Data Processing Agreement

This Data Processing Agreement describes the conditions for the processing of personal data by Learned B.V., on behalf of the Customer, based on the Connection Contract agreed between the Parties. This Data Processing Agreement forms an integral and inseparable part of the Terms and Conditions applicable to the Learned Platform.

Article 1) Definitions

1. In this Data Processing Agreement, the term “GDPR” is understood to mean the General Data Protection Regulation and all laws and regulations that may replace this Act in the future.
2. Terms defined in the GDPR have the same definition in this Data Processing Agreement, unless a different definition is provided here.
3. The Customer is designated as the Controller within the meaning of Article 4, paragraph 7 of the GDPR.
4. Learned is designated as a Processor within the meaning of Article 4, paragraph 8 of the GDPR.
5. The term “Personal Data” is understood to mean Personal Data relating to the personnel of the Controller, 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 “Sub-processor” means a legal entity that is or will be 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 may receive Personal Data or access to Personal Data.

Article 2) Goals and means

1. The Customer has control over the personal data that it provides to the Processor as the data controller in the context of the execution of the Connection Contract, including all updates, changes, corrections, and/or additions to such personal data.
2. The Processor agrees that the purposes of the processing of personal data shall be determined solely by the Client 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 shall process the personal data solely to the extent necessary for the performance of its services to the Client and with due observance of the purposes as determined by the Client (and described in Appendix 1) or to the extent required by law. The personal data shall not be stored, retained, or processed in any other manner by the Processor for any other purposes.
4. The GDPR (from 25 May 2018), the Telecommunications Act, and all other applicable (European) privacy regulations apply to this Data Processing Agreement.

Article 3) Security

1. The Processor shall take the appropriate technical and organisational measures required under Article 32 of the GDPR to ensure a level of security commensurate with the risk level. These measures shall be implemented in such a manner as to guarantee an appropriate and risk-comparable level of security, confidentiality, integrity and availability of the personal data, taking into account the state of the art and the costs of implementation. These measures shall include, in any event:
   - measures to ensure that only authorized personnel have access to the personal data for the purposes set out in Annex 1 of 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 vulnerabilities regarding the processing of personal data in the systems used to provide services to the Customer.
2. Without the Customer's written consent, the Processor shall not carry out (or have carried out) the processing of personal data in a country outside the European Economic Area without an adequate level of protection, nor shall the processing be carried out by a third party. The Customer shall not withhold its

consent on unreasonable grounds. The Processor shall 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 shall inform the Customer of the measures taken as referred to in Article 3, paragraphs 1 and 2, including in any event 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 shall submit proposals to the Customer as soon as possible for the modification of 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 the Processor for the protection of the personal data or the rights and interests of the data subjects. The Customer shall not withhold its approval of the proposed measures if these are reasonable in view of the risks associated with the nature of the personal data, the intended processing operations, the state of the art, and the costs of implementation. The costs of implementing the proposed measures shall be borne by the Processor.
4. The Processor will support the Client in complying with the Client's obligations under Articles 32 to 36 of the GDPR, such as assisting with the execution of a Data Protection Impact Assessment (also known as "DPIA"), should this be necessary. If necessary, Learned may charge costs for the assistance provided, based on Learned's standard hourly rates.

Article 4) Enabling Subprocessors

1. The Processor may engage Sub-processors in the processing of Personal Data. The Customer grants the 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 that process system-critical personal data if this is necessary for the performance of the services. The Processor must request written consent for engaging Sub-processors that process sensitive personal data.
3. The Processor shall inform the Customer by email one month before a Sub-processor is engaged that processes sensitive personal data. The Customer has the right to object in writing and with reasons within 30 days to the engagement of third parties by the Processor if there are valid grounds for doing so. In that case, the parties shall enter into consultation to reach a joint solution.
4. If the Parties are unable to reach an agreement regarding the Sub-processor to be engaged, the Processor is entitled to engage the Sub-processor, and the Customer is entitled to terminate the Agreement as of the date on which the new Sub-processor is engaged.
5. If the Customer does not object to the engagement of a new Sub-processor within 30 days of notification, the Customer shall be deemed to consent to the engagement of the new Sub-processor.
6. The Processor ensures that Sub-processors assume obligations comparable in writing to those agreed between the Processor and the Customer. For instance, the Processor has concluded at least a Standard Contractual Clause (SCC) with Sub-processors outside the EU.

Article 5) Confidentiality

1. The Processor is obliged, subject to legal requirement, to keep the personal data confidential and not to make it available to third parties, directly or indirectly.
2. The Processor shall ensure that its personnel and any third party(ies) who necessarily need to access the personal data in the context of the execution of the Connection Contract adhere to the same confidentiality obligation.
3. The Processor shall immediately notify the Customer of any request for access to, provision of, or other form of retrieval and disclosure of the personal data that is in violation of this confidentiality obligation.

Article 6) Duty to provide information and cooperate

1. Processor shall provide Customer with all information regarding the processing(s) of the personal data by Processor or by third parties engaged by Processor upon request. Processor shall provide the requested information as soon as possible, but no later than seven (7) days.

2. The Processor shall, at the request of the Customer, provide full cooperation in the event of a complaint or question from a data subject, or in connection with 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 shall forward the request to the Customer immediately, but no later than within two (2) working days.
4. The Processor shall immediately execute all reasonable instructions given by the Client to the Processor as a result of a request by a data subject for access, correction, deletion, or data portability of personal data.
5. The Processor shall immediately execute any other reasonable instruction from the Customer to delete personal data, including in any event instructions to delete personal data for which the retention period has expired and the deletion of personal data at the request of a data subject.
6. Processor shall immediately notify Customer of any change in the organizational structure of Processor or the control over Processor insofar as such changes have a significant impact on the manner in which the personal data are processed or protected or on the obligations of Processor under this Agreement.

Article 7) Risk assessments and data breach notification obligation

1. The Customer is at all times responsible for reporting a Personal Data breach (also referred to as a "Data Breach") to the supervisory authority and the data subjects. To enable the Customer to comply with this legal obligation, the Processor shall notify the Customer within 24 hours of discovering the Data Breach.
2. To the extent required, the Processor shall cooperate in informing the relevant authorities and any data subjects. 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, but is not limited to, the following:
   - the (alleged) cause of the data leak;
   - the (currently known and/or expected) consequence (for those involved);
   - the (proposed) solution; and
   - the measures already taken.

Article 8) Destruction of personal data

1. Immediately after termination of this Agreement, the Processor shall transfer all personal data to the Customer and delete and destroy it from its systems, or return it at the Customer's request, unless a statutory retention obligation prevents such deletion or destruction. The Processor shall provide proof of this at the Customer's first request. After the expiration of the twelve (12) month backup period, the data will be permanently deleted from the database.
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. Such destruction shall never take place later than the moment at which the statutory retention period for the relevant personal data has expired. Upon the Customer's first request, the Processor shall provide proof of this.

Article 9) Location of 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 may only be cancelled, dissolved, or otherwise terminated to the extent provided for in this Article 10.
4. This Agreement enters into force on the first day of signing of the Connection Contract by the Parties and continues for an indefinite period to the extent that the Processor processes personal data in the context of its services to the Customer. Upon termination of the services by the Customer to the Processor, this Agreement shall terminate by operation of law.

5. Termination of this Agreement shall expressly not release the Parties from those obligations which by their nature are intended to remain in force, including the provisions regarding (limitation of) liability, indemnification, obligations as a processor of personal data, and applicable law and dispute resolution.

Article 11) General

6. Amendments to this Data Processing Agreement are valid only if agreed upon in writing between the Parties.
7. If one or more articles of this Agreement are invalid or otherwise non-binding, this shall not affect the validity of the remaining articles of this Agreement. The Agreement shall then be amended to the extent necessary, in such a way that the non-binding articles are replaced by provisions that differ as little as possible from the relevant non-binding articles.
8. This Data Processing Agreement is governed exclusively by Dutch law.
9. All disputes arising from or related to this Agreement and the processing of personal data shall be submitted exclusively to the District Court of Utrecht.

Appendix 1a | Overview of Personal Data

Categories of personal data

Furthermore, Learned itself distinguishes between two different types of personal data of the data subjects, namely: system-critical personal data and sensitive personal data. These categories influence and are used in the overview of engaged sub-processors.

Categories of personal data	System critical	Sensitive personal data
	User ID	Name
	Email	Date of birth
	Username + password	Gender
	IP address	Profile picture (optional)
	Complaint and improvement details.	Phone (optional)
	Type device	Job title
		Educational history
		Competencies
		Development data
		The certification
		Assessment data
		Completed questionnaires
		Meeting notes
		Salary data

Purposes for which the personal data are processed

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

The Client warrants 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 Client.

Appendix 1b | Overview of Sub-processors

Learned has the right to engage the processors listed below in the execution of the Connection Contract:

Name	Sub-processor target	Type of personal data	Category of personal data	Regio/Land
Google Cloud Platform	The platform's server.	All	Both	Frankfurt (europe-west3)
MongoDB	The platform's database.	All	Both	Frankfurt (europe-west3)
PostHog	Productanalyses	IP addresses, device and browser data, user IDs	System critical	Frankfurt (europe-west3)
Hubspot	Email software. Integrated chat and helpdesk in the platform.	Name, Email	System critical	Frankfurt, Germany
Sentry	Performance and incident monitoring software	User ID, browser type, device type	System critical	Frankfurt, Germany
Auth0	Authentication platform. It is used for secure login and Multi-Factor Authentication.	Name, username, password	System critical	Frankfurt (europe-west3)
OpenAI Ireland Limited	Delivery of AI services	IP addresses, user IDs, Text input (prompts),	Both	Frankfurt (europe-west3)
Mailgun	Email server for sending email (notifications).	Name, Email	System critical	Frankfurt, Germany
Kombo Technologies GmbH	Integration platform (unified API) for connections with the Customer's HRIS, ATS and payroll systems.	User IDs, name, email, job title, salary data	Both	Netherlands (Google Cloud, EU)