

DATA PROCESSING AGREEMENT FOR VESET CUSTOMER ('DPA')

This DPA is made between Veset and the Customer identified in the Order that references this DPA and describes certain data processing and transfer obligations of the parties. This DPA is subject to the terms of the Agreement pursuant to which Veset may Process certain Personal Data on behalf of Customer in connection with Customer's use of Veset services ("Veset Service" or "Veset Services") and is incorporated therein by reference. In the event of any inconsistency between this DPA and the Agreement, or between this DPA and the Order, this DPA shall prevail.

1. Definitions. In this DPA, the following terms shall have the meanings set out below. Other capitalized terms used but not otherwise defined herein shall have the meanings ascribed to such terms in the Agreement.
 - 1.1. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party.
 - 1.2. "Agreement" means the agreement between the Controller and the Processor for the provision of the Veset Services.
 - 1.3. "CCPA Consumer" means a "consumer" as such term is defined in the CCPA.
 - 1.4. "CCPA Personal Information" means the "personal information" (as defined in the CCPA) that Veset processes on behalf of the Customer in connection with the Veset's provision of the Veset Services.
 - 1.5. "Controller" is the Customer.
 - 1.6. "Data Protection Laws and Regulations" means laws and regulations applicable to the Processing of Personal Data under the Agreement, including: (i) California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. ("CCPA"); and (ii) applicable laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, and the United Kingdom, including without limitation Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" or "GDPR"), the UK Data Protection Act 2018 and EU Directive 2002/58/EC on Privacy and Electronic Communications ("e-Privacy Directive") or, the superseding Regulation on Privacy and Electronic Communications ("e-Privacy Regulation"), once effective.
 - 1.7. "Data Subject" shall have the same meaning as in Data Protection Laws and Regulations.
 - 1.8. "DPA" means this data processing agreement together with its schedules.
 - 1.9. "Personal Data" means any information relating to a Data Subject that is Processed by Veset on behalf of the Customer pursuant to the terms of the Agreement, including "personal data" (as defined in the GDPR) and "personal information" as defined in the CCPA, as applicable.

- 1.10. “Personal Data Breach” means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
- 1.11. “Process,” “Processes,” “Processed” or “Processing” shall have the same meaning as in Data Protection Laws and Regulations.
- 1.12. “Processor” means Veset.
- 1.13. “Security Policy” means the Processor’s security document as updated from time to time set out in Schedule B of this DPA.
- 1.14. “Sell” and “Sale” have the meaning given in the CCPA.
- 1.15. “Standard Contractual Clauses” means the EU model clauses for Personal Data transfer to countries outside the European Union, European Economic Area (EEA), Switzerland and the UK Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en
- 1.16. “Subprocessor” means any person or entity engaged by the Processor or its Affiliates to process Personal Data in the provision of Veset Services to the Controller, as further described in Section 2.4 of this DPA.

2. Protection of Personal Data

- 2.1. Relationship of Parties: For the purposes of the Agreement, Customer is the Controller and appoints Veset as a Processor to Process Personal Data on behalf of Customer in connection with Customer’s use of Veset Services pursuant to the Agreement. The Processor and Controller shall each comply with their respective obligations under Data Protection Laws and Regulations and this DPA.

For the purposes of the CCPA, the Parties acknowledge and agree that Veset will act as a “Service Provider” as such term is defined in the CCPA, in its performance of its obligations pursuant to the Agreement

- 2.2. Purpose Limitation: Veset shall Process Personal Data on behalf of the Customer in order to perform Veset’s obligations, or as otherwise permitted, under the Agreement as a Processor, in compliance with the applicable Data Protection Laws and Regulations. The purposes of Processing are as described in the Agreement, including Schedule A to this DPA, and any other exhibits, statements of work or addenda attached to or otherwise incorporated into the Agreement (the “Permitted Purpose”).

Veset shall not retain, use or disclose CCPA Personal Information for any purpose other than for the specific purpose of providing the Veset Services, or as otherwise permitted by the CCPA. Veset acknowledges and agrees that it shall not retain, use or disclose CCPA Personal Information for a commercial purpose other than for the Permitted Purpose.

2.3. Cross-Border Transfers: The Customer agrees that the Processor, its Affiliates and Sub-Processors may transfer Personal Data for the purpose of providing the Veset Services to the Customer in accordance with the Agreement to countries outside the European Union, European Economic Area (EEA), Switzerland and the UK. The Processor confirms that Affiliates and Sub-Processors: (i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) have entered into Standard Contractual Clauses with the Processor; or (iii) have other legally recognised appropriate safeguards in place.

2.4. Subprocessing:

a. Customer acknowledges and agrees that Affiliates of Veset may be used as Subprocessors. Veset and its Affiliates may engage Subprocessors in connection with the provision of Veset Services. Below is a list of approved Subprocessors as of the Effective Date of this DPA:

Data Processors	Purpose , Service type	Legal basis (GDPR Article)	Data (PII)	Location of data processor	Data transfer Mechanism	Supplemental Measures
Asana	Task management service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f) Processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6, 1.(c)	Contact persons: Name, email address, job title, company, country.	USA, EU	SCCs https://asana.com/terms#data-processing	Data encrypted end-to-end and at rest. https://asana.com/terms#privacy-commitment
Atlassian	Software development and management services support, issue tracking	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f) Processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6, 1.(c)	Contact persons: Name, email address, job title, company, country. Device identification data (IP address, browser type and version, web logs).	Australia, USA, EU	https://www.atlassian.com/legal/data-processing-addendum SCCs	Data is encrypted at rest and in transits. See more: https://www.atlassian.com/trust/security/security-practices#encryption-of-data https://www.atlassian.com/trust/privacy/guidelines-for-law-enforcement https://www.atlassian.com/trust/privacy/

						how-we-handle-your-data
AWS (Amazon Web Services)	Cloud services and data storage provider for Veset services	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f) Processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6, 1.(c)	Customer service users: username, email, Optional user, First name, Last name, phone number, address, Optional org, address All application data except payment details. Customer contact persons: All application data except payment details.	USA, EU	SCCs	AWS takes technical and contractual measures to protect data: Encryption of data in transit and at rest. Encryption key stored in the EU. https://dl.awsstatic.com/legal/laws-gdpr/AWS_GDPR_DPA.pdf https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/ https://aws.amazon.com/blogs/security/new-standard-contractual-clauses-now-part-of-the-aws-gdpr-data-processing-addendum-for-customers/

Box.com	Content, document management	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Name, email address, job title, company, country. Agreement documents, document copies with PII. Payment data (account No, bank details, address).	EEA, UK, USA	SCCs	Data is encrypted at rest and in transits. https://www.box.com/gdpr https://blog.box.com/update-new-standard-contractual-clauses-edpb-guidance
Calendly https://calendly.com/	Meeting scheduling service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Name, email address.	EEA, UK, USA, Canada	SCCs	Encryption of data in transit and at rest. All connections from the browser to the Calendly platform are encrypted in transit using TLS SHA-256 with RSA Encryption. Calendly requires HTTPS for all services. Calendly uses HSTS to ensure browsers interact with Calendly only over HTTPS and is on the HSTS preloaded lists for both Google Chrome and Mozilla Firefox. https://calendly.com/

						ly.com/security
CapsuleCRM	CRM service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Name, email address, job title, company, country. Correspondence.	USA	SCCs	Data is encrypted at rest and in transit. https://capsulecrm.com/security/
Docusign	Electronic document signing service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f) Processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6, 1.(c)	Name, email address, job title, company, country.	USA	BCRs (binding corporate rules)	Data is encrypted at rest and in transit. https://www.docusign.com/trust/privacy/gdpr
Google LLC	Collaboration services	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Contact persons: Name, email address, job title, company, country.	EU, USA	SCCs	Encryption of data in transit and at rest for Google Cloud Platform and Google Workspace. https://cloud.google.com/terms/data-processing-terms EU Data Protection Compliance: Google Cloud International Data Transfer Mechanisms

HelpDocs	Document management service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Unstructured information Contains PII.	EU, USA	SCCs	Data is encrypted at rest and in transit. https://support.helpdocs.io/article/13xkvjme6a-is-helpdocs-gdpr-compliant
LogMeIn	LastPass secret management service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Name, email address.	USA	SCCs	Data encrypted at rest and in transit. https://logmeincdn.azureedge.net/legal/gdpr-v2/LastPass-GDPR-Snapshot-Final-120418.pdf https://www.logmein.com/trust/privacy
MailChimp	Client communication service. marketing, communication services	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Name, email address, job title, company, country.	USA	SCCs	Data encrypted at rest and in transit. https://mailchimp.com/gdpr/
MongoDB Atlas (cloud service)	Database services	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f) Processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6, 1.(c)	Name, email address.	USA, EU, UK	SCCs	Data encrypted at rest and in transit. https://www.mongodb.com/cloud/trust/compliance/gdpr

Slack Technologies LLC	Collaboration tools	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f) Processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6, 1.(c)	Name, email address, job title, company, country.	USA, Ireland	SCCs	Encryption of data at rest and in transit. https://slack.com/intl/en-de/blog/news/a-note-to-our-customers-on-international-data-transfers Slack's Security Whitepaper
Telia Latvia	Cloud services and data storage provider	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	All application data except payment details. Unstructured information contains PII.	Latvia, Denmark (EU)	Agreement	Data encrypted at rest and in transit. https://www.telia.lv/en/privacy-notice/
Webflow	Website content management service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Name, email address, job title, company, country.	USA	SCCs	Encryption of data in transit and at rest. https://webflow.com/security
Zoom	Video call service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Name, email address.	EEA, USA	SCCs	Data encrypted at rest and in transit. https://explore.zoom.us/en/gdpr/
Zapier	Workflow automation service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f)	Name, email address, job title, company, country.	USA	SCCs	https://zapier.com/help/account/data-management/data-privacy-security-faqs https://zapier.com/help/account/data-management/data-privacy-at-zapier

ASGL	Financial accounting Online accounting service	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f) Processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6, 1.(c)	Customer contact persons: Name, email address, job title, company, country.	Latvia (EU)	Agreement	Closed document cabinets, video surveillance, electronic keys. Safe processing of electronic information: use subprocessor Paytraq.
A/S Māris Gailis	Document storage, Contract management	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 6, 1.(f) Processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6, 1.(c)	Unstructured information contains PII.	Latvia (EU)	Agreement	Closed document cabinets, video surveillance. Access to the office premises with an electronic key.

- b. Veset will enter into a written agreement with each Subprocessor containing data protection obligations no less protective than those of the Veset set out in this DPA or as may otherwise be required by applicable Data Protection Laws and Regulations and shall ensure each such Sub-Processor complies with all such obligations. Veset shall remain liable for any breach by a Subprocessor of its obligations under this DPA.
- c. Veset will give the Customer prior notice of any changes to the Subprocessor List before authorising any new or replacement Subprocessor to Process Personal Data. If Customer objects to the appointment of a new or replacement Subprocessor, then Customer must notify Veset in writing, within 10 days following receipt of the notice of proposed change to the Subprocessor List. Upon receipt of Customer's written notice, Customer and Veset will work together without unreasonable delay on an alternative

arrangement. If a mutually-agreed alternative arrangement is not found, and Customer has a termination right under applicable Data Protection Laws and Regulations, then those Veset Services that cannot be provided without the use of the new Subprocessor may be terminated by Customer without penalty.

2.5. Notices and Consents

- a. General: Customer shall comply with its obligations as a Controller under Data Protection Laws and Regulations, including: (a) providing all required notices and appropriate disclosures to all Data Subjects regarding Customer's, and Veset's, Processing and transfer of Personal Data; and (b) obtaining all necessary rights and valid consents from Data Subjects (including Data Subjects within Customer's Content) to permit Processing by Veset, its Affiliates and Subprocessors for the purposes of fulfilling Veset's obligations, or as otherwise permitted, under the Agreement; and (c) obtaining any and all necessary permissions and authorisations necessary to perform the Controller's obligations under Data Protection Laws and Regulations.
- b. All Affiliates of the Customer who use the Veset Services shall comply with the obligations of the Customer set out in this DPA.
- c. Children; Special Category Data: Customer is responsible for compliance with all applicable Data Protection Laws and Regulations regarding its Content, including without limitation those that regulate content directed toward children (as defined under applicable Data Protection Laws and Regulations; for example, under 13 years old in the United States or under 13, 15 or 16 years old in certain other countries). Customer's use of Veset Services in connection with the distribution of Content and/or Processing of special category data of a Data Subject (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or an individual's genetic data, biometric data, health data, or data regarding sex life or sexual orientation) must be in compliance with all applicable Data Protection Laws and Regulations, including obtaining any explicit consent from Data Subjects whose special category data is provided to Veset for Processing.
- d. Veset shall promptly inform the Customer, if in Veset's opinion, any of the instructions regarding the Processing of Personal Data provided by the Customer, breach any Data Protection Laws and Regulations.
- e. Our appointed Data Protection Officer can be contacted at complaintsgdpr@veset.tv.

3. Cooperation and Data Subjects' Rights

- a. Veset will provide reasonable and timely assistance, at Customer's request, to the extent the request is lawful, to enable Customer to respond to: (a) a request from a Data Subject to exercise any rights under applicable Data Protection Laws and Regulations (including but not limited to rights of access, correction, objection, erasure and data portability, as applicable); and (b) any

other correspondence, inquiry or complaint received from a Data Subject,

unless prohibited by law. If a Data Subject contacts Vezet directly to request access to, or correction or deletion of, Personal Data in connection with services provided to Customer by Vezet, Vezet will promptly notify Customer of the request, to enable the Customer to deal with the request. The Customer shall reimburse Vezet for all costs incurred resulting from providing reasonable assistance in dealing with any requests. In the event that Vezet is legally required to respond to any request, the Customer will fully cooperate with Vezet as applicable.

- b. Vezet will notify the Customer promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Customer, unless such notification is not permitted under applicable law or a relevant court order.
- c. The Customer and Vezet, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority or regulatory authority in the performance of their respective obligations under this DPA and Data Protection Laws and Regulations.
- d. No Sale of CCPA Personal Information. Vezet shall not sell any CCPA Personal Information to another business or third party without the prior written consent of the Customer.

4. Investigations and Audits

- 4.1. Regulatory Audit. Vezet shall reasonably assist and support Customer in the event of an investigation by a data protection regulator or similar authority, if and to the extent that such investigation relates to Vezet's Processing of Personal Data.
- 4.2. Customer Audit. Vezet shall make available to the Customer all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections. Upon at least 30 days' advance written request by Customer, at mutually agreed times and subject to Vezet's reasonable audit guidelines, Vezet shall provide to Customer, its authorised representatives and/or independent inspection body designated by Customer:
 - a. reasonable access to records of Vezet's Processing of Personal Data; and
 - b. reasonable assistance and cooperation of Vezet's relevant staff for the purpose of auditing Vezet's compliance with its obligations under this DPA. Vezet reserves the right to restrict access to its proprietary information, including but not limited to its network architecture, internal and external test procedures, test results and remediation plans. Customer will use best efforts to minimise disruption to Vezet Services and Vezet's business operations.

Customer further agrees that:

- c. personnel (or designated third parties) performing said audits will be bound by the confidentiality obligations set forth in the Agreement;
- d. all findings will be deemed Vezet's Confidential Information;
- e. Customer will share all findings with Vezet; and

- f. Veset will classify and remediate all findings in accordance with Veset's risk management program.

Customer is limited to one audit in any 12-month period, except (i) if and as required by a competent data protection authority; or (ii) Customer believes a further audit is necessary as a result of a Personal Data Breach relating to Veset Services.

- 4.3. Data Protection Impact Assessment. Veset shall, upon Customer's written request and taking into account the nature of the Processing and the information available to Veset, provide Customer with reasonable cooperation and assistance to fulfill Customer's obligations under applicable Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of Veset Services and, if necessary, consult with Customer's relevant Supervisory Authority.
 - 4.4. Customer acknowledges and agrees that some instructions from the Customer, including destruction or return of data, Veset assisting with audits, inspections, DPIAs or providing any assistance under this DPA, may result in additional fees. Veset shall be entitled to charge the Customer for its costs and expenses in providing any such assistance, upon agreeing these in advance with the Customer.
 - 4.5. Veset may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.
5. Notice of Non-Compliance
- 5.1. If required by applicable Data Protection Laws and Regulations, in the event that Veset is unable to comply with its obligations in this DPA, Veset shall promptly notify Customer, and if Veset is unable to take reasonable and appropriate steps to remediate the non-compliance within a mutually-agreed upon timeframe, Customer may take any one or more of the following actions: (a) suspend the transfer of Personal Data to Veset; (b) require Veset to cease Processing Personal Data to the extent technically possible; (c) demand the return or destruction of Personal Data; and/or (d) terminate this DPA in accordance with the Agreement.
6. Data Security
- 6.1. Veset will ensure that all personnel with access to Personal Data are subject to written obligations of confidentiality and that Personal Data is Processed only for the Permitted Purpose.
 - 6.2. Veset and the Customer shall take steps to ensure that any natural person acting under the authority of the Customer or Veset who has access to Personal Data does not Process them except on the instructions from the Customer unless he or she is required to do so by any Data Protection Laws or Regulations.
 - 6.3. Veset confirms it shall process Personal Data on behalf of the Customer and shall ensure that all employees, agents, officers and contractors involved in the handling of

Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

- 6.4. Security Measures. The Customer and Veset shall implement appropriate technical and organisational procedures to protect Personal Data, 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 risks of varying likelihood and severity for the rights and freedoms of natural persons. At a minimum, such measures shall include those identified in the Security Policy. The Customer and Veset shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The measures taken by Veset shall include inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
- 6.5. Taking into account the nature of the processing and the information available to Veset, Veset shall assist the Customer by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights and the Customer's compliance with the Customer's data protection obligations in respect of the processing of Personal Data.
- 6.6. Breach Notification. If Veset becomes aware of a Personal Data Breach involving Personal Data of the Customer, Veset shall: (a) promptly, and without undue delay following Veset's discovery thereof, notify Customer of such Personal Data Breach; (b) investigate, remediate and mitigate the effects of the Personal Data Breach; (c) reasonably cooperate with Customer's investigation of the Personal Data Breach to the extent that such cooperation does not compromise Veset's security; (d) take any additional actions and provide any additional cooperation to Customer as may reasonably be required to assist the Customer in meeting the Customer's obligations under applicable Data Protection Laws and Regulations; and (e) upon resolution, provide Customer with a written incident report describing the breach, actions taken during the response and plans for future actions to prevent a similar breach from occurring in the future.

7. Deletion or Return of Personal Data

7.1. Upon termination or expiration of the Agreement or at any time at Customer's written request, Veset shall at the choice of the Customer: return to Customer or destroy all Personal Data. All Personal Data shall be deleted in any event within 2 days of termination or expiry of the Agreement, except where Veset is required or permitted to retain Personal Data under applicable Data Protection Laws and Regulations or where partial Customer data is stored in backups for up to 60 days after termination or expiry of the Agreement.

8. Liability

8.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

8.2 The parties agree that Veset shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent Veset would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

8.3 The parties agree that the Customer shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Customer itself.

8.4 The Customer shall not be entitled to recover more than once in respect of the same loss.

9. Miscellaneous

9.1. This DPA is effective as of the effective date of the Agreement and will terminate automatically when the Agreement terminates or expires, without further action required by either party. Provisions of this DPA that by their nature and on their face should survive, will survive any such termination or expiration.

9.2. This DPA shall be governed by and construed in accordance with the governing law set forth in the Agreement, except where otherwise required by applicable Data Protection Laws and Regulations.

Schedule A

Data Processing Description

This Schedule A forms part of this DPA and describes the Processing of Personal Data that Vezet will perform on behalf of Customer.

1. Controller

Controller (Customer) uploads Content to Vezet Services, directs distribution of Content via the UI, elects to collect Viewer data, which may include Personal Data if using certain Vezet Services.

2. Processor

Processor (Vezet) is a provider of cloud solutions for transcoding, hosting and delivering video to internet-connected devices. Vezet Services includes analytics and other usage data relating to Customer's use of Vezet Services.

3. Data subjects

The Personal Data to be Processed concerns the following categories of Data Subjects:

- Business information (such as email addresses) of Customer's employees who use Vezet Services ("Users").
- End users who view Customer's Content ("Viewers") via Vezet Services.
- Natural persons whose images (or other Personal Data) are included in Customer's video Content.

4. Categories of data

The Personal Data to be Processed include the following categories of data (some or all of which may not be considered Personal Data under applicable Data Protection Laws and Regulations):

- Viewers: userID, IP addresses, location data, names, email, address, title, industry, login credentials, device ID.
- Users: Names, phone numbers, email and login credentials.
- Images of natural persons included in video Content.

5. Special categories of data (if appropriate)

The Personal Data to be Processed concern the following special categories of data:

- None.

6. Processing operations

The Personal Data will be subject to the following basic Processing activities:

- Video Content will be transcoded, hosted, transferred and distributed by Veset Services in accordance with Customer's selections via the U/I or the Veset Service's APIs.
- Name, email, address, title, industry and/or other Personal Data of Viewers may be collected at Customer's request if Customer is using certain Veset Services.
- IP addresses and geolocation data is collected to operate Veset Services and provide.
- User login credentials and contact information will be used to authenticate User access and to provide Veset Services and support to Customer.

Schedule B

Security Policy

Veset shall use commercially reasonable efforts to implement appropriate network security and encryption technologies, including but not limited to the following technologies or any technologies that provide comparable or enhanced protections:

1. IT Network Security. Veset maintains appropriate IT network segmentation, including but not limited to, firewalls and Virtual Private Cloud, to segregate its internal networks from the internet, and maintains intrusion detection, monitoring, and logging systems to detect and respond to attacks.
2. Application Security. To the extent that Veset develops applications or application code on behalf of Customer, Veset conducts security testing to ensure that the application or application code is secure against the vulnerabilities described in (i) the version of the OWASP Top Ten List available as of the Effective Date, and (ii) any changes to the OWASP Top Ten List after the Effective Date (within a reasonable time after such changes are initially published). The term “OWASP Top Ten List” shall mean the Open Web Application SecurityProject's Top Ten list (available at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).
3. Vulnerability and Patch Management. Following receipt of any update release from the manufacturer, Veset will apply manufacturer-recommended security updates to all systems, devices, or applications Processing Personal Data within a reasonable period of time, taking into account the nature and severity of the risk. Veset will install, within a reasonable period of time following Veset’s receipt from the manufacturer, any software patches designated by manufacturers, vendors, or Veset as “critical”. Veset conducts regular vulnerability scans and penetration tests of any network storing or processing Personal Data and remediates any identified critical vulnerability in accordance with Veset’s defined remediation schedule
4. Access Controls.
 - a. Access Management. Only those Veset personnel that reasonably need access to Personal Data to perform the services described in the Agreement or to deliver Veset Services are granted such access. If Veset personnel no longer need access to Personal Data, whether because of termination or re- assignment, then access privileges are promptly disabled.

- b. Usernames and Passwords. Accounts used to access systems, software, equipment, or networks must comply with Veset’s complex password requirements (“Password Policy”) and such Password Policy is automatically enforced by Veset’s operating system.
 - c. Multi-Factor Authentication. Veset shall have in place multi-factor authentication for its employees to access Personal Data. For the purposes of this requirement, the implementation and use of appropriate and commercially- reasonable identity verification systems and physical access controls that limit access to systems containing Personal Data may be considered a “factor”.
 - d. Training. Veset personnel that may have access to Personal Data are required to undergo regular training on commercial best practices for data security.
- 5. Data Transmission. Personal Data is encrypted when transmitted over networks other than those administered by Customer or Veset. External data transmissions are protected using TLS, current-generation cipher suites and SSL certificates as follows:
 - a. Client communications are secured with server-priority based TLS. Backend communications are secured with either TLS for service-to-service communications, AES-based encryption for backend file transfer over SSH or AES/HMAC-based VPN tunnels for inter-datacenter communication; and
 - b. All SSL certificates are created and updated with RSA 2048-bit key length and SHA-256.
- 6. Auditing and Testing.
 - a. Veset maintains information system audit records to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorised or inappropriate information system activity.
 - b. Veset’s security policies, standards and procedures are designed to monitor and protect the Veset Service. Such policies, standards and procedures are reviewed at least annually and updated as necessary.
 - c. A third party conducts network, system and application vulnerability scanning, and penetration testing, on at least an annual basis, to evaluate the implementation of Veset’s information security measures. Veset conducts regularly-scheduled internal vulnerability scans against its business and production operations networks.

0.