Amperity Data Processing Addendum to the Agreement

This Data Processing Addendum and its Schedules, including the Standard Contractual Clauses and UK Addendum as applicable ("**DPA**"), is entered into between Amperity, Inc. ("**Amperity**") and the entity identified as the Customer ("**Customer**") (each, a "**Party**" and collectively, the "**Parties**") and is appended to the Services Agreement, or other such agreement, governing the Customer's access and use of the Amperity platform and related services (the "**Agreement**"). The Parties agree that this DPA shall be incorporated into and form part of the Agreement and subject to the provisions therein. All capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Law, in the name and on behalf of its Permitted Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term “Customer” shall include Customer and such Permitted Affiliates.

This DPA is effective as of the date signed by the Customer, but only if Amperity receives the signed DPA in accordance with the instructions below.

Instructions

This DPA sets forth the terms and conditions under which Amperity may receive and process Customer Personal Data. In order for this DPA to be effective, Customer must:

1. *Complete and sign the execution block below with the Customer's full legal entity name, address, and signatory information; and*
2. *Submit the completed and signed DPA to your Amperity Representative or email to: legal@amperity.com.*

If Customer makes any deletions or revisions to this DPA, those deletions or revisions will be deemed as rejected and invalid, unless agreed by Amperity. Customer's signatory represents and warrants that he or she has the authority to bind the Customer to this DPA. This DPA will terminate automatically upon termination of the Agreement, or as earlier terminated pursuant to the terms of this DPA.

Data Processing Terms

1. Definitions

"**Applicable Data Protection Law**" means all data protection laws and regulations applicable to the processing of Customer Personal Data under the Agreement, including (i) European Data Protection Law, (ii) US Data Protection Law, and (iii) other data protection laws enacted in other countries with similar data protection requirements which are applicable to the Processing of Customer Personal Data under the Agreement.

"Controller" means an entity that alone or jointly with others determines the purposes and means of Processing Personal Data, which may include, as applicable, a "Business" as defined under the CCPA.

"**Customer Personal Data**" means any Personal Data that is processed by Amperity on behalf of Customer while providing the Services, as more particularly described in Schedule 1 of this DPA.

"**Europe**" means, for the purposes of this DPA, the European Economic Area ("**EEA**"), the United Kingdom ("**UK**") and Switzerland.

"**European 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 GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the UK Data Protection Act 2018 (collectively, "**UK Data Protection Law**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) the Swiss Federal Act on Data Protection of 25 September 2020 and its corresponding ordinances ("**Swiss FADP**"), and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) (iii) or (iv); in each case as may be amended, superseded or replaced from time to time;

"Permitted Affiliate" means any Affiliate of Customer which: (i) is subject to Applicable Data Protection Law and the Controller with respect to the Personal Data; and (ii) is permitted to use the Services pursuant to the Agreement, but has not signed its own Order Form with Amperity and is not a "Customer" as defined under the Agreement.

“Personal Data” means any information relating to an identified or identifiable natural person that is Processed in connection with the Services ("**Data Subject**"), and includes “personal data” "personally identifiable information" and/or “personal information” under Applicable Data Protection Law.

"Process," "Processes," "Processing," "Processed" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity that Processes Personal Data on behalf, and in accordance with the instructions, of the Controller, which may include as applicable, a "Service Provider" as defined under the CCPA.

"Restricted Transfer" means (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK Data Protection Law 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 (iii) where the Swiss FADP applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

"Standard Contractual Clauses" or **"SCCs"** means the contractual clauses annexed to the European Commission's 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.

"**Security Incident**" means a confirmed breach of security leading to any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data. A "Security Incident" shall not include an unsuccessful attempt to access Customer Personal Data or activities that do not compromise the security of Customer Personal Data.

"Services" means any product or service provided by Amperity to Customer pursuant to the Agreement.

"**Subprocessor**" means any third-party Processor (including any Amperity Affiliates) engaged by Amperity to process any Customer Personal Data in connection with the provision of Services (excluding Amperity employees, contractors or consultants).

"Supervisory Authority" means any regulatory, supervisory, governmental, state agency, Attorney General or other competent authority with jurisdiction or oversight over compliance with Applicable Data Protection Law.

"UK Addendum" means the International Data Transfer Addendum to the Standard Contractual Clauses (version B1.0) issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as may be amended, superseded or replaced from time to time.

"US Data Protection Law" means (i) the California Consumer Privacy Act (the "**CCPA**"), as amended by the California Privacy Rights Act ("**CPRA**") and its implementing regulations (collectively referred to herein as the **CCPA**); (ii) the Virginia Consumer Data Protection Act ("**VCDPA**"); (iii) the Colorado Privacy Act ("**CPA**"); (iv) the Utah Consumer Privacy Act ("**UCPA**"); (v) the Connecticut Data Privacy Act ("**CTDPA**"); and (vi) any other applicable US state data privacy/protection laws that become effective on or after the effective date of this DPA, in each case as may be amended or superseded from time to time.

2. Roles and Scope of Processing

2.1 The Parties acknowledge and agree that for the purposes of this DPA, (i) Customer is the Controller (or a Processor on behalf of a third-party Controller) with respect to the Processing of Customer Personal Data, and (ii) Amperity shall Process Customer Personal Data only as a Processor on behalf of Customer. Where applicable, Customer shall be responsible for any communications, notifications, assistance and/or authorizations that Amperity may be required to provide to or receive from a third party Controller.

2.2 Amperity will Process Customer Personal Data only in accordance with Customer's documented lawful instructions and will not Process Customer Personal Data for its own purposes, except where required by applicable laws and the Agreement. The Agreement,

including this DPA, along with Customer's configuration of any settings or options in the Services (as Customer may be able to modify from time to time), constitute Customer's complete and final instructions to Amperity regarding the Processing of Customer Personal Data, including for purposes of the Standard Contractual Clauses, and (if applicable) include and are consistent with all instructions from third party Controllers. Additional instructions outside the scope of such Processing instructions (if any) require prior written agreement between the Parties.

2.3 Each Party shall comply with its obligations under applicable laws, including Applicable Data Protection Law, in respect of any Customer Personal Data it Processes under or in connection with the Services or this DPA. Amperity shall promptly notify Customer if it makes a determination that Customer's instructions infringe Applicable Data Protection Law, but without the obligation to actively monitor Customer's compliance with Applicable Data Protection Law, and in such event, Amperity shall not be obligated to undertake such Processing until such time as the Customer has updated its Processing instructions and Amperity has determined that the incidence of non-compliance has been resolved. Amperity shall also notify Customer if it makes a determination that it can no longer meet its obligations under Applicable Data Protection Law.

2.4 Customer shall have the sole responsibility for the accuracy, quality and legality of the Customer Personal Data and the means by which Customer acquired the Customer Personal Data. Customer warrants and represents that (i) it has provided, and will continue to provide, all notices, and obtained, and will continue to obtain, all consents, permissions and rights necessary for Amperity and its Subprocessors to lawfully Process Customer Personal Data, in accordance with Applicable Data Protection Law, for the purposes contemplated by the Agreement (including this DPA), and (ii) it shall ensure its Processing instructions comply with applicable laws (including Applicable Data Protection Law) and that the processing of Customer Personal Data by Amperity in accordance with Customer's instructions will not cause Amperity to be in breach of Applicable Data Protection Law.

2.5 For the purposes of US Data Protection Law (to the extent applicable), Amperity shall not (a) "sell" Customer Personal Data, as the term "sell" is defined by US Data Protection Law; (b) "share" Customer Personal Data, as the term "share" is defined by the CCPA; (c) disclose or transfer Customer Personal Data to a Subprocessor or any other third parties that would constitute "selling" as the term is defined by US Data Protection Law or "sharing" as the term is defined by the CCPA; (d) retain, use, disclose, or otherwise Process the Customer Personal Data for any purposes other than the specific purposes described in the Agreement and Annex 1 of this DPA; (e) retain, use, disclose, or otherwise Process the Customer Personal Data outside of the direct business relationship between Amperity and Customer; and (f) combine the Personal Data received from Customer with Personal Data that it collects or receives from or on behalf of any third party, unless as otherwise permitted by US Data Protection Law.

3. Subprocessing

3.1 Customer grants Amperity a general authorization to subcontract the Processing of Customer Personal Data to a Subprocessor, including those Subprocessors listed in

Amperity's website at https://docs.amperity.com/support/subcontractors.html ("**Subprocessor List**").

3.2 Amperity will:

(a) enter into a written agreement with each Subprocessor containing data protection terms that provide at least the same level of protection for Customer Personal Data as those contained in this DPA, to the extent applicable to the nature of the services provided by each Subprocessor; and

(b) remain responsible to Customer for any acts or omissions of the Subprocessor that cause Amperity to breach any of its obligations under this DPA.

3.3 Prior to the addition of any new Subprocessor, Amperity shall provide notice to Customer not less than ten (10) calendar days prior to the date on which the Subprocessor shall commence Processing Customer Personal Data. Amperity provides a subscription form along with the Subprocessor list for Customers to subscribe to receive automatic notifications of changes to the Subprocessor List. Customer acknowledges and agrees that it shall subscribe to Amperity's notice mechanism provided in the Subprocessor List to receive the notices and that Amperity will only provide the corresponding notice to the email address provided in the subscription form.

3.4 Customer may object to Amperity's appointment of any new or replacement Subprocessor promptly in writing within ten (10) calendar days of receipt of the automatic notice in accordance with 3.3 above and on reasonable grounds related to Subprocessor's ability to comply with Applicable Data Protection Law. In such case, the Parties shall discuss Customer´s concerns in good faith with a view to achieving a commercially reasonable resolution. If the Parties cannot reach such resolution, Amperity shall, at its sole discretion, either not appoint the Subprocessor at issue, or permit Customer to suspend or terminate the applicable Order Form and/or the Agreement without liability to either Party. In the event Customer exercises its right of termination under this Section 3.4, Amperity will refund to Customer a pro rata share of any prepaid unused fees for the remaining and unexpired portion of the applicable Subscription Term from the date of termination, as the Customer's exclusive remedy.

4. Cooperation

4.1 To the extent Amperity is required under Applicable Data Protection Law and/or Customer does not already have access to the relevant information, Amperity shall reasonably cooperate with Customer to enable Customer to respond to any requests, complaints or other communications from Data Subjects and Supervisory Authorities relating to the Processing of Customer Personal Data, including requests from Data Subjects seeking to exercise their rights under Applicable Data Protection Law. In the event that any such request, complaint or communication is made directly to Amperity, Amperity shall(once it has identified the request is from or related to a Data Subject for whom the Customer is responsible), pass this onto Customer and shall not respond to such communication, without Customer's express authorization, except to direct the Data Subject and their request, complaint or other communication to the Customer or as otherwise required to do so in order to comply with applicable laws.

4.2 To the extent Amperity is required under Applicable Data Protection Law and/or Customer does not already have access to the relevant information, Amperity shall provide reasonably requested information regarding Amperity's Processing of Customer Personal Data to enable the Customer to (i) conduct data protection impact assessments, risk assessments, cybersecurity audits or similar as required by Applicable Data Protection Law, and (ii) to respond to queries, inquiries, complaints or to conduct prior consultations with Supervisory Authorities as required by Applicable Data Protection Law.

4.3 If a Supervisory Authority sends Amperity a demand for Customer Personal Data (for example, through a subpoena or court order), Amperity will attempt to redirect the Supervisory Authority to request that Customer Personal Data directly from Customer. As part of this effort, Amperity may provide Customer's basic contact information to the Supervisory Authority. If compelled to disclose Customer Personal Data to the Supervisory Authority, then Amperity will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Amperity is legally prohibited from doing so.

5. Data Access & Security Measures

5.1 Amperity will ensure that any personnel tasked with the Processing of Customer Personal Data are subject to an appropriate duty of confidentiality (whether a contractual or statutory duty).

5.2 Amperity will implement and maintain reasonable and appropriate technical and organizational security measures designed to protect Customer Personal Data from Security Incidents in accordance with the measures described in Schedule 2 ("**Security Measures"**). Customer acknowledges that the Security Measures are subject to technical progress and development and that Amperity may update or modify the Security Measures from time to time, provided that such updates and modifications do not materially diminish the overall security of the Services.

6. Security Incidents

Upon becoming aware of a Security Incident, Amperity shall notify Customer without undue delay to the email address for notices provided under the Order Form or other email address provided under the Agreement to Amperity from time to time and shall provide Customer with timely information in accordance with Applicable Data Protection Law as it becomes known or as is reasonably requested by Customer. Amperity shall provide reasonable cooperation to Customer to allow Customer to fulfil its reporting obligations under Applicable Data Protection Law and shall take reasonable steps to investigate, remedy or mitigate the effects of the Security Incident, to the extent the remediation is within Amperity's control. Amperity's notification of or response to a Security Incident under this Section 6 shall not be construed as an acknowledgment by Amperity of any fault or liability with respect to the Security Incident. The obligations set forth in this Section 6 shall not apply to Security Incidents that are caused by the Customer or its users.

7. Security Reports & Inspections

7.1 Upon Customer's written request, Amperity shall, no more than annually and on reasonable notice, provide Customer (on a confidential basis) access to reasonably requested documentation related to its Processing of Customer Personal Data (including copies of any certifications, audit report summaries and/or other relevant documentation it holds), where reasonably required by Customer to verify Amperity's compliance with this DPA.

7.2 While it is the Parties' intention ordinarily to rely on Amperity's obligations set forth in Section 7.1 to verify Amperity's compliance with this DPA, following a confirmed Security Incident or where a Supervisory Authority requires it, Customer may provide Amperity with thirty (30) days' prior written notice requesting that a third-party conduct an audit of Amperity's operations and facilities ("**Audit"**); provided that (i) any Audit shall be conducted at Customer's expense; (ii) the Parties shall mutually agree upon the scope, timing and duration of the Audit; and (iii) the Audit shall not unreasonably impact Amperity's regular operations.

7.3 Any written responses or Audit described in this Section 7 shall be subject to the confidentiality provisions of the Agreement. The Parties agree that the audits described in Clause 8.9 of SCCs shall be carried out in accordance with this Section 7.

8. Data Transfers

8.1 Customer Personal Data that Amperity Processes under the Agreement may be Processed in any country in which Amperity, its Amperity Subsidiaries and Subprocessors maintain facilities to perform the Services, as further detailed in the Subprocessor List. Amperity shall at all times ensure such transfers (and onward transfers) are made in compliance with the requirements of Applicable Data Protection Law.

8.2 The Parties agree that, when the transfer of Customer Personal Data from Customer (as "**data exporter**") to Amperity (as "**data importer**") under this DPA is deemed a Restricted Transfer and European Data Protection Law requires that appropriate safeguards are put in place, such transfer shall be governed by the SCCs, which shall be deemed incorporated by reference and form an integral part of this DPA as set out below. In the event that any provision of this DPA contradicts, directly or indirectly, the SCCs, the SCCs shall prevail.

8.3 In relation to Customer Personal Data that is protected by the EU GDPR, the SCCs will apply as follows:

(a) Module Two (C2P) or Module Three (P2P) will apply;

(b) in Clause 7, the optional docking clause shall apply;

(c) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 3.4 of this DPA;

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

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

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

(g) Annex I of the SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and

(h) Annex II of the SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA.

8.4 In relation to Customer Personal Data that is protected by UK Data Protection Law, the SCCs (i) shall apply as completed in accordance with Section 8.3. above; and (ii) shall be deemed amended as specified by the UK Addendum, which shall be deemed executed by the Parties and incorporated into and form an integral part of this DPA. Any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Schedules 1 and 2 of this DPA and table 4 in Part 1 shall be deemed completed by selecting "neither party".

8.5 In relation to transfers of Customer Personal Data protected by the Swiss FADP, the SCCs will also apply in accordance with Section 8.3. above, with the following modifications:

(a) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP;

(b) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss FADP;

(c) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland", or "Swiss law";

(d) the term "member state" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

(e) Clause 13(a) and Part C of Annex I shall not be used and the "competent supervisory authority" shall be the Swiss Federal Data Protection Information Commissioner;

(f) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

(g) in Clause 17, the SCCs shall be governed by the laws of Switzerland; and

(h) Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

8.6 It is not the intention of either Party to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the DPA, the SCCs shall prevail to the extent of such conflict.

8.7 If Amperity adopts an alternative lawful data export mechanism for the transfer of Personal Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which the relevant Customer Personal Data is transferred).

9. Deletion or Return

9.1 Upon Customer's request, or upon termination or expiry of the Agreement, Amperity shall return to Customer or destroy all Customer Personal Data in its possession or control in accordance with the Agreement. This requirement shall not apply to the extent that Amperity is required by any applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data Amperity shall securely isolate and protect from any further Processing and eventually delete in accordance with Amperity's deletion policies, except to the extent required by such law. The Parties agree that the certification of deletion of Personal Data described in Clause 8.5 and 16(d) of the SCCs shall be provided by Amperity to Customer only upon Customer's written request.

10. Liability

10.1 Amperity and its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA (including the SCCs and UK Addendum) and all data processing agreements between Customer, Permitted Affiliates and Amperity, whether in contract, tort, or under any other theory of liability, is subject to the limitations and exclusions of liability set forth in the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement, this DPA and the SCCs.

10.2 Any claims against Amperity or its Affiliates under or in connection with this DPA (including, where applicable, the Standard Contractual Clauses) shall be brought solely by the Customer entity that is a party to the Agreement.

11. Permitted Affiliates

11.1 When a Permitted Affiliate becomes a Party to the DPA, then such Permitted Affiliate shall be entitled to exercise its rights and remedies available under this DPA to the extent required under Applicable Data Protection Law. However, if Applicable Data Protection Law requires the Permitted Affiliate to directly exercise a right or remedy against Amperity directly by itself, the Parties agree that to the extent permitted under applicable laws: (i) only the Customer that is the contracting entity to the Agreement shall exercise any such right or seek any such remedy on behalf of the Permitted Affiliate; and (ii) the Customer that is the contracting party to the DPA shall exercise any such rights under this DPA in a combined manner for all of its Permitted Affiliates together, instead of doing so separately for each Permitted Affiliate. The Customer that is the contracting entity is responsible for coordinating all communication with Amperity under the DPA and be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

12. General

12.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between any provision in this DPA and any provision in the Agreement, this DPA controls and takes precedence. With effect from the effective date, this DPA is part of, and incorporated into the Agreement.

12.2 In no event does this DPA restrict or limit the rights of any Data Subject or of any Supervisory Authority.

12.3 This DPA may not be modified except by a subsequent written instrument signed by both Parties.

12.4 If there is any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) Standard Contractual Clauses and/or UK Addendum (where applicable); then (b) this DPA; and then (c) the main body of the Agreement.

12.5 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law or the SCCs and UK Addendum.

IN WITNESS WHEREOF, the Parties hereby cause their duly authorized representatives to execute this DPA as of the date hereof.

Amperity, Inc.	**Customer**
Name:	**Name:**
Position:	**Position:**
Date:	**Date:**
Signature:	**Signature:**

SCHEDULE 1

Description of Data Processing

A. LIST OF PARTIES

Data exporter(s):

Name:	**The entity identified as the "Customer" in the DPA.**
Address:	**The address for the Customer associated with its Amperity account or otherwise specified in the DPA or this Agreement.**
Contact person's name, position and contact details:	**The contact details associated with Customer's account, or otherwise specified in this DPA, Order Form or the Agreement.**
Activities relevant to the data transferred under these Clauses:	**The activities specified in Schedule 1(B) of the DPA.**
Signature and date:	**This Schedule 1(A) shall automatically be deemed executed when the execution block within this DPA is executed by the Customer.**
Role (controller/processor):	**Controller or processor**

Data importer(s):

Name:	**Amperity, Inc. (Amperity)**
Address:	**701 5th Ave 26th floor, Seattle, WA 98104**
Contact person's name, position and contact details:	**VP Legal: Wade Foley** **Email: Legal@amperity.com**
Activities relevant to the data transferred under these Clauses:	**The activities specified in Schedule 1(B) of the DPA**
Signature and date:	**This Schedule 1(A) shall automatically be deemed executed when the execution block within this DPA is executed by Amperity.**
Role (controller/processor):	**Processor**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	**The Data Subjects include individuals about whom Personal Data is processed by Amperity via the Services by or at the direction of the Customer. This includes Customer's employees, consultants, agents and third parties authorized to use the Services as "Users" under Customer's Amperity account.**
Categories of personal data transferred	**Customer Personal Data uploaded to the Services under Customer's Amperity account, including**

	name, email and contact information of Customer's customer and employees. [To be updated by Customer if necessary]
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 data exporter is prohibited from submitting special categories of data or sensitive data to the Services.**
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	**Continuous basis depending on the use of the Services by data exporter.**
Nature of the processing	**The provision of the Services as described in the Agreement and initiated by the Customer from time to time.**
Purpose(s) of the data transfer and further processing	**Amperity will Process Customer Personal Data as necessary to perform the Services pursuant to the Agreement, as further instructed by Customer in its use of the Services.**
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	**The duration of the Processing is the term of the Agreement plus any period after the termination or expiry of the Agreement during which Amperity will process Customer Personal Data in accordance with the Agreement and the DPA.**
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As per **the information provided above.**

C. COMPETENT SUPERVISORY AUTHORITY

With respect to Personal Data subject to the EU GDPR, the competent supervisory authority is the Data Protection Commission of Ireland. With respect to Personal Data to which UK Data Protection Law applies, the competent supervisory authority is the Information Commissioner's Office. With respect to Personal Data to which Swiss FADP applies, the competent supervisory authority is the Swiss Federal Data Protection Information Commissioner.

SCHEDULE 2

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE PERSONAL DATA

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.

Amperity uses the following technical and organizational measures to protect Personal Data:

- Measures of pseudonymisation and encryption of personal data
- Measures to anonymize and aggregate personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- 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
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Measures for user identification and authorisation Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration Measures for internal IT and IT security governance and management Measures for certification/assurance of processes and products
- Measures for ensuring data minimisation
- Measures for ensuring data quality
- Measures for ensuring limited data retention
- Measures for ensuring accountability
- Measures for allowing data portability and ensuring erasure