Order processing contract (AVV) according to Art. 28 Para. 3 GDPR

This agreement is an addition to the terms and conditions dated _____
(hereinafter "Main Agreement") and will

between

Customer (hereinafter "Responsible Person")

and

IDENTsmart GmbH (hereinafter "processor")

Carl-von-Ossietzky-Str. 3
83043 Bad Aibling
Germany

(both parties jointly hereinafter "Contracting Parties")

closed.

With the conclusion of this agreement, the contracting parties enter into an order processing relationship. In this agreement, the corresponding definitions of terms of the GDPR (General Data Protection Regulation - Regulation (EU) 2016/679) apply. Therefore, if the term “data” is used in this contract, then it means “personal data” within the meaning of the GDPR. If this agreement and the main contract contradict each other regarding the processing of personal data, this agreement takes precedence over the main contract in case of doubt.

§ 1: Subject matter of the contract and duration of the contract

1.1.: This contract applies to all processing of personal data resulting from the main contract between the contracting parties, provided that the processor processes this personal data on behalf of the controller.

1.2.: The order processing contract comes into effect from the time it is signed by both parties. It applies as an accessory to the main contract and remains valid for the duration of the provision of services from the main contract that is relevant under data protection law. If the main contract is completely eliminated, this agreement also expires automatically. In this case, no separate termination is required.

1.3.: This contract and thus the entire order processing relationship can be terminated by the contracting parties at any time without notice if the other party seriously violates this agreement or the relevant data protection law.

Such a serious violation occurs, for example, if the processor does not comply with the obligations arising from this agreement and from Art. 28 GDPR. Furthermore, the person responsible can terminate the contract without notice if the processor does not follow an instruction of the person responsible, if the processor refuses the contractually defined control rights of the person responsible or if the processor fails to take mandatory or agreed security measures.

§ 2: Type and purpose of processing

2.1.: The processor processes the personal data provided by the person responsible exclusively for the fulfillment of his contractual obligations from the main contract. The processing is therefore carried out on the basis of the main contract, this agreement or in accordance with an instruction from the person responsible. The processor is prohibited from processing personal data for its own or third-party purposes or from passing on personal data to third parties without prior written instructions from the person responsible. The duplication or copying of personal data by the processor is only permitted to the extent that this has been approved in advance by the person responsible or it is absolutely necessary to ensure proper data processing (copy for backup) or to comply with legal obligations (e.g. legal storage obligations). is.

2.2.: The specific types of processing (Art 4 Z 2 DSGVO) and purposes of the processing of the processor can be found in the main contract.

§ 3: Type of personal data, categories of data subjects

The types of personal data processed by the processor and the categories of data subjects can be found in Annex 1. Annex 1 forms part of this agreement.

§ 4: Rights and obligations of the person responsible

4.1.: The person responsible is solely responsible for deciding on the means and purposes of processing the personal data he has provided.

4.2.: The person responsible undertakes to comply with EU law and national data protection regulations as well as this agreement. In particular, he is responsible for assessing the legality of the processing of personal data (Article 6 GDPR) and for ensuring that the rights of the data subjects are protected in accordance with Articles 12 - 22 GDPR. At the same time, the decision to answer a request from a data subject regarding their rights as a data subject rests exclusively with the person responsible and the corresponding communication takes place only through this person.

4.3.: The person responsible is entitled to issue instructions and orders to the processor regarding the type and scope of the processing of personal data.

These orders and instructions must always be issued by the person responsible in a documented and written or electronic manner. If instructions are given verbally, they must be confirmed in writing or in a documented electronic format.

An instruction is understood in this contract as an order to the processor regarding the handling of personal data.

4.4.: Data carriers or data sets that the person responsible leaves to the processor remain the property of the person responsible. The person responsible is entitled to order the processor to delete, correct, release, adapt or restrict data processing at any time.

4.5.: The person responsible immediately reports errors and abnormalities that he notices in the results of the order processing to the processor.

4.6.: The person responsible is obliged to inform the processor immediately if there is a change in the data protection officer.

§ 5: Obligations of the processor

5.1.: The processor processes the personal data only on the basis of documented instructions from the controller, unless the processor is required to do so by Union or Member State law. In such a case, the Processor shall notify the Controller of those legal requirements before processing, unless the law in question prohibits such notification because of an important public interest.

5.2.: The processor is obliged to delete, correct, release, adapt or limit personal data if this is ordered by the controller.

5.3.: The processor must ensure that the persons authorized to process the personal data are bound to confidentiality or are subject to an appropriate statutory duty of confidentiality.

5.4.: The processor undertakes to take all technical and organizational measures (TOMs) within the meaning of Art. 32 GDPR that are necessary for the security of the processing of personal data. The TOMs set by the processor are described in more detail in Appendix 2. Appendix 2 forms part of this Agreement.

5.5.: The person responsible agrees to the additional processors listed in Appendix 3 (hereinafter "sub-processors"). These listed sub-processors are required to fulfill the main contract. The processor will not use any other processors without prior separate or general written approval. In the case of general written approval, the processor is obliged to inform the controller of any intended change in relation to the involvement or replacement of other sub-processors. The person responsible then has the opportunity to object to the change within a reasonable period of time.

5.6.: The processor concludes a contractual agreement with commissioned sub-processors that guarantees at least the same level of data protection as this contract between the controller and the processor. All legal and contractual requirements are taken into account, in particular the technical and organizational measures in accordance with Art. 32 GDPR.

5.7.: If a sub-processor violates its data protection obligations, the processor is liable to the person responsible for compliance with the obligations of the sub-processor. In the event of a violation of data protection obligations by the sub-processor, the person responsible can instruct the processor to terminate the employment of the sub-processor in whole or in part.

5.8.: The processor supports the person responsible as far as possible so that he can fulfill the rights of the person concerned according to Chapter III of the GDPR within the legal deadlines. The processor takes technical and organizational measures for this. If a request is made to the processor in error and it is apparent that it should have been made to the controller, the processor will immediately forward the request to the controller and notify the controller.

5.9.: Taking into account the nature of the processing, the processor supports the controller in complying with the obligations set out in Articles 32 to 36 GDPR (data security measures, notifications of personal data breaches to the supervisory authority, notification of those affected by a personal data breach person, data protection impact assessment, prior consultation with the supervisory authority).

5.10.: The processor undertakes to either delete or return all personal data at the discretion of the person responsible after the processing services have been provided or before this by order of the person responsible and to delete existing copies at the latest upon termination of the main contract.

The processor is entitled to keep documentation, taking into account the relevant retention periods, as evidence of the order and proper data agreement even after the end of the contractual relationship.

5.11.: The processor agrees that the person responsible carries out checks and inspections regarding compliance with the regulations on data protection and data security at the processor itself or through third parties. The processor provides all the information required for this and provides support. In principle, the person responsible must make an appointment for these checks and inspections. The controller may only exercise its control rights to an appropriate and necessary extent.

5.12.: The processor will inform the person responsible immediately if there are serious disruptions to operations, if he believes that an instruction violates statutory data protection regulations, violations by employees or sub-processors occur or if irregularities arise in the course of processing processing of the data of the person responsible. The processor can suspend the execution of instructions that violate legal data protection regulations until they have been confirmed or changed by the person responsible.

§ 6: Confidentiality

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

§ 7: Written form for changes

Any changes or additions to this agreement must be made in writing to be effective.
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 contracting party is solely and unrestrictedly liable internally for adverse consequences of violations of data protection obligations within the scope of their own contractually and legally defined area of responsibility.
In this context, both the person responsible and the processor undertake to fully indemnify and hold the other party harmless in the event of claims by third parties.

This includes, in particular, administrative fines that were imposed on one contracting party due to conduct attributable to the other contracting party.

§ 9: Choice of Law and Place of Jurisdiction

This agreement is subject to German law and the relevant Union law, in particular the GDPR. The exclusive place of jurisdiction is the registered office of the processor.

§ 10: Severability Clause

Should individual provisions of this contract be unenforceable or ineffective, the effectiveness of the remaining provisions shall not be affected.

.....
Date, place (processor)

.....
Signature (processor)

.....
First name, last name, position (processor)

Appendix 1: Data Processing Specifications

Explanation of terms for the type of data processing

	Description of data processing
user accounts	Login data, passwords, username
personal identification data	Name, title, address (private and professional), previous addresses, telephone number (private, professional), identification numbers assigned by the person responsible for processing.
No personal Data	
payment details	height, date...
financial transactions	Amounts owed and paid by the data subject, credit granted, guarantees, payment methods, overview of payments, deposits and other guarantees.
Financial Identification Data	Bank identification and bank account number, credit and debit card numbers, secret codes.
presence and discipline	Overview of attendance, motives for absence, disciplinary action. Vacation, compensatory time off, sick leave
Professional Activities	Type of activities, goods or services used or provided by the data subject, business contacts.

Area: 01 time recording

processing	01.01 Account creation, login and login management
purpose of processing	The account creation, the login as well as the login management of users are handled via Auth0.
type of data processing	• user accounts • Personal Identification Data
recipient	• Auth0

processing	01.02 Hosting
purpose of processing	Both the frontend and the backend are stored on Google Cloud. The servers are located exclusively in Europe. Backups are also stored in the saved to Google Cloud.
type of data processing	• No personal data
recipient	• Google Cloud EMEA Limited

processing	01.03 Payment Processing
purpose of processing	You can use a credit card to process payments deposit. The payments are then made via a payment service provider settled.
type of data processing	• payment details • financial transactions • Financial Identification Data
recipient	• Stripe, Inc.

processing	01.04 Sending of invitation links and reports
Purpose of processing	Invitation link and reports are sent via a
type of data processing	• Personal Identification Data
recipient	• twilio sendgrid

processing	01.05 Recording of working hours

purpose of processing	As part of time recording, employees must first be created by users of the system. The first and last name as well as the RFID token number are mandatory. Address, e-mail address, telephone number, date of birth and personnel number are optional. Work time recordings, overtime, sick leave as well as vacation requests and times are processed and stored.
type of data processing	• attendance and discipline • Personal Identification Data • Professional Activities
recipient	

Appendix 2: Technical organizational measures (Article 32 (1) GDPR)

Degree of Protection: 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 lock)	08.03.2022
1.1.1.06 The issue, loss and return of keys, transponders, chip cards or codes to persons is documented	08.03.2022
1.1.1.07 The use of chip cards, transponders or the use of access codes is logged (e.g. time, place of use, key)	08.03.2022
1.1.1.08 It is ensured that people only have access where they need access to fulfill their tasks	08.03.2022
1.1.1.14 Visitors or staff from external companies are accompanied by employees	08.03.2022
1.1.1.19 Light barriers or motion detectors trigger the outdoor lighting of company buildings	08.03.2022

Degree of protection: 1.1.2 confidentiality: access control (sensitive rooms)

designation	Last audit
1.1..2.04 Personnel files are kept in lockable filing cabinets	08.03.2022
1.1.2.01 Personal data are processed in separate rooms (e.g. personnel office)	08.03.2022
1.1.2.03 The entrance doors to rooms in which personal data are processed have an automatic closing and locking mechanism or are locked when leaving	08.03.2022
1.1.2.05 Screens on which personal data are processed cannot be seen from the outside (window) or inside (glass door or glass front).	08.03.2022

Degree of Protection: 1.2 Confidentiality: Access Control

designation	Last audit
1.2.02 Laptops or smart devices (Ipad etc.) are kept locked after the end of the working day or are taken home	08.03.2022

1.2.05 Registration on a client takes place via personal user accounts (user name and password or similar procedures (face recognition, fingerprint, etc.))	08.03.2022
1.2.06 The user on the client computer has no administrator rights or a user without administrator rights is used for day-to-day work	08.03.2022
1.2.09 Anti-virus software is installed on each client computer and is updated daily or when a new user registers	08.03.2022
1.2.11 Incoming emails are checked for spam online on the mail server (hoster).	08.03.2022
1.2.14 Access to the internal network (WLAN) is secured with a separate password	08.03.2022
1.2.15 Access to systems (server, software) from outside the company is via encrypted connections (VPN, access via Citrix)	08.03.2022

Degree of Protection: 1.3 Confidentiality: Access Control

designation	Last audit
1.3.01 The number of administrators for the server and central software is reduced to the "necessary".	08.03.2022
1.3.05 User passwords are of sufficient complexity (contain upper and lower case letters, special characters and numbers and have a minimum length of 8 characters)	08.03.2022
1.3.06 The management of user rights for the software used is carried out centrally by specified system administrators	08.03.2022
1.3.08 On the basis of the "need to know" principle, each user only receives the access rights (to data, systems, software, file storage systems) that he absolutely needs for his work	08.03.2022
1.3.09 When a user leaves the company, it is ensured that his access rights are removed immediately and that the user is also deleted after a certain period of time.	08.03.2022
1.3.11 If a user no longer needs one or more access rights, the rights will be revoked promptly	08.03.2022

Degree of protection: 1.4 Confidentiality: Separation requirement

designation	Last audit

1.4.02 In the case of software applications that process personal data, there is a separation between the 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 storages to which several users have access are equipped with an authorization system.	08.03.2022
1.4.06 The processing of personal data takes place only for the specified purposes	08.03.2022
1.4.07 Personal data is only passed on for the specified purposes	08.03.2022

Degree of Protection: 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

Degree of protection: 2.1 Integrity: 1. Input control

designation	Last audit
2.1.01 Documents or forms in which sensitive data is collected are kept if they are automatically processed in order to be able to correct incorrect data transfers.	08.03.2022
2.1.03 The entry, modification and deletion of data by individual users (not user groups) can be traced	08.03.2022

Degree of protection: 2.2. Integrity: 2. Propagation Control

designation	Last audit
2.2.03 Computers are only accessed via remote maintenance with the user's consent. Exceptions to this are updates and configuration processes on the computer with the help of 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 they are passed on internally or externally	08.03.2022

2.2.06 In the case of printers or fax machines, their internal data carriers are erased, formatted, physically destroyed or erased according to the manufacturer's specifications before they are passed on externally	08.03.2022

Degree of protection: 3.1 Availability and resilience: Availability control

designation	Last audit
3.1.01 Updates and security patches are regularly installed on clients and servers	08.03.2022
3.1.06 Premises in which personal data are processed are equipped with a fire and smoke alarm system	08.03.2022
3.1.07 Premises in which personal data are processed are easily accessible and have suitable extinguishing equipment for firefighting (e.g. fire extinguisher)	08.03.2022
3.1.10 No gas or water-carrying pipes run above or through rooms in which servers are located	08.03.2022

Degree of Protection: 4.1 Verification Procedure: Privacy Management

designation	Last audit
4.1.01 An internal or external data protection officer has been appointed	08.03.2022
4.1.02 A register of processing activities is kept and continuously updated	08.03.2022
4.1.03 An audit/review of the effectiveness of the technical and organizational measures takes place annually	08.03.2022
4.1.04 Procedures are in place to fulfill the rights of data subjects	08.03.2022
4.1.05 Data protection management software is in use	08.03.2022
4.1.06 The information requirements (data protection declaration) are checked regularly	08.03.2022
4.1.07 There is a deletion concept that defines when and what data is to be deleted. The deletion of data is randomly or regularly checked.	08.03.2022
4.1.10 All employees are committed to confidentiality and data secrecy	08.03.2022

Degree of Protection: 4.2 Procedures for Verification: Incident Response Management

designation	Last audit

4.2.01 Incorrect login attempts lead to an automatic blocking of the user login. The lock remains in place for a defined period of time (see password policy).	08.03.2022
4.2.02 There is a procedure for reporting security breaches to the data protection authority and data subjects	08.03.2022
4.2.07 Processing is checked with regard to a data protection impact assessment. Such a review is also carried out and documented if necessary	08.03.2022

Appendix 3: Subcontractors (other processors)

designation	Land	Transfer to third country
Auth0	deer	third country
Google Cloud EMEA Limited	Ireland	EU
Stripe, Inc.	deer	third country
twilio sendgrid	Ireland	EU