Data Processing Agreement

CLASSROOM MANAGER

Sveriges Kommuner och Regioner adda inera

Version 1.2.1 (200102)

Table of contents

DATA PROCESSING AGREEMENT

Agreement in accordance with Article 28(3) of the General Data Protection Regulation (EU) 2016/679[1]

1. PARTIES, POSITIONS OF THE PARTIES, CONTACT DETAILS AND CONTACT PERSONS

Controller	**Processor**
	Online Partner AB
Corporate ID No.	**Corporate ID No.**
	556566-5527
Mailing address	**Mailing address**
	Mejerivägen 3 117 43 Stockholm
Contact person for the administration of this Data Processing Agreement	**Contact person for the administration of this Data Processing Agreement**
Name: E-mail: Tel:	Name: Fredrik Linnander E-mail: fredrik@onlinepartner.se Tel: 08-420 004 44
Contact person for cooperation between the parties about data protection	**Contact person for cooperation between the parties about data protection**
Name: E-mail: Tel:	Name: Fredrik Linnander E-mail: fredrik@onlinepartner.se Tel: 08-420 004 44

2. DEFINITIONS

In addition to the terms defined in the running text of this Data Processing Agreement, the following terms, whether in singular or plural, with definite or indefinite article, shall have the meaning defined below whenever they are capitalised.

Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[1]The General Data Protection Regulation (EU) 2016/679 stipulates that there must be a written agreement on the processing of personal data by the Processor on behalf of the Controller.

Data protection legislation	Refers to all privacy and personal data legislation, along with any other legislation (including regulations and directives) applicable to the Processing carried out in accordance with this Agreement, including national legislation and EU legislation.
Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Instruction	The written instructions that more specifically define the object, duration, type and purpose of Personal Data, as well as the categories of Data Subjects and special requirements that apply to the Processing.
Log	A Log is the result of Logging
Logging	Logging is a continuous collection of information about the Processing of Personal Data that is performed according to this Agreement and which can be associated with an individual natural person.
Processor	A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
Personal Data	Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed
Data Subject	Natural person whose Personal Data is Processed.
Third Country	A state that is not a member of the European Union (EU) or the European Economic Area (EEA).
Subprocessor	A natural or legal person, public authority, agency or other body which, in the capacity of subcontractor to the Processor, Processes Personal Data on behalf of the Controller.

3. BACKGROUND AND AIM

3.1 Through this Agreement, the Instructions and a list of possible Subprocessors (hereafter jointly referred to as “the Agreement”), the Controller regulates Processor’sProcessing of Personal Data on behalf of the Controller. The aim of the Agreement is to safeguard the freedoms and rights of the Data Subject during Processing, in accordance with what is stipulated in Article 28(3) of the General

Data Protection Regulation (EU) 2016/679 (“GDPR”) equivalent to the the UK Data Protection Act 2018.

When this Agreement is one of several contractual documents comprising another agreement, the other agreement is referred to as the “Main Agreement” in this Agreement.

3.3 In the event that anything stipulated in items 1, 16, 17, 18.2, 19–22 of this Agreement is regulated otherwise in the Main Agreement, the Main Agreement shall take priority.

3.4 Any reference in this Agreement to national or union legislation refers to the provisions applicable at any given time.

4. PROCESSING OF PERSONAL DATA AND SPECIFICATION

The Controller hereby appoints the Processor to carry out Processing on behalf of the Controller, pursuant to the provisions of this Agreement.

4.2 The Controller shall give written Instructions to the Processor as to how the Processor shall carry out the Processing.

4.3. The Processor may only perform the Processing in accordance with this Agreement and the Instructions applicable at any given time.

5. OBLIGATIONS OF THE CONTROLLER

5.1 The Controller undertakes to ensure that there is a legal basis for the Processing at all times, and to issue correct instructions so that the Processor and any Subprocessors can carry out their duties in accordance with this Agreement and the Main Agreement, where applicable.

5.2 The Controller undertakes to inform the Processor without undue delay of any changes in the Processing that may affect the Processor’s obligations pursuant to the Data Protection Legislation.

5.3 The Controller is responsible for informing Data Subjects of the Processing and to safeguard the rights of Data Subjects in accordance with the Data Protection Legislation, as well as to take every other measure required of the Controller pursuant to the Data Protection Legislation.

6. OBLIGATIONS OF THE PROCESSOR

6.1 The Processor undertakes to only perform the Processing in accordance with this Agreement and the Instructions and to comply with the Data Protection Legislation. The Processor also undertakes to stay informed of currently applicable laws and regulations in this area.

6.2 The Processor shall take measures to protect the Personal Data against all kinds of Processing that is not in compliance with this Agreement, the Instructions and the Data Protection Legislation.

6.3 The Processor undertakes to ensure that all natural persons who work under its supervision comply with this Agreement and the Instructions, and that these natural persons are informed about relevant legislation.

6.4 At the request of the Controller, the Processor shall assist the former in ensuring compliance with the obligations pursuant to Articles 32–36 of GDPR, and shall respond to requests regarding the exercise of Data Subjects' rights pursuant to Chapter III of GDPR, taking into consideration the type of Processing and the information available to the Processor.

6.5 In the event that the Processor finds the Instructions to be unclear, in violation of the Data Protection Legislation or non-existent, and the Processor is of the opinion that new or supplementary Instructions are necessary in order to fulfil its undertakings, the Processor shall inform the Controller of this without delay, temporarily suspend the Processing and await new Instructions.

6.6 In the event the Controller provided the Processor with new or amended Instructions, the Processor shall inform the Controller, without undue delay after receiving them, whether the implementation of the new Instructions will entail any changed costs for the Processor.

7. SECURITY MEASURES

7.1 The Processor is obligated to take all technical and organisational security measures required by the Data Protection Legislation in order to prevent Personal Data Breaches, by ensuring that the Processing complies with the requirements of GDPR and that the rights of the Data Subjects are protected.

7.2 The Processor shall continuously ensure that the technical and organisational security relating to the Processing maintains an appropriate level of confidentiality, integrity, availability and resilience.

7.3 Any future or modified requirements for protective measures coming from the Controller once the Parties have entered this Agreement shall be considered new Instructions in accordance with this Agreement.

7.4 The Processor shall use an authorisation control system to allow access to the Personal Data only for such natural persons who work under the supervision of the Processor and who need such access in order to perform their duties.

7.5 The Processor undertakes to continuously Log access to the Personal Data pursuant to this Agreement, to the extent required according to the Instruction. Logs may not be purged until at least five (5) years after the time of Logging, unless otherwise specified in the Instruction. Logs shall be subject to the necessary protective measures pursuant to the Data Protection Legislation.

7.6 The Processor shall systematically test, examine and evaluate the effectiveness of the technical and organisational measures that are intended to ensure the security of the Processing.

8. SECRECY/DUTY OF CONFIDENTIALITY

8.1 The Processor and all natural persons who work under its supervision shall observe both secrecy and the duty of confidentiality during Processing. Personal Data may not be used or disseminated for other purposes, neither directly or indirectly, unless otherwise agreed.

8.2. The Processor is required to ensure that all natural persons working under its supervision who participate in the Processing are bound by a confidentiality agreement regarding the Processing. However, this is not required if those persons are already subject to a statutory duty of confidentiality with criminal liability. The Processor also undertakes to ensure that there is a confidentiality agreement with its Subprocessor, as well as between the Subprocessor and all natural persons working under its supervision who participate in the Processing

8.3 The Processor shall immediately inform the Controller of any contacts with the supervisory authority regarding the Processing. The Processor shall not be entitled to represent the Controller or act on behalf of the Controller vis-à-vis supervisory authorities in matters relating to the Processing.

8.4 If the Data Subject, supervisory authority or a third party requests information from the Processor regarding the Processing, the Processor shall inform the Controller thereof. Information regarding the Processing may not be divulged to the Data Subject, supervisory authority or third party without the written consent of the Controller, unless the obligation to disclose the information is prescribed by law. The Processor shall assist in the communication of such information as is the subject of consent or legal requirement.

9. INSPECTION, SUPERVISION AND AUDITING

9.1 At the request of the Controller, the Processor shall without undue delay provide information, as part of its undertakings in accordance with Article 28(1) of GDPR, regarding the technical and organisational security measures used to ensure that the Processing complies with the requirements of this Agreement and Article 28(3)(h) of GDPR.

9.2 The Processor must at least once (1) per year review the security of the Processing through self-monitoring in order to ensure that the Processing complies with the Agreement. The result of this self-monitoring shall be made available to the Controller upon request

9.3 The Controller has the right to inspect, or to appoint a third party (who must not be a competitor of the Processor) to inspect the Processor's compliance with the requirements of this Agreement, the Instruction and the Data Protection Legislation. In connection with such inspection, the Processor shall assist the Controller or the person carrying out the inspection on behalf of the Controller, with documentation, access to premises, IT systems and other assets required to verify the Processor's compliance with this Agreement, the Instructions and the Data Protection Legislation. The Controller shall ensure that the personnel carrying out the inspection are subject to secrecy or duty of confidentiality pursuant to law or contract.

9.4 The Processor, as an alternative to the provisions of items 9.2–9.3, may offer other approaches to inspection of the Processing, such as inspection by an independent third party. In that case, the Controller shall be entitled, but not obligated, to apply this alternative approach to the inspection. In the event of this kind of inspection, the Processor shall give the Controller or the third party the assistance needed to perform the inspection.

The Processor shall enable the supervisory authority, or other government agency with legal authority, to conduct supervision at the authority's request and pursuant to the applicable legislation at any given time, even if such an supervision would otherwise violate the provisions of the Agreement.

9.6 The Processor shall ensure that the Controller has rights in relation to the Subprocessor which correspond to all the rights that the Controller has in relation to the Processor pursuant to item 9 of the Agreement.

10. HANDLING OF CORRECTIONS, DELETIONS, ETC.

10.1 In the event that the Controller has requested a correction or deletion as a result of incorrect Processing by the Processor, the Processor shall take appropriate measures, without undue delay, no later than thirty (30) days from the date on which the Processor received the required information from the Controller. When the Controller has requested deletion, the Processor may only perform Processing of the Personal Data in question as a part of the correction or deletion process.

10.2 If technical and organisational measures (e.g. upgrades or troubleshooting) are taken by the Processor with regard to the Processing, and these can be expected to affect the Processing, the Processor shall inform the Controller in writing in accordance with the provisions on notifications set out in Section 19 of the Agreement. This information shall be communicated well in advance of the measures being taken.

11. PERSONAL DATA BREACHES

The Processor shall have the ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident as defined in Article 32(1)(c) of GDPR.

11.2 In considering the nature of the Processing and the information available to the Processor, the Processor undertakes to assist the Controller in fulfilling its obligations in the event of a Personal Data Breach involving the Processing. At the request of the Controller, the Processor shall also assist in investigating suspicions of possible unauthorised Processing of and/or access to Personal Data.

11.3 In the case of a Personal Data Breach that the Processor has been made aware of, the Processor shall, without undue delay, notify the Controller in writing of the incident. In considering the nature of the Processing and the information available to the Processor, the Processor shall provide the Controller with a written description of the Personal Data Breach.

The description shall include:

1. The nature of the Personal Data Breach, and, if possible, the categories and the number of Data Subjects affected, as well as the categories and number of personal data items affected,
2. the probable consequences of the Personal Data Breach, and
3. measures that have been taken or proposed, as well as measures to mitigate the potential negative effects of the Personal Data Breach.

11.4 If it is not possible for the Processor to provide the entire description as set out in item 11.3 of the Agreement at the same time, the description may be provided in stages without undue additional delay.

12. SUBPROCESSOR

12.1 The Processor is entitled to hire the Subprocessor(s) listed in the Subprocessor appendix.

12.2 The Processor undertakes to enter a written agreement with the Subprocessor to regulate the Processing that the Subprocessor carries out on behalf of the Controller and to only hire Subprocessors who provide adequate guarantees to carry out appropriate technical and organisational measures to ensure that the Processing fulfils the requirements of GDPR. When it comes to data protection, such an agreement shall entail the same obligations for the Subprocessor as are set out for the Processor in this Agreement.

12.3 The Processor is fully responsible in relation to the Controller for any Processing carried out by a Subprocessor.

12.4 The Processor is entitled to hire new sub processors and to replace existing sub processors.

12.5 When the Processor intends to hire a new subprocessor or replace an existing one, the Processor shall verify the Subprocessor's capacity and ability to meet their obligations in accordance with the Data Protection Legislation. The Processor shall notify the Controller in writing of

1. the Subprocessor's name, corporate identity number and head office (address and country),
2. which type of data and categories of Data Subjects are being processed, and
3. where the Personal Data will be processed.

12.6 The Controller is entitled within thirty (30) days of the notice pursuant to item 12.5 to object to the Processor's hiring of a new subprocessor and, due to such an objection, to cancel this Agreement to be terminated in accordance with the provisions of item 17.4 of this Agreement.

12.7 When the Processor stops using the Subprocessor, the Processor shall notify the Controller in writing that they will no longer be using the Subprocessor.

12.8 At the Controller's request, the Processor shall send a copy of the agreement regulating the Subprocessor's Processing of Personal Data in accordance with item 12.2.

13. LOCALISATION AND TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

13.1 The Processor shall ensure that the Personal Data will be handled and stored within the EU/EEA by a natural or legal person who is established in the EU/EEA, unless the parties to this Agreement agree otherwise.

13.2 The Processor is only entitled to transfer Personal Data to a Third Country for Processing (e.g. for service, support, maintenance, development, operations or other similar handling) if the Controller has given advance written approval of such transfer and has issued Instructions to this end.

13.3 Transfer to a Third Country for Processing pursuant to item 13.2 of the Agreement may be carried out only if it complies with the Data Protection Legislation and fulfils the requirements for the Processing set out in this Agreement and the Instructions

14. LIABILITY FOR DAMAGES IN CONNECTION WITH THE PROCESSING

14.1 In the event that compensation for damages in relation to Processing is payable to the Data Subject, through a legally binding judgement or settlement, due to a violation of the Agreement, Instructions and/or applicable provision of the Data Protection Legislation, Article 82 of GDPR is applicable.

14.2 Fines in accordance with Article 83 of GDPR or Chapter 6, Section 2 of the Data Protection Act (2018:218) shall be paid by the party to this Agreement that has been levied such a fee.

14.3 If either party becomes aware of circumstances that could be detrimental to the other party, the first party shall immediately inform the other party of this and work actively with the other party to prevent and minimise the damage or loss.

14.4 Notwithstanding any of the provisions of the Main Agreement, items 14.1 and 14.2 of this Agreement take precedence over other rules regarding the allocation between the parties of claims regarding the Processing.

15. CHOICE OF LAW AND DISPUTE RESOLUTION

15.1 Swedish law shall apply to this agreement. Any interpretation or dispute arising from the Agreement which the parties cannot resolve on their own shall be settled by a Swedish general court.

16. CONCLUSION, TERM AND TERMINATION OF THE AGREEMENT

16.1 The Agreement shall enter into force from the time the Agreement has been signed by both parties and until further notice. Either party has the right to terminate the Agreement with thirty (30) days' notice.

17. AMENDMENTS, TERMINATION WITH IMMEDIATE EFFECT, ETC.

17.1 Each party to the Agreement shall be entitled to invoke a renegotiation of the Agreement if there is a major change of the ownership of the other party or if applicable legislation or interpretation thereof changes in a way that significantly affects the Processing. The invoking of a renegotiation pursuant to the first sentence does not mean that any part of the Agreement will cease to be in effect, but only means that a renegotiation of the Agreement will commence.

17.2 Additions and amendments to the Agreement must be made in writing and signed by both parties.

17.3 If either party becomes aware that the other party is acting in violation of the Agreement and/or Instructions, the first party shall inform the other party without delay of the actions in question. The

party is then entitled to suspend the performance of its obligations pursuant to the Agreement until such time as the other party has declared that the actions have ceased, and the explanation has been accepted by the party that made the complaint.

17.4 If the Controller objects to the Processor using a new subprocessor, pursuant to item 12.6 of this Agreement, the Controller is entitled to terminate the Agreement with immediate effect.

18. MEASURES IN THE EVENT OF TERMINATION OF THE AGREEMENT

18.1 Upon termination of the Agreement, the Controller shall, without undue delay, request that the Processor transfers all Personal Data to the Controller or deletes them, according to the preference of the Controller. If the Personal Data is transferred, this must take place in an open and standardised format. "All Personal Data" means all Personal Data that have been the subject of Processing, as well as other related information such as Logs, Instructions, system solutions, descriptions and other documents that the Processor received through an exchange of information pursuant to the Agreement.

18.2 Transfers and deletions pursuant to item 18.1 of the Agreement shall be carried out no later than thirty (30) days from the time notice of termination was given in accordance with item 16.1 of this Agreement.

18.3 Processing performed by the Processor after the time specified in item 18.2 shall be considered unauthorised Processing.

18.4 The provisions regarding secrecy and confidentiality in item 8 of this Agreement shall remain in effect even if the Agreement otherwise ceases to apply.

19. NOTIFICATIONS WITHIN THE PURVIEW OF THIS AGREEMENT AND THE INSTRUCTIONS

19.1 Notifications regarding the Agreement and its administration, including termination, shall be sent to the respective party's contact person for the Agreement.

Notifications regarding the parties' cooperation on data protection, as it applies to the Processing, shall be sent to the respective party's contact person for the parties' cooperation on data protection.

19.3 Notifications within the purview of the Agreement and Instructions shall be sent in writing. A notification shall be considered to have been received by the addressee no later than one (1) working day after the notification has been sent.

20. CONTACT PERSONS

20.1 Each party shall appoint one contact person for the Agreement

20.2 Each party shall appoint one contact person for the parties' data protection collaboration.

21. RESPONSIBILITY FOR INFORMATION REGARDING PARTIES, CONTACT PERSONS, AND CONTACT INFORMATION

21.1 Each party is responsible for ensuring that the information provided in item 1 of the Agreement is up to date. Changes to the information in item 1 shall be communicated in writing pursuant to item 19.1 of the Agreement.

22. THE PARTIES' SIGNATURES ON THE AGREEMENT

22.1 This Agreement can be produced either in digital format for electronic signing, or in paper format for signing in ink. If the Agreement is provided in digital format, items 22.2–22.3 will be deleted.

22.2 Signature of the Controller

Place Date

……

Signature

……

Name in block letters

22.3 Signature of the Processor

Place Date

……

Signature

……

Name in block letters

Version management

Version	Date	Changes	Responsible
1.1	19/12/2018	10.1, 14.1, 18.2,	PR
1.2	17/12/2019	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,	NE

		17.3, 17.4, 18.2, 18.3, 18.4, 21.1, 22.1	
1.2.1	02/01/2020	17.4	PR
1.3.1	24/11/2022	Appendix update	SB, PB, CC

APPENDIX 1. PROCESSING DESCRIPTION

In addition to what is already set out in the Processor Agreement, the Processor shall also comply with the following Instructions:

1. Purpose, object and nature

Personal data is processed in the **Class Manager** application that brings structure and order when managing Google Classroom.
No sensitive personal data shall be processed in the service.

The personal data that we store for the student and teacher is linked to a specific test in the application and the submission in their Google Drive. We also store the e-mails of all administrators and teachers in order to provide the service. Personal data is also stored for 90 days in our server logs in order to troubleshoot and provide support to the customer.

2. The processing includes the following types of personal data

Personal data in the system consists of:

- First name
- Last name
- E-mail address
- IP address

3. The processing covers categories of registered Persons

The categories of data subjects include those of the Controller:

- Staff
- Pupils

4. Specify the specific processing requirements in relation to the Processing of Personal Data by the Processor(s)

- At the request of the Personal Data Controller, the Personal Data Processor shall delete specified information containing personal data. After the request, the counsellor has 30 days to delete the information provided by the Personal Data Controller.
- In the case of conditions for the cancellation of personal data (archiving) including the deletion of the data in the database, this must be done at the request of the Personal Data Controller. Following such a request, the counsel has 60 days to produce the information that the Personal Data Controller has asked to be deleted and to remove the information from the database.
-

5. Specify the specific technical and organisational security measures with regard to the Processing of Personal Data carried out by the Processor(s)

- We encrypt all data at rest and data in transit
- We conduct ongoing internal reviews to ensure and develop our ability to continuously ensure the confidentiality, integrity, availability and resilience of our systems.
- We are committed to restoring, as far as technically possible, the availability and accessibility of personal data in a timely manner in the event of a physical or technical incident.

- We regularly test, examine and evaluate the effectiveness of the technical and organisational measures that ensure the security of the processing.
- We limit access to data within our organisation to the direct needs of staff based on their ability to perform their duties to customers.
- All services where we store personal data are protected by two-factor login requirements.
- We restrict third-party vendor access via Google Cloud access approval

6. Specify specific requirements for Logging with regard to the Processing of Personal Data and who should have access to them

General use of logs in the application

- the documentation of the access (logs) shows what action has been taken with the data of a data subject,
- the logs show the unit where the action was taken,
- the logs show the time at which the measures were taken,
- the identity of the user and the data subject is shown in the logs,
- systematic and regular spot checks of the logs are carried out,
- checks of the logs are automatically documented through audit logs.

Audit logs are kept for 400 days. (E.g. account X did operation Y in product Z)

- History of Online Partner employees who have retrieved data

Server logs are saved for 90 days (E.g. user X called Y on API)

- History of change for individual students and who made the change.
- History of change for individual employees and who implemented the change.

Access transparency logs

- History of what, when, why and from whom Google has been given access to parts of Online Partner’s projects for the purpose of support.

7. Localisation and transfer of Personal Data to Third Countries

- As part of the performance by the Processor of the services provided under the Service Agreement, de-identified personal data related to staff support issues and personal data in the form of contact details such as name, telephone number and e-mail address pertaining to the Controller's staff may be transferred to third countries via the Processor's subcontractor, see Appendix 2.
- The processor shall ensure that transfers to third countries comply with the requirements of the GDPR. See Appendix 3.

8. Other Instructions on the Processing of Personal Data by the Processor(s)

- The Personal Data Processor shall be able to provide the Personal Data Controller with a complete extract from the register covering only the personal data of a data subject processed in the system at the request of the Personal Data Controller.

- The Personal Data Processor shall have procedures to assist the Personal Data Controller in complying with the requirement to report a personal data breach within 72 hours of the Personal Data Controller becoming aware of the personal data breach.
- Appendix 3 and the safeguards presented therein in relation to Case C-311/18, "Schrems II" will be reviewed and updated on an ongoing basis.

APPENDIX 2. LIST OF SUBCONTRACTORS FOR THE CLASS MANAGER APPLICATION

Subcontractor: Google Cloud Platform	**Contact information:** Privacy Help Centre – Policies Help
Geographical location and agreements: Servers within EU/EEA Frankfurt. (May be processed in third countries on specific occasions. See Appendix 3.) Our Cloud Data Privacy Commitments Google Cloud Platform: EU Model Contract Clauses	**Type of service:** Operation of database and applications. (Cloud service)
Used by the following services: Class Manager teacher panel	**Data processed:** Names, e-mail addresses, groups, Public IP address

SUBCONTRACTORS FOR THE TRELSON CLASSROOM MANAGER APPLICATION FOR SPECIFIC SERVICES AND CONTRACTS

Subcontractor: Zendesk	**Contact information:** Zendesk's Global Privacy Counsel: Rachel Tobin, AGC, EMEA and Global Privacy Counsel, Zendesk International Ltd. 55 Charlemont Place, Saint Kevin's, Dublin, D02 F985 Ireland privacy@zendesk.com
Geographical location and agreements: EU, USA Privacy Policy Privacy and Data Protection (With information on Binding corporate rules and Standard contract clauses) Update on Privacy Shield Invalidation by the European Court of Justice	**Type of service:** Support system to manage and respond to customer requests.
Used by the following services: Online Partner Support	**Data processed:** First name, Last name, E-mail address

Subcontractor: Mailjet	**Contact information:** Data Protection Officer, Darine Fayed, Head of Legal. privacy@mailjet.com Mailjet, privacy@mailgun.com
Geographical location and agreements: EU, USA (Only in limited circumstances, See Appendix 3.) https://www.mailjet.com/legal/privacy-policy/	**Type of service:** Mailjet is used to send a reminder email for teachers about automatic archiving of their Google Classroom courses three days prior to taking that action. Mailjet is also used to notify the specified users mentioned under the application's settings menu, about the summary of the orphaned courses being adopted.
Used by the following services: Trelson Class Manager Backend	**Data processed:** First name, Last name, E-mail address

APPENDIX 3. ADDITIONAL SAFEGUARDS TO ENSURE TRANSFERABILITY, USING STANDARD CONTRACT CLAUSES AND BINDING CORPORATE RULES (BCR), TO THE THIRD COUNTRY CONCERNING Classroom Manager

Following the 16 July 2020 "Schrems II" ruling (Case C-311/18), the Privacy Shield no longer applies as a legal basis for the processing of personal data transferred to the US. Companies that need to transfer personal data to the US must now enter into Standard Contractual Clauses and, where appropriate, take additional safeguards. This document describes the additional safeguards we as a company (Online Partner AB) have put in place to further protect personal data when processed in the United States.

This document and safeguards will be reviewed and updated on an ongoing basis.

Online Partner has noted that the following services and subcontracts involve or may involve transfer to the United States. Online Partner has considered and analysed the case where the Trelson Classroom Manager application can be provided without the services listed below. After analysing the market and the purpose and content of the service, it has been concluded that the services are necessary to provide Trelson Classroom Manager to our customers and users. Online Partner has therefore analysed the services and taken additional protective measures.

1 GENERAL ORGANISATIONAL SECURITY MEASURES AT ONLINE PARTNER

Account management at Online Partner

Online Partner staff receive an account in Google workspace upon accessing their service, which is used as an SSO service against all other applications used in the company. In order to log in to their Google Workspace account on Online Partner, all employees must use the two-factor login policy set by the company. Other than the specific employee, only an administrator can reset an account to access personal data. This administrator is managed with a no-reply account that has a physical two-factor login on a USB stored in a secure location.

Access to users' personal data on Online Partner

At Online Partner, we work on the premise that only those persons whose job duties require them to handle users' personal data have access to the personal data. This means that only the staff of each specific service has access to the personal data. Staff have confidentiality obligations regarding the personal data processed.

Physical units in the company

All devices used on Online Partner use the latest security updates and hard drive encryption. The services used are cloud-based and protected by an additional layer with two-factor login. See "Account management on Online Partner 1.1"

Shell protection in the company

The office is located on the second and third floors and is accessible only from the stairwell and fire escape at the rear. The front door to the premises is Daloc and steel, it is classified according to SSF Certificate 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 working rooms.

Access to users' personal data on Online Partner

At Online Partner, we work on the premise that only those persons whose job duties require them to handle users' personal data have access to the personal data. This means that only the staff of each specific service has access to the personal data. Staff have confidentiality obligations regarding the personal data processed.

Physical units in the company

All devices used on Online Partner use the latest security updates and hard drive encryption. The services used are cloud-based and protected by an additional layer with two-factor login. See "Account management on Online Partner 1.1"

Shell protection in the company

The office is located on the second and third floors. The front door to the premises is made of steel, it is classified according to the SSF Certificate.

The door has two separate locking devices; night lock and day lock.

Burglar alarm

We have a burglar alarm linked to Bevakningsassistans Stockholm, which sends out security guards in the event that the alarm is triggered.

Camera surveillance

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

2 DATA PROCESSORS FOR THE TRELSON CLASSROOM MANAGER APPLICATION

Google Cloud Platform

2.1.1 Analysis of possible transfer to third countries

To which country outside the EU can data be sent?

In exceptional cases, the USA.

When might personal data be transferred to the US?

Google Cloud may process personal data outside the EU through the Firebase Hosting service. Firebase Hosting provides global edge caching based on the country you are physically located in when using Classroom Manager.. Edge caching works by selecting the nearest server based on your geographical location. The servers that manage Firebase Hosting when the service is used within the EU are located in Zurich (europe-west6) and Frankfurt (europe-west3). These servers will be the natural servers when the service is used in Sweden. Europe-west3 is also the server on which we operate our other parts of Google Cloud due to its geographical proximity. **This means that the only likely time that personal data may be transferred to the US is if the user is outside the EU. The purpose of our service is to be used in Sweden, which is why Online Partner expects that transfers to the United States will only be made to a very limited extent.**

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

More information about Firebase Hosting can be found here:

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

What personal data may be transferred to the US

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

Type of personal data related to Google Cloud Platform

E-mail, first name, last name, group membership, IP address

2.1.2 Additional safeguards

Google's Global Safeguards:

Google has a global infrastructure designed to manage information securely throughout its lifecycle. This infrastructure enables the 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.

The security of the infrastructure is built from the ground up in progressive layers, starting with the security of Google's data centre and ending with the processes for managing the services.

Google invests heavily in the security of its infrastructure and has hundreds of staff 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

Restricting access to data for Google employees through Access approval

All projects in Google Cloud that involve personal data and are owned by Online Partner have the strictest level of access approval, which means that access to projects by Google employees will require explicit approval from an Online Partner employee with sufficiently high authority in the project.

Read more about Access approval at Google here:

https://cloud.google.com/access-approval/docs?hl=e

Review of data access for Google employees through Access transparency

If permission is granted for Google employees to access Online Partner’s projects in Google Cloud, all actions taken by them will be saved in special audit logs for the projects.

Read more about Access transparency here:

https://cloud.google.com/logging/docs/audit/access-transparency-overview

Restricting access to data for Online Partner employees

Online Partner has previously restricted all access to data and personal information in Google Cloud Platform. Only staff with a direct need have access to personal data. This is in order to perform their duties so that our users receive the best level of service from the Trelson Classroom Manager service. Staff have confidentiality obligations regarding the personal data processed.

Audit logs

Online Partner saves audit logs of administrative events and data access in Google Cloud Platform. This is in order to be able to deal with possible personal data incidents.

Encrypted network communication

Online Partner uses encrypted communication protocols between service to service and service to 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 accounts for Single Sign On with two-factor authentication.

Documentation in relation to SCC (Standard contract clauses)
https://cloud.google.com/terms/sccs
https://cloud.google.com/security/privacy

3 DATA PROCESSORS FOR THE CLASSROOM MANAGER APPLICATION REGARDING SPECIFIC SERVICES AND CONTRACTS

Zendesk

3.1.1 Analysis of possible transfer to third countries To which country outside the EU can data be sent?

In exceptional cases, USA

When might personal data be transferred to the US?

Support system to manage and respond to user requests. This means that Zendesk is only used for support issues and not for using the application. Under FISA and the Cloud Act, the US government can request personal data from European citizens in relation to serious crimes against the US. Online Partner has signed a Data Processing Agreement with Zendesk.

Type of personal data related to Zendesk

First name, last name, e-mail address

What personal data may be transferred to the US

First name, last name, e-mail address

Documentation in relation to ECC/SCC (EU/Standard contract clauses) and BCR (Binding Corporate Rules)

https://www.zendesk.com/company/privacy-and-data-protection/

3.1.2 Additional security measures

Zendesk's security measures

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

All data at rest and in transit is encrypted

Independent penetration testing is conducted on an annual basis

All data is restricted by role-based access control

How We Protect Your Service Data (Enterprise Services)

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

Data storage

All personal data processed by Zendesk is stored on servers within the EU.

Restricting access to data

Only staff with a direct need have access to personal data. This is in order to perform their duties so that our customers receive the best level of service from the Trelson Classroom Manager service. Staff have confidentiality obligations regarding the personal data processed. Online Partner has regular training for support staff in personal data management.

Procedures for deletion

Updated procedure for the deletion of cases. When a case is closed, we keep the case for 6 months for possible follow-up.

Training

We regularly train our support staff in relation to managing 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 data other than the e-mail address and name submitted to Online Partner in support cases is masked, i.e. permanently hidden.

Login

All login to Zendesk is through SSO for G Suite where two-factor login is a requirement. See "Account management on Online Partner" 1.1

Zendesk support

Account takeover by Zendesk support is disabled and can only be activated by administrators. The account takeover procedure is only temporary during the process of the actual support case.

Mailjet

3.2.1 Analysis of possible transfer to third countries

To which country outside the EU can data be sent?

In exceptional cases, the USA.

When might personal data be transferred to the US?

Except for the limited circumstances personal data is not shared with third parties. When there is a need to provide personal data to third parties, it is shared to an extent necessary to provide you with Mailjet's services, and it's ensured that it is in place of data protection requirements with these third parties (including standard contractual clauses as well as the requisite technical and organisational measures).

Personal data as required or permitted by law and as to optimally provide Mailjet's services through third party providers as described below.

Mailjet Service processes the personal data outside the EU through third parties including Google Cloud Platform, AWS® and Rackspace®. Our platform will be hosted from third parties data centres throughout the United States or Europe, based on where we have selected to deploy Mailjet's services. **This means that the only likely time that personal data may be transferred to the US is if the user is outside the EU. The purpose of our service is to be used in Sweden, which is why Online Partner expects that transfers to the United States will only be made to a very limited extent.**

What personal data may be transferred to the US

E-mail, first name, last name

Type of personal data related to Mailjet

E-mail, first name, last name

Documentation in relation to ECC/SCC (EU/Standard contract clauses) and BCR (Binding Corporate Rules)

https://www.mailjet.com/legal/dpa/

3.2.2 Additional security measures

Mailjet's Security Measures:

To ensure internal IT and IT security governance and management as well as assurance of processes and products

- *ISO 27001 certification*
- *ISO 27701 certification*
- *SOC 2 Type 2 report*

Mailjet complies with the European General Data Protection Regulation 2016/679 (GDPR) as well as all applicable data protection laws. For all transfers of personal data from the EU and EEA, they maintain EU Standard contractual clauses where necessary, ensure additional safeguards such as data encryption and data minimization, as well as perform audits and controls on our important sub processors.

https://www.mailjet.com/legal/privacy-policy/

https://www.mailjet.com/legal/dpa/

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

Data storage

All personal data processed by Mailjet is stored on servers within the EU

Restricting access to data

Online Partner has previously restricted all access to data and personal information. Only staff with a direct need have access to personal data. This is in order to perform their duties so that our users receive the best level of service from the Trelson Classroom Manager service. Staff have confidentiality obligations regarding the personal data processed.

Procedures for deletion

The personal data are deleted upon change/removal of users under settings of Trelson Class Manger application by the administrators**.**