Data Processing Agreement

Table of contents

DATA PROCESSING AGREEMENT

Agreement pursuant to Article 28.3 of the General Data Protection Regulation EU 2016/679[1]

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

Data Controller	**Data Processor**
	Trelson AB
Corporate ID no.	**Corporate ID no.**
	559459-4649
Mailing address	**Mailing address**
	Mejerivägen 3 117 43 Stockholm
Contact person for administration of this Data Processing Agreement	**Contact person for administration of this Data Processing Agreement**
Name: Email: Phone:	Name: Jonatan Brown Email: jonatan.brown@trelson.com Phone: +46 760225820
Contact person for cooperation between the Parties about data protection	**Contact person for cooperation between the Parties about data protection**
Name: Email: Phone:	Name: Ramón Navarro Marttinen Email: ramon.marttinen@onlinepartner.se Phone: 08-420 004 21

2 DEFINITIONS

2.1 In addition to the concepts defined in the text for the Data Processing Agreement, these definitions shall, regardless of whether they are used in the plural or singular, in definite or indefinite form, have the following meaning when entered with capital letters as the initial letter.

[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.

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..

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, where an identifiable natural person is a person who directly or indirectly can be identified in particular by reference to an identifier such as name, social security number, location data or online identifiers or one or more factors which are specific to the natural person's physical, physiological, genetic, psychological, economic, cultural or social identity.

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's Processing 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").

3.2 When this Agreement forms one of several contractual documents within the framework of another agreement, the second agreement is referred to as the "Main Agreement" in this Agreement.

3.3 If anything stipulated in item 1, paragraph 3.2, item 15 or 16, paragraph 17.6, items 18–20 or 22 in this Agreement is otherwise regulated in the Main Agreement, the regulation of the Main Agreement shall have precedence.

3.4 References in this Agreement to national or EU legislation refer to applicable regulations at any given time.

4 PROCESSING OF PERSONAL DATA AND SPECIFICATION

4.1 The Controller hereby appoints the Processor to carry out the Processing on behalf of the Controller in accordance with this Agreement.

4.2 The Controller shall give written instructions to the Processor on how the Processing should be carried out.

4.3 The Processor may only carry out the Processing pertaining to this Agreement and the instructions in force 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 for compiling correct Instructions with regard to the nature of the Processing so that the Processor and any Subprocessor can fulfil their tasks according to this Agreement and Main Agreement, where applicable.

5.2 The Controller shall, without unnecessary delay, inform the Processor of changes in the Processing which affect the Processor's obligations pursuant to Data Protection Legislation.

5.3 The Controller is responsible for informing Data Subjects about the Processing and protecting the rights of Data Subjects according to Data Protection Legislation as well as taking any other action incumbent on the Controller according to Data Protection Legislation.

6 OBLIGATIONS OF THE PROCESSOR

6.1 The Processor undertakes to only perform the Processing in accordance with this Agreement and for the specific purposes stipulated in the Instructions, as well as to comply with Data Protection Legislation. The Processor also undertakes to continuously remain informed about applicable law in this area.

6.2 The Processor shall take measures to protect the Personal Data against all types of Processing which are incompatible with this Agreement, Instructions and Data Protection Legislation.

6.3 The Processor undertakes to ensure that all natural persons working under its management follow this Agreement and Instructions and that such natural persons are informed of relevant legislation.

6.4 The Processor shall, at the request of the Controller, assist in ensuring that the obligations pertaining to Articles 32-36 in the GDPR are fulfilled and respond to requests for the exercise of a Data Subject's rights pertaining to the GDPR, Chapter III, taking into account the type of Processing and the information which the Processor has access to.

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, if the Parties have not agreed otherwise.

6.6 If the Controller provides the Processor with new or revised Instructions, the Processor shall without unnecessary delay from receipt, communicate to the Controller whether the implementation of the new Instructions causes changed costs for the Processor.

7 SECURITY MEASURES

7.1 The Processor shall take all appropriate technical and organisational security measures required pertaining to Data Protection Legislation to prevent Personal Data Breaches, by ensuring that the procedure of Processing meets the requirements of the GDPR and that the rights of the Data Subjects are protected.

7.2 The Processor shall continuously ensure that the technical and organisational security in connection with Processing is executed with an appropriate level of confidentiality, integrity, accessibility and resilience.

7.3 Any added or revised requirements for protective measures from the Data Controller, after the Parties have signed this Agreement, will be considered as new Instructions pertaining to this Agreement.

7.4 The Processor shall, through its control systems for authority, only grant access to the Personal Data for such natural persons working under the Processor's management and who need access to be able to perform their duties.

7.5 The Processor undertakes to continuously log access to the Personal Data in accordance with this Agreement to the extent required according to the Instructions. Logs may be erased only five (5) years after the logging event, unless otherwise stated in the Instructions. Logs will be subject to the required protection measures pertaining to Data Protection Legislation.

7.6 The Processor shall systematically test, investigate and evaluate the effectiveness of the technical and organisational measures which will ensure the security of the Processing.

8 SECRECY/DUTY OF CONFIDENTIALITY

8.1 The Processor and all natural persons working under its management shall observe both confidentiality and professional secrecy during the Processing. The Personal Data may not be used or disseminated for other purposes, either directly or indirectly, unless otherwise agreed.

8.2 The Processor shall ensure that all natural persons working under its management, participating in the Processing, are bound by a confidentiality agreement pertaining to the Processing. However, this is not a requirement if they are already covered by a legally sanctioned duty of confidentiality. The Processor also undertakes to ensure that there is a nondisclosure agreement with its Subprocessor and confidentiality agreement between the Subprocessor and all natural persons working under its management, participating in the Processing.

8.3 The Processor shall promptly inform the Controller of any contacts with supervisory authorities pertaining to the Processing. The Processor does not have the right to represent the Controller or act on behalf of the Controller towards supervisory authorities in matters relating to the Processing.

8.4 If the Data Subject, supervisory authority or third Party requests information from the Processor pertaining to the Processing, the Processor shall inform the Controller about the matter. Information about the Processing may not be submitted to the Data Subject, supervisory authority or third parties without written consent from the Controller, unless mandatory law so stipulates that such information must be provided. The Processor shall assist with the communication of the information covered by a consent or legal requirement.

9 INSPECTION, SUPERVISION AND AUDITING

9.1 The Processor shall, without unnecessary delay, as part of its guarantees, pursuant to Article 28.1 of the GDPR, be able to report, at the request of the Controller, which technical and organisational security measures are being used for the processing to meet the requirements according to the DPA and Article 28.3.h of the GDPR.

9.2 The Processor shall review the security of the Processing at least once a year by performing a check to ensure that the Processing complies with this Agreement. Upon request, the results of such checks shall be shared with the Controller.

9.3 The Controller or a third party it appoints (who cannot be a competitor of the Processor) is entitled to check that the Processor meets the requirements of this Agreement, Instructions and Data Protection Legislation. During such a check, the Controller shall assist the Controller, or the person carrying out the review on behalf of the Controller, with documentation, access to premises, IT systems and other assets needed to be able to check the compliance of the Controller with this Agreement, Instructions and Data Protection Legislation. The Controller shall ensure that staff who carry out the check are subject to confidentiality or non-disclosure obligations pertaining to law or agreement.

9.4 As an alternative to the stipulations of items 9.2–9.3, the Processor is entitled to offer other means of checking the Processing, such as checks carried out by independent third parties. In

such a case, the Controller shall have the right, but not the obligation, to apply such alternative means. In the event of such a check, the Processor shall provide the Controller or third party with the assistance needed for performing the check.

9.5 The Processor shall provide the supervisory authority, or other authority which has the legal right to do so, the means to carry out supervision according to the authority's request pertaining to the legislation in force at any time, even if such supervision would otherwise be in conflict with the provisions of this Agreement.

9.6 The Processor shall assure the Controller rights towards any Subprocessor corresponding to all of the rights of the Controller towards the Processor according to section 9 of this Agreement.

10 HANDLING OF CORRECTIONS AND DELETIONS ETC

10.1 In the case of the Controller requesting correction or deletion due to incorrect processing by the Processor, the Controller shall take appropriate action without unnecessary delay, within thirty (30) days at the latest, from the time the Processor has received the required information from the Controller. When the Controller requests deletion, the Processor may only carry out Processing of the Personal Data in question as part of the process for correction or deletion.

10.2 If technical and organisational measures (e.g., upgrades or troubleshooting) are taken by the Processor in the Processing, which can have an effect on the Processing, the Processor shall inform the Controller in writing pursuant to what is stipulated about notifications in item 18 of this Agreement. The information shall be submitted in good time prior to the measures being taken.

11 PERSONAL DATA BREACHES

11.1 The Processor shall have the capability to restore accessibility and access to Personal Data within a reasonable time in the event of a physical or technical incident pertaining to Article 32.1.c of the GDPR.

11.2 The Processor undertakes to, with regards to the type of processing and the information that the Processor has access to, assist the Controller to fulfil its obligations in the case of a personal data breach in regards to processing. The Processor shall at the request of the Controller also assist in investigating suspicions of possible unauthorised access or processing of Personal Data.

11.3 In the event of a Personal Data Breach, which the Processor has been made aware of, the Processor shall notify the Controller of the Breach in writing without unnecessary delay. The Processor shall, taking into account the type of Processing and the information available to the Processor, provide the Controller with a written description of the Personal Data Breach.

11.4 The description shall give an account of:

a. The nature of the Personal Data Breach and, if possible, the categories and number of Data Subjects affected and the categories and number of Personal Data records affected,
b. the likely impact of the Personal Data Breach, and
c. measures taken or proposed and measures to mitigate the potential negative effects of the Personal Data Breach.

11.5 If it is not possible for the Processor to provide the full description at the same time, according to item 11.3 of this Agreement, the description may be provided in instalments without unnecessary further delay.

12 SUBPROCESSOR

12.1 The Processor is entitled to hire the Subprocessor(s) listed in the Subprocessor appendix. 2.

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. The Subprocessor shall 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 shall ensure in its agreement with the Subprocessor that the Controller is entitled to terminate the Subprocessor and instruct the Subprocessor to, for instance, erase or return the Personal Data if the Processor has ceased to exist in the actual or legal sense, or has entered into insolvency.

12.4 The Processor shall be fully responsible for the Subprocessor's Processing on behalf of the Controller. The Processor shall promptly inform the Controller if the Subprocessor fails to fulfil its undertakings under the Agreement.

12.5 The Processor is entitled to hire new subprocessors and to replace existing subprocessors unless otherwise stated in the Instructions.

12.6 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

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

12.7 The Controller is entitled within thirty (30) days of the notice pursuant to item 12.6 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 16.4 of this Agreement.

12.8 The data processor shall at all times keep a correct and updated list of the subprocessors hired for the Processing of Personal Data on behalf of the Controller and make the list accessible to the Controller. The list shall specifically state in which country the Subprocessor Processes Personal Data and types of Processing the Subprocessor carries out.

12.9 When the Processor ends its collaboration with a Subprocessor, the Processor shall notify the Controller in writing. When an agreement terminates, the Processor shall ensure that the Subprocessor erases or returns the Personal Data.

12.10 At the Controller's request, the Processor shall send a copy of the agreement regulating the Subprocessor's Processing of Personal Data in accordance to item 12.2 and the list of subprocessors in accordance with item 12.1.

13 LOCALISATION AND TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

13.1 The Processor shall ensure that the Personal Data shall 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 in accordance with 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 DAMAGE IN CONNECTION WITH THE PROCESSING

14.1 In the event of a compensation for damage in connection with Processing, through a judgement given or settlement, to be paid to a Data Subject due to an infringement of a provision in the Agreement, Instructions and/or applicable provision in Data Protection Legislation, Article 82 of the GDPR shall apply.

14.2 Fines pursuant to Article 83 of the GDPR, or Chapter 6, Section 2 of the Data Protection Act (2018:218) with supplementary provisions to the EU's data protection regulation shall be borne by the Party to the Agreement named as recipient of such sanctions.

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 Regardless of the content of the Main Agreement, items 14.1 and 14.2 of this Agreement take precedence to other rules on the distribution between the Parties of claims among themselves as far as the processing is concerned.

15 CONCLUSION, TERM AND TERMINATION OF THIS AGREEMENT

15.1 This Agreement shall enter into force from the time the Agreement is signed by both Parties and until further notice. Either party has the right to terminate the Agreement with thirty (30) days' notice.

16 AMENDMENTS AND TERMINATION WITH IMMEDIATE EFFECT, ETC.

16.1 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.

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

16.3 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.

16.4 If the Controller objects to the Processor using a new Subprocessor, pursuant to item 12.7 of this Agreement, the Controller is entitled to terminate the Agreement with immediate effect.

17 MEASURES IN THE EVENT OF TERMINATION OF THE AGREEMENT

17.1 Upon termination of the Agreement, the Processor shall, without unnecessary delay, depending on what the Controller chooses, either delete and certify to the Controller that it has been carried out, or return

a. all Personal Data Processed on behalf of the Controller and

b. all associated information such as Logs, Instructions, system solutions, descriptions and other documents which the Processor has obtained through information exchange in pursuance of the Agreement.

17.2 In connection with the return of data, the Processor shall also delete existing copies of Personal Data and associated information.

17.3 The obligation to delete or return Personal Data or/and associated information does not apply if storage of the Personal Data or information is required under EU law or relevant national law where Processing may be carried out pursuant to the Agreement.

17.4 If Personal Data or associated information is returned, it must be in a commonly used and standardised format, unless the Parties have agreed to another format.

17.5 Until the data is deleted or returned, the Processor shall ensure compliance with the Agreement.

17.6 Return or deletion pertaining to the Agreement shall be carried out no later than thirty (30) calendar days counting from the time of termination of the Agreement, unless otherwise stated in the Instructions. Processing of Personal Data which the Processor subsequently carried out shall be regarded as unauthorised Processing.

17.7 Confidentiality/professional secrecy in item 8 shall continue to apply even if the Agreement otherwise ceases to apply.

18 NOTIFICATIONS WITHIN THE PURVIEW OF THIS AGREEMENT AND THE INSTRUCTIONS

18.1 Notifications about the Agreement and its administration, including termination, shall be submitted via email or in any other manner agreed by the Parties to each Party's contact person for the Agreement.

18.2 Notifications about the collaboration of the Parties regarding the data protection shall be submitted via email or in any other manner agreed by the Parties to each Party's contact for the Parties' cooperation on data protection.

18.3 A notification shall be deemed to have reached the recipient no later than one (1) business day after the notification has been sent.

19 CONTACT PERSONS

19.1 Each Party shall appoint their contact person for the Agreement.

19.2 Each Party shall appoint their contact person for the Parties' cooperation on data protection.

20 RESPONSIBILITY FOR INFORMATION REGARDING PARTIES, CONTACT PERSONS AND CONTACT INFORMATION

20.1 Each Party is responsible for the information entered in item 1 of the Agreement always being current and correct.

20.2 Change of information in item 1 shall be communicated to the other Party pursuant to item 18.1 of the Agreement.

21 CHOICE OF LAW AND DISPUTES

21.1 When interpreting and applying the Agreement, Swedish law shall apply with the exception of the choice of law rules. Disputes regarding the Agreement shall be settled by a competent Swedish court.

22 THE PARTIES' SIGNATURES ON THE AGREEMENT

22.1 The Agreement can be produced either in digital format for electronic signature or in paper format for manual signature. In the latter case, the Agreement is drawn up in two identical copies, whereof each Party receives one.

22.2 If the Agreement is signed electronically, the page with signature shall be ignored.

_____

[Rest of the page has intentionally been left blank. Signature page follows.]

Controller	**Processor**
	Trelson AB
Place and date:	Place and date:
_____	_____
Name in print	Name in print
_____	_____
Signature	Signature

Appendix 1 - The Controller's instruction for the processing of Personal Data

In addition to what is already mentioned in the Data Processing Agreement, the Processor shall also follow the following Instructions:

1. The purpose, object and nature
1 a. The object of the Processing of Personal Data by the Processor for the Controller is to: Personal data is processed in the Trelson Assessment application to provide a service for digital tests, such as national tests. 1 b. The objective of the Processing of Personal Data by the Processor for the Controller is to: The personal data is used to link which user(s) will have access to the test and which test they have submitted. 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. 1 c. The Processing of Personal Data by the Processor on behalf of the Controller refers mainly to the following measure of Processing (type or nature of the Processing): Types of processing include reading, storage, transfer, structuring and usage.
2. The Processing includes the following types of Personal Data
The Processor has the right to Process the following types of Personal Data on behalf of the Controller: ● First name ● Last name ● E-mail address ● Group membership ● IP address ● Submissions and feedback

3. Processing covers certain categories of Data Subject

The Processor has the right to process Personal Data regarding the following categories of Data Subjects:

- Staff
- Pupils

4. Specify special requirements when it comes to Processing of Personal Data carried out by the Processor

The Processor must observe the following Processing requirements when Processing Personal Data on behalf of the Controller:

- At the request of the Personal Data Controller, the Personal Data Processor shall delete specified information containing personal data. After the request, the Processor 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 Processor 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 special technical and organisational security measures which apply to the Processing of Personal Data by the Processor

The Processor shall take the following security measures when Processing Personal Data:

- 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 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 special requirements for logging with regard to the Processing of Personal Data and who should have access to them

The Processor shall observe the following requirements regarding the user activity and Processing of logs:

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 Trelson employees who have retrieved data

● 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 Trelson's projects for the purpose of support

7. Location and transfer of Personal Data to Third Countries

The Processor shall observe the following requirements regarding the location of Personal Data:

The Processor is only entitled to Process the Personal Data at the following locations:

- EU/EES, USA

If the Controller has not given instructions on the transfer of Personal Data to a Third Country, the Processor shall not have the right to make such a transfer.

The Processor shall observe the following requirements for transferring Personal Data to a Third Country:

● 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.
● Google and Zendesk are certified in accordance to the EU-US Data Privacy Framework
● Transfer of personal data to the USA is covered by standard contractual clauses
● The processor shall ensure that transfers to third countries comply with the requirements of the GDPR. See Appendix 3.

8. Duration of Processing

The Processor will manage personal data in accordance with the DPA until the agreement ceases.

9. Other Instructions regarding the Processing of Personal Data carried out by the Processor

● 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 approved Subprocessors

The Controller approves the hiring of the Subprocessors below by the Processor for the Processing of Personal Data.

Company/organisation	Address and contact details	Location of Personal Data (address, country)	Types of Personal Data Processed by the Subprocessor	Purpose of processing by the Subprocessor	Processing time	Additional information about the Subprocessor's Processing of Personal Data
Google Cloud Platform	Privacy Help	Servers within EU/EES Frankfurt.	Names, E-mail, Groups, Public IP-adress, Submissions and feedback	Operation of database and applications (Cloud service)	Personal data will be continually managed as long as the DPA is valid.	Our Cloud Data Privacy Commitments Google Cloud Platform: EU Standard Contractual Clauses Google-LLC are certified in accordance with the EU-US Data Privacy Framework.
Zendesk	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	EU, USA	First name, Last name, E-mail	Support system for answering and managing customer questions and issues.	Zendesk is used by support and not as part of the regular application usage. The subprocessor managed personal data in accordance with the subprocessor agreement.	Trust Center Update on Privacy Shield Zendesk are certified in accordance with the EU-US Data Privacy Framework.
Mailjet	Contact form	Germany, Belgium	E-mail	Processes e-mail address if the end-user subscribes to the newsletters.	Personal data is processed as long as end-user is subscribed to	Privacy Policy

					the newsletters.	

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

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. On July 10, 2023, the European Commission adopted a decision on an adequate level of protection for the United States. The European Commission's decision means that transfers to organizations covered by the EU-US Data Privacy Framework can now take place without the need for appropriate safeguards, such as standard contractual clauses, under Article 46 of the General Data Protection Regulation. Google and Zendesk are certified under the EU-US Data Privacy Framework. This document describes the additional safeguards we as a company (Trelson 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.

Trelson has noted that the following subcontracts involve or may involve transfer to the United States. Trelson has considered and analysed the case where the Trelson Assessment 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 Assessment to our customers and users. Trelson has therefore analysed the services and taken additional protective measures.

1 GENERAL ORGANISATIONAL SECURITY MEASURES AT Trelson

Account management at Trelson

Trelson 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 Trelson, 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 Trelson

At Trelson, 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 Trelson 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 Trelson 1.1"

Shell protection in the company

The office is located on the fifth floor and is accessible only from the stairwell and fire escape at the rear. The front door to the premises is from Thoruns AB of the brand Forster Presto.

Burglar alarm

The office is equipped with a burglar alarm and camera surveillance.

2 DATA PROCESSORS FOR THE TRELSON ASSESSMENT APPLICATION

Google Cloud Platform 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 Trelson 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 Trelson have the strictest level of access approval, which means that access to projects by Google employees will require explicit approval from a Trelson 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 Trelson'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 Trelson employees

Trelson 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 Assessment service. Staff have confidentiality obligations regarding the personal data processed.

Audit logs

Trelson 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

Trelson uses encrypted communication protocols between service to service and service to end user.

End-user login with Single Sign On

Trelson 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 TRELSON ASSESSMENT 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. Trelson 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 Trelson 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 Assessment service. Staff have confidentiality obligations regarding the personal data processed. Trelson 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

Trelson 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 Trelson 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 Trelson" 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.