Order in the cloud

Appendix 1

Personal Data Processor Agreement

2020-10-23

Online Partner AB (hereinafter referred to as “Online Partner” or the “Data Processor”), and
The Customer (hereinafter referred to as the “Customer” or the “Data Controller”)
(jointly referred to as the “Parties”).

The parties have entered into this Data Processing Agreement (the “Agreement”).

1. Background

1.1. The Parties have previously, or in conjunction with this Agreement, entered into an agreement regarding services provided by Online Partner from time to time (hereinafter referred to as the “Service Agreement”) to which Online Partner’s General Terms and Conditions [regarding Service and Software] apply.

1.2. Pursuant to the undertakings which follow from the Service Agreement, the Data Processor may process Personal Data as well as other information on behalf of the Customer.

1.3. As a consequence thereof, the Parties are entering into this Agreement to govern the conditions for Online Partner’s processing of Personal Data when carrying out the services that are regulated in the Service Agreement (hereinafter “the Services”). This Agreement shall apply to all agreements executed between the Parties in which the Online Partner is the Data Processor on behalf of the Customer, and this Agreement shall remain in force for as long as Online Partner processes Personal Data on the Customer’s behalf.

2. Definitions

2.1. For the purposes of this Agreement, terms that are defined in Article 4 in (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (“Data Protection Regulation”) shall have the same meaning given to them therein.

2.2. Otherwise, the terms listed below shall have the following meaning:
"Data Protection Law" refers to the Data Protection Regulation as well as related European and national implementing regulations, as well as instructions and binding decisions from the EU data protection authorities.

2.3. "Sub-processor" refers to such data processor (subcontractor) who has been hired by the Data Processor and who processes Personal Data on behalf of the Data Controller.

3. Scope of the Agreement

3.1. The Data Processor provides the Services agreed with the Data Controller from time to time. The Data Processor's main establishment and central administration is in Sweden.

3.2. The Service involves storage and transfer of user details provided by the user of the Services. Such data may directly or indirectly identify a natural person.

3.3. The Data Processor will solely process the Personal Data provided by the Data Controller in order to perform its obligations according to the Service Agreement.

3.4. The Personal Data that may be processed by the Data Processor on behalf of the Data Controller is irrevocably and automatically deleted upon the termination of the Service Agreement (provided storage of Personal Data is not required pursuant to national law or Union law).

3.5. The Parties hereby agree that the processing, the categories of Personal Data, the data subjects or the purposes of processing may at any time and by mutual agreement be clarified with respect to their specification and/or be enlarged with respect to their volume or scope. Any such changes shall be made in writing to be valid in due course after receipt of knowledge of such changes. Unless otherwise agreed by the Parties, the terms and conditions as set forth in this Agreement shall apply accordingly.

4. Obligations of the Data Processor

4.1. The Data Controller shall have the full power of disposition regarding the Personal Data.

4.2. The Data Processor agrees that it will:

a) provide the processing of Personal Data solely in accordance with the documented instructions of the Data Controller ("Instructions"), including with regard to transfers of Personal Data to a third country or an international organisation, for the purpose set forth in the Service Agreement, according to the rules and the provisions contained in this Agreement and in accordance with the applicable Data Protection Law,

b) will implement the security measures specified herein,

c) not acquire any rights in or to the Personal Data,

d) not use the Personal Data for any purpose other than for the performance of its obligations under this Agreement and the Service Agreement, or for fault localization in the Data Processor's system, and

e) not process the Personal Data for its own purposes without the prior written approval of the Data Controller.

4.3. Where the Data Processor believes that any Instruction would result in a violation of the Data Protection Regulation or other applicable Data Protection Law, the Data Processor may suspend the

execution of the Instruction until their lawfulness is confirmed by an authorized person of the Data Controller or is changed in writing.

4.4. The Data Processor will assist the Data Controller to the extent possible for the fulfilment of the Data Controller's obligations to respond to requests for exercising the data subject's rights as stated in Chapter III in the Data Protection Regulation.

4.5. The Data Processor will assist the Data Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the Data Processor.

5. Notification Obligations of the Data Processor

5.1. The Data Processor shall promptly notify the Data Controller of any unauthorized access to Personal Data and/or any accidental or wilful disclosure of Personal Data to unauthorized third parties it becomes aware of.

5.2. The Data Processor shall promptly notify the Data Controller of any material breach of applicable Data Protection Laws in connection with this Agreement it becomes aware of.

5.3. If the Data Processor considers that any Instruction from the Data Controller is in violation with the Data Protection Law, it shall immediately report this to the Data Controller.

6. Obligations of the Data Controller

6.1. The Data Controller shall provide the Data Processor instructions for the processing of the Personal Data. The Instructions must be in written form (whether physical or electronic).

6.2. The Instructions shall, inter alia, state the subject of the processing, the duration of the processing, the nature and purpose of the processing, the type of Personal Data, and categories of data subjects.

6.3. The Data Controller has the sole obligation to inform data subjects of the processing of their Personal Data by the Data Processer, and to ensure that the data subject is aware of its rights according to the applicable legislation.

6.4. The Data Controller is obligated to in any other manner perform its obligations in accordance with applicable Data Protection Law. Nothing in this Agreement shall be construed as a transfer of the Data Controller's obligations stipulated in applicable Data Protection Law, to the Data Processor.

7. Transfer of Personal Data to a third country

7.1. For the purpose of providing the agreed Services, the Data Processor's servers are located in Finland and in an additional approximately 5 countries worldwide (within EU and in a third countries).

7.2. The Data Controller is aware and accepts that in third countries, the servers are located under co-location agreement with collaborators. Such parties have no right of access to data on the servers, and limited right of physical access to the servers, when the data is transferred between the

Data Processor's servers, the data in encrypted. The servers are remotely or directly operated by the Data Processors sub-processor.
7.3. The Data Controller commits that the data subjects have been informed or will be informed before the processing by the Data Processor that his or her data could be transmitted to a country outside of EU/EES.

7.4. If transfer of Personal Data to a third country or an international organisation is required by Union Law or National Law, the Data Processor may carry out such processes. In such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless the Data Protection Law prohibits such information on important grounds of public interests.

8. Audit Rights

8.1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the Data Protection Regulation and at the Data Controller's request allow the data processing facilities of Processor to be audited with regard to the processing activities covered by this Agreement. The Data Processor will cooperate and provide assistance for such audit as may reasonably be required by the Data Controller and the organization carrying out the audit. The Data Controller is aware that for security reasons, there are limitations and regulations concerning whom may enter the premises where the servers are located.

8.2. Parties shall mutually agree which organization will carry out the audit.

8.3. The Data Controller will pay all costs, fees and expenses of the organization carrying out the audit.

9. Sub-processors

9.1. The Data Controller acknowledges and agrees that (a) the Data Processor's affiliates may be retained as sub-processors; and (b) the Data Processor and the Data Processor's affiliates respectively may engage third-party sub-processors in connection with the provision of the Services. The Data Processor has or shall enter into a written agreement with each sub-processor containing data protection obligations not less protective than those in this Agreement. In any such Personal Data processor agreement, the sub-processor shall provide sufficient warranties in respect of taking suitable technical and organisational measures so that the processing meets the requirements of the Data Protection Regulation.

9.2. The Data Processor shall make available to the Data Controller the current list of sub-processors for the Services provided by the Data Processor. Such sub-processor lists shall include contact information of those sub-processors and their country of location. The Data Processor shall provide notification of new sub-processor(s) before authorizing any new sub-processor(s) to process Personal Data in connection with the provision of the applicable services.

9.3. The Data Controller may object to the Data Processor's use of a new sub-processor by notifying the Data Processor promptly in writing within ten (10) business days after receipt of the Data Processor's notice. In the event the Data Controller objects to a new sub-processor, the Data Processor will use reasonable efforts to make available to the Data Controller a change in the Services or recommend a commercially reasonable change to the Data Controller's configuration or use of the Services to avoid processing of Personal Data by the objected-to new sub-processor

without unreasonably burdening the Data Controller. If the Data Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, the Data Controller may terminate the agreement with respect only to those services which cannot be provided by the Data Processor without the use of the objected-to new sub-processor by providing written notice to the Data Processor.

9.4. The Data Controller must have justified reason to make such objection. With 'justified reasons', means circumstances on the new sub-processor's side that significantly affect, or most likely risk to affect, the protection of the data subject's personal integrity, such as the new sub-processor does not meet the requirements of the Data Protection Law.

9.5. If the sub-processor does not fulfil the obligations regarding the processing of Personal Data set forth in this Agreement, the Data Processor shall remain fully liable to the Data Controller for the sub-processor's failure to comply with the obligations.

10. Security and confidentiality

10.1. The Data Processor has provided sufficient guarantees that it shall take suitable technical and organisational measures to ensure that the processing of Personal Data meets the requirements of the Data Protection Law and ensures protection of the rights of the data subject.

10.2. The Data Processor has implemented and will maintain measures to maintain the security of the service as set forth in Exhibit A.

10.3. The Parties agree that the security measures specified in Exhibit A to this Agreement are appropriate technical and organisational measures to ensure a level of security appropriate to the risk, such as the protection of Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access to Personal Data transmitted, stored or otherwise processed, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposing as well as the risk for the rights and freedoms of natural persons.

10.4. The Data Processor undertakes to not hand out or disclose information about Personal Data that is covered by this agreement to a third party. The confidentiality obligation applies after this agreement has otherwise expired.

10.5. In the event that the Data Processor is legally obliged to disclose to third parties or to a relevant supervisory authority, Personal Data to satisfy legal requirements, comply with law or respond to lawful requests or binding decisions by relevant authority the Data Processor shall, unless prohibited by law, notify the Data Controller without undue delay in writing or email of the reason and the form of the disclosure after it becomes aware of the obligation to disclose. The Data Processor shall wait, unless prohibited by law, for further instructions from the Data Controller concerning the requested disclosure.

10.6. The Data Processor shall ensure that all persons who have been given the authority to process Personal Data have entered into a separate confidentiality agremeent or are informed that a special duty of confidentiality exists according to agreement or applicable law.

10.7. The Data Processor shall takes all measures required pursuant to Article 32 in the Data Protection Regulation.

11. Miscellaneous

11.1. The provisions of Online Partner's General Terms and Conditions regarding term and termination, liability, jurisdiction and competent court apply accordingly to this Agreement.

11.2. Amendments and supplements to this Agreement must be in writing. Except as amended by this Agreement, this Agreement will remain in full force and effect. If there is a conflict between the Service Agreement and this Agreement, the terms of this Agreement will take precedence.

Exhibit A, Technical and Organisational Security Measures

Online Partner will implement not less than the controls listed below, or their equivalent, during the term of this Agreement:

Access control to premises

The Data Processor will implement suitable measures for the purpose of preventing unauthorized persons from gaining access to the data processing equipment by the following means:

- Access authorizations for employees and third parties
- Protection and restriction of entrances and exits (restricted keycards and/or passes)
- Security of relevant premises (alarms and/or security guards)

Access control to data and user control

The Data Processor commits that any and all personnel with access to the Personal Data has this authority on a need-to-know-basis, for the purpose pf providing the Services in the Service Agreement, by means of:

- All staff uses hardened authentication using two-factor authentication
- Requirements for user authorization and strict access control
- Confidentiality obligations
- Differentiated access policies (e. g. partial blocking)
- Controlling destruction and the removal of data media
- Logging of events and activities (monitoring of break-in attempts, or attempts of unauthorised access)
- Issuing and safeguarding the identification codes
- Use of encryption where deemed appropriate by Data Processor
- Automatic log-off of user IDs that have not been used for a substantial period of time
- Ensuring that Customers only have access to their own Data

Transfer of data

The Data Processor will secure the Personal Data transferred and/or otherwise processed in accordance with the Service Agreement and Instructions by means of:

- Policies controlling the production of backup copies
- Documentation of the transfer, retrieval, and transmission programs
- Authorization policy
- Encrypting external online transmission
- Deleting remaining data before changing data media
- The traffic between the user and the service is encrypted SSL certificates.
- Personal Data is not transferred to a third Party without the Data Controller's prior written consent, unless legally obliged

Organizational control

The Data Processor will maintain its internal organization in a manner that meets the requirements of Data Protection Law, by means of:

- Binding internal policies for personnel and/or consultants regarding security and the process of Personal Data, and/or instructions
- Internal emergency plan for recovery and safeguard of Personal Data
- Authority to access data for personnel based on a strictly need-to-know-basis
- No customer data will be copied to external devices (USB sticks, CD i.e) without taking the necessary security measurements, such as encryption or password protection

Exhibit B, List of data subprocessors for ChromEx

Subprocessor: Google Cloud Plattform	**Contact information**: Privacy Help Center - Policies Help
Geographic placement and agreement: Servers in EU/EES Frankfurt. (Possibly processed outside the EU on specific occasions. For more info see Exhibit C.) Our Cloud Data Privacy Commitments Google Cloud Platform: EU Model Contract Clauses	**Type of service:** Operations and maintenance for application. (Cloud service)
Used by the following services ChromEx Chrome-addon, ChromEx teacher panel, ChromEx student application	**Data being processed:** Name, e-mail address, groups, Public IP-address

Subprocessor: Google Fonts (Google Ireland Limited)	**Contact information**: Privacy Help Center - Policies Help
Geographic placement and agreement: Ireland (Possibly processed outside the EU on specific occasions. For more info see Exhibit C.) Privacy Policy – Privacy & Terms – Google	**Type of service:** **Distribution network for fonts** Only a public IP-number is used for statistics in this service. Use of Google Fonts is unauthenticated. No cookies are sent by website visitors to the Google Fonts API. Requests to the Google Fonts API are made to resource-specific domains, such as fonts.googleapis.com or fonts.gstatic.com, so that your requests for fonts are separate from and do not contain any credentials you send to google.com while using other Google services that are authenticated, such as Gmail.
Used by the following services ChromEx Chrome-addon, ChromEx teacher panel, ChromEx student application	**Data being processed:** Public IP-address

Subprocessors for application ChromEx regarding specific services and agreements

Subprocessor: Zendesk	**Contact information**: 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
Geographic placement and agreement: EU, USA Privacy Policy Update on Privacy Shield Invalidation by the European Court of Justice	**Type of service:** Support system for handling and answering requests from customers.
Used by the following services Support at Online Partner	**Data being processed:** Name, email address

Subprocessor: Stripe	**Contact information**: Stripe 510 Townsend Street San Francisco, CA 94103, USA Attention: Stripe Legal privacy@stripe.com
Geographic placement and agreement: USA Privacy Policy - Sweden Stripe Privacy Center	**Type of service:** Stripe is a service for handling credit card payments. If you pay by invoice you are not affected by this service..
Used by the following services Service for credit cards	**Data being processed:** User data, Payment data

Exhibit C - Additional protection measures to ensure standard contract clauses in the event of transfer to third countries regarding ChromEx.

Based on the judgment of 16 July 2020 "Schrems II" (Case C-311/18), the Privacy Shield no longer applies as a legal basis for the processing of personal data transferred to the United States. Companies that need to transfer personal data to the United States must now enter into so-called Standard Contractual Clauses and take appropriate protective measures. This document describes the additional protection measures we as a company (Online Partner AB) have taken to further protect personal data during processing in the USA.

This document and safeguard measures will be revised and updated when the EDPB (European Data Protection Board) and / or the Datainspektionen (Swedish data protection authority) present guidelines for the security measures to be taken.
(https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en)

Online Partner has noted that the following services and subprocessors involve or may involve transfer of data to the United States. Online Partner has considered and analyzed if the ChromEx application can be provided without the services below. After analysis on the market and of the purpose and content of the service, it has been established that the services are necessary to be able to provide ChromEx to our customers and users. Online Partner has therefore analyzed the services and taken additional protection measures.

1 General organizational security measures at Online Partner

1.1 Account management at Online Partner

Upon access to their service, the staff at Online Partner receive an account in Google Workspace which is used as an SSO service in relation to all other applications used in the company. To be able to log in to their Google Workspace account at Online Partner, all employees must use the company's determined policy for two-factor login. In addition to the specific employee, only an administrator can restore an account to access personal information. This administrator is managed with a no-reply account that has a physical two-factor login on a USB.

1.2 Access to user data at Online Partner

At Online Partner, we work on the premise that only those persons who, due to their work tasks, are tasked with managing users' personal data have access to the personal data. This means that only personnel for each specific service have access to personal data. The staff have confidentiality obligations regarding the personal data that is processed.

1.3 Physical devices at Online Partner

All devices used on Online Partner use the latest security updates and hard disk encryption. The services used are cloud-based and protected by an extra layer with two-factor authentication. See “Account Management on Online Partner 1.1”

1.4 Perimeter protection at Online Partner

The office is located on the second and third floors and is only accessible from the stairwell and fire escape at the back. The front door to the room is of the Dalloc brand and in steel, it is classified according to SSF Certifkat C95-337 Class 2.

The door has two separate locking devices, night lock and day lock, the day lock can be opened from the outside with a key and from the inside via a knob or electronic remote opening from the majority of the workrooms.

1.5 Security alarm

We have a security alarm connected to Bevakningsassistans Stockholm, which sends out guards in the event of an alarm.

1.6 Camera surveillance

Online Partner has camera surveillance at entry points to the office.

2 Subprocessor for the application ChromEx

2.1 Google Cloud Platform

2.1.1 Analysis of possible transfer to third country

To which country outside the EU can data be sent?

In exceptional cases, the United States.

When can personal data be transferred to the United States?

Google Cloud may process personal data outside the EU through the Firebase Hosting service. Firebase Hosting involves a global edge caching that is controlled based on which country you are physically in when you use ChromEx. Edge caching works by selecting the nearest server based on your geographic location. The servers that handle Firebase Hosting when the service is used within the EU are located in Zurich (europe-west6) and Frankfurt (europe-west3). The mentioned servers will be the most likely servers when the service is used in most of Europe. Europe-west3 is also the server on which we operate other services on Google Cloud due to its geographical proximity. This means that the only probable time that personal data will be transferred to the USA is in the event that the user is outside the EU. The purpose of our service is that it will be used in European Union, which is why Online Partner sees that transfer to the USA will only take place to a very limited extent.

According to FISA and the Cloud Act, the US government can request personal data from European citizens in relation to felonies if there is any processing of data in the US.

More information about Firebase Hosting can be read here:

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

Type of personal data related to Google Cloud Platform

Name, e-mail address, Google group, Public IP-address

What personal information may be transferred to the United States

The only personal information shared with Firebase Hosting when the user is outside the EU is a public IP number.

2.1.2 Additional protective measures

Google Global Protection Measures:

Google has a global infrastructure designed to securely manage information throughout its lifecycle. This infrastructure enables secure deployment of services, secure storage of data, secure communication between services, secure communication between services and end users, and secure administration of services. Google uses this infrastructure to build its services such as Google Workspace and Google Cloud.

Infrastructure security is built from the ground up in progressive layers, starting with the security of Google's data center to the services for administering the services.

Google invests heavily in the security of its infrastructure and has hundreds of dedicated engineers dedicated to maintaining and improving both security and privacy throughout Google.

Read more about Google's security measures here:

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

Security measures taken by Online Partner in addition to Google's own security measures

Restriction of access to data

Online Partner has previously restricted all access to data and personal information in the Google Cloud Platform. Only personnel with immediate needs have access to the personal data. This is to be able to perform their tasks so that our users get the best level of service from the ChromEx service. The staff have confidentiality obligations regarding the personal data that is processed.

Audit logs

Online Partner saves audit logs of administrative events and access data in the Google Cloud Platform. This is to be able to handle any incidents of personal data.

Encrypted network communication

Online Partner uses encrypted communication protocols between service to service and service to the end user.

End user login with Single Sign On

Online Partner uses the open industry standard OpenID Connect 2.0 which allows users to reuse their existing Single Sign On accounts.

Documentation in relation to ECC / SCC (EU / Standard contractual clauses)
https://cloud.google.com/terms/eu-model-contract-clause
https://cloud.google.com/security/privacy

2.2 Google Fonts

2.2.1 Analysis of possible transfer to third country

To which country outside the EU can data be sent?

In exceptional cases, the United States.

When can personal data be transferred to the United States?

Google Fonts may process personal data outside the EU. Google Fonts uses global edge caching, which is controlled based on which country you are physically in when using ChromEx. Edge caching works by selecting the nearest server based on your geographic location. Servers within the EU will be the natural servers when the service is used in Sweden. The purpose of our service is that it will be used in Sweden, which is why Online Partner sees that transfer to the USA will only take place to a very limited extent.

According to FISA and the Cloud Act, the US government can request personal data from European citizens in relation to felonies against the US if there is any processing in the US.

More information about Google fonts and its processing of data:

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

Type of personal data related to Google Fonts:

Public IP address

What personal information may be transferred to the United States

The only personal information that could be sent via Google Fonts is a public IP number. Google fonts are completely separate from Google or Google Workspace. No user data contained in e.g. Gmail or other services provided by Google are used by Google Fonts. Only a public IP number is used to manage statistics.

2.2.2 Additional protective measures

Google Global Protection Measures:

Google has a global infrastructure designed to securely manage information throughout its lifecycle. This infrastructure enables secure deployment of services, secure storage of data, secure communication between services, secure communication between services and end users, and secure administration of services. Google uses this infrastructure to build its services such as Google Workspace and Google Cloud.

Infrastructure security is built from the ground up in progressive layers, starting with the security of Google's data center to the services for administering the services.

Google invests heavily in the security of its infrastructure and has hundreds of dedicated engineers dedicated to maintaining and improving both security and privacy throughout Google.

Read more about Google's security measures here:

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

Security measures taken by Online Partner in addition to Google's own security measures

Restriction of access to data

Online Partner has previously restricted all access to data and personal information in Google Fonts. Only personnel with immediate needs have access to the personal data. This is to be able to perform their tasks so that our users get the best level of service from using ChromEx. The staff have confidentiality obligations regarding the personal data that is processed.

Documentation in relation to ECC / SCC (EU / Standard contract clauses)

https://policies.google.com/privacy

3 Subprocessors for application ChromEx regarding specific services and agreements

3.1 Zendesk

3.1.1 Analysis of possible transfer to third country

To which country outside the EU can data be sent?

USA

When can personal data be transferred to the United States?

Support system for handling and responding to user requests. This means that Zendesk is only used for support matters, not when using the application. Everyone who emails to Online Partner Support agrees that their personal information is processed in relation to Zendesk's user agreement.

According to FISA and the Cloud Act, the US state can request personal data from European citizens in relation to serious crime against the USA.

Type of personal data related to Zendesk

First name, Last name, E-mail address

What personal information may be transferred to the United States

First name, Last name, E-mail address

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

3.1.2 Additional protective measures

Zendesk safeguards

Zendesk is certified according to SOC 2 Type 2, ISO 27001: 2013, ISO 27001: 2014

All data at rest and during transport is encrypted

Independent penetration testing is performed on an annual basis

All data is restricted through role-based access control

Security measures taken by Online Partner in addition to Zendesk's own security measures

Restriction of access to data

Only personnel with immediate needs have access to the personal data. This is to be able to perform their tasks so that our customers receive the best level of service from the ChromEx service. The staff have confidentiality obligations regarding the personal data that is processed. Online Partner has regular training for support staff in personal data management.

Routines for data erasure

Updated routine for data erasure cases. When a case has been processed and closed, we save the case for 90 days for possible follow-up. Thereafter, the case is anonymized, but the case itself is saved for follow-up and quality control.

Training

We regularly train our support staff in relation to handling personal data in Zendesk.

Masking of personal data

Online Partner uses a specific service from Zendesk - Ticket Redaction App. This service means that all personal information in addition to the email address and name received by Online Partner in support tickets are masked, i.e. hidden.

Login

All login in Zendesk takes place through SSO for Google Workspace where two-factor login is a requirement. See “Online Partner Account Management” 1.1

3.2 Stripe

3.2.1 Analysis of possible transfer to third country

To which country outside the EU can data be sent?

USA

When can personal data be transferred to the United States?

Stripe is a payment service used for card payments in ChromEx. For anyone who pays in other ways, e.g. through bundle with Chrome licenses or invoice, no personal data is handled in Stripe. According to FISA and the Cloud Act, the US state can request personal data from European citizens in relation to felonies.

Type of personal data related to Stripe

User information linked to payment, payment information

What personal information may be transferred to the United States

User information linked to payment, payment information

Documentation in relation to ECC / SCC (Standard contract clauses)
https://stripe.com/privacy-center/legal#data-transfers

3.2.2 Additional protective measures

Stripe safeguards

- Physical access control to prevent unauthorized persons from accessing the data processing systems available in premises and facilities (including databases, application servers and related hardware) where personal data is processed.

- Control of data access to ensure that persons entitled to use a data processing system only access such personal data in accordance with their access rights, and that personal data cannot be read, copied, modified or deleted without permission.

- Disclosure control to ensure that personal data cannot be read, copied, modified or deleted without permission during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal persons Personal data is disclosed.

- Access control to check if data has been entered, changed or deleted (deleted), and by whom, from data processing systems.

- Accessibility control to ensure that personal data is protected against accidental destruction or loss (physical / logical).

- Separation control to ensure that personal data collected for different purposes can be processed separately.

- Stripe enforces HTTPS for all services using TLS (SSL), including its public website and dashboard

- All card numbers are encrypted at rest with AES-256. Encryption keys are stored on separate machines. None of Stripe's internal servers and services can read card numbers in plain text.

Security measures taken by Online Partner in addition to Stripe's own security measures

Restriction of access to data

Only personnel with immediate needs have access to the personal data. This is to be able to perform their tasks so that our users get the best level of service from the ChromEx service. The staff have confidentiality obligations regarding the personal data that is processed. Online Partner has regular training for support staff in personal data management.

Routines for data erasure

As long as the user uses the Stripe service, no personal data is erased in the service. When the user terminates the Stripe service, history and payment information are deleted and transferred to analogue storage for saving based on laws and regulations for accounting. Chapter 7 of the Accounting Act (1999: 1078), Archiving of and accounting information, etc. The digital storage of personal data in Stripe will be deleted.

Training

We regularly train relevant personnel in relation to handling personal data in Stripe.

Login

All login in Stripe takes place through SSO for Google Workspace where two-factor login is a requirement. See “Online Partner Account Management” 1.1

PARTIES, POSITION OF THE PARTIES, CONTACT DETAILS AND CONTACT PERSONS

Personal data controller	**Personal data processor**
	Online Partner AB
Organisation number	**Organisationsnummer**
	556566-5527
Postal address	**Postal address**
	Västberga Allé 60 126 30 Hägersten
Contact for administration of this data processing agreement.	**Contact for administration of this data processing agreement.**
Name: E-mail: Tel:	Name: Fredrik Linnander E-mail: fredrik@onlinepartner.se Tel: 08-420 004 44
Contact for the parties for collaboration of data protection	**Contact for the parties for collaboration of data protection**
Name: E-mail: Tel:	Name: Fredrik Hedström E-mail: hedstrom@onlinepartner.se Tel: 08-420 004 08

SIGNATURES OF PARTIES

Data controller

Place Date

.....

Signature

.....

Print Name

Data processor

Place Date

Hägersten

.....

Signature

.....

Print name **Fredrik Linnander**