de personuppgifter som behandlas.

1.6 **Fysiska enheter på företaget**

Alla enheter som används på Online Partner använder senaste säkerhetsuppdateringar samt kryptering av hårddisk. Tjänsterna som används är molnbaserade och skyddas utav ett extra lager med tvåfaktorsinloggning. Se “Kontohantering på Online Partner 1.1”

1.7 **Skalskydd på företaget**

Kontoret är beläget på andra och tredje våningsplan och nås endast från trapphuset och brandstege på baksidan. Ytterdörren till lokalen är av märket Dalloc och i stål, den är klassad enligt SSF Certifkat C95-337 Klass 2.

Dörren har två separata låsanordningar nattlås och dagslås, daglåset kan öppnas utifrån med nyckel och inifrån via vred alternativt elektronisk fjärröppning från majoriteten av arbetsrummen.

1.8 **Inbrottslarm**

Vi har ett inbrottslarm kopplat till Bevakningsassistans Stockholm, som skickar ut väktare vid larm.

1.9 Kameraövervakning

Online Partner har kameraövervakning på inträdespunkter till kontoret.

2 Personuppgiftsbiträden för applikationen ChromEx

2.1 Google Cloud Platform

2.1.1 Analys av eventuell överföring till tredje land

Vilket land utanför EU kan uppgifter skickas till?

I undantagsfall USA.

När kan personuppgifter komma att överföras till USA?

Google Cloud kan komma att behandla personuppgifter utanför EU genom tjänsten Firebase Hosting. Firebase Hosting medför en global edge caching som styrs utifrån vilket land du fysiskt befinner dig i när du använder ChromEx. Edge cachingen fungerar på så sätt att den väljer den närmaste servern utifrån din geografiska placering. De servrar som hanterar Firebase Hosting när tjänsten används inom EU finns i Zurich (europe-west6) och Frankfurt (europe-west3). Nämnda servrar kommer att vara de naturliga servrarna när tjänsten används i Sverige. Europe-west3 är också den server som vi driftar våra andra delar av Google Cloud på grund av dess geografiska närhet. Detta innebär att den enda troliga gången som personuppgifter kan komma att överföras till USA är för det fall användaren befinner sig utanför EU. Syftet med vår tjänst är att den ska användas i Sverige varför Online Partner ser att överföring till USA endast kommer att ske i mycket begränsad omfattning.

Enligt FISA och Cloud Act kan amerikanska staten begära ut personuppgifter från europeiska medborgare i relation till grov brottslighet om det sker någon behandling i USA.

Mer information kring Firebase Hosting finns att läsa här:

https://firebase.google.com/support/privacy

Typ av personuppgifter relaterade till Google Cloud Platform

e-post, förnamn, efternamn, gruppmedlemskap, IP-adress

Vilka personuppgifter kan komma att överföras till USA

Den enda personuppgift som delas med Firebase Hosting när användaren befinner sig utanför EU är ett publikt IP-nummer.

2.1.2 Ytterligare skyddsåtgärder

Googles Globala skyddsåtgärder:

Google har en global infrastruktur designad för att säkert hantera information i hela dess livscykel. Denna infrastruktur möjliggör säker driftsättning av tjänster, säker lagring av data, säker kommunikation mellan tjänster, säker kommunikation mellan tjänster och slutanvändarna, och säker administration av tjänster. Google använder denna infrastruktur för att bygga sina tjänster såsom G Suite och Google Cloud.

Säkerheten i infrastrukturen är byggd från grunden i progressiva lager som börjar med säkerheten för Googles datacenter till processerna för administrationen av tjänsterna.

Google investerar mycket i säkerheten av sin infrastruktur och har hundratals anställda ingenjörer dedikerade till att underhålla och förbättra både säkerheten och sekretessen inom hela Google.

Läs mer om Googles säkerhetsåtgärder här:
https://cloud.google.com/security/infrastructure/design

Säkerhetsåtgärder som Online Partner vidtagit utöver Googles egna säkerhetsåtgärder

Begränsning av åtkomst till data

Online Partner har sedan tidigare begränsat all åtkomst till data och personuppgifter i Google Cloud Platform. Det är endast personal med direkt behov som har tillgång till personuppgifterna. Detta för att kunna utföra sina arbetsuppgifter så att våra användare får bästa servicenivå av tjänsten ChromEx. Personalen har sekretessåtaganden avseende de personuppgifter som behandlas.

Audit loggar

Online Partner sparar audit loggar av administrativa händelser och åtkomst av data i Google Cloud Platform. Detta för att kunna hantera eventuella incidenter av personuppgifter.

Krypterad nätverkskommunikation

Online Partner använder sig av krypterade kommunikationsprotokoll mellan tjänst till tjänst och tjänst till slutanvändaren.

Inloggning av slutanvändare med Single Sign On

Online Partner använder sig av den öppna industristandarden OpenID Connect 2.0 som tillåter användarna att återanvända deras befintliga konton för Single Sign On.

Dokumentation i relation till SCC (Standard contract clauses)
https://cloud.google.com/terms/eu-model-contract-clause
https://cloud.google.com/security/privacy

2.2 Google Fonts

2.2.1 Analys av eventuell överföring till tredje land

Vilket land utanför EU kan uppgifter skickas till?

I undantagsfall USA.

När kan personuppgifter komma att överföras till USA?

Google Fonts kan komma att behandla personuppgifter utanför EU. Google Fonts använder sig av global edge caching som styrs utifrån vilket land du fysiskt befinner dig i när du använder ChromEx. Edge cachingen fungerar på så sätt att den väljer den närmaste servern utifrån din geografiska placering. Servrar inom EU kommer att vara de naturliga servrarna när tjänsten används i Sverige. Syftet med vår tjänst är att den ska användas i Sverige varför Online Partner ser att överföring till USA endast kommer att ske i mycket begränsad omfattning.

Enligt FISA och Cloud Act kan amerikanska staten begära ut personuppgifter från europeiska medborgare i relation till grov brottslighet mot USA om det sker någon behandling i USA.

Mer information kring Google fonts och dess behandling av data:

https://developers.google.com/fonts/faq2#what_does_using_the_google_fonts_api_mean_for_the_privacy_of_my_users

Typ av personuppgifter relaterade till Google Fonts:

Publik IP-adress

Vilka personuppgifter kan komma att överföras till USA

Den enda personuppgift som skulle kunna skickas via Google Fonts är ett publikt IP-nummer. Google fonts är helt separerat från Google eller G Suite. Ingen användardata som finns i t.ex. Gmail eller andra tjänster som tillhandahålls av Google används av Google Fonts. Enbart ett publikt IP-nummer används för att hantera statistik.

2.2.2 Ytterligare skyddsåtgärder

Googles Globala skyddsåtgärder:

Google har en global infrastruktur designad för att säkert hantera information i hela dess livscykel. Denna infrastruktur möjliggör säker driftsättning av tjänster, säker lagring av data, säker kommunikation mellan tjänster, säker kommunikation mellan tjänster och slutanvändarna, och säker administration av tjänster. Google använder denna infrastruktur för att bygga sina tjänster såsom G Suite och Google Cloud.

Säkerheten i infrastrukturen är byggd från grunden i progressiva lager som börjar med säkerheten för Googles datacenter till processerna för administrationen av tjänsterna.

Google investerar mycket i säkerheten av sin infrastruktur och har hundratals anställda ingenjörer dedikerade till att underhålla och förbättra både säkerheten och sekretessen inom hela Google.

Läs mer om Googles säkerhetsåtgärder här:

https://cloud.google.com/security/infrastructure/design

Säkerhetsåtgärder som Online Partner vidtagit utöver Googles egna säkerhetsåtgärder

Begränsning av åtkomst till data

Online Partner har sedan tidigare begränsat all åtkomst till data och personuppgifter i Google Fonts. Det är endast personal med direkt behov som har tillgång till personuppgifterna. Detta för att kunna utföra sina arbetsuppgifter så att våra användare får bästa servicenivå av tjänsten ChromEx. Personalen har sekretessåtaganden avseende de personuppgifter som behandlas.

Dokumentation i relation till SCC (Standard contract clauses)

https://policies.google.com/privacy

3 PERSONUPPGIFTSBITRÄDEN FÖR APPLIKATIONEN CHROMEX AVSEENDE SPECIFIKA TJÄNSTER OCH AVTAL

3.1 Zendesk

3.1.1 Analys av eventuell överföring till tredje land

Vilket land utanför EU kan uppgifter skickas till?

USA

När kan personuppgifter komma att överföras till USA?

Supportsystem för att hantera och besvara förfrågningar från användare. Det innebär att Zendesk endast används vid supportärenden inte vid användning av applikationen. Alla som mailar in till Online Partner Support samtycker att dess personuppgifter behandlas i relation till Zendesk användaravtal.

Enligt FISA och Cloud Act kan amerikanska staten begära ut personuppgifter från europeiska medborgare i relation till grov brottslighet mot USA.

Typ av personuppgifter relaterade till Zendesk

Förnamn, Efternamn, E-postadress

Vilka personuppgifter kan komma att överföras till USA

Förnamn, Efternamn, E-postadress

Dokumentation i relation till ECC/SCC (EU/Standard contract clauses)
https://www.zendesk.com/company/privacy-and-data-protection/#gdpr-sub

3.1.2 Ytterligare skyddsåtgärder

Zendesks skyddsåtgärder

Zendesk är certifierat enligt SOC 2 Typ 2, ISO 27001:2013, ISO 27001:2014

Alla data i vila och under transport är krypterad

Oberoende penetrationstestning genomförs på årlig basis

All data är begränsad genom rollbaserad åtkomstkontroll

Säkerhetsåtgärder som Online Partner vidtagit utöver Zendesk egna säkerhetsåtgärder

Begränsning av åtkomst till data

Det är endast personal med direkt behov som har tillgång till personuppgifterna. Detta för att kunna utföra sina arbetsuppgifter så att våra kunder får bästa servicenivå av tjänsten ChromEx. Personalen har sekretessåtaganden avseende de personuppgifter som behandlas. Online Partner har regelbunden utbildning för supportpersonal i personuppgiftshantering.

Rutiner för gallring

Uppdaterat rutin för gallring av ärenden. När ett ärende är färdigbehandlat och stängt så sparar vi ärendet i 90 dagar för möjlig uppföljning. Därefter anonymiseras ärendet men ärendet i sig sparas för att uppföljning och kvalitetskontroll.

Utbildning

Vi utbildar regelbundet vår supportpersonal i relation till att hantera personuppgifter i Zendesk.

Maskning av personuppgifter

Online Partner använder sig av en specifik tjänst från Zendesk - Ticket Redaction App. Denna tjänst medför att alla personuppgifter utöver e-postadress och namn som inkommer till Online Partner i supportärenden maskas, dvs döljs.

Inloggning

All inloggning i Zendesk sker genom SSO för G Suite där tvåfaktorsinloggning är ett krav. Se “Kontohantering på Online Partner” 1.1

Administratörer kan ej sätta lösenord på andra användare. Alla användare behöver själva återställa sina lösenord vid behov.

Zendesk support

Kontoövertagande av Zendesk support är avstängt och kan enbart aktiveras av administratörer. Rutinen för kontoövertagande sker enbart tidsbegränsat under tiden för det faktiska supportärendet.

3.2 Stripe

3.2.1 Analys av eventuell överföring till tredje land

Vilket land utanför EU kan uppgifter skickas till?

USA

När kan personuppgifter komma att överföras till USA?

Stripe är en betaltjänst som används vid kortbetalning i ChromEx. För alla som betalar på andra sätt, t.ex. genom bundle med Chrome-licenser eller faktura så hanteras ingen persondata i Stripe. Enligt FISA och Cloud Act kan amerikanska staten begära ut personuppgifter från europeiska medborgare i relation till grov brottslighet.

Typ av personuppgifter relaterade till Stripe

Användaruppgifter kopplade till betalning, betaluppgifter

Vilka personuppgifter kan komma att överföras till USA

Användaruppgifter kopplade till betalning, betaluppgifter

Dokumentation i relation till ECC/SCC (Standard contract clauses)
https://stripe.com/privacy-center/legal#data-transfers

3.2.2 Ytterligare skyddsåtgärder

Stripes skyddsåtgärder

- Fysisk åtkomstkontroll för att förhindra obehöriga från att få tillgång till de databehandlingssystem som finns tillgängliga i lokaler och anläggningar (inklusive databaser, applikationsservrar och relaterad hårdvara) där personuppgifter behandlas.

- Kontroll av datatillgång för att säkerställa att personer som är berättigade att använda ett databehandlingssystem endast får tillgång till sådana personuppgifter i enlighet med deras åtkomsträttigheter, och att personuppgifter inte kan läsas, kopieras, ändras eller raderas utan tillstånd.

- Utlämningskontroll för att säkerställa att personuppgifter inte kan läsas, kopieras, modifieras eller raderas utan tillstånd under elektronisk överföring, transport eller lagring på lagringsmedia (manuell eller elektronisk), och att det kan verifieras till vilka företag eller andra juridiska personer Personuppgifter är avslöjas.

- Tillträdeskontroll för att granska om data har matats in, ändrats eller tagits bort (raderats), och av vem, från databehandlingssystem.

- Tillgänglighetskontroll för att säkerställa att personuppgifter skyddas mot oavsiktlig förstörelse eller förlust (fysisk / logisk).

- Separationskontroll för att säkerställa att personuppgifter som samlas in för olika ändamål kan behandlas separat.

- Stripe tvingar HTTPS för alla tjänster som använder TLS (SSL), inklusive dess offentliga webbplats och instrumentpanel

- Alla kortnummer krypteras i vila med AES-256. Krypteringsnycklar lagras på separata maskiner. Ingen av Stripes interna servrar och tjänster kan läsa kortnummer i klartext.

Säkerhetsåtgärder som Online Partner vidtagit utöver Stripes egna säkerhetsåtgärder

Begränsning av åtkomst till data

Det är endast personal med direkt behov som har tillgång till personuppgifterna. Detta för att kunna utföra sina arbetsuppgifter så att våra användare får bästa servicenivå av tjänsten ChromEx. Personalen har sekretessåtaganden avseende de personuppgifter som behandlas. Online Partner har regelbunden utbildning för supportpersonal i personuppgiftshantering.

Rutiner för gallring

Så länge användaren nyttjar tjänsten Stripe så gallras inga personuppgifter i tjänsten. När användaren avslutar tjänsten Stripe så raderas och överförs historik och betaluppgifter till analog lagring för att sparas utifrån lagar och regler för bokföring Kap 7 i bokföringslagen (1999:1078), Arkivering av och räkenskapsinformation m.m. Den digitala lagringen av personuppgifter i Stripe raderas.

Utbildning

Vi utbildar regelbundet berörd personal i relation till att hantera personuppgifter i Stripe.

Inloggning

All inloggning i Stripe sker genom SSO för G Suite där tvåfaktorsinloggning är ett krav. Se “Kontohantering på Online Partner” 1.1