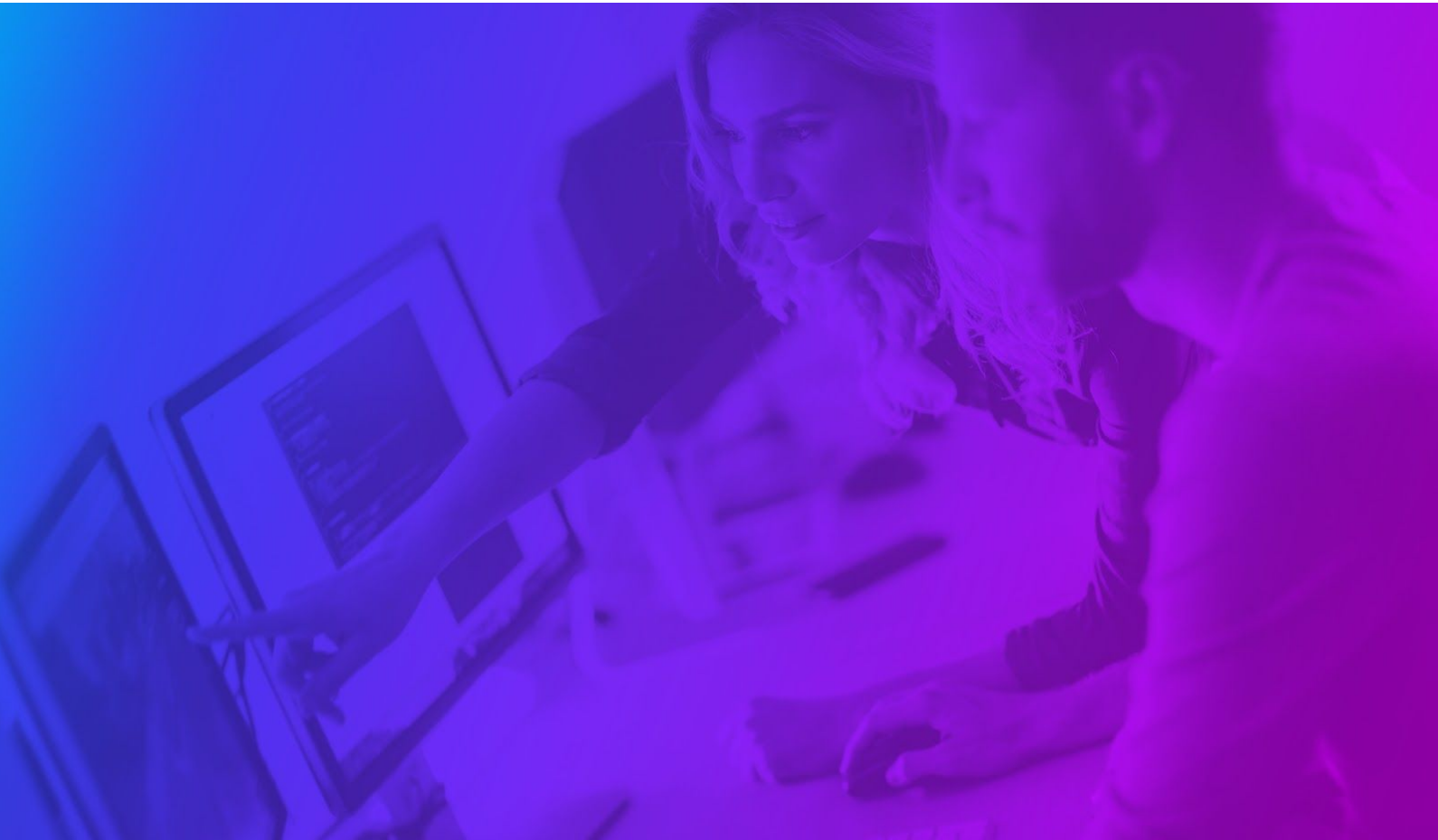




TERMS OF SERVICE

GDPR Addendum



ADDRESS

Level 21, 60 Margaret St.
Sydney NSW 2000

CONTACT

info@jepto.com
www.jepto.com

Table of Contents

Table of Contents	1
Customer GDPR Addendum	2
1. Definitions	2
2. Article 28 Requirements	3
3. Subprocessors	4
4. Personal Data Breaches	5
5. Conflicting Terms	5
6. Survival	5
Exhibit A: Description of Processing of Customer Personal Data	6
Exhibit B: List of Approved Subprocessors	7

Customer GDPR Addendum

This General Data Protection Regulation (“GDPR”) Addendum (“Addendum”) amends those the Terms of Use (<https://www.jepto.com/terms>) (the “Agreement”) accepted by you as the user pursuant to Customer’s use of the services provided by Jepto Pty Ltd, located at 21/Margaret St, Sydney NSW 2000 Australia (“Jepto”). Customer and Jepto are each a “Party” and collectively are the “Parties”.

This Addendum sets forth the GDPR requirements applicable to Personal Data Processed by Jepto or through Jepto’s (or a Subprocessor’s) systems in connection with providing the services set forth in the Agreement (collectively, the “Services”). Exhibit A hereto sets out the Parties’ understanding of the Customer Personal Data to be Processed by Jepto pursuant to this Addendum, as required by Article 28(3) of the GDPR. Customer will inform Jepto of any changes to Exhibit A required in order to reflect Customer’s actual use of the Services. Exhibit A does not create any obligation or rights for any Party. The Parties acknowledge that for purposes of this Addendum, Customer is a Controller and Jepto is a Processor.

With effect from 25 May 2018, the date on which the GDPR will apply (the “Effective Date”), the Parties agree as follows:

1. Definitions

Capitalised terms used in this Addendum have the meaning set forth in Article 4 of the GDPR, unless defined in this

Addendum or in the Agreement:

- a) “Customer Personal Data” means Personal Data that is provided by Customer to Jepto pursuant to the latter’s provision of the Services.
- b) “Member State” means any relevant member state of the European Union (“EU”) or European Economic Area (“EEA”) from time to time.
- c) “Personal Data Breach” has the meaning set forth in Article 4 of the GDPR, and shall apply to Customer Personal Data.

d) “Subprocessor” means any third party (other than Jepto’s employees), including any affiliate of Jepto that Jepto engages in accordance with the Agreement, that Processes Customer Personal Data on behalf of Jepto in order to provide the Services.

e) “Transfer”, “Transferred” or “Transferring” means, whether by physical or electronic means, across national borders, both (i) the moving of Customer Personal Data from one location or person to another, and (ii) the granting of access to Customer Personal Data by one location or person to another.

2. Article 28 Requirements

In accordance with GDPR Article 28(3), Jepto will (and ensure that any Subprocessor acting under Jepto’s authority also will):

a) Process the Customer Personal Data solely (i) as needed to provide the Services; (ii) in accordance with the specific documented instructions provided by Customer, including with regard to any Transfers, as set forth in the Agreement and this Addendum; or (iii) as required to comply with any EEA or Member State law (in which case, Jepto shall provide prior notice to Customer of such legal requirement, unless that law prohibits this disclosure on important grounds of public interest); provided, however, that Jepto will not have any obligation to monitor EEA or Member State requirements.

b) Ensure that persons authorized to Process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c) Take all security measures required by GDPR Article 32. Namely, taking into account 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, Jepto shall implement all reasonable measures, which include appropriate technical and organisational security measures to ensure a level of security appropriate to the risk, including, as appropriate: (i) the pseudonymisation and encryption of Customer Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

d) Assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising Data Subjects' rights as set forth in GDPR Chapter III, taking into account the nature of the Processing.

e) Assist the Customer with the obligations regarding Customer Personal Data Breaches (GDPR Articles 33 and 34 and section 5 below), data protection impact assessments (GDPR Article 35), and prior consultation of the supervisory authority (GDPR Article 36), in all cases, taking into account the nature of Processing and the information available to Jepto.

f) At the Customer's discretion, delete all the Customer Personal Data to the Customer after the end of the provision of Services relating to Processing, and delete existing copies (it being expressly understood that Customer has the ability to and may at its discretion export (return) all Customer Personal Data to Customer), unless applicable EEA or Member State law requires Jepto to store the Customer Personal Data.

g) Provide the Customer with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.

h) Immediately inform Customer if, in Jepto's opinion, an instruction infringes the GDPR or other EEA or Member State data protection provisions; provided, however, that Jepto will not have any obligation to monitor EEA or Member State data protection provisions.

3. Subprocessors

a) Jepto shall not share any Customer Personal Data with or engage any Subprocessor without prior specific or general written authorisation of the Customer; provided, however, that Customer hereby specifically authorises Jepto to Transfer Customer Personal Data to Subprocessors listed in Exhibit B hereto for purpose of providing the Services, subject to the following conditions: (i) Jepto maintains a list of the Subprocessors to which it makes such Transfers and provides this list to the Customer upon written request; (ii) Jepto provides to the Customer at least 30 days prior notice of the addition of any Subprocessor to this list so that the Customer may have an opportunity to object to such addition(s); and (iii) if the Customer makes such an objection on reasonable grounds and Jepto is unable to modify the Services to prevent the Transfer to the additional Subprocessor, the Customer shall have the right to terminate the relevant Processing. In addition, Jepto will impose on any Subprocessor the data protection

obligations as set out in this Addendum. Where a Subprocessor fails to fulfil its data protection obligations, Jepto shall remain fully liable to the Customer for the performance of the Subprocessor's obligations.

4. Personal Data Breaches

a) Jepto shall promptly and thoroughly investigate all allegations of unauthorised access to, use or disclosure of Customer Personal Data. In accordance with GDPR Article 33, paras. (1) and (2), Jepto will notify Customer without undue delay in the event of any Personal Data Breach.

5. Conflicting Terms

This Addendum supplements, and does not replace, any existing obligations related to the privacy and security of Customer Personal Data as already set forth in the Agreement. In the event of a conflict between the terms of this Addendum and the Agreement, Jepto shall comply with the obligations that provide the most protection for Customer Personal Data, in particular, in terms of security.

6. Survival

Notwithstanding anything to the contrary in the Agreement, the obligations pursuant to this Addendum shall survive termination of the Agreement for as long as Jepto holds or Processes Customer Personal Data on behalf of the Customer.

Exhibit A: Description of Processing of Customer Personal Data

Subject matter and duration of the Processing of the Personal Data

Jepto's Processing of the Customer Personal Data is done in connection with the Customer's use of the Services. Customer allows Jepto to retain Personal Data related to the Services beyond the termination of Services, but Jepto agrees to delete any retained Personal Data at the request of the Customer (it being expressly understood that Customer has the ability to, and may at its discretion, export (return) all Customer Personal Data to Customer at any time).

The nature and purpose of the Processing of the Personal Data

Jepto's Processing of the Customer Personal Data is done for the express purpose and to the extent necessary to provide the Services.

The categories of Data Subject to whom the Personal Data relates

Customers, employees and agents of Customers, and/or end users of Customers' services.

The types of Personal Data to be Processed

May include IP addresses, names, email addresses, or other personal contact information uploaded to our Service by the Customer, or its employees and agents, or via the Customer's Sites and their use of our Services.

The obligations and rights of Customer

The obligations and rights of Customer and Jepto are set out in the Agreement and in this Addendum.

Exhibit B: List of Approved Subprocessors

Entity Name	Location
Amazon Web Services	United States
Epsagon	United States
Sendgrid	United States
Intercom	United States
FullStory	United States
Chargebee	United States