Zone&Co

Data Processing Agreement

Last Updated: 1 February 2026

This data processing agreement ("Data Processing Agreement") is entered into by and between ZONE (hereafter: "ZONE") and Customer and applies to all Agreements under which ZONE processes personal data on behalf of Customer in accordance with Applicable Data Protection Laws

The Customer is deemed to be the controller within the meaning of article 4 (7) of the EU General Data Protection Regulation and the UK General Data Protection Regulation (collectively, the "GDPR"); and ZONE is deemed to be the processor within the meaning of article 4 (8) of the GDPR. Where, in this Data Processing Agreement, reference is made to terms that are defined in the GDPR, such as "controller", "processor" and "personal data", such terms will have the meanings given to them in the GDPR.

Article 1. Processing objectives

1.1. ZONE undertakes to process personal data on behalf of Customer in accordance with the conditions laid down in this Data Processing Agreement. The processing will be executed exclusively within the framework of the Agreement, for the processing of Customer Data through the Services provided by ZONE, and for all such purposes as may be agreed to subsequently.

1.2. The personal data (to be) processed by ZONE under this Data Processing Agreement include the following categories:

a. Name and address
b. Payment data such as bank account
c. VAT Number

1.3. The categories of data subjects to whom the personal data relates are as follows:

a. Suppliers
b. Customers
c. Employees

1.4. ZONE will refrain from making use of the personal data for any other purpose than as specified by Customer. Customer will inform ZONE of any processing purposes to the extent not already mentioned in this Data Processing Agreement. ZONE may use the personal data to improve the quality of their Services, for example by performing statistical research with regard to its Services, provided ZONE processes such data in anonymized or aggregated form.

1.5. ZONE will not take any unilateral decisions about the processing of personal data for other purposes. The control over the personal data processed pursuant to this Data Processing Agreement and/or other agreements between the Parties rests with Customer.

1.6. All personal data processed on behalf of Customer will remain the property of Customer and/or the relevant data subjects.

Article 2. Processor's obligations

2.1. ZONE will comply with the laws and regulations relating to the protection of personal data in connection with the processing of personal data by ZONE, such as the GDPR.

2.2. At the request of Customer, ZONE will furnish Customer with details regarding the measures it has adopted to comply with its obligations under this Data Processing Agreement.

2.3. ZONE's obligations arising under the terms of this Data Processing Agreement also apply to whomsoever processes personal data under ZONE's instructions.

2.4. ZONE will provide any reasonably necessary assistance if a data protection impact assessment, or a prior consultation with a supervisory authority, is necessary with respect to the processing of personal data. Such assistance shall be provided as mutually agreed between the parties (including in respect of any reasonable costs in connection therewith).

Article 3. Transmission of personal data

3.1. ZONE may at its option (a) process the personal data in countries within the European Union, European Economic Area, Switzerland and UK (collectively, "Europe"); and (b) subject to complying with requirements under Applicable Data Protection Law transfer the personal data to a country outside Europe, including to Affiliates and sub-processors. Without limiting the foregoing, the Customer acknowledges and agrees that ZONE and certain of its Affiliates established outside Europe have entered into EU Standard Contractual Clauses with UK Addendum (Module 3) to enable the transfers of the personal data between and among ZONE and such Affiliates.

3.2. At the request of Customer, ZONE will inform Customer about the country or countries outside Europe in which the personal data will be processed.

Article 4. Allocation of responsibility

4.1. The authorized processing will be carried out by ZONE within a (semi-) automated environment.

4.2. ZONE will be responsible for the processing of personal data under this Data Processing Agreement, in accordance with the documented instructions of Customer and under the (ultimate) responsibility of Customer.

4.3. ZONE is expressly not responsible for other processing of personal data, including but not limited to, the collection of personal data by Customer and processing for purposes that are not reported by Customer to ZONE.

4.4. Customer represents and warrants that it has explicit consent and/or another legal basis to process the relevant personal data and that it has informed the data subjects of the processing of personal data under this Agreement, in line with its duty thereto under the GDPR. Furthermore, Customer represents and warrants that the

content, the use and the instruction to process the personal data within the meaning of this Data Processing Agreement are not unlawful and do not infringe any rights of a third party. In this context, Customer indemnifies ZONE of all claims and actions of third parties related to the processing of personal data under this Data Processing Agreement.

Article 5. Sub-processors

5.1. As also stated in Section 8.2 of the Agreement, ZONE may engage third-party subprocessors and the Customer hereby grants ZONE general authorization to do so. A current list of ZONE'S subprocessors can be found at: https://help.zoneandco.com/hc/en-us/articles/26302640972955-Zone-Third-Party-Sub-processors. ZONE may add, remove and/or exchange subprocessors in its sole discretion upon no less than thirty (30) days' notice to Customer. Should Customer object in writing raising valid and reasonable objections to the appointment of an additional subprocessor within fourteen (14) calendar days of such notice, ZONE shall have the right to cure the objection through one of the following actions at ZONE'S sole discretion: (a) offer to Customer an alternative method to provide the Services without such subprocessor; (b) take corrective steps that, in ZONE'S reasonable discretion, address Customer's objection; (c) cease to provide to Customer the particular aspect of the Services that would involve the use of such subprocessor If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the parties within thirty (30) days after ZONE'S receipt of Customer's objection, either party may terminate the Agreement, inclusive of this Data Processing Agreement, and, as applicable, Customer will be entitled to a pro-rata refund for prepaid fees for Services not performed as of the date of termination.

5.2. ZONE will, in any event, ensure that such third parties will be obliged to agree in writing to the same duties as agreed by Customer and ZONE in this Data Processing Agreement.

Article 6. Security

6.1. ZONE and Customer will take adequate technical and organizational measures against loss or any form of unlawful processing (such as unauthorized disclosure, deterioration, alteration or disclosure of personal data) in connection with the performance of processing personal data under this Data Processing Agreement. Please refer to **Schedule 1** to this Data Processing Agreement for **ZONE's TECHNICAL AND ORGANISATIONAL MEASURES (TOMS)**.

6.2. ZONE does not warrant that the security measures are effective under all circumstances. ZONE will endeavor to ensure a level of security appropriate to the risk taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Article 7. Personal data breaches

7.1. In the event of a personal data breach, within the meaning of the GDPR, ZONE will notify Customer thereof without undue delay but at least within forty-eight (48) hours upon its discovery. Customer will use reasonable endeavors to ensure that the provided

information is complete, correct and accurate. Customer will then decide whether or not to notify the data subjects and/or the relevant supervisory authorities.

7.2. If required by applicable laws and/or regulations, ZONE will cooperate in notifying the relevant authorities and/or data subjects. Customer will determine whether or not to inform the relevant regulatory authorities and/or the data subjects. Customer remains the responsible party for any statutory notification obligations in respect thereof.

7.3. The notification obligation includes in any event the duty to report the fact that a breach has occurred, including details regarding:

a. the (suspected) cause of the breach;
b. the contact point where more information can be obtained;
c. the approximate number of data subjects and number of personal data records concerned;
d. the (currently known and/or anticipated) consequences thereof;
e. the (proposed) solution;
f. the measures that have already been taken.

Article 8. Handling requests from data subjects

8.1. In the event that a data subject submits a request to ZONE to exercise his/her rights under applicable privacy laws and regulations, ZONE will notify Customer and Customer will be responsible for handling the request. ZONE may notify the data subjects of the fact that their requests have been forwarded and will be handled by Customer. Where necessary, ZONE will reasonably assist Customer in implementing appropriate technical and organizational measures. Such assistance shall be provided at no additional charge to Customer.

Article 9. Non-disclosure and confidentiality

9.1. All personal data received by ZONE from Customer within the framework of this Data Processing Agreement is subject to a duty of confidentiality vis-à-vis third parties.

9.2. This duty of confidentiality will not apply in the event that Customer (i) has expressly authorized the provision of such information to third parties, (ii) where the provision of the information to third parties is reasonably necessary taking into account the nature of the instructions and the implementation of this Data Processing Agreement, or (iii) if there is a statutory obligation to provide the information to a third party.

Article 10. Audit

10.1. In order to confirm compliance with all points in this Data Processing Agreement, Customer will be entitled to have audits carried out by an independent third party who is bound to confidentiality.

10.2. The audit will only take place after Customer has requested and assessed similar audit reports made available by ZONE (including ISO 27001 and SOC 2 certifications) and provided reasonable arguments that justify an audit initiated by Customer. Such an audit is justified when the audit reports provided by ZONE give no or insufficient information regarding ZONE's compliance with this Data Processing Agreement. The audit initiated by Customer will take place no more than once a year and after Customer has provided

two weeks prior notification.

10.3. ZONE will cooperate in the audit and will make available any reasonably necessary information, including supporting information such as system logs and employees as timely as possible.

10.4. The findings in respect of the performed audit will be discussed and evaluated by the Parties and, where applicable, implemented by one of the Parties or jointly by both Parties.

10.5. The costs of the audit will be borne by Customer, it being understood that the costs for the engaged independent third party will always be borne by Customer.

Article 11. Duration and termination

11.1. This Data Processing Agreement is entered for the duration set out in the Agreement.
11.2. This Data Processing Agreement may not be terminated for convenience.

11.3. Upon termination of the Data Processing Agreement, ZONE will, at the request of Customer, return the personal data to Customer and/or will securely destroy such personal data, and provide written confirmation of such return or destruction, except to the extent the Data Processing Agreement, Agreement or applicable laws and regulations provide otherwise.

11.4. Amendments to this Data Processing Agreement may only be agreed by the Parties in writing.

11.5. Parties will provide their full cooperation in amending this Data Processing Agreement in the event of any amended privacy laws and regulations.

Article 12. Miscellaneous

12.1. This Data Processing Agreement forms an integral part of the Terms of Service. All rights and obligations under the Terms of Service, including the limitations on liability and applicable law, apply mutatis mutandis to this Data Processing Agreement.

Zone&Co

Data Processing Agreement

Schedule 1

Technical And Organisational Measures (TOMS)

1. Organization of Information Security

- **Security Management:** Zone maintains an Information Security Committee (ISC) composed of senior managers that meets quarterly to review risks, software changes, and vendor engagements.
- **Policy Review:** Policies are reviewed and updated at least annually or upon major changes to applications/infrastructure.
- **Asset Management:** The ISC maintains an inventory of production information systems, including hardware, software, and communication links.

2. Access Control

- **Remote-First Model:** Zone is primarily and predominantly a remote-first organization.
- **Cloud Hosting:** Data is primarily stored on third-party hosting services (CSPs). Zone ensures these vendors handle data destruction appropriately.
- **Workstation Security:** All unattended workstations must be locked. Portable devices offsite must be physically secured (e.g., locked in a desk or cabinet) and never left unattended in a vehicle.
- **Least Privilege:** Access to systems is restricted based on the principle of "least privilege," granting only permissions necessary for assigned tasks.
- **User Authentication:**
    - **Unique Accounts:** Users must use unique passwords for work accounts and are prohibited from sharing credentials.
    - **Multi-Factor Authentication (MFA):** MFA is required for all privileged accounts and highly encouraged for all work-related accounts.
    - **Password Standards:** Passwords must be a minimum of 12 characters, with a preference for passphrases.
- **Access Reviews:** Access to critical IT systems is reviewed semi-annually and approved by the ISC Leader.
- **Offboarding:** Accounts of terminated or transferred users are deactivated immediately.

3. Data Encryption (Transmission & Storage)

- **Encryption Standards:**
    - **Symmetric:** AES is strongly recommended.
    - **Asymmetric:** RSA and Elliptic Curve Cryptography (ECC) are strongly recommended.
- **Data in Transit:** All data collected or generated by Zone applications is encrypted in transit. Servers using SSL/TLS must have valid certificates from trusted providers.
- **Data at Rest:** All data is encrypted at rest, including backups. Workstations containing sensitive information must employ hard disk encryption.
- **Key Management:** Cryptographic keys are generated using industry-standard random number generators (RNG) and stored securely.

4. Availability, Resilience & Disaster Recovery

- **Backups:** Production data is backed up daily to highly available storage.
- **Recovery Objectives:**
  - **RTO (Recovery Time Objective):** Services restored within 4 hours.
  - **RPO (Recovery Point Objective):** Applications recovered to a state within 6 hours prior to the incident.
- **Testing:** Disaster recovery plans are tested annually via tabletop exercises.

5. Vulnerability Management & System Hardening

- **Endpoint Protection:** All workstations must have approved endpoint protection/anti-malware tools installed, enabled, and updated in real-time.
- **Patch Management:** Patches are installed daily if available.
- **Firewalls:** Workstations connecting to the internet must have host-based firewalls enabled.
- **Logging:** Logs of security-relevant events (including login attempts and privileged user activity) are retained for at least six months.

6. Incident Management

- **Response Plan:** Zone maintains a formal Incident Response Plan (IRP) covering preparation, identification, containment, eradication, recovery, and lessons learned.
- **Response Timelines:**
  - **High Severity:** Response < 1 hour (e.g., complete system unavailability).
  - **Medium Severity:** Response < 6 hours (e.g., partial unavailability).
  - **Low Severity:** Response < 12 hours.
- **Notification:** Confirmed breaches are reported to the Head of Security & IT, and communication plans are coordinated with legal/HR for internal and public notification.

7. Personnel & Vendor Security

- **Training:** All employees must complete security awareness training upon hire and annually thereafter. Topics include phishing, social engineering, and data privacy.
- **Clean Desk Policy:** Sensitive information must be locked away when not in use; printouts are removed immediately, and documents are shredded.
- **Vendor Management:** All sub-processors and partners must agree to comply with Zone's Information Security Policy or bound by substantially similar policies.

8. Sub-Processor Assistance Measures

- Contractual Flow-Down: Zone sub-processors enter into Data Processing Agreements (DPAs) that mandate technical security measures substantially similar to Zone’s own standards.
- Assistance with Data Subject Rights: Sub-processors are required to provide technical capabilities (such as data export tools, deletion APIs, or dedicated support channels) to enable Zone to fulfill requests for data access, rectification, or erasure.

- Breach Notification Assistance: Sub-processors are contractually obligated to notify Zone without undue delay of any security incident and provide necessary technical details to enable Zone to meet its regulatory reporting obligations to Controllers and Authorities.