Processing agreement

This processing agreement describes the conditions for the processing of personal data by Learned BV, on behalf of the Customer, on the basis of the Connection Contract agreed between the Parties.
This processing agreement forms an integral and inseparable part of the Terms and Conditions that apply to the Learned Platform.

Article 1) ***Definitions***

1. In this Processing Agreement, the term “GDPR” means the General Data Protection Regulation and all laws and regulations that may replace this law in the future.
2. Terms defined in the GDPR have the same definition in this Processing Agreement, unless a different definition is given here.
3. The Customer is regarded as the Controller within the meaning of Article 4(7) of the GDPR.
4. Learned is regarded as a Processor within the meaning of Article 4(8) of the GDPR.
5. The term “Personal Data” includes Personal Data relating to the Controller's personnel, its customers and/or other relations. Learned distinguishes between two categories of personal data “System critical personal data” and “Sensitive personal data”.

6. The term “Subprocessor” is understood to mean a legal entity that is or is engaged by and on behalf of the Processor for the purpose of processing Personal Data in the context of the provision of Services by the Processor to the Controller, whereby the engaged legal entity has Personal Data or access can receive Personal Data.

Article 2) ***Goals and means***

1. Customer has control over the personal data that it, as controller, provides to Processor in the context of the execution of the Connection Contract, including all updates, changes, corrections and/or extensions of that personal data.
2. Processor agrees that the purposes of processing personal data will be determined solely by Customer in its capacity as controller. The personal data, data subjects and purposes for which the personal data are processed are set out in Appendix 1.

3. The Processor will only process the personal data to the extent necessary for the performance of its services to the Customer and taking into account the purposes as determined by the Customer (and described in Appendix 1) or to the extent that this is required on the basis of a legal requirement.
   The personal data will not be stored, retained or processed in any other way by the Processor for other purposes.
4. The GDPR (from May 25, 2018), the Telecommunications Act and all other applicable (European) privacy regulations apply to this Processing Agreement.

Article 3) ***Security*** 1.

The processor will take the appropriate technical and organizational measures required under Article 32 GDPR to ensure a level of security appropriate to the risk level. These measures will be implemented in such a way that they guarantee an appropriate level of security, confidentiality, integrity and availability of the personal data tailored to the risk, taking into account the state of the art and the costs of implementation. These measures concern in any case:

- measures to ensure that only authorized personnel have access to the personal data for the purposes set out in Appendix 1 to this Agreement;
- measures to protect personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;

- measures to identify weaknesses with regard to the processing of personal data in the systems used to provide services to the Customer.

2. Without written permission from the Customer, the Processor will not carry out the processing of personal data in a country outside the European Economic Area without an adequate level of protection or have the processing carried out by a third party. Customer will not withhold its consent on unreasonable grounds. The processor will take appropriate safeguards to ensure that the transfer of personal data to a country outside the European Economic Area without an adequate level of protection takes place lawfully.

3. At the request of the Customer, the Processor will inform the Customer about the measures taken as referred to in Article 3, paragraphs 1 and 2, including in any case the location of the servers and other equipment on which the personal data are stored or with which the personal data are otherwise processed. The Processor will make proposals to the Customer as soon as possible for changes to the measures if the Customer is of the opinion that the measures taken are insufficiently effective or appropriate in relation to the risks identified by the Customer or Processor for the protection of personal data or the rights and interests of The involved. The Customer will not withhold its approval of the proposed measures if they are reasonable in view of the risks associated with the nature of the personal data, the intended processing, the state of the art and the costs of implementation.
The costs of implementing the proposed measures are borne by the Processor.

4. Processor will support the Customer in meeting the Customer's obligations under Articles 32 to 36 of the GDPR, such as supporting the implementation of a Data Protection Impact Assessment (also known as: “DPIA”), if this are necessary. If necessary, Learned may charge costs for the cooperation provided, based on Learned's usual hourly rates.

Article 4) ***Enabling Subprocessors***

1. The Processor may engage Sub-processors when processing Personal Data. The Customer grants Processor specific permission to engage the Sub-processors listed in Appendix 1b: Sub-processors.

2. During the collaboration, the processor may engage new sub-processors who process system-critical personal data if this is necessary for the performance of the service.
To engage Sub-processors who process sensitive personal data, the Processor must request written permission.

3. The processor will inform the customer by email one month before a Subprocessor is engaged that processes sensitive personal data. The Customer has the right to object in writing and with reasons to the involvement of third parties by the Processor within 30 days if there are valid reasons for doing so. In that case, the parties will enter into consultations to arrive at a joint solution.

4. If the Parties cannot reach an agreement on the Subprocessor to be engaged, the Processor is entitled to engage the Subprocessor and the Customer is entitled to terminate the Agreement on the date on which the new Subprocessor is engaged.

5. If the Customer does not object to the engagement of a new Subprocessor within 30 days after announcement, the Customer is deemed to consent to the engagement of the new Subprocessor.
to vote.

6. The Processor ensures that Sub-Processors undertake similar obligations in writing as agreed between the Processor and the Customer. For example, the Processor has in any case concluded a Standard Contractual Clause (SCC) with Sub-processors outside the EU.

Article 5) ***confidentiality***

1. Unless required by law, the processor is obliged to keep the personal data confidential not to make it available directly or indirectly to third parties.

2. The Processor will ensure that its staff and any third parties who necessarily need to take note of the personal data in the context of the execution of the Connection Contract adhere to the same confidentiality obligation.

3. The Processor will immediately inform the Customer of any request for access, provision or other form of retrieval and communication of personal data that is in conflict with this confidentiality obligation.

Article 6) Obligation to provide information and cooperation

1. Upon request, the Processor will provide the Customer with all information about the processing(s) of personal data by the Processor or third parties engaged by the Processor. The processor will provide the requested information as quickly as possible, but no later than within seven (7) days.
2. At the request of the Customer, the Processor will provide full cooperation in the event of a complaint or question data subject, or investigations or inspections by the Dutch Data Protection Authority.
3. If the Processor receives a request directly from a data subject for access, correction, deletion or data portability of his or her personal data, the Processor will forward the request to the Customer immediately, but no later than within two (2) working days.
4. The Processor will immediately carry out all reasonable instructions that the Customer gives to the Processor as a result of a request for access, correction, deletion or data portability of personal data by a data subject.

5. The Processor will immediately carry out any other reasonable instructions from the Customer to delete personal data, including in any case instructions to delete personal data for which the retention period has expired and deletion of personal data at the request of a data subject.

6. Processor will immediately inform Customer of any change in the organizational structure of Processor or control over Processor insofar as this has a significant impact on the way in which the personal data is processed or protected or on the obligations of Processor under this Agreement.

Article 7) Risk assessments and data breach reporting obligations

1. The Customer is at all times responsible for reporting a breach in connection with Personal Data (also known as: “Data Breach”) to the supervisory authority and those involved. To enable the Customer to comply with this legal obligation, the Processor will notify the Customer within 24 hours of discovering the Data Breach.

2. To the extent required, the Processor will cooperate in informing the relevant authorities and any involved parties. The controller is responsible for reporting to the relevant authorities and data subjects.

3. The reporting obligation consists of reporting the data breach and providing all relevant information, insofar as this information is available. This includes at least, but not exclusively, the following:
   - the (alleged) cause of the data breach;
   - the (as yet known and/or expected) consequence (for those involved);
   - the (proposed) solution; and
   - the measures already taken.

Article 8) Destruction of personal data

1. Processor will, within twelve (12) months after termination of this Agreement, all transfer personal data to the Customer and remove and destroy it from its systems, or return it at the request of the Customer, unless a legal retention obligation prevents such removal or destruction. At the Customer's first request, the Processor will provide evidence of this.
2. The Processor is obliged to destroy all personal data without delay as soon as the Processor no longer necessarily needs it for the execution of the Connection Contract. This destruction will never take place later than the moment at which the legal retention period of the personal data concerned has expired. At the Customer's first request, the Processor will provide evidence of this.

Article 9) Location processing personal data

1. Personal data is processed within the European Union (EU) and stored in Germany.

Article 10) Duration and Termination

3. The Agreement can only be canceled, dissolved or otherwise terminated to the extent stated in this Article 10 has been determined.
4. This Agreement takes effect on the first day of signing of the Connection Contract Parties and continues indefinitely to the extent that the Processor processes personal data in the context of its services to the Customer. Upon termination of the provision of services by the Customer to the Processor, this Agreement will terminate by operation of law.
5. Termination of this Agreement expressly does not release the Parties from those obligations that by their nature are intended to be maintained, including the provisions regarding (limitation of) liability, indemnification, the obligations as a processor of personal data, and applicable law and dispute resolution.

Article 11) General

6. Changes to this Processing Agreement are only valid if they are between the Parties agreed in writing.
7. If one or more articles of this Agreement are invalid or otherwise not binding, the validity of the other articles of this Agreement will not be affected. The Agreement will then be amended to the extent necessary, in the sense that the non-binding articles are replaced by provisions that differ as little as possible from the non-binding articles in question.

8. This Processing Agreement is exclusively governed by Dutch law.
9. All disputes arising from or related to this Agreement, the processing of personal data, will be submitted exclusively to the Utrecht District Court.

Appendix 1a | Overview of Personal Data

When executing the Connection Contract, Learned will process the following personal data of the following categories of Data Subjects on behalf of the Customer:

Categories of data subjects

	Colleague
personal	Name
	E-mail
	User ID
	IP address
	Username + password
	Telephone (optional)
	Profile picture
	Job title
	Education history
	Competences
	Development dates
	Certifications
	Assessment dates
	Conversation notes

Categories of personal data

Learned also makes a distinction between two different personal data of the data subjects, namely; system critical personal data and sensitive personal data. These categories affect and are used in the overview of enabled subprocessors.

	System critical	Sensitive personal data
Categories	User ID	Name
	E-mail	Profile photo (optional)
	Username + password	Telephone (optional)
	Device type	Job title
	IP address	Education history
	Complaint and improvement data.	Competences
		Development dates
		Certifications
		Assessment dates
		Conversation notes

Purposes for which the personal data are processed

- Create business environment
- Setting up the business environment and digitizing HR/business processes
- Supporting and implementing HR/business processes
- Complaint and incident handling

The Customer guarantees that the personal data and categories of data subjects described in this overview are complete and correct, and indemnifies Learned against any defects and claims resulting from an incorrect representation by the Customer.

Appendix 1b | Overview of Subprocessors

Learned has the right to engage the following processors for the execution of the Connection Contract:

Name	Purpose of sub-processor	Type of personal data	Category personal facts	Region/Land	Standard Contractual Clauses concluded (EU/US)*
Google Cloud Platform	The platform's server.	All	Both	Frankfurt (europe-west3)	Yes
MongoDB	The platform's database.	All	Both	Frankfurt (europe-west3)	Yes
Active-Campaign	Email software. It is used for software update emails.	Name, Email	System critical	Ireland	AFTER
Sentry	Performance and incident monitoring software	User ID, browser type, device type	System critical	USA	Yes
Intercom	Integrated chat and help desk in the platform. Data is sent encrypted.	Name, users ID, Investigation, complaint and improvement facts	System critical	USA	Yes
Auth0	Authentication platform. It is used for secure login and Multi-Factor Authentication.	Name, username, password	System critical	Frankfurt, Germany	AFTER
Mailgun	Email server for it sending from email (notifications).	Name, Email	System critical	Frankfurt, Germany	Yes

*The alternative to the Privacy Shield, which has been rejected by the European Commission. See here for more information.