ESPRESSIVE DATA PROCESSING AGREEMENT FOR CUSTOMERS

This Data Processing Agreement (DPA) is entered into by Espressive, acting on its own behalf and as an agent for each Espressive Affiliate and _____, referred to as Customer, acting on its own behalf, as of the effective date of the Master Service Agreement (MSA), if applicable, or this agreement, whichever is executed earlier.

This data processing agreement (**DPA**) describes the parties' obligations, including under applicable privacy, data security, and data protection laws, with respect to the processing and security of Customer Personal Data (as defined below).

1. DEFINITIONS AND INTERPRETATION

1.1 The terms defined below shall have the meaning given to them, but only for the purposes of this DPA.

Agreement means the written or electronic contract under which the Provider has agreed to provide the Services to the Customer.

Audits has the meaning given in clause 6.3.

Customer means the party identified in the Agreement receiving Services from the Provider under the Agreement.

Customer Personal Data means personal data provided to the Provider by, or on behalf of, the Customer in connection with the Services, including personal data which is (i) entered by the Customers or its users into or derived from their use of the Services and (ii) supplied to or accessed by the Provider in order to provide the Services.

EEA means the European Economic Area.

Data Protection Legislation means, as applicable to the processing of Customer Personal Data, any data protection and data privacy laws, rules, and regulations, including the GDPR.

GDPR means the General Data Protection Regulation ((EU) 2016/679).

Provider means Espressive Inc, registered at 5201 Great America Parkway Suite 110, Santa Clara, CA 95054, United States.

SCCs has the meaning given in clause 7.2.

Security Incident has the meaning given in clause 5.1.

Security Measures has the meaning given in clause 4.1.

Services means the services to be provided by the Provider under the Agreement.

1.2 The terms 'business', 'service provider', 'sale', 'personal data', 'data subject', 'processing', 'controller', and 'processor' have the meanings defined in the Data Protection Legislation.

1.3 This DPA, its annexes, and the documents, including the SCCs, referred to herein form part of the Agreement and will have effect as if set out in full in the body of the Agreement.

1.4 A reference to writing or written includes email.

1.5 In the case of conflict or ambiguity between:

1.5.1 any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA will prevail; and

1.5.2 any of the provisions of this DPA and any of the SCC, the provisions of the SCC will prevail.

2. GENERAL PROVISIONS

2.1 Roles of the parties. The Customer and the Provider agree and acknowledge that for the purposes of the Data Protection Legislation, the Customer is the controller or business, and it appoints the Provider as a processor (service provider) of Customer Personal Data.

2.2 Compliance with law. The Customer acts as a single point of contact and shall obtain any relevant authorisations, consents, and permissions for the processing of Customer Personal Data in accordance with this DPA. The Customer remains responsible for its compliance obligations under the applicable Data Protection Legislation, including but not limited to providing any required notices and for the written processing instructions it gives to the Provider. Where authorisations, consent, permissions, or instructions are provided by the Customer, these are provided not only on behalf of the Customer but also on behalf of any other controller using the Services through the Customer.

2.3 Purpose limitation. The Provider will only process Customer Personal Data as permitted under the Agreement and the Data Protection Legislation. The Provider will not sell (as the term is defined under Data Protection Legislation) any Customer Personal Data to any third party.

2.4 Instructions. The Provider will, and will ensure that its personnel, process Customer Personal Data only in accordance with the Customer's written instructions unless required to do so by applicable law to which the Provider is subject. The Agreement, including this DPA, constitutes the initial Customer's instructions, and each use of the Services constitutes further Customer's instructions to the Provider in relation to the processing of Customer Personal Data. The Provider is not responsible for determining whether Customer's instructions are compliant with applicable law. However, the Provider will notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation unless applicable law prohibits such notification on important grounds of public interest.

2.5 Processing details. Annex A describes the subject matter, duration, nature, and purpose of the processing and the personal data categories and data subject types in respect of which the Provider may process Customer Personal Data.

3. SUBPROCESSORS

3.1 Consent to subprocessor engagement. The Customer hereby authorises the Provider to use subprocessors located in any jurisdiction to process Customer Personal Data provided the Provider contractually requires subprocessors to abide by terms not less restrictive than this DPA. The Provider will be liable to the Customer if its subprocessors fail to fulfil their data protection obligations in connection with the processing of Customer Personal Data.

3.2 Information about subprocessors. The Provider will provide the Customer with a list of subprocessors that it engages to support the provision of the Services upon Customer's request. The details of the current Provider's subprocessors are also described at https://www.espressive.com/legal/subprocessor.

3.3 Opportunity to object to subprocessors. The Provider will notify the Customer of any intended engagement of a new subprocessor at least thirty (30) days before the new subprocessor starts processing any Customer Personal Data. The Customer may, within thirty (30) days after being notified of the intended engagement, object to such engagement by immediately terminating the Agreement for convenience (i) in accordance with that Agreement's termination for convenience provision or (ii) if there is no such provision, by notifying the Provider.

4. SECURITY AND CONFIDENTIALITY

4.1 Provider's security measures. The Provider will use appropriate technical and organisational measures to protect Customer Personal Data as required by the Data Protection Legislation and will follow industry-standard security practices, including the security measures set out in Annex B (**Security Measures**). The Provider may update or modify the Security Measures provided that such updates and modifications do not result in a material degradation of the overall security of its processing of Customer Personal Data.

4.2 The Customer acknowledges and agrees that the level of security provided by the Security Measures is appropriate to the risk inherent in the processing of Customer Personal Data by the Provider.

4.3 Confidentiality. The Provider shall not process more than the minimum amount of Customer Personal Data necessary to perform the Services for the Customer under the Agreement. The Provider will ensure that only persons, including Provider's personnel, who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality may process Customer Personal Data for the purposes of performing the Services under the Agreement.

5. SECURITY INCIDENTS

5.1 The Provider will notify the Customer without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised access, disclosure or use of Customer Personal Data while processed by the Provider (each, **Security Incident**) to assist the Customer with its reporting or notice obligations under the Data Protection Legislation.

5.2 The Provider will investigate the Security Incident and provide the Customer with relevant information about the Security Incident as required under the Data Protection Legislation. The Provider will use reasonable efforts to assist the Customer in mitigating, where possible, the adverse effects of any Security Incident. Provider's notification of a Security Incident will not be deemed an acknowledgement of its fault or liability.

6. COOPERATION AND AUDITS

6.1 Upon Customer's written request, the Provider shall assist the Customer, as required by the Data Protection Legislation from the Provider, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to the Security Measures it has implemented to protect Customer Personal Data, data subject rights, data protection impact assessments and reporting to and consulting with the relevant regulator under the Data Protection Legislation. The Provider is not obliged to respond directly to data subject requests unless so required by the Data Protection Legislation.

6.2 Upon Customer's written request and subject to obligations of confidentiality, the Provider will make available to the Customer all information necessary to demonstrate Provider's compliance with this DPA.

6.3 The Customer (or an independent auditor mandated by the Customer) may audit the Provider's compliance with this DPA at the applicable facility or if there are indications of non-compliance with the terms of this DPA (**Audits**). Audits will only be performed following the Customer's written request at least sixty (60) days prior to the proposed start date and the Customer providing a reasonably detailed audit plan describing the proposed scope, start date and duration. Before the commencement of an Audit, the parties will agree on a final Audit plan. Audits will be conducted during the Provider's regular business hours, subject to the published policies of the audited facility, and may not unreasonably interfere with business activities. The personnel conducting the Audit on behalf of the Customer or an independent auditor mandated by the Customer must enter into an appropriate written confidentiality agreement acceptable to the Provider prior to conducting the Audit and will be accompanied by Provider's representatives. The Provider reserves the right to not share information that could expose or compromise its security, privacy, employment policies or obligations to other customers or third parties or share confidential information. Records may not be copied or removed from Provider's facilities. The Customer will generate and provide the Provider with an audit report as soon as possible and in any case not later than within sixty (60) days after the Audit. All information obtained or generated in connection with an Audit, including audit reports, must be kept strictly confidential. The Customer will pay or reimburse Provider's reasonable costs for allowing for and contributing to Audits.

7. INTERNATIONAL DATA TRANSFERS

7.1 The Customer hereby authorises the Provider and its subprocessors to transfer Customer Personal Data to locations outside of its country of origin for the performance of the Agreement provided that the Provider ensures such data transfers comply with the Data Protection Legislation.

7.2 In the case of a transfer of Customer Personal Data from the EEA, the UK, or Switzerland to locations outside that jurisdiction, the Customer will be bound by the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 including the provisions in Modules 2 and 3, as applicable, and the UK's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses made under s119 A(i) of the UK's Data Protection Act 2018 (collectively, **SCCs**) in the capacity of 'data exporter', and the Provider in the capacity of 'data importer' as those terms are defined therein. The parties acknowledge that (i) the information required to be provided in the SCCs is set out in Annex A below, and (ii) the description of the technical organizational measures is set out in Annex B below.

8. TERMINATION

8.1 Upon termination of the Agreement, at Customer's option, the Provider will return, delete, or anonymise all Customer Personal Data except to the extent the Provider is required by applicable law to retain Customer Personal Data or for compliance, audit, or security purposes in which case the terms of this DPA will continue to apply to the retained Customer Personal Data.

8.2 This DPA, including the SCCs, will terminate automatically upon deletion or anonymization of the Customer Personal Data covered by it, with respect to such Customer Personal Data.

9. NOTICES

The Customer shall promptly inform the Provider of the email address to which notices under this DPA must be sent, by emailing SecurityCompliance@Espressive.com. The Customer is responsible for informing the Provider of any changes to that email address.

ANNEX A. PROCESSING DETAILS

A. LIST OF THE PARTIES	
Controller / Data exporter	Customer (as detailed in the Agreement)
Processor / Data importer	Provider (as detailed in the Agreement)
B. DETAILS OF PROCESSING/TRANSFER	
Categories of data subjects	Customer Personal Data is determined and controlled by the Customer in Customer's sole discretion and may include, without limitation, personal data of the following categories of data subjects: employees, contractors, temporary workers, agents, advisors, or consultants (current, former, prospective) of the Customer, Customer's users of the Services, any other data subjects as may be described in the Agreement.
Categories of personal data	Customer Personal Data is determined and controlled by the Customer in Customer's sole discretion and may include, without limitation, the following categories of Customer Personal Data: User personal data (such as first name, last name, email address, job title, office location, employee ID, employee status, hire date, home address, mobile phone number, work phone number, date of birth); IT systems and operational information (such as unique identifiers, IP addresses, domains, apps installed, browsing and support logs, mobile device ID, geo-location network data, location data derived from use of wi-fi access points, UUID, IMEI-number, SIM card number, MAC address); Information about activities linked to the use of the Services; Any information that Customer's users enter into the Services.
Special categories of data	N/A
Frequency	Dependent on the Customer's use of the Services, the Provider may host, remotely access, or otherwise process Customer Personal Data on a one-off basis or on a continuous basis when providing the Services as described in the Agreement.
Nature and purpose of the processing	The Provider and its subprocessors are providing Services or fulfilling contractual obligations to the Customer as described in the Agreement. The Services may include the processing of Customer Personal Data by the Provider and/or its subprocessors. Customer Personal Data is subject to the following basic processing activities: • use of Customer Personal Data to set up, operate, monitor, and provide the Services (including operational and technical support); • continuous improvement of service features and functionalities provided as part of the Services including automation, transaction processing and machine learning; • communication with Customer and its users; • storage of Customer Personal Data in dedicated data centres; • release, development and upload of any fixes or upgrades to the Services;

	• computer processing of Customer Personal Data, including data transmission, data retrieval, data access; • network access to allow Customer Personal Data transfer; • monitoring, troubleshooting, and administering the underlying infrastructure and database; • security monitoring, network-based intrusion detection support, penetration testing; and • execution of instructions of the Customer in accordance with the Agreement.
Retention	Customer Personal Data will be retained in accordance with the Agreement unless applicable law requires storage of Customer Personal Data for a longer period.
Transfer to subprocessors	The Provider may process and transfer Customer Personal Data to subprocessors in relation to the performance of the Agreement and in accordance with the following scope: **Subject Matter**: the subject matter of the processing under the Agreement is Customer Personal Data as specified above; **Nature of the processing**: the Provider and its subprocessors are providing Services or fulfilling contractual obligations to the Customer as described in the Agreement. These Services may include the processing of Customer Personal Data by the Provider and/or its subprocessors.; **Duration**: the duration of the processing under the Agreement is determined by the Customer and as set forth in the Agreement.
C. COMPETENT SUPERVISORY AUTHORITY	
For the purposes of Clause 13 of the SCCs, the competent supervisory authority for the Customer shall be the supervisory authority applicable to the Customer in its EEA country of establishment or, where it is not established in the EEA, in the EEA country where its representative has been appointed pursuant to Article 27(1) of Regulation (EU) 2016/679. For purposes of the UK's International Data Transfer Addendum, any reference to a supervisory authority shall refer to the UK Information Commissioner. For the purposes of transfers from Switzerland, any reference to a supervisory authority shall refer to the Swiss Federal Data Protection and Information Commissioner.	
D. GOVERNING LAW AND CHOICE OF FORUM	
Governing law	For Clause 17, Option 1 will apply and the SCCs will be governed by: • for transfers from the EEA, by the laws of Ireland; • for transfers from the UK, by the laws of England and Wales; • for transfers from Switzerland, by the laws of Switzerland.
Choice of forum	For the purposes of Clause 18 of the SCCs, the parties agree that: • for transfers from the EEA, the courts of Ireland will have jurisdiction; • for transfers from the UK, the courts of England and Wales will have jurisdiction; • for transfers from Switzerland, the courts of Switzerland will have jurisdiction.
E. OTHER	

Where the SCCs identify optional provisions or provisions with multiple options the following will apply:	For Clause 7 (Docking Clause), the parties agree to include SCCs' Clause 7.
	For Clause 9(a), option 2 will apply. The parties will follow the process agreed in clause 63 (Subprocessors).
	For Clause 11(a) (Redress), the optional provision will not apply.

ANNEX B. SECURITY MEASURES

Espressive has the following certifications:

[X] Type 2 SOC 2

[X] ISO 20243:2018

[X] CSA STAR: LEVEL 1

Additionally, Espressive has implemented and shall maintain its written comprehensive data protection program that includes the following safeguards:

• Appropriate user authentication controls, including secure methods of assigning, selecting, and storing access credentials and restricting access to active users.

• Secure access controls, including controls that limit access to Personal Data to individuals who have a demonstrable genuine business need-to-know, supported by appropriate policies, protocols, and controls to facilitate access authorization, establishment, modification, and termination.

• Appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security.

• Appropriate and timely adjustments to data protection program based on: periodic risk assessments; regular comprehensive evaluations (such as third-party assessments) of the data protection program; monitoring and regular testing of the effectiveness of safeguards, including vulnerability assessment and penetration testing; and a review of safeguards at least annually and whenever there is a material change in the technical environment or business practices that may implicate the confidentiality, availability, integrity, or security of the data importer's information systems.

• Appropriate ongoing training and awareness programs designed to ensure workforce members and others acting on Espressive's behalf are aware of and adhere to the data protection program's policies, procedures, and protocols.

• Appropriate monitoring of information systems in a manner designed to ensure data integrity and prevent loss or unauthorized access to, or acquisition, use, or disclosure of, Personal Data.

• Appropriate technical security measures designed to prevent unauthorized intrusions and access, including firewall protection, antivirus protection, security patch management, logging of access to or use or disclosure of Personal Data, and intrusion detection.

• Appropriate use of encryption of Personal Data submitted to the Services.

• With respect to storage of Personal Data, contracting with sub-processors who have appropriate facility security measures, including access controls, designed to prevent unauthorized access to premises, information systems, and data.

• Safeguards ensuring disposal of Personal Data renders that data permanently unreadable and unrecoverable.

• Appropriate data loss prevention policies and technologies, including, but not limited to the monitoring of end points to ensure that there is no unauthorized use or loss of Personal Data.