Annex 1 Agreement for the processing of personal data on behalf of a controller pursuant to Art. 28 GDPR

Data Processing Agreement **("DPA")** between payever GmbH, Rödingsmarkt 20, 20459 ("**Processor**") and its Business Customer ("**Controller**")

Preamble

1 Subject Matter of the Agreement

When providing the services pursuant to the General Terms and Conditions for Business Customers (the "**Main Agreement**"), it is necessary for the Processor to process personal data for which the Controller is the data controller within the meaning of data protection law (hereinafter "**Controller Data**"). This DPA specifies the data protection rights and obligations of the parties in connection with the Processor's processing of Controller Data for the performance of the Main Agreement.

2 Scope of processing

2.1 The Processor shall process Controller Data on behalf of and according to the instructions of the Controller in accordance with Article 28 of the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"). The Controller remains the data controller in the sense of data protection law.

2.2 The processing of Controller Data by payever is carried out exclusively in the manner, scope and for the purpose specified in **Appendix 1** to this Annex; the processing involves exclusively the types of personal data and categories of data subjects set forth in Appendix 1.

2.3 The duration of the processing corresponds to the term of the Main Agreement.

2.4 The Processor reserves the right to anonymize or aggregate Controller Data so that identification of individual data subjects is no longer possible, and to use such data for the purpose of needs-based design, further development, and optimization of the service agreed under the Main Agreement. The Parties agree that anonymized or aggregated Controller Data as described above shall no longer be considered Controller Data within the meaning of this DPA.

2.5 The Processor may process and use Controller Data for its own purposes and under its own responsibility, to the extent permitted by data protection law and outside the scope of this DPA, if a statutory provision or a data subject's consent allows this. This DPA does not apply to such processing.

2.6 The processing of Controller Data by the Processor shall in principle take place within the European Union or another contracting state of the European Economic Area (EEA). In particular, the relevant data centers are located within the EEA. Only in the context of technical maintenance services may data access from the USA occur in individual and exceptional cases. Such access does not occur regularly, but only in exceptional cases. Beyond this, the Processor is permitted to process Controller Data outside the EEA in compliance with the provisions of this DPA if the requirements of Art. 44–48 GDPR are met or an exception under Art. 49 GDPR applies.

3 Authority of the Controller to issue instructions

3.1 The Processor processes Controller Data according to the Controller's instructions, unless the Processor is legally obliged to process otherwise. In such cases, the Processor shall inform the Controller of these legal requirements prior to processing, unless the relevant law prohibits such notification for important public interest reasons.

3.2 The Controller's instructions are generally conclusively set out and documented in the provisions of this DPA. Individual instructions that deviate from or impose additional requirements to those of this DPA require the Processor's prior consent and shall be carried out in accordance with to the amendment procedure set out in the Main Agreement, in which the instruction must be documented andthe assumption of any additional costs incurred by the Controller due to the instruction is to be regulated by the Processor..

3.3 The Processor shall ensure that it processes Controller Data in accordance with the Controller's instructions. If the Processor believes that an instruction from the Controller violates this DPA or applicable data protection law, it is entitled, after notifying the Controller, to suspend execution of the instruction until the Controller confirms it. The parties agree that the Controller bears sole responsibility for the processing of Controller Data in accordance with instructions.

4 Responsibility of the Controller

4.1 The Controller is solely responsible for the lawfulness of the processing of Controller Data and for safeguarding the rights of data subjects in the relationship between the parties. If third parties assert claims against the Processor due to the processing of Controller Data in accordance with this DPA, the Controller shall indemnify the Processor from all such claims upon first request.

4.2 If the Processor is required to provide information about the processing of Controller Data to a governmental authority or a person, or to otherwise cooperate with such authorities, the Controller is obliged to support the Processor upon first request in providing such information or fulfilling other cooperation obligations.

5 Requirements for personnel

The Processor shall commit all persons who process Controller Data to confidentiality regarding the processing of Controller Data.

6 Security of processing

6.1 The Processor will implement necessary and appropriate technical and organizational measures in accordance with Art. 32 GDPR, taking into account the state of the art, implementation costs, and the nature, scope, circumstances, and purposes of the processing of Controller Data, as well as the varying likelihood and severity of risks to the rights and freedoms of data subjects, to ensure a level of security appropriate to the risk.

6.2 The specific measures to be taken by the Processor are set out in Appendix 3 to this DPA.

6.3 The Processor may change or adapt technical and organizational measures during the term of the DPA, provided they continue to meet the requirements set out in Section 6.1 of this

DPA.

7 Use of additional sub-processors

7.1 The Controller hereby grants the Processor general authorization to engage further sub-processors with regard to the processing of Controller Data. The sub-processors engaged at the time of conclusion of the contract are listed in **Appendix** 2. Contractual relationships with service providers whose subject is the inspection or maintenance of data processing procedures systems by other entities, or other ancillary services, are generally not subject to approval, even if access to Controller Data cannot be excluded, provided the Processor has made appropriate arrangements to protect the confidentiality of Controller Data.

7.2 The Processor shall inform the Controller of intended changes regarding the addition or replacement of sub-processors. The Controller has the right to object to the engagement of a potential new sub-processor on a case-by-case basis, but only for a significant reason which must be demonstrated to the Processor. If the Controller does not object within 30 days of receiving notification, the right to object lapses. If the Controller objects, the Processor is entitled to terminate the Main Agreement and this DPA in accordance with the regular notice period specified in the Main Agreement.

7.3 The contract between the Processor and the sub-processor must impose the same obligations on the sub-processor as are imposed on the Processor by this DPA. The parties agree that this requirement is fulfilled if the contract provides a level of protection equivalent to this DPA or imposes the obligations set out in Art. 28(3) GDPR on the sub-processor.

7.4 Subject to compliance with the requirements of Section 2.6 of this DPA, the provisions of this Section 7 shall also apply if another processor is engaged in a third country.

8 Rights of the data subjects

8.1 Taking into account the nature of the processing, the Processor shall assist the Controller with appropriate technical and organizational measures, as far as possible, in fulfilling its obligation to respond to requests to exercise the rights of data subjects under Chapter III of the GDPR.

8.2 If a data subject makes a request to exercise their rights directly to the Processor, the Processor will promptly forward the request to the Controller.

8.3 The Processor may claim reimbursement of expenses and costs as well as reasonable remuneration from the Controller for its support under Sections 8.1 and 8.2 of this DPA, unless the support was required due to a breach of law or contract by the Processor.

9 Notification and support obligations of the Processor

9.1 If the Controller is subject to a statutory obligation to report or notify a breach of Controller Data protection (in particular under Art. 33, 34 GDPR), the Processor shall promptly inform the Controller of reportable events within its area of responsibility. The Processor shall support the Controller in fulfilling its reporting and notification obligations upon request, within the scope of what is reasonable and necessary.

9.2 The Processor shall support the Controller, as far as reasonable and necessary, in any data protection impact assessments to be carried out by the Controller and any subsequent consultations with supervisory authorities under Art. 35, 36 GDPR.

9.3 The Processor may claim reimbursement of expenses and costs as well as reasonable remuneration from the Controller for fulfilling its notification and support obligations, unless the obligation arose due to a breach of law or contract by the Processor.

10 Deletion and return of data

10.1 Upon termination of this DPA, the Processor shall, at the Controller's choice, delete or return the Controller Data and delete any existing copies, unless the Processor is required by law to continue storing the Controller Data. Backups may be retained in accordance with standard market backup routines for the corresponding period.

10.2 Documentation serving as proof of proper and contract-compliant processing of Controller Data may be retained by the Processor even after the end of the contract.

11 Evidence and audits

11.1 The Processor shall provide the Controller with all information necessary and available to the Processor to demonstrate compliance with its obligations under this DPA upon request.

11.2 The Controller shall be entitled to audit the Processor's compliance with the provisions of this DPA, in particular the implementation of technical and organizational measures, including through inspections.

11.3 For the purpose of conducting inspections under Section 11.2, the Controller is entitled, during normal business hours (Monday to Friday, 10 a.m. to 6 p.m.), upon timely prior notice in accordance with Section 11.5, at its own expense, without disrupting business operations and under strict confidentiality of the Processor's business and trade secrets, to enter the Processor's business premises where Controller Data is processed. Entry may only occur in the constant presence of a representative of the Processor, who is authorised to make decisions regarding the course of the inspection as necessary to avoid disruption of the Processor's business operations and to maintain confidentiality obligations towards third parties. The Controller shall reimburse the Processor for costs arising from such physical inspections. For data hosting, the standard audit options provided by the hosting provider apply.

11.4 The Processor is entitled, at its own discretion and taking into account the Controller's legal obligations, not to disclosure information that is sensitive with regard to the Processor's business or where disclosure would violate legal or other contractual provisions. The Controller is not entitled to access data or information about other customers of the Processor, information regarding costs, quality controll and contract management reports, or any other confidential data of the Processor not directly relevant to the agreed audit purposes.

11.5 The Controller shall inform the Processor in good time (generally at least four weeks in advance) of all circumstances related to the audit. The Controller may conduct one audit per calendar year. Further audits are subject to reasonable remuneration and in coordination with the Processor, unless the audit is required due to a breach of law or contract by the Processor.

11.6 If the Controller appoints a third party to conduct the audit, the Controller must obligate the third party in writing in the same way as the Controller is obligated to the Processor under this Section 11. In addition, the Controller shall obligate the third party to confidentiality, unless the third party is subject to a professional confidentiality obligation. Upon request, the Controller must promptly provide the Processor with the third party's confidentiality agreements. The corresponding obligations must establish a contractual obligation directly towards the Processor. The Controller may not appoint a competitor of the Processor to conduct the audit.

12 Term and termination

The term and termination of this DPA are governed by the provisions on term and termination of the Main Agreement. Termination of the Main Agreement automatically results in termination of this DPA. Isolated termination of this DPA is excluded.

13 Liability

13.1 The exclusions and limitations of liability under the Main Agreement shall apply to the Processor's liability under this DPA. If third parties assert claims against the Processor that are caused by a culpable breach of this DPA or any of the Controller's obligations as a data controller, the Controller shall indemnify the Processor from such claims upon first request.

13.2 The Controller undertakes to indemnify the Processor upon first request from any fines imposed on the Processor to the extent that the Controller shares responsibility for the breach sanctioned by the fine.

14 Final provisions

14.1 In case individual provisions of this DPA are ineffective or become ineffective or contain a gap, the remaining provisions shall remain unaffected. The parties undertake to replace the ineffective provision with a legally permissible provision that comes closest to the purpose of the ineffective provision and meets the requirements of Art. 28 GDPR.

14.2 In the event of conflicts between this DPA and other agreements between the parties, in particular the Main Agreement, the provisions of this DPA shall prevail.

Appendices:

Appendix 1: Details of data processing

Appendix 2: List of subcontractors

Appendix 3: Technical and organizational measures

Date [01.12.2025]

Appendix 1 – Details of data processing

1. Subject matter of processing

The subject matter of the processing is the processing of personal data in the context of the Processor's services, in particular the tracking of sales, payment, or financing transactions.

2. Purpose and nature of processing

Purpose of processing

The data processing is carried out to the extent necessary for the respective service. The details of the service description apply. Data processing takes place as far as the respective service has been commissioned.

Two basic types of services/data processing are distinguished:

Order and payment tracking: Data processing related to downstream measures in the context of payment or financing of orders or transactions online and in-store (e.g., payment processing, order information, customer management, shipping, analytics, etc.).

Marketing and sales support: Data processing for sales-promoting measures, especially in the context of marketing and sales support (e.g., customer support, newsletters, email marketing).

The payment or financing transaction is not carried out on behalf of the Controller, but on behalf of the respective payment or financing service provider.

Nature of processing

For these purposes, data is processed as follows:

Order/payment tracking: The Processor centrally provides the Controller with various information on payment/financing status together with the respective order and/or cancellation status.

Marketing and sales support: The Processor processes various personal information for the Controller such as name, address, email address, or telephone number.

3. Types of personal data

- Data contained in orders (e.g., name, address)
- Order data (e.g., product data, price)
- Information on order status
- Information on payment or financing status

4. Categories of data subjects

- Customers
- Prospects

- Visitors to the website and apps of the Processor
- Suppliers
- Partners of the Processor

5. Location of processing

- Nuremberg, Germany
- Falkenstein/Vogtland, Germany
- Dublin, Ireland
- Amsterdam, Netherlands

Appendix 2 – List of subcontractors

Name	Address	Country
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855	Luxembourg
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay, Dublin 2	Ireland
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Germany
Microsoft Ireland Operations Limited	Atrium Building Block A, Carmen Hall Road, Sandyford Industrial Park, Dublin	Ireland
One.com Group AB	Carlsgatan 3 211 20 Malmö	Sweden
Token GmbH	c/o Industrious Schicklerstraße 5 10179 Berlin	Germany
Twilio, Inc.	375 Beale Street, Suite 300 San Francisco, CA 94105	USA
Zendesk, Inc.	1019 Market Street San Francisco, CA 94103	USA

Appendix 3 – Technical and organizational measures

The technical and organizational measures documented in this appendix in accordance with Art. 32 GDPR by payever (1) and the cloud providers used by payever (2) concern the protection of data processing.

1 Security Measures by payever

1.1 Confidentiality (Art. 32(1)(b) GDPR)

1.1.1 Physical access control

payever implements the following technical and organizational measures for physical access control:

Technical measures:

- Alarm system,
- Manual locking system,
- Securing of building shafts,
- Doors with knob on the outside,
- Video surveillance of entrances.

Organizational measures:

- Key management / list.
- Visitor log / protocol.
- Visitors accompanied by employees.
- Careful selection of cleaning services.

1.1.2 System access control

payever implements the following technical and organizational measures for system access control:

Technical measures:

- Login with username and password,
- Antivirus software on servers,
- Antivirus software on clients,
- Firewall,
- Intrusion detection systems,
- Mobile device management,
- Use of VPN for remote access,
- Encryption of data carriers,
- Encryption of smartphones,
- Blocking of external interfaces (USB),
- Encryption of notebooks/tablets.

Organizational measures:

- Management of user permissions,
- Creation of user profiles,
- “Secure password” policy,
- “Delete/Destroy” policy,
- “Clean desk” policy,
- General data protection and/or security policy,
- Mobile device policy,
- Instruction “Manual desktop lock”.

1.1.3 Data access control

payever implements the following technical and organizational measures for data access control:

- Document shredders (at least level 3, cross cut),
- Physical deletion of data carriers,
- Logging of access to applications, specifically for input, modification, and deletion of data.

Organizational measures:

- Use of authorization concepts,
- Minimal number of administrators,
- Management of user rights by administrators.

1.1.4 Separation control

payever implements the following technical and organizational measures for separation control:

Technical measures:

- Separation of production and test environments,
- Physical separation (systems/databases/data carriers),
- Multi-tenancy of relevant applications.

Organizational measures:

- Control via authorization concept,
- Definition of database rights.

1.1.5 Pseudonymization (Art. 32(1)(a) GDPR, Art. 25(1) GDPR)

payever implements the following technical and organizational measures for pseudonymization:

Technical measure:

- Separation of assignment data and storage in a separate and secured system (if possible, encrypted).

Organizational measure:

- Internal instruction to anonymize/pseudonymize personal data as much as possible in the event of transfer or after expiry of the statutory deletion period.

1.2 Integrity (Art. 32(1)(b) GDPR)

1.2.1 Transfer control

payever implements the following technical measures for transfer control:

- Email encryption (S/MIME / PGP),
- Use of VPN,
- Secure transport containers,
- Provision via encrypted connections such as sftp, https,
- Use of signature procedures.

1.2.2 Input Control

payever implements the following technical and organizational measures for input control:

Technical measures:

- Technical logging of input, modification, and deletion of data,
- Manual or automated control of logs.

Organizational measure:

- Clear responsibilities for deletions.

1.3 Availability and Resilience (Art. 32(1)(b) GDPR)

payever implements the following technical and organizational measures regarding availability and resilience:

Technical measures:

- Fire and smoke detectors
- Fire extinguishers in server rooms
- Air-conditioned server room
- Video surveillance of server room
- Alarm notification in case of unauthorized access to server room.

Organizational measures:

- Backup & recovery concept (written out)
- Regular tests for data recovery and logging of results
- Storage of backup media in a secure location outside the server room
- No sanitary connections in or above the server room
- Existence of an emergency plan (e.g., BSI IT Grundschutz 100-4)

1.4 Procedures for Regular Review, Assessment, and Evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

1.4.1 Data Protection Management

payever implements the following technical and organizational measures for data protection management:

Technical measures:

- Central documentation of all procedures and regulations on data protection with access for employees as required/authorized (e.g., wiki, intranet, etc.),
- Other documented security concept,
- Effectiveness of technical security measures is reviewed at least annually.

Organizational measures:

- Use of an external data protection officer,
- Training and commitment of employees to confidentiality/data secrecy,
- Regular sensitization of employees at least annually,
- Data protection impact assessment (DPIA) is carried out if necessary,
- The organization complies with the information obligations under Art. 13 and 14 GDPR,
- Formalized process for handling data subject requests is in place.

1.4.2 Incident-Response-Management

payever implements the following technical and organizational measures for incident response management:

Technical measures:

- Use of firewall and regular updates,
- Use of spam filter and regular updates,
- Use of virus scanner and regular updates,
- Implementation of an intrusion detection system (IDS),
- Implementation of an intrusion prevention system (IPS).

Organizational measures:

- Documented process for detecting and reporting security incidents/data breaches (including notification obligation to supervisory authority),
- Documented procedure for handling security incidents,
- Involvement of ISB (information security officer) in security incidents and data breaches,
- Documentation of security incidents and data breaches, e.g., via ticket system,
- Formal process and responsibilities for follow-up of security incidents and data breaches.

1.4.3 Data Protection-Friendly Default Settings (Art. 25(2) GDPR)

payever implements the following technical measure for data protection-friendly default settings:

- No more personal data is collected than is necessary for the respective purpose.

1.4.4 Order Control

payever implements the following organizational measures for order control:

- Prior review of the security measures taken by the Processor and their documentation,
- Selection of the Processor based on due diligence (especially regarding data protection and data security),
- Conclusion of the necessary data processing agreement or EU Standard Contractual Clauses,
- Written instructions to the processor,
- Commitment of the Processor's employees to data secrecy,
- Agreement of effective control rights vis-à-vis the Processor,
- Ensuring the destruction of data after the end of the assignment,
- In the case of longer cooperation: ongoing review of the Processor and its protection level.

2 Security Measures of Cloud Providers

payever uses established cloud providers. Their security measures are available via the following links:

- Azure
- Hetzner
- Google Cloud
- AWS