Data Processing Agreement (DPA) pursuant to Article 28(3) GDPR

This agreement constitutes a supplement to the General Terms and Conditions dated December 15, 2022 (hereinafter referred to as the "Main Agreement") and is entered into

between the

Customer (hereinafter referred to as the "Controller")

and

IDENTsmart GmbH (hereinafter referred to as the "Processor")

Bergfeldstrasse 9,
86307 Holzkirchen
Germany

(both parties collectively referred to as the "Contracting Parties").

By entering into this agreement, the Contracting Parties establish a data processing relationship. The definitions of terms under the General Data Protection Regulation (GDPR - Regulation (EU) 2016/679) apply to this agreement. Therefore, when the term "data" is used in this contract, it refers to "personal data" within the meaning of the GDPR. In case of any conflict between this agreement and the main contract regarding the processing of personal data, this agreement prevails in doubt.

§ 1: Object of the Contract and Duration of the Agreement

1.1: This contract applies to all processing of personal data arising from the main contract between the Contracting Parties, provided that the Processor processes such personal data on behalf of the Controller.

1.2: The Data Processing Agreement comes into effect from the moment it is signed by both parties. It is supplementary to the main contract and remains in force for the duration of the data protection-relevant services provided under the main contract. In the event of the complete termination of the main contract, this agreement also automatically terminates. In this case, no separate termination is required.

1.3: This contract, and therefore the entire data processing relationship, can be terminated by the Contracting Parties at any time without observing a notice period if the respective other party materially violates this agreement or the relevant data protection laws.

Such a material violation occurs, for example, if the Processor fails to fulfill the obligations arising from this agreement and Article 28 of the GDPR. Additionally, the Controller may terminate the contract immediately if the Processor fails to comply with a directive from the Controller, denies the Controller the contractually stipulated audit rights, or neglects essential or agreed-upon security measures.

§ 2: Nature and Purpose of Processing

2.1: The Processor shall process the personal data provided by the Controller exclusively to fulfill its contractual obligations under the main contract. The processing is therefore based on the main contract, this agreement, or in accordance with the Controller's instructions. The Processor is prohibited from processing personal data for its own or third-party purposes or disclosing personal data to third parties without the Controller's prior written instructions. Duplication or copying of personal data by the Processor is only permitted to the extent approved in advance by the Controller or if necessary for ensuring proper data processing (copy for backup) or compliance with legal obligations (e.g., legal retention obligations).

2.2: The specific types of processing (Art. 4(2) GDPR) and purposes of the Processor's processing are detailed in the main contract.

§ 3: Types of Personal Data, Categories of Data Subjects

The types of personal data processed by the Processor, as well as the categories of data subjects, are detailed in Annex 1. Annex 1 constitutes a part of this agreement.

§ 4: Rights and Responsibilities of the Controller

4.1: The Controller alone has the authority to decide on the means and purposes of processing the personal data provided by them.

4.2: The Controller undertakes to comply with EU legal and national data protection regulations, as well as this agreement. They are particularly responsible for assessing the lawfulness of the processing of personal data (Art. 6 GDPR) and ensuring that the rights of data subjects are safeguarded according to Articles 12–22 of the GDPR. Simultaneously, the decision to respond to a request from a data subject regarding their rights is solely the responsibility of the Controller, and communication in this regard is conducted only by them.

4.3: The Controller has the right to give instructions and orders to the Processor regarding the nature and scope of the processing of personal data. These instructions and orders must generally be given to the Processor in a documented and written or electronic format. If instructions are given verbally, they must be confirmed in writing or in a documented electronic format. For the purposes of this contract, an instruction refers to an order to the Processor regarding the handling of personal data.

4.4: Data carriers or records provided by the Controller to the Processor remain the property of the Controller. The Controller is entitled to order the deletion, correction, handover, adaptation, or restriction of data processing at any time.

4.5: The Controller promptly reports to the Processor any errors and anomalies noticed in the results of data processing.

4.6: The Controller is obligated to promptly inform the Processor in the event of a change in the Data Protection Officer.

§ 5: Responsibilities of the Processor

5.1: The Processor processes personal data solely based on the documented instructions of the Controller, unless the Processor is obligated by Union or Member State law to do so. In such a case, the Processor informs the Controller of these legal requirements before processing, unless the relevant law prohibits such notification due to an important public interest.

5.2: The Processor is obliged to delete, correct, hand over, adapt, or restrict personal data as instructed by the Controller.

5.3: The Processor must ensure that individuals authorized to process the personal data are bound by confidentiality or are subject to an appropriate legal confidentiality obligation.

5.4: The Processor commits to implementing all technical and organizational measures (TOMs) as per Article 32 GDPR necessary for the security of processing personal data. The TOMs implemented by the Processor are described in Annex 2. Annex 2 constitutes a part of this agreement.

5.5: The Controller agrees to the additional processors (hereinafter "Sub-Processors") listed in Annex 3. These listed Sub-Processors are necessary for the fulfillment of the main contract. Without prior separate or general written approval, the Processor does not engage any additional Sub-Processors. In the case of general written approval, the Processor is obliged to inform the Controller of any intended changes regarding the engagement or replacement of other Sub-Processors. The Controller then has the opportunity to object to the change within a reasonable period.

5.6: The Processor enters into a contractual agreement with appointed Sub-Processors, ensuring at least the same level of data protection as provided in this agreement between the Controller and Processor. All legal and contractual requirements are considered, particularly the technical and organizational measures according to Article 32 GDPR.

5.7: If a Sub-Processor violates its data protection obligations, the Processor is liable to the Controller for ensuring compliance with the Sub-Processor's obligations. In the event of a breach of data protection obligations by the Sub-Processor, the Controller may instruct the Processor to terminate the employment of the Sub-Processor wholly or partially.

5.8: The Processor assists the Controller to the best of its ability in fulfilling the rights of the data subjects under Chapter III of the GDPR within the legal deadlines. To achieve this, the Processor takes technical and organizational measures. If a request is mistakenly submitted to the Processor and it is evident that it should have been directed to the Controller, the Processor promptly forwards the request to the Controller and notifies them accordingly.

5.9: Considering the nature of the processing, the Processor supports the Controller in meeting the obligations specified in Articles 32 to 36 of the GDPR (data security measures, reporting personal data breaches to the supervisory authority, notifying the data subject affected by a personal data breach, data protection impact assessment, prior consultation with the supervisory authority).

5.10: Following the provision of processing services or, at the instruction of the Controller, and no later than upon termination of the main contract, the Processor undertakes to either delete or return all personal data, along with erasing any existing copies, at the choice of the Controller. The Processor is authorized to retain documentation, taking into account relevant retention periods, for proof of contractual and proper data processing even after the termination of the contractual relationship.

5.11: The Processor agrees that the Controller, either directly or through third parties, may conduct inspections and audits to verify compliance with data protection and data security regulations at the Processor's premises. The Processor provides all necessary information and cooperates in facilitating such inspections. The Controller generally schedules appointments for these inspections, and the exercise of their auditing rights is limited to a reasonable and necessary extent.

5.12: The Processor promptly informs the Controller if there are significant disruptions to the operational processes, if the Processor believes that an instruction violates legal data protection provisions, if there are violations by employees or Sub-Processors, or if irregularities arise during the processing of the Controller's data. The Processor may suspend the execution of instructions that violate legal data protection provisions until confirmed or modified by the Controller.

§ 6: Confidentiality

The Contracting Parties undertake to treat all knowledge of internal business secrets or data protection security measures of the other party confidentially and not to disclose them to third parties. This obligation continues to apply even after the termination of the contract.

§ 7: Written Form for Amendments

Any changes or additions to this agreement require written form for their effectiveness. This also applies to changes to this written form clause.

§ 8: Liability

Any liability privileges regulated in the main contract do not apply to this agreement. Each party is solely and unrestrictedly liable in the internal relationship for adverse consequences resulting from breaches of data protection obligations within their contractually and legally determined own area of responsibility. In this context, both the Controller and the Processor undertake to indemnify and hold each other harmless in full if claimed by third parties.

This also includes regulatory fines imposed on one party due to the behavior attributable to the other party.

§ 9: Choice of Law and Jurisdiction

This agreement is governed by German law, including the relevant Union law, especially the GDPR. The exclusive place of jurisdiction is the registered office of the Processor.

§ 10: Severability Clause

If individual provisions of this contract are infeasible or ineffective, the effectiveness of the remaining provisions shall not be affected.

.....

Date, Location (Processor)

.....

Signature (Processor)

.....

First Name, Last Name, Position (Processor)

Annex 1: Data Processing Specifications

Explanations of Terms Regarding the Type of Data Processing

	Description of Data Processing
User Accounts	Login Credentials, Passwords, Username
Personal Identification Data	Name, Title, (Personal and Professional) Address, Previous Addresses, (Personal, Professional) Phone Number, Identifiers assigned by the person responsible for processing.
No personal data	
Payment Information	Amount, Date...
Financial Transactions	Amounts owed and paid by the data subject, granted credit, guarantees, payment methods, overview of payments, deposits, and other guarantees.
Financial Identification Data	Bank identification and account number, credit and debit card numbers, PINs (Personal Identification Numbers).
Presence and Discipline	Overview of attendance, reasons for absence, disciplinary measures. Vacation, compensatory time off, sick leave.
Professional Activities	Type of activities, goods, or services used or provided by the data subject, business contacts.

Category: 01 Time Recording

Processing	**01.01 Account Creation, Login, and Login Management**
Purpose of Processing	Both account creation, login, and user login management are handled through Auth0.
Type of Data Processing	• User Accounts • Personal Identification Data
Recipients	• Auth0

Processing	**01.02 Hosting**
Purpose of Processing	Both the frontend and backend are stored on Google Cloud. The servers are exclusively located in Europe. Backups are also stored in Google Cloud.
Type of Data Processing	• No personal data
Recipients	• Google Cloud EMEA Limited

Processing	**01.03 Payment Processing**
Purpose of Processing	For payment processing, there is the option to provide a credit card. Payments are then processed through a payment service provider.
Type of Data Processing	• Payment Information • Financial Transactions • Financial Identification Data
Recipients	Stripe, Inc.

Processing	**01.04 Sending Invitation Links and Reports**
Purpose of Processing	Invitation links and reports are sent through
Type of Data Processing	• Personal Identification Data
Recipients	Twilio SendGrid

Processing	**01.05 Time Recording**
Purpose of Processing	As part of time recording, employees must be created by system users in the first step. Mandatory information includes the first and last name, as well as the RFID token number. Optional details may include address, email address, phone number, date of birth, and personnel number. The processing and storage involve time recording, overtime records, sick leave notifications, as well as vacation requests and durations.
Type of Data Processing	• Presence and Discipline • Personal Identification • Data Professional Activities
Recipients	-

Annex 2: Technical and Organizational Measures (Article 32(1) GDPR)

Protection Category: 1.1.1 Confidentiality: Access Control

Designation	Last Audit
1.1.1.04 Entrance doors to company buildings or rooms are secured by a standardized locking system (security locks, chip cards, transponders, code locks).	08.03.2022
1.1.1.06 The assignment, loss, and return of keys, transponders, chip cards, or codes to individuals are documented.	08.03.2022
1.1.1.07 The use of chip cards, transponders, or access codes is logged (e.g., time, location of use, key).	08.03.2022
1.1.1.08 It is ensured that individuals only have access where it is necessary for the fulfillment of their tasks.	08.03.2022
1.1.1.14 Visitors or personnel from external companies are accompanied by employees.	08.03.2022
1.1.1.19 Photoelectric barriers or motion detectors trigger the exterior lighting of company buildings.	08.03.2022

Protection Category: 1.1.2 Confidentiality: Access Control (Sensitive Areas)

Designation	Last Audit
1.1.2.04 Personnel files are kept in lockable file cabinets.	08.03.2022
1.1.2.01 Personal data is processed in separate premises (e.g., personnel office).	08.03.2022
1.1.2.03 The entrance door to rooms where personal data is processed has an automatic closing and locking mechanism or is locked upon leaving.	08.03.2022
1.1.2.05 Screens where personal data is processed are not visible from outside (window) or inside (glass door or glass front).	08.03.2022

Protection Category: 1.2 Confidentiality: Access Control

Designation	Last Audit
1.2.02 Laptops or smart devices (iPad, etc.) are locked away or taken home after the end of the workday.	08.03.2022
1.2.05 Access to a client is done through personal user accounts (username and password or similar methods like facial recognition, fingerprint, etc.).	08.03.2022
1.2.06 The user on the client computer does not have administrator rights, and daily work is carried out using a user account without administrator privileges.	08.03.2022
1.2.09 Every client computer has antivirus software installed, and it is updated daily or upon new login.	08.03.2022
1.2.11 Incoming emails are checked for spam online at the mail server.	08.03.2022
1.2.14 Access to the internal network (WLAN) is secured with a dedicated password.	08.03.2022
1.2.15 Access to systems (servers, software) from outside the company is done through encrypted connections (VPN, access via Citrix).	08.03.2022

Protection Category: 1.3 Confidentiality: Access Control

Designation	Last Audit
1.3.01 The number of administrators for servers and central software is minimized to the "necessary" level.	08.03.2022
1.3.05 User passwords have sufficient complexity (include uppercase and lowercase letters, special characters, and numbers, with a minimum length of 8 characters).	08.03.2022
1.3.06 User rights management for used software is centrally controlled by designated system administrators.	08.03.2022

1.3.08 Each user is granted access rights (to data, systems, software, file storage systems) based on the "need to know" principle, limited to what is essential for their specific tasks.	08.03.2022
1.3.09 When a user leaves the company, it is ensured that their access permissions are promptly revoked, and the user is deleted after a certain period.	08.03.2022
1.3.11 If the need for one or more access rights for a user diminishes, the corresponding rights are promptly revoked.	08.03.2022

Protection Category: 1.4 Confidentiality: Separation Principle

Designation	Last Audit
1.4.02 Software applications that process personal data have a separation between test and production systems.	08.03.2022
1.4.03 Access to data in databases is regulated.	08.03.2022
1.4.05 Software applications and file repositories accessible by multiple users are equipped with an authorization system.	08.03.2022
1.4.06 Processing of personal data only occurs for the specified purposes.	08.03.2022
1.4.07 The transfer of personal data only occurs for the specified purposes.	08.03.2022

Protection Category: 1.6 Confidentiality: Encryption

Designation	Last Audit
1.6.04 Encrypted connections such as https (website) or sftp (FTP server) are used for data transfer.	08.03.2022
1.6.06 The latest version of the TLS encryption protocol is used.	08.03.2022

Protection Category: 2.1 Integrity: 1. Input control

Designation	Last Audit
2.1.01 Documents or forms containing sensitive data that are subject to automatic further processing are retained to correct data entry errors.	08.03.2022
2.1.03 The input, modification, and deletion of data by individual users (not user groups) can be traced.	08.03.2022

Protection Category: 2.2. Integrity: 2. Transfer Control

Designation	Last Audit
2.2.03 Access to computers via remote maintenance is only done with the user's consent. This does not apply to update and configuration processes on the computer using automatic installation tools.	08.03.2022
2.2.05 Other data carriers (USB sticks, mobile hard drives, removed hard drives) are deleted, formatted, or physically destroyed before their internal or external transfer.	08.03.2022
2.2.06 For printers or fax machines, their internal data carriers are erased, formatted, physically destroyed, or deleted according to the manufacturer's specifications before external transfer.	08.03.2022

Protection Category: 3.1 Availability and Resilience: Availability Control

Designation	Last Audit
3.1.01 Updates and security patches are regularly applied on clients and servers.	08.03.2022

3.1.06 Premises where personal data is processed are equipped with a fire and smoke detection system.	08.03.2022
3.1.07 Premises where personal data is processed are equipped, easily accessible, with suitable firefighting agents (e.g., fire extinguishers).	08.03.2022
3.1.10 There are no gas or water-carrying pipelines above or through rooms where servers are located.	08.03.2022

Protection Category: 4.1 Verification Procedures: Data Protection Management

Designation	Last Audit
4.1.01 An internal or external data protection officer has been appointed.	08.03.2022
4.1.02 A record of processing activities is maintained and regularly updated.	08.03.2022
4.1.03 An audit/assessment of the effectiveness of technical and organizational measures is conducted annually.	08.03.2022
4.1.04 Processes are in place to fulfill the rights of data subjects.	08.03.2022
4.1.05 A Data Protection Management Software is in use.	08.03.2022
4.1.06 Information obligations (privacy policy) are regularly reviewed.	08.03.2022
4.1.07 There is a deletion concept specifying when and which data are to be deleted. The deletion of data is checked randomly or regularly.	08.03.2022
4.1.10 All employees are obligated to confidentiality and data secrecy.	08.03.2022

Protection Category: 4.2 Verification Procedures: Incident Response Management

Designation	Last Audit
4.2.01 Incorrect login attempts result in an automatic lockout of the user login. The lockout persists for a defined period (see Password Policy).	08.03.2022
4.2.02 There is a procedure for reporting security breaches to the Data Protection Authority and affected individuals.	08.03.2022
4.2.07 Processing activities are assessed for data protection impact. Such an assessment is conducted and documented when necessary.	08.03.2022

Appendix 3: Subcontractors (additional data processors)

Designation	Land	Transfer to a third country
Auth0	USA	Third Country
Google Cloud EMEA Limited	Ireland	EU
Stripe, Inc.	USA	Third Country
Twilio SendGrid	Ireland	EU