Data Processing Agreement

This Data Processing Agreement (the "**Data Processing Agreement**") supplements the offer you received, or any other agreement between Customer and Zivver governing Customer's use of the Zivver-service (collectively, the "**Agreement**") when the GDPR applies to your use of the Zivver-Service to process any Personal Data.

This Data Processing Agreement is an agreement between you and the entity you represent ("**Customer**" or "**you**") and the applicable Zivver contracting entity under the offer or other agreement ("**Zivver**"). Customer and Zivver hereinafter jointly referred to as "**Parties**", and individually "**Party**";

WHEREAS:

(A) The Data Processing Agreement has been concluded for the delivery of the Zivver-service by Zivver to Customer, for the execution of the Agreement;

(B) Zivver may process certain Personal Data on behalf of Customer pursuant to the Agreement;

(C) Customer is hereby deemed to be a controller within the meaning of Article 4 (7) of the General Data Protection Regulation ("**GDPR**") and Zivver is hereby deemed to be a processor within the meaning of article 4 (8) of the GDPR; and

(D) this Data Processing Agreement contains the conditions and respective rights and obligations of the Parties regarding the Processing of Personal Data within the meaning of article 28 (3) of the GDPR.

HAVE AGREED AS FOLLOWS:

1. Definitions

1.1. The definitions in this Data Processing Agreement (written with a capital letter) regarding the Processing of Personal Data (such as but not limited to: Personal Data, Processing, Data Subject, Controller, Processor and Third Party) shall have the meaning of the corresponding definitions in the GDPR.

1.2. Applicable Law: all laws and regulations applicable to the Processing of Personal Data, including but not limited to the GDPR and its Dutch Implementation Act.

2. Processing of Personal Data

Zivver delivers its services on the basis of the Agreement as a Processor for Customer. Customer remains the Controller regarding all Personal Data that is processed based on the Agreement. The categories of Personal Data and Data Subjects and the purpose of the Processing by Zivver are described in **Annex 1** (Personal Data and Processing Activities).

3. Controller's obligations

3.1. As a Controller, Customer must comply with its obligations under Applicable Law, the Agreement and this Data Processing Agreement.

3.2. Controller instructs Processor to Process the Personal Data on behalf of Controller and in accordance with Applicable Law. Controller's Processing instructions are laid down in **Annex 1** (Peronal Data and Processing Activities).

3.3. Controller may give additional or adjusted Processing instructions, provided that such instructions are in accordance with the conditions of the Agreement and this Data Processing Agreement, and these are reasonable and in accordance with Applicable Law. Controller shall notify Processor of such instructions in writing.

4. Processor's obligations

4.1. As a Processor, Zivver must comply with its obligations under the Agreement, this Data Processing Agreement and Applicable Law.

4.2. Processor shall (a) act in accordance with the written instructions of Controller; (b) refrain from Processing the Personal Data for its own purposes; and (c) only Process the Personal Data to the extent necessary for the performance of the activities of Processor pursuant to the Agreement; unless a European or Member State law applicable to Processor obliges him to act differently and Processor informs Controller thereof without undue delay in accordance with Article 4.5 (ii).

4.3. If, during the term of this Data Processing Agreement, Processor receives a request from a Data Subject regarding his/her Personal Data pursuant to Chapter III of the GDPR, Processor shall refer the Data Subject to Controller without undue delay. Controller is at all times responsible for answering such requests. Processor shall provide the assistance reasonably required by Controller in order to enable Controller to fulfill its obligations with regard to responding to requests from Data Subjects to exercise their rights.

4.4. Processor shall provide the assistance required by Controller in its capacity as Processor to enable Controller to perform a Data Protection Impact Assessment and a possible subsequent prior consultation from a Supervisory Authority.

4.5. Processor shall inform Controller without undue delay in the following cases:

(i) a European or Member State law applicable to Processor prevents Processor from complying with the written instructions from Controller, unless such legislation prohibits Processor from providing such information;

(ii) Processor holds the opinion that an instruction from Controller infringes Applicable Law.

4.6. Upon termination of the Agreement or, if earlier, after the end of the delivery of Processing Activities, Processor shall return all Personal Data to Controller in a common format and/or delete all copies of such Personal Data, at the discretion of Controller, unless a European or Member State law applicable to Processor prohibits Processor to return or delete Personal Data.

4.7. Processor may charge reasonable costs for providing assistance to Controller with complying with its obligations under Applicable Law.

5. Subprocessors

5.1. By this Data Processing Agreement, Controller gives specific permission for the engagement of the third parties referred to in **Annex 1** as Subprocessor for the performance of Processing Activities arising from the Agreement and this Data Processing Agreement. In addition, if Processor intends to engage a new or different Subprocessor, Controller hereby grants general authorization, provided that Processor informs Controller of any such intended changes. Controller may object, in writing and substantiated by well-founded arguments, to the engagement or modification of this Subprocessor. If the Controller objects, the Parties shall enter into consultation to find a workable solution.

5.2. Processor shall impose the engaged Subprocessor(s) corresponding obligations as agreed between Controller and Processor on the basis of the Data Processing Agreement.

5.3. Processor remains responsible for any acts or omissions on the part of a Subprocessor that causes Processor to breach its obligations under the Agreement or this Data Processing Agreement.

6. Confidentiality

6.1. Processor shall maintain confidentiality with regard to the Personal Data. Processor is not permitted to provide Personal Data to third parties or affiliated parties, except: (a) if this is permitted under the Agreement; or (b) in accordance with Article 5; or (c) with the explicit consent of Controller; or (d) in case of a statutory obligation to provide Personal Data to a third party. When Processor is legally obliged to provide Personal Data to a third party, it will inform Controller thereof before such provision, unless Applicable law prohibits Processor to do so on important grounds of public interest.

6.2. Processor shall limit the distribution of the Personal Data to those employees of Processor to whom the Processing of Personal Data is assigned pursuant to the Agreement, and only to the extent that it is necessary for them to be aware of and/or take note of the Personal Data (“need to know” basis).

7. Security and Personal Data Breaches

7.1. Processor shall implement appropriate technical and organizational measures to protect the confidentiality, integrity and availability of Personal Data that are in line with Applicable law, including protection against destruction, loss, unauthorized disclosure or access or any form of unlawful processing.

7.2. **Annex 2** (Security Measures) describes the measures that Processor has implemented and shall maintain. Processor may update or adjust the Security Measures from time to time, provided that such updates and/or adjustments do not lead to a reduction in the level of protection.

7.3. Processor shall inform Controller without undue delay of a Personal Data Breach (which is understood as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, transmitted, stored or otherwise processed Personal Data). Processor shall adhere to procedures aimed at discovering, responding to and resolving Personal Data Breaches.

7.4. The notification contains at least a description of:

(i) the nature of the Personal Data Breach, where possible stating the categories and the estimated number of Data Subjects and Personal Data involved;

(ii) whether the Personal Data are encrypted, anonimyzed or otherwise made incomprehensible;

(iii) the name and contact details of the Data Protection Officer or another contact point where more information can be obtained;

(iv) the likely consequences of the Personal Data Breach; and

(v) the measures that Processor has taken or proposes to take to resolve the Personal Data Breach, including, where appropriate, measures to limit any adverse consequences thereof.

7.5. Controller is responsible for compliance with its (statutory) obligations to notify. Processor shall, on request of Controller, assist Controller in order to ensure that the relevant Supervisory Authority and/or Data Subjects are adequately informed.

8. Audit

8.1. Controller has the right to have an audit performed by an independent third party who shall be bound by confidentiality to verify compliance with this Data Processing Agreement.

8.2. The audit may only take place after Controller has requested, assessed and submitted reasonable arguments in writing that justify an audit initiated by Controller. Such an audit is justified if the similar reports present at Processor do not provide sufficient or conclusive information about Processor's compliance with this Data Processing Agreement or if Controller has reasonable doubt about such compliance.

8.3. The audit initiated by Controller will take place at least two weeks after prior announcement by Controller on a date and time to be determined by the Parties in joint consultation.

8.4. The costs of the audit will be borne by Controller.

9. Transfer of Personal Data outside the EEA

9.1. The Parties acknowledge that Applicable Law contains restrictions with regard to the transfer of Personal Data from a country in the European Economic Area ("EEA") to countries or organizations outside the EEA that do not guarantee an adequate level of protection and that are not considered safe by the European Commission, including making the Personal Data accessible from such a country or such an organization ("**Transfer**").

9.2. The Processor's primary data processing location is within the EEA. For specific purposes the sub-processor does process data outside the EEA. This includes product integrations and product detection improvements (the product detection improvements is an optional feature). The Processor may Transfer Personal Data in compliance with applicable laws and regulations.

9.3. Exclusively applicable in case of Zivver Academy (e-learning): subprocessor EasyGenerator hosts the data within the EEA, but uses some sub-processors outside the EEA. Transfers to these sub-processors are subject to standard contractual clauses. By agreeing to this DPA, Customer consents to the Transfer of Personal Data outside the EEA in accordance with https://www.easygenerator.com/en/scc/.

10. Term and termination

10.1. This Data Processing Agreement forms an integral part of the Agreement and terminates automatically upon termination of the Agreement.

10.2. If any provisions in this Data Processing Agreement are declared void, this will not affect the validity of the entire Data Processing Agreement. For the purpose of replacing such a provision, the Parties will lay down one or more new provision(s) that reflect the purpose of the original provision as far as possible under the law.

11. Applicable law and dispute settlement

11.1. This Data Processing Agreement and the execution thereof are governed by Dutch law.

11.2. All disputed that may arise between the Parties in connection with this Data Processing Agreement, will be submitted to the court of Amsterdam.

Annex 1

Personal Data and Processing Activities

To create an account & authentication for admin users

Email address admin

Credentials

To identify user mailboxes to protect

User directory with email addresses

To scan and analyze emails, add classifications and apply proper actions (like quarantine)

EML files including the following personal data

- Email address sender
- Email address recipient
- IP address sender
- Subject of message
- Attachment names
- Content of the email and attachments
- Data behind embedded links

Classifications given by the customer (if classification is manually updated by the admin)

Logging of admin actions within the application

Email address admin

Timestamps

Actions performed by admin

To improve the product

Event data (data about how the product is used)

To improve detection rules (opt in feature - only when shared by customers)

EML files

Classification given by the customer

Participating in e-Learning Zivver Academy (optional feature)

Name and email address of participants
Name and date of e-learnings followed
Answers of participants on test questions on how to use Zivver products
Answers of participants on feedback questions regarding the e-learning
Optional: a video message of the internal ‘champion’ (only applicable to custom build e-learnings)

Processing Activities & Sub – Processors

Activity	Sub-processor	Comments
Zivver Email Threat Protection Full application	Sublime Security	SOC2 Type2 report available. DPA is signed.
Zivver e-Learning Hosts e-learning platform	EasyGenerator	ISO27001 certified. Data storage in the EEA. DPA is signed.

Annex 2

Security Measures

Technical and Organizational Security Measure	**Details**
Measures of pseudonymisation and encryption of personal data	Secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest. The use of only recommended secure cipher suites and protocols to encrypt all traffic in transit and Customer Data is securely encrypted with strong ciphers and configurations when at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Customer agreements contain strict confidentiality obligations. Additionally, every downstream Subprocessor is required to sign confidentiality provisions that are substantially similar to those contained in Company's customer agreements. Zivver and Sublime Security have undergone a SOC 2 Type 2 audit.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Daily, weekly and monthly backups of production datastores are taken. Backups are periodically tested in accordance with information security and data management policies.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Zivver and Sublime Security have undergone a SOC 2 Type 2 audit.
Measures for user identification and authorization	The use of secure access protocols and processes and follows industry best-practices for authentication, including Multi Factor Authentication and Single Sign On (SSO). All production access requires the use of two-factor authentication, and network infrastructure is securely configured to vendor and industry best practices to block all unnecessary ports, services, and unauthorized network traffic.
Measures for the protection of data during transmission	Deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Only uses recommended secure cipher suites and protocols to encrypt all traffic in transit (i.e. TLS 1.2)
Measures for the protection of data during storage	Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by AWS.

Measures for ensuring physical security of locations at which personal data are processed	All processing occurs in physical data centers that are managed by AWS. https://aws.amazon.com/compliance/data-center/controls/
Measures for ensuring events logging	Monitoring of access to applications, tools, and resources that process or store Customer Data, including cloud services. Monitoring of security logs is managed by the security and engineering teams. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	A change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. All production changes are automated through CI/CD tools to ensure consistent configurations.
Measures for internal IT and IT security governance and management	An ISO 27001-compliant risk-based information security governance program. The framework for Company's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.
Measures for certification/assurance of processes and products	Zivver and Sublime Security have undergone a SOC 2 Type 2 audit.
Measures for ensuring data minimisation	Customers unilaterally determine what data they route through the Services. As such, we operate on a shared responsibility model. Company gives Customers control over exactly what data enters the platform. Additionally, there is self-service functionality to the Services that allows Customers to delete and suppress data at their discretion.
Measures for ensuring data quality	A multi-tiered approach for ensuring data quality. These measures include: (i) unit testing to ensure quality of logic used to process API calls, (ii) database schema validation rules which execute against data before it is saved to our database, (iii) a schema-first API design to enforce a strict contract between official clients and API resolvers. These measures are applied across the board, both to ensure the quality of any Usage Data that is collected and to ensure that the Platform is operating within expected parameters.
Measures for ensuring limited data retention	Customers unilaterally determine what data they route through the Services. As such, we operate on a shared responsibility model. If a Customer is unable to delete Personal Data via the self-services functionality of the Services, then Processor deletes such Personal Data upon the Customer's written request, within the timeframe specified in this DPA and in accordance with Applicable Data Protection Law. All Personal Data is deleted from the Services following service termination.

Measures for ensuring accountability	Adopted measures for ensuring accountability, such as implementing data protection and information security policies across the business, recording and reporting Personal Data Breaches, and formally assigning roles and responsibilities for information security and data privacy functions. Additionally, regular third-party audits to ensure compliance with our privacy and security standards are conducted.
Technical and organizational measures of sub-processors	The Processor enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this DPA.