Data Processing Addendum- Lumerate Brands

Version 2.0 - March 22, 2023

1. Data Protection

1.1. *Definitions:* In this Data Processing Addendum, the following terms shall have the following meanings:

(a) "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**" and "**Processing**" (and "**Process**") shall have the meanings given in EU/UK Data Protection Law;

(b) "**Data Protection Laws**" means all applicable data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, EU/UK Data Protection Law;

(c) "**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

(d) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

(e) "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 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 ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

1.2. *Relationship of the parties:* You instruct Us to process the Personal Data described in Annex I (the "**Data**") on Your behalf. In respect of such Processing, You shall be the Controller and We shall be a Processor.

1.3. *Purpose limitation:* We shall process the Data for the purposes described in Annex I and strictly in accordance with Your documented instructions (the "**Permitted Purpose**"), except where otherwise required by law(s) that are not incompatible with Data Protection Law. In no event shall We process the Data for our own purposes or those of any third party. We shall immediately inform You if We become aware that such Processing instructions infringe Data Protection Law (but without obligation to actively monitor Your compliance with Data Protection Laws).

1.4. *Restricted transfers:* The parties agree that when the transfer of Data from You to Us is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) in relation to Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 1.9 of this Data Processing Addendum;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this Agreement;

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this Agreement; and

(b) in relation to Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(i) For so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of Personal Data to Processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("**Prior C2P SCCs**") for transfers of Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between the parties on the following basis:

(A) Appendix 1 shall be completed with the relevant information set out in Annex I to this Agreement;

(B) Appendix 2 shall be completed with the relevant information set out in Annex II to this Agreement; and

(C) the optional illustrative indemnification Clause will not apply.

(ii) Where sub-clause (b)(i) above does not apply, but the parties are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:

(A) The EU SCCs, completed as set out above in clause 1.4(a) of this Data Processing Addendum shall also apply to transfers of such Data, subject to sub-clause (B) below;

(D) The UK Addendum shall be deemed executed between the parties, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Data.

(iii) If neither sub-clause (b)(i) or sub-clause (b)(ii) applies, then the parties shall cooperate in good faith to implement appropriate safeguards for transfers of such Data as required or permitted by the UK GDPR without undue delay.

(c) in the event that any provision of this Data Processing Addendum contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

1.5. *Onward transfers:* We shall not participate in (nor permit any subprocessor to participate in) any other Restricted Transfers of Data (whether as an exporter or an importer of the Data) unless the Restricted Transfer is made in full compliance with Data Protection Laws.

1.6. *Confidentiality of Processing:* We shall ensure that any person that We authorise to process the Data (including Our staff, agents and subprocessors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to Process the Data who is not under such a duty of confidentiality. We shall ensure that all Authorised Persons Process the Data only as necessary for the Permitted Purpose.

1.7. *Security:* We shall implement appropriate technical and organisational measures to protect the Data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access (a "**Security Incident**").

1.8. *Subprocessing:* We shall not subcontract any Processing of the Data to a third party subprocessor without Your prior written consent. Notwithstanding this, You consent to Us engaging third party subprocessors to process the Data provided that: (i) We provide at

least 14 days prior notice of the addition or removal of any subprocessor (including details of the Processing it performs or will perform), which may be given by posting details of such addition or removal at the following URLs: https://welcome.zymewire.com/privacy-policy, https://welcome.zapyrus.com/privacy/privacyhome; (ii) We impose data protection terms on any subprocessor We appoint that protects the Data, in substance, to the same standard provided for by this Data Processing Addendum; and (iii) We remain fully liable for any breach of this Data Processing Addendum that is caused by an act, error or omission of Our subprocessor. If You refuse to consent to Our appointment of a third party subprocessor on reasonable grounds relating to the protection of the Data, then We will either not appoint the subprocessor or You may elect to suspend or terminate the Subscription Agreement without penalty.

1.9. *Cooperation and Data Subjects' rights:* We shall provide all reasonable and timely assistance (including by appropriate technical and organisational measures) to You (at Your expense) to enable You to respond to: (i) any request from a Data Subject to exercise any of its rights under Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the Processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Us, We shall promptly inform You providing full details of the same.

1.10. *Data Protection Impact Assessment:* We shall provide You with all such reasonable and timely assistance as You may require in order to enable You to conduct a data protection impact assessment in accordance with Data Protection Laws including, if necessary, to assist You to consult with Your relevant data protection authority.

1.11. *Security incidents:* Upon becoming aware of a Security Incident, We shall inform You without undue delay and shall provide all such timely information and cooperation as You may require in order for You to fulfil Your data breach reporting obligations under (and in accordance with the timescales required by) Data Protection Laws. We shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep You informed of all developments in connection with the Security Incident.

1.12. *Deletion or return of Data:* Upon termination or expiry of this Data Protection Addendum, We shall (at Your election destroy or return to You by making it available for export or download, all Data (including all copies of the Data) in Our possession or control (including any Data subcontracted to a third party for Processing). This requirement shall not apply to the extent that We are required by any applicable law to retain some or all of the Data, in which event We shall isolate and protect the Data from any further Processing except to the extent required by such law until deletion is possible.

1.13. *Audit:* You acknowledge that We are regularly audited against SOC 2 standards by independent third-party auditors. Upon request, We shall supply a summary copy of our audit report(s) to You, which reports shall be subject to the confidentiality provisions of the Subscription Agreement. We shall also respond to any written audit questions submitted to Us by You, provided that You shall not exercise this right more than once per year.

Annex I

Data Processing Description

This Annex I forms part of the Agreement and describes the Processing that the Processor will perform on behalf of the Controller.

A. LIST OF PARTIES

Controller(s) / Data exporter(s): [*Identity and contact details of the Controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1.	**Name:**	You (as per the Subscription Agreement)
	Address:	Your registered address, as per the most recent Order Form you have executed.
	Contact person's name, position and contact details:	The Services system administrator designated by You in accordance with clause 13.2 of the Subscription Agreement
	Activities relevant to the data transferred under these Clauses:	We provide Services to You in accordance with the Subscription Agreement
	Signature and date:	As per the execution of the Subscription Agreement
	Role (Controller/Processor):	Controller

Processor(s) / Data importer(s): *[Identity and contact details of the Processor(s) /data importer(s), including any contact person with responsibility for data protection*]

1.	**Name:**	Lumerate Inc.
	Address:	326-1665 Dupont St, Toronto, Ontario, Canada, M6P 3T1
	Contact person's name, position and contact details:	Beth Adams, Chief Operating Officer privacy@lumerate.com
	Activities relevant to the data transferred under these Clauses:	We provide Services to You in accordance with the Subscription Agreement
	Signature and date:	As per the execution of the Subscription Agreement
	Role (Controller/Processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is transferred:	Individuals at Your potential marketing targets
Categories of Personal Data transferred:	Name, title, city and business contact details (email and phone)
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous during the provision of the Services under the Subscription Agreement
Nature of the Processing:	We will Process the Personal Data for the purposes of providing the Services in accordance with the Subscription Agreement
Purpose(s) of the data transfer and further Processing:	To provide the Services in accordance with the Subscription Agreement
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	As necessary to provide the Services under the Subscription Agreement, and deletion at the latest in accordance with clause 1.3 of the Subscription Agreement.
For transfers to (sub-) Processors, also specify subject matter, nature and duration of the Processing:	Where We engage subprocessors We will do so in compliance with the terms of the EU SCCs. The subject matter, nature and duration of the Processing activities carried out by the subprocessor will not exceed the subject matter, nature and duration of the Processing activities as described in this Annex I.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	The supervisory authority in the country in which Your main establishment or single establishment is located.

Annex II

Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the Data Importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

○ Measure	Description
Measures of pseudonymisation and encryption of personal data	○ Encryption is in place in transit. We implement encryption to AES 256 standard. ○ Encryption is in place, where practicable at rest. Data is not stored in plain text. ○ We also utilise TLS, DMARC and SSL encryption.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	○ We have the following measures in place to ensure CIA and resilience of processing systems: ○ Remote, offsite back-ups and data replication ○ Back-up policy and processes to ensure data can be restored in an agreed SLA ○ Minimised single points of failure and services secure with redundancy built into design ○ Continuous risk assessment and disaster recovery plans in place which are tested in regular annual cycles ○ Designated incident management group to oversee business continuity plans in event of emergency ○ External attacks mitigated by a number of methods including Next Generation firewalls, web application firewalls, IPS and 24/7 monitoring
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	○ Remote, offsite back-ups and data replication at regular intervals ○ Back-up policy and processes to ensure data can be restored within an agreed SLA ○ Continuous risk assessment and disaster recovery plans in place which are tested in regular annual cycles ○ Designated incident management group to oversee business continuity plans in event of emergency
Processes for regularly testing, assessing and evaluating the effectiveness of technical and	● Internal and client IT / information security audits ● Regular penetration testing and vulnerability assessments by CREST approved companies

organisational measures in order to ensure the security of the processing	● Business continuity exercises and war-gaming incidents ● Ongoing assessments under information security accreditations including SOC 2
Measures for user identification and authorisation	○ Access to data is controlled using a layered security process at the domain, application and server levels, allowing access to data to be granted selectively ○ A designated team within our IT manages user account creation / removal, change and data access controls ○ Access is based on the principle of least privilege and users shall only access data required to fulfil role and no more ○ Access is granted to individuals and accounts and passwords are handled and protected as confidential data ○ Multi-Factor authentication in place for core enterprise systems and applications ○ Strong password policy requiring at least two (2) of alphabetic, numeric, or special characters; minimum ten (10) characters ○ Privileged access is regulated by our Administrators Access policy and access is subject to continuous review ○
Measures for the protection of data during transmission	○ We utilise TLS, DMARC and SSL encryption.
Measures for the protection of data during storage	○ Encryption is in place, where practicable at rest. Data is not stored in plain text.
Measures for ensuring physical security of locations at which personal data are processed	○ Physical security in place 24 x7 in our cloud services data center (e.g. premises, server room access controls, alarms, power supply etc.) ○ Card access systems are use at our our cloud services data center to restrict access to employees and cleared contract personnel ○ Server rooms at our cloud services data center are controlled by door access systems, limited to approved personnel only ○ Data Centre server rooms are fitted with appropriate environmental controls; Universal Power Supply (UPS) and fire suppression systems as standard ○ Controlled fire / emergency alarm systems throughout at our cloud services data center ○ CCTV in place at our cloud services data center and recorded for strategic access areas

Measures for ensuring events logging	○ Abnormal behaviour detection is in place ○ Continuous access logging & monitoring is in place. Data is collated by 3rd party outsourced security team and constantly reviewed by Security Team ○ The following monitoring tools are in place: New Relic, Bugsnag, Loggly, Alertra, Splunk-based IDS
Measures for ensuring system configuration, including default configuration	○ Data is backed-up on a regular cycle with backups held in remote location ○ External attacks mitigated by a number of methods including Next Generation firewalls, web application firewalls, IPS and 24/7 monitoring ○ Encryption is in place at in transit and at rest where practicable ○ Access is based on the principle of least privilege and users shall only access data to fulfil role ○ Access is granted to individuals and accounts and passwords are handled and protected as confidential data ○ Multi-Factor authentication in place ○ User devices are covered by virus and malware protection including defence against advanced persistent threats ○
Measures for internal IT and IT security governance and management	We perform an annual internal review of all security management policies and procedures and conduct quarterly security review meetings. External auditors perform an annual review of these policies and procedures. ○ We are committed to safeguarding the confidentiality, availability and security of the information that our customers have entrusted to us, including the personal data subject to the GDPR. ○ This commitment is overseen at the executive level by the CEO. ○ The board receives quarterly reports. ○ We train employees and contractors on their information security requirements and responsibilities. ○ Training covers a range of data protection subjects including information security, information privacy, GDPR, phishing training etc. ○ We have instituted a third-party service provider assessment program to vet its providers who may

	store, process, transmit, access, or potentially have access to, personal data subject to GDPR. ○ The vendor process is designed to ensure that sub-processors have systems in place to ensure that they can meet data protection requirements
Measures for certification/assurance of processes and products	○ We have been audited by a third-party firm and achieved SOC 2 Type 1 compliance, attesting to the controls that safeguard information processed by the our applications.
Measures for ensuring data minimisation	● We incorporate a checklist in our software design process to to flag new projects that may come in contact with personal data. ● We use software logic to minimise what personal data is returned in any scenarios involving API queries to external systems. ● We limit any personal information to the scope of information that is required in a business-to-business interpersonal transaction (name, title, city, business email, business phone).
Measures for ensuring data quality	○ We have standard operating procedures in place to check the accuracy of the data we collect, and we record the source of that data. ○ In the event that one customer sees inaccurate data, we have software features in place that allow customers to report the inaccuracies. ○ We maintain logs of changes to personal data where logging is possible. ○ Applications are designed to filter and avoid display of duplicate records of personal information.
Measures for ensuring limited data retention	● We maintain Data Retention policies that undergo internal review and external audit on an annual basis. ● We maintain Customer Data Tiering policy that stipulates data categories and outlines acceptable and unacceptable logging and storage practices ● We train employees on Data Retention policies and procedures on an annual basis. ● We incorporate design features into our products that auto-delete key personal information
Measures for ensuring accountability	○ We maintain records of processing activities ○ We conduct regular privacy reviews by retaining external privacy law experts. ○ We train all staff on key privacy regulations and track the annual status of retraining.

	○ We keep evidence of the steps we take to comply with UK GDPR ○ We have policies in place to record and, where necessary, report personal data breaches. ○
Measures for allowing data portability and ensuring erasure	● We provide measures for data portability and erasure in accordance with the Subscription Agreement and the relevant privacy policy (Zymewire, Zapyrus).

Subject Rights (clause 10(b) of Module 2 or Module 3 of the EU SCCs)

Each member of our Group shall assist the Parties (on request) in complying with any subject rights requests.