DATA PROCESSING ADDENDUM

1. Preamble. This Data Processing Addendum ("DPA"), forms part of the Master SaaS Subscription Agreement (the "Agreement") between Tamr, Inc. ("Company") and the entity that has engaged Company to provide the Service (as defined below) ("Customer") and shall be effective as of the effective date of the Agreement. Terms used and not otherwise defined herein shall have the meanings ascribed to them in the Agreement. In this DPA, "Service" means the service provided to Customer by the Company in accordance with the terms of the Agreement.

2. In this DPA the following terms shall have the meanings set out in this Section 2, unless expressly stated otherwise:

   a. "Addendum Effective Date" means the effective date of the Agreement.
   b. "Applicable Data Protection Laws" means the privacy, data protection and data security laws and regulations of (i) any EEA jurisdiction, (ii) the United Kingdom and (iii) Switzerland as applicable to the processing of European Personal Data under the Agreement, including, without limitation, EU GDPR and UK GDPR (as and where applicable).
   c. "European Personal Data" means any Personal Data Processed by Company or any of its Affiliates or Subprocessors on behalf of Customer to perform the Services under the Agreement (including, for the avoidance of doubt, any such Personal Data comprised within Customer Data).
   d. "Data Subject Request" means the exercise by a Data Subject of its rights in accordance with Applicable Data Protection Laws in respect of European Personal Data and the Processing thereof.
   e. "Data Subject" means the identified or identifiable natural person to whom European Personal Data relates.
   f. "EEA" means the European Economic Area.
   g. "FADP" means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; "FADP") and, as and when it enters into force on 1 January 2023, its revised version of 25 September 2020.
   h. "FDPIC" means the Swiss Federal Data Protection and Information Commissioner.
   i. "GDPR" means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR"); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("UK GDPR"), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to "Articles" and "Chapters" of, and other relevant defined terms in, the GDPR shall be construed accordingly.
   j. "Incident" means a breach of Company's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, European Personal Data in Company's possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of European Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).
   k. "Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
   l. "Restricted Transfer" means the disclosure, grant of access or other transfer of European Personal Data to any person located in: (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an "EU Restricted Transfer"); and (ii) in the context of the UK, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a "UK Restricted Transfer"), and/or (iii) in the context of Switzerland, a country or territory outside of Switzerland ("Swiss Restricted Transfer"), which would be prohibited without a legal basis under Chapter V of the GDPR.
   m. "SCCs" means in respect of: (i) any EU Restricted Transfer, the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914.
   n. "Service Data" means any data relating to the use, support and/or operation of the Services, which is collected directly by Company from and/or about users of the Services and/or Customer's use of the Service for use for its own purposes (certain of which may constitute Personal Data).
   o. "Services" means those services and activities to be supplied to or carried out by or on behalf of Company for Customer pursuant to the Agreement, including the Product Offerings.
   p. "Subprocessor" means any third party appointed by or on behalf of Company to Process European Personal Data.
   q. "Supervisory Authority": (i) in the context of the EEA and the EU GDPR, shall have the meaning given to that term in the EU GDPR; and (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office.
   r. "Transfer Mechanism(s)" means the SCCs and/or the UK Transfer Addendum as applicable to the relevant Restricted Transfer.

s. "UK Transfer Addendum" means the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the Mandatory Clauses included in Part 2 thereof.

The following terms have the meanings given in the GDPR: "controller", "personal data", "processor", "data subject" and "processing".

3. Subject Matter, Nature, Purpose and Duration. Sections 1 through 9 of this DPA apply to the processing of Personal Data relating to Data Subjects located in the EEA or the United Kingdom, or that is otherwise regulated by the GDPR, by the Company solely on behalf of Customer for the purpose of providing the. As between the parties, (i) Customer is a controller and the Company is a Processor on behalf of Customer with regard to European Personal Data or (ii) Customer is a Processor and the Company is a Subprocessor on behalf of Customer with regard to European Personal Data. The subject matter and purposes of European Personal Data processing, type of European Personal Data, categories of data subjects, nature of the European Personal Data processing, and Customer's data processing instructions for the Company, are set forth on Exhibit A to this DPA and as otherwise as provided in reasonable written instructions by Customer to the Company from time to time. This DPA shall remain in effect, and the duration of the processing under this DPA shall continue, as long as the Company carries out European Personal Data processing operations regarding European Personal Data .

4. Processing Covenants. In processing European Personal Data hereunder, the Company shall:

a. process European Personal Data only on documented instructions from Customer, unless otherwise required to do so by applicable law, in which case the Company will inform Customer of that legal requirement before processing, unless applicable law prohibits the Company from informing Customer. For the avoidance of doubt, this DPA shall constitute Customer's documented instructions to the Company to process European Personal Data in connection with the Company's provision of the Service to Customer;

b. use commercially reasonable efforts intended to ensure that persons authorized to process European Personal Data hereunder have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality or are subject to ethical rules of responsibility that include confidentiality;

c. 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 risk of varying likelihood and severity for the rights and freedoms of natural persons, implement commercially reasonable technical and organizational measures intended to meet the security requirements described in Article 32 of the GDPR and as described in Exhibit C1 (Security). Company represents and warrants that (i) Company has not purposefully created backdoors or similar programming that could be used to access its systems or Personal Data, (ii) Company has not purposefully created or changed its business processes in a manner that facilitates access to its systems or to Personal Data by public authorities and shall not voluntarily cooperate with public authorities in relation to the same, and (iii) no applicable law or government policy to which Company is subject requires Company to create or maintain backdoors or to facilitate access to Personal Data or systems or for Company to be in possession of any corresponding encryption keys;

d. taking into account the nature of the processing, use commercially reasonable efforts to assist Customer, at Customer's expense, by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to Data Subject Request. If Company receives a Data Subject Request, Customer will be responsible for responding to any such request. Company shall:
    i. promptly notify Customer if it receives a Data Subject Request; and
    ii. not respond to any Data Subject Request, other than to advise the data subject to submit the request to Customer, except on the written instructions of Customer or as required by Applicable Data Protection Laws.

e. taking into account the nature of processing and the information available to the Company, use commercially reasonable efforts to assist Customer, at Customer's expense, in ensuring compliance with any data protection impact assessments and prior consultations with Supervisory Authorities which Customer reasonably considers to be required of it by Article 35 or Article 36 of the GDPR, in each case solely in relation to processing of European Personal Data by Company;

f. notify Customer promptly if the Company becomes actually aware of an Incident, provided that the provision of such notice by the Company shall not be construed as an acknowledgement of fault or liability with respect to any such Incident. Customer is solely responsible for complying with notification obligations under Applicable Data Protection Laws applicable to Customer and fulfilling any third-party notification obligations related to any Incident;

g. If Customer determines that an Incident must be notified to any Supervisory Authority, any data subject(s), the public or others under Applicable Data Protection Laws, to the extent such notice directly or indirectly refers to or identifies Company, where permitted by applicable laws, Customer agrees to:

   i. notify Company in advance; and
   ii. in good faith, consult with Company and consider any clarifications or corrections Company may reasonably recommend or request to any such notification, which: (i) relate to Company's involvement in or relevance to such Incident; and (ii) are consistent with applicable laws.

h. at the written request of Customer, delete or return all European Personal Data to Customer promptly after the end of the provision of the Service to Customer and delete existing copies unless applicable law requires retention of European Personal Data. In the event that Customer does not instruct Company in writing to either delete or return European Personal Data within a calendar month after termination of the Agreement, Company shall promptly after the expiry of the aforementioned time period either (at its option) delete; or irreversibly render anonymous, all European Personal Data then within Company possession to the fullest extent technically possible in the circumstances. Company may retain European Personal Data where permitted or required by applicable law, for such period as may be required by such applicable law, provided that Company shall: (i) maintain the confidentiality of all such European Personal Data; and (ii) process the European Personal Data only as necessary for the purpose(s) specified in the applicable law permitting or requiring such retention.

i. make available upon Customer's reasonable request information reasonably necessary to demonstrate material compliance with the obligations laid down in this DPA and allow for and contribute to audits (each, an "Audit"), at Customer's expense, including inspections of processing facilities under the Company's control, conducted by Customer or another auditor chosen by Customer (an "Auditor"), during normal business hours, no more frequently than once during any twelve (12) month period, and upon reasonable prior notice, provided that no Auditor shall be a competitor of the Company, and provided further that in no event shall Customer have access to the information of any other Customer of the Company and the disclosures made pursuant to this Section 4(i) ("Audit Information") shall be held in confidence as the Company's Confidential Information and subject to any confidentiality obligations in the Agreement, and provided further that no Audit shall be undertaken unless or until Customer has requested, and the Company has provided, documentation pursuant to this Section 4(i) and Customer reasonably determines that an Audit remains necessary to demonstrate material compliance with the obligations laid down in this DPA. Without limiting the generality of any provision in the Agreement, Customer shall employ the same degree of care to safeguard Audit Information that it uses to protect its own confidential and proprietary information and in any event, not less than a reasonable degree of care under the circumstances, and Customer shall be liable for any improper disclosure or use of Audit Information by Customer or its agents. If the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request ("Audit Report") and Company has confirmed in writing that there are no known material changes in the controls audited and covered by such Audit Report(s), Customer agrees to accept provision of such Audit Report(s) in lieu of requesting an audit of such controls or measures.

5. Subprocessors. Customer hereby grants the Company general authorization to engage Subprocessors to assist the Company in processing European Personal Data as set out in this DPA. The Company shall enter into contractual arrangements with such Subprocessors requiring the same level of data protection compliance and information security as that provided for herein. Customer hereby consents to the processing of European Personal Data by, and the disclosure and transfer of European Personal Data to, the Subprocessors listed on Exhibit B to this DPA. The Company shall inform Customer of any intended changes concerning the addition or replacement of Subprocessors at least ten (10) calendar days before the new Subprocessor processes European Personal Data. Customer may object to such changes in writing within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection (an "Objection"). In the event of an Objection, the parties will discuss such concerns in good faith with the intention of achieving a resolution. If the parties are not able to achieve a resolution as described in the previous sentence, Customer, as its sole and exclusive remedy, may terminate the Agreement for convenience, on the condition that Customer provides written notice to the Company within five (5) calendar days of being informed of the engagement of the Subprocessor. Customer agrees to pay for authorized work completed, expenses incurred in accordance with the applicable Statement(s) of Work, and any non-cancellable commitments.

6. Customer Obligations. Customer agrees that, without limiting Company's obligations under Section 4(c) (Security), Customer is solely responsible for its use of the Services, including (i) making appropriate use of the Services to maintain a level of security appropriate to the risk in respect of the European Personal Data; (ii) securing the account authentication credentials, systems and devices Customer uses to access the Services; (iii) securing Customer's systems and devices that Company uses to provide the Services; and (iv) backing up European Personal Data. Customer represents, warrants, and covenants that (i) it shall comply with its obligations as a controller under the GDPR in

respect of its processing of European Personal Data and any processing instructions it issues to the Company as referred to in Section 4(a); (ii) that there is, and will be throughout the term of the Agreement, a valid legal basis for the processing by Company of European Personal Data in accordance with this DPA and the Agreement (including, any and all instructions issued by Customer from time to time in respect of such processing) for the purposes of all Applicable Data Protection Laws (including Article 6, Article 9(2) and/or Article 10 of the GDPR (where applicable)) and has provided all required notices and statements (including as required by Article 12-14 of the GDPR (where applicable)); and (iii) provided all required consents, in each case (i) and (ii) relating to the processing by Company of European Personal Data.. If Customer is a processor, Customer represents and warrants to the Company that Customer's instructions and actions with respect to European Personal Data, including its appointment of the Company as another processor, have been duly authorized by the relevant controller. Customer shall indemnify, defend and hold the Company harmless against any claims, actions, proceedings, expenses, damages and liabilities (including without limitation any governmental investigations, complaints and actions) and reasonable attorneys' fees arising out of Customer's violation of this Section 6. Notwithstanding anything to the contrary in the Agreement, Customer's indemnification obligations under this Section 6 shall not be subject to any limitations of liability set forth in the Agreement.

7. Data Transfer. The parties acknowledge and agree that Company's access to and processing of personal data under this DPA may involve a Restricted Transfer. Customer hereby consents to the transfer of European Personal Data to, and the processing of European Personal Data in, the United States of America and/or in any other jurisdiction in which Company or its subprocessors have operations. The relevant Transfer Mechanism(s) shall apply and have effect as required under the GDPR to establish a valid basis under Chapter V thereof in respect of any such Restricted Transfer.

   a. EU Restricted Transfers. To the extent that any processing of personal data under this DPA involves an EU Restricted Transfer, the Parties shall comply with their respective obligations set out in the SCCs. The Parties acknowledge and agree that where Customer is a controller of the transferred personal data, the parties will rely on the Module 2 (controller to processor) of the SCCs. However, where Customer is a processor of the transferred personal data, the Parties will rely on the Module 3 (processor to processor) of the SCCs. Any SCCs applicable in accordance with Section 7(a) shall be deemed: (i) populated in accordance with Part 1 of Exhibit C; and (ii) entered into by the Parties and incorporated by reference into this DPA.

   b. UK Restricted Transfers. To the extent that any processing of personal data under this DPA involves a UK Restricted Transfer, the parties shall comply with their respective obligations set out in the UK Addendum, which are hereby deemed entered into and incorporated by reference into this DPA under Part 2 of Exhibit C; and the parties agree that the manner of the presentation of the information included in the UK Addendum shall not operate or be construed so as to reduce the Appropriate Safeguards (as defined in Section 3 of Part 2 of the UK Addendum).

   c. Company may on notice vary this DPA and replace the relevant SCCs with:

      i. any new form of the relevant SCCs or any replacement therefor prepared and populated accordingly (e.g., standard data protection clauses adopted by the European Commission for use specifically in respect of transfers to data importers subject to Article 3(2) of the EU GDPR); or

      ii. another transfer mechanism, other than the SCCs,

      that enables the lawful transfer of European Personal Data to Company under this DPA in compliance with Chapter V of the GDPR.

   d. In the event of any conflict or inconsistency between:

      i. this DPA and the Agreement, this DPA shall prevail; or

      ii. any SCCs entered into and this DPA and/or the Agreement, the SCCs shall prevail in respect of the Restricted Transfer to which they apply.

   e. Swiss Restricted Transfer. In respect of processing covered hereby that is subject to the FADP, for the purposes of this DPA, including if and as applicable, in respect of any Swiss Restricted Transfer, the SCCs entered into in relation to a relevant Restricted Transfer; and the following terms are deemed to have the following substituted meanings:

      i. "GDPR" means the FADP;
      ii. "European Union", "Union" and "Member State(s)" each means Switzerland; and

iii. "supervisory authority" means the FDPIC.

In respect of any Swiss Restricted Transfers, nothing in any applicable SCCs (as deemed amended pursuant to Section 7(e)) should be interpreted or construed in such a way as would limit or exclude the rights of Data Subjects under Clause 18(c) of those SCCs (as deemed amended pursuant to Section 7(e)) to bring legal proceedings against the relevant party before the courts in Switzerland where Switzerland is that Data Subject's place of habitual residence.

f. Provision of full-form Data Transfer Mechanism(s). In respect of any given Restricted Transfer, if requested of either Party ("Requesting Party") by a Supervisory Authority or Data Subject, on specific written request (made to the contact details set out Exhibit A to this DPA, the other Party shall provide Requesting Party with an executed version of the relevant Data Transfer Mechanism(s) responsive to the request made of Requesting Party for countersignature by Requesting Party, onward provision to the relevant requestor and/or storage to evidence Requesting Party's compliance with Applicable Data Protection Laws.

8. Access to Personal Data by public authorities.

a. Company shall notify Customer immediately in writing of any subpoena or other judicial or administrative order by a public authority or proceeding seeking access to or disclosure of Personal Data. Such notification shall include details regarding the Data Subject concerned, Personal Data requested, the requesting authority, the legal basis for the request, and any responses provided.

b. Company shall (i) assess the legality of the request under applicable laws; (ii) seek interim measures to suspend the effects of the order until the competent court has decided on the merits of the case; (iii) exhaust all available remedies to challenge the request where there are legal grounds to do so; (iv) document such legal assessment and challenges to the request; (v) upon request, make such documentation available to Customer and competent Supervisory Authority. Company shall reasonably cooperate with Customer in relation to such request and provide Customer with prompt updates at regular intervals with regards to any additional information related to the request.

c. To the extent permitted by applicable laws, Customer shall have the right to defend such legal challenge in lieu of and/or on behalf of Company. Customer may, if it so chooses, seek a protective order. Company shall reasonably cooperate with Customer in such defense.

d. To the extent permitted by applicable laws, Company shall not disclose the Personal Data requested until all available remedies to challenge the request have been exhausted and shall provide the minimum of information permissible when responding to an order to disclose the Personal Data.

e. Where Company is prohibited from satisfying Section 8(a) under applicable laws, Company shall use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. Company agrees to document its best efforts in order to be able to demonstrate them on request of Customer.

f. Where Company becomes aware of any direct access by public authorities to Personal Data (including the reasonable suspicion thereof), Company shall promptly notify Customer with all information available to Company, unless otherwise prohibited by applicable laws.

9. Service Data. Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that the Company may collect, use and disclose Service Data for its own business purposes, such as: (i) for accounting, tax, billing, audit, and compliance purposes; (ii) to provide, improve, develop, optimize and maintain the Services; (iii) to investigate fraud, spam, wrongful or unlawful use of the Services; and/or (iv) as otherwise permitted or required by applicable law. In respect of any such processing described in this Section, Company: (i) independently determines the purposes and means of such processing; (ii) shall comply with Applicable Data Protection Laws (if and as applicable in the context); (iii) shall process such Service Data as described in Company's relevant privacy notices/policies, as updated from time to time; and (iii) where possible, shall apply technical and organizational safeguards to any relevant personal data that are no less protective than the Security Measures. For the avoidance of doubt, this DPA shall not apply to Company's collection, use, disclosure or other processing of Service Data, and Service Data does not constitute European Personal Data. From and after the CCPA Effective Date (as defined in Section 8), to the extent any such data is considered personal information (as defined in, and regulated by, the CCPA (as defined in Section 8)), the Company is the business (as defined in the CCPA) with respect to such data and accordingly shall process (as defined in the CCPA) such data in accordance with the Company's privacy policy and the CCPA.

10. CCPA Provisions. This Section 8 shall apply from and after the CCPA Effective Date (as defined below) and shall not apply before such CCPA Effective Date. As between the parties, Company is a service provider to Customer with respect to Consumer Information.

a. In this Section 9:

i. "CCPA" means the California Consumer Privacy Act of 2018.

ii. "CCPA Effective Date" means January 1, 2020 or the date the CCPA becomes enforceable, whichever is later.

iii. "Consumer Information" means any personal information that is processed by Company solely on behalf of the Customer.

iv. "Medical Information" means any Consumer Information, in electronic or physical form, regarding a California resident's medical history or medical treatment or diagnosis by a health care professional.

v. "Health Insurance Information" means a California resident's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the California resident, or any information in a California resident's application and claims history, including any appeals records.

vi. "Sensitive Consumer Information" means any Consumer Information that constitutes either of the following: (A) California resident's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (I) social security number; (II) driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific California resident; (III) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an California resident's financial account; (IV) Medical Information; (V) Health Insurance Information; (VI) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific California resident (except that unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes) or (B) a username or email address in combination with a password or security question and answer that would permit access to an online account. Sensitive Consumer Information does not include publicly available Consumer Information that is lawfully made available to the general public from federal, state, or local government records.

vii. The following terms have the meanings given in the CCPA: "personal information", "processing", "service provider", "sell", "selling", "sale" and "sold".

b. From and after the CCPA Effective Date, except as otherwise required by applicable law, Company shall:

i. implement and maintain commercially reasonable security procedures and practices appropriate to the nature of the Sensitive Consumer Information intended to protect such Sensitive Consumer Information from unauthorized access, destruction, use, modification, or disclosure;

ii. not retain, use or disclose Consumer Information for any purpose outside the scope of the business relationship of the parties and other than for the specific purpose of providing the Company Service (including retaining, using or disclosing the Consumer Information for a commercial purpose other than providing the Company Service) or as otherwise permitted by the CCPA as applicable to service providers;

iii. not collect or use Consumer Information except as reasonably necessary to provide the Company Service;

iv. not sell Consumer Information;

v. to the extent necessary, use commercially reasonable efforts to assist Customer, at Customer's expense, in Customer's fulfilment of Customer's obligation to respond to California residents' requests to exercise rights with respect to their Consumer Information under the CCPA; and

vi. use commercially reasonable efforts to assist Customer, at Customer's expense, to the extent necessary to support Customer's compliance with Customer's obligations under the CCPA.

c. Company understands the restrictions provided in Section 8(b)(ii) and (iv) and will comply with them.

d. Customer agrees that (i) it shall comply with its obligations under the CCPA in respect of its processing of Consumer Information and any processing instructions it issues to Company; and (ii) it has provided notice (including pursuant to Section 1798.135 of the CCPA) and obtained all consents and rights required by the CCPA for Company to process Consumer Information pursuant to the Agreement and this DPA. Customer shall indemnify, defend and hold Company harmless against any claims, actions, proceedings, expenses, damages and liabilities (including without limitation any governmental investigations, complaints and actions) and reasonable attorneys' fees arising out of Customer's violation of this Section 8(d).

e. Nothing in this DPA shall prevent Company from engaging its own service providers in the processing of Consumer Information, provided that Company shall enter into contractual arrangements with such service providers requiring a substantially similar level of data protection compliance and information security as that provided in this Section 8 with respect to Consumer Information.

11. PIPEDA Provisions. This Section 9 applies to the extent the Company has access to, collects, uses or discloses any Canadian Personal Information (as defined in Exhibit F to this DPA) while performing the Services under the Agreement that is subject to Canadian Privacy Laws (as defined in Exhibit F to this DPA), including *The Personal Information Protection and Electronic Documents Act* ("PIPEDA"). Attached to this DPA, as Exhibit F, is the PIPEDA Data Protection Schedule, which forms part of the DPA.

12. Integration. This DPA, including the SCCs, and the Agreement constitute the parties' entire agreement and understanding with respect to the subject matter hereof. Except as set forth in Sections 5 and 8(d), the obligations contained in this DPA are (i) subject to any limitations of liability set forth in the Agreement and (ii) in addition to the other obligations contained in the Agreement. In the event of a conflict between this DPA and any other terms in the Agreement, the terms of this DPA will govern. For the avoidance of doubt, to the extent that the Agreement excludes any types of information from confidentiality obligations, those exclusions shall not apply to information relating to any identified or identifiable natural person.

13. Integration and Liability. This DPA and the Agreement constitute the parties' entire agreement and understanding with respect to the subject matter hereof. In no event shall Company's total liability under or in relation to this DPA and the Agreement, regardless of the basis of the claim, exceed the total fees paid or payable by Customer to Company under the Agreement in the year immediately preceding the claim.

Exhibit A

Data Processing Details

1. Details of the Parties

Company / Data Importer Details

Name:	Tamr, Inc.
Address:	66 Church St., Cambridge, MA 02138
Contact Details for Data Protection:	Role: Privacy/legal team Email: privacy@tamr.com
Tamr Activities:	Tamr works with leading organizations around the world to solve their data challenges. It is a data mastering solution that offers cloud-native, SaaS, and hybrid deployments.
Role:	Processor

Customer / Data Exporter Details

Name:	The entity or other person who is a counterparty to the Agreement
Address:	As set out in the Agreement
Contact Details for Data Protection:	Customer's contact details are Customer's contact details submitted by Customer and associated with Customer's account for the Company Services – unless otherwise notified to Company via email.
Customer Activities:	Customer's activities relevant to this DPA are the use and receipt of the Company Services under and in accordance with, and for the purposes anticipated and permitted in, the Agreement as part of its ongoing business operations.
Role:	▪ Where Module Two applies: Controller ▪ Where Module Three applies: Processor

2. Subject Matter, Nature, Purpose and Duration of the Processing

a. Type of European Personal Data: May include

Representatives of Customer: First name, last name, title, workplace address, email address, telephone number(s), internet protocol address, analytics/audit logging features (logins, file views, modifying data); browser type and version, time zone setting and location, username, browser plug-in types and versions, operating system and platform and other technology on the devices used to access the Service, website usage data, website user marketing and communication preferences; and

Individuals whose European Personal Data is included in files uploaded to the Service by Customer or are submitted by Individuals invited to use the Service: Any European Personal Data included in files uploaded to the Service by Customer and/or its representatives, or uploaded to the Service by the Data Subjects themselves, the extent of which is determined and controlled by Customer in its sole discretion, including but not limited to: First name, last name, contact information, email address, IP address, information concerning their use of the Service, and any other data pursuant to the Agreement and this DPA.

b. Categories of Data Subject:

Representatives of Customer; Individuals whose European Personal Data is included in files uploaded to the Service by Customer or uploaded to Service by the data subjects invited to use the Service.

c. Subject Matter and Purposes European Personal Data Processing:

Company's provision of the Service to Customer in accordance with the Agreement.

d. Nature of the Processing:

The European Personal Data will be subject to basic processing, including but not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction for the purpose of providing the Service by the Company to Customer in accordance with the terms of the Agreement.

Exhibit B

Subprocessors

Subprocessors	Data Processing Location	Service
Google Cloud Platform	US	Data Center
Google Cloud Platform	EU - Belgium	Data Center
Loqate	UK	Address Validation
SmartyStreets	US	Address Validation
Dun & Bradstreet	US	Organizational data enrichment
Google Maps	US	Address Validation
Newrelic	US	Log Aggregation contains customer IP addresses
Alcazar	US	Phone number validation & enrichment
Heap.io	US	Collects IP addresses, analytics

Exhibit C

Part 1: POPULATION OF SCCs

Notes:

- The SCCs populated in accordance with this Part 1 of Exhibit C are incorporated by reference into and form an effective part of the DPA.
- Where Customer is a controller of the transferred Personal Data, the Parties will rely on Module 2 (controller to processor). Where Customer is a processor of the transferred Personal Data, the Parties will rely on Module 3 (processor to processor).
- Capitalized terms used in this Part 1 of Exhibit C have the meanings given to them in the DPA.

1. SIGNATURE OF THE SCCs:

1.1 Where applicable in accordance with Paragraph 7(a) of the DPA:

(a) each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs; and

(b) those SCCs are entered into by and between the Parties with effect from (i) the Addendum Effective Date; or (ii) the date of the first EU Restricted Transfer to which they apply in accordance with Paragraph 7(a) of the DPA, whichever is the later.

2. POPULATION OF THE BODY OF THE SCCs

2.1 For each Module of the SCCs, the following applies as and where applicable to that Module and the Clauses thereof:

(a) The optional 'Docking Clause' in Clause 7 is not used and the body of that Clause 7 is left intentionally blank.

(b) In Clause 9:

(i) OPTION 2: GENERAL WRITTEN AUTHORISATION applies, and the minimum time period for advance notice of the addition or replacement of Sub-Processors shall be the advance notice period set out in Paragraph 5 of the DPA; and

(ii) OPTION 1: SPECIFIC PRIOR AUTHORISATION is not used and that optional language is deleted; as is, therefore, Annex III to the Appendix to the SCCs.

(c) In Clause 11, the optional language is not used and is deleted.

(d) In Clause 13, all square brackets are removed and all text therein is retained.

(e) In Clause 17:

(i) OPTION 1 applies, and the Parties agree that the SCCs shall governed by the law of Ireland; and

(ii) OPTION 2 is not used and that optional language is deleted.

(f) For the purposes of Clause 18, the Parties agree that any dispute arising from the SCCs shall be resolved by the courts of Ireland, and Clause 18(b) is populated accordingly.

2.2 In this Paragraph 2, references to "Clauses" are references to the Clauses of the SCCs.

3. POPULATION OF ANNEXES TO THE APPENDIX TO THE SCCs

3.1 Annex I to the Appendix to the SCCs is populated with the corresponding information detailed in Exhibit A to the DPA, with: Customer being 'data exporter' and Company being 'data importer' with respect to EU Restricted Transfers involving European Personal Data.

3.2 Part C of Annex I to the Appendix to the SCCs is populated as below:

The competent supervisory authority shall be determined as follows:

- Where the data exporter is established in an EU Member State: the competent supervisory authority shall be the supervisory authority of that EU Member State in which the data exporter is established.
- Where the data exporter is not established in an EU Member State, Article 3(2) of the GDPR applies and the data exporter has appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State in which the data exporter's EU representative relevant to the processing hereunder is based (from time-to-time).
- Where the data exporter is not established in an EU Member State, Article 3(2) of the GDPR applies, but the data exporter has not appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State notified in writing to the data importer's contact point for data protection identified Exhibit A to the DPA, which must be an EU Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located.

3.3 Annex II to the Appendix to the SCCs is populated as below:

Please refer to Paragraph 4 (c) of the DPA and Exhibit C1 (Security) to the DPA.

Part 2: International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Notes:

- The UK Transfer Addendum set out in this Part 2 of Exhibit C is incorporated into and forms an effective part of the DPA.
- Unless otherwise defined in this Part 2 of Exhibit C, capitalized terms used in this Part 2 of Exhibit C have the meanings given to them in the DPA.

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

<u>Part 1:</u> Tables

Table 1: Parties

All relevant information and details are as set out in Exhibit A to the DPA and it is noted that the UK Addendum is deemed to have been signed by the Parties pursuant to and with effect from the Addendum Effective Date.

Table 2: Selected SCCs, Modules and Selected Clauses

The version of the Approved SCCs which this UK Addendum is appended to, detailed below, including the Appendix Information:

Date: Addendum Effective Date
Reference (if any): the SCCs
Other identifier (if any): n/a

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties: As set out in Exhibit A to the DPA
Annex 1B: Description of Transfer: As set out in Exhibit A to the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in Exhibit C1 to the DPA
Annex III: List of Sub processors (Modules 2 and 3 only): n/a

Table 4: Ending this Addendum when the Approved Addendum Changes

Which Parties may end this Addendum as set out in Section 19: Data Importer

Part 2: Mandatory Clauses

The Mandatory Clauses are incorporated by reference and form a binding and effective part of this UK Transfer Addendum.

Exhibit C1 - Data Security Exhibit

1. Program. Company will implement and maintain a comprehensive written information security program ("**Information Security Program**"), which contains appropriate administrative, technical and organizational safeguards that comply with this Exhibit C1 and that ensures the security, integrity, availability, resilience and confidentiality of Customer's Confidential Information and that meet or exceed generally accepted industry standards.
2. Access Controls. Company will: (a) abide by the "principle of least privilege," pursuant to which Company will permit access to Customer's Confidential Information by its personnel solely on a need-to-know basis; (b) promptly terminate its personnel's access to Customer's Confidential Information when such access is no longer required for performance under the Agreement; (c) log the details of any access to Customer's Confidential Information, and retain such records for no less than 90 days; and (d) be responsible for any processing of Customer's Confidential Information by its personnel.
3. Account Management. Company will use reasonable measures to manage the creation, use, and deletion of all account credentials used to access the Company Systems, including by implementing: (a) a segregated account with unique credentials for each user; (b) strict management of administrative accounts; (c) password best practices, including the use of strong passwords and secure password storage; and (d) periodic audits of accounts and credentials. **"Company Systems"** means the facilities, systems, equipment, hardware, and software used in connection with Company's Processing of Customer's Confidential Information.
4. Vulnerability Management. Company will: (a) use automated vulnerability scanning tools to scan the Company Systems; (b) log vulnerability scan reports; (c) conduct periodic reviews of vulnerability scan reports over time; (d) use patch management and software update tools for the Company Systems; (e) prioritize and remediate vulnerabilities by severity; and (f) use compensating controls if no patch or remediation is immediately available.
5. Incident Response. Company will notify Customer of any accidental or unlawful destruction, loss, or alteration of Customer Confidential Information, or any unauthorized access to, or use or disclosure of, Customer Confidential Information ("**Security Incident**") without undue delay (and in any event within 24 hours) after becoming aware of any actual or reasonably suspected Security Incident. In any such notice, Company will include: (a) a description of the Security Incident, including the number and categories of any individuals affected, (b) categories and number of records concerned, (c) types of information affected, (d) date and time of the Security Incident, (e) a summary of the circumstances that caused the Security Incident and any ongoing risks that the Security Incident poses, (f) a description of the measures proposed or taken by Company to address the Security Incident, and (e) any other information reasonably requested by Customer relating to the Security Incident. If and solely to the extent it is not possible to provide the above information at the same time, the information may be provided in phases without undue delay. Company will provide reasonable assistance to Customer to investigate, remediate or take any other action Customer deems reasonably necessary regarding the Security Incident, including in connection with any dispute, inquiry, investigation or claim concerning the Security Incident.
6. Security Segmentation. Company will use reasonable measures to monitor, detect and restrict the flow of information on a multi-layered basis within the Company Systems using tools such as firewalls, proxies, and network-based intrusion detection systems.
7. Data Loss Prevention. Company will use reasonable data loss prevention measures to identify, monitor and protect Customer's Confidential Information in use, in transit and at rest. Such data loss prevention processes and tools will include: (a) automated tools to identify attempts of data exfiltration; (b) the prohibition of, or secure and managed use of, portable devices; (c) use of certificate-based security; and (d) secure key management policies and procedures.
8. Encryption. Company will encrypt, using industry standard encryption tools, Customer's Confidential Information that Company: (i) transmits or sends wirelessly or across public networks or within the Company Systems; (ii) stores on laptops or storage media, and (iii) stores on portable devices or within the Company System. Company will safeguard the security and confidentiality of all encryption keys associated with encrypted information.
9. Pseudonymization. Company will, where possible and consistent with the Services, use industry standard and reasonable pseudonymization techniques to protect Customer's Confidential Information.
10. Secure Software Development. Company represents and warrants that any software used in connection with the processing of Customer's Confidential Information is or has been developed using secure software development practices, including: (a) segregating development and production environments; (b) filtering out potentially malicious character sequences in user inputs; (c) using secure communication techniques, including encryption; (d) using sound memory management practices; (e) using web application firewalls to address common web application attacks such as cross-site scripting, SQL injection and command injection; (f) implementing the OWASP Top Ten recommendations, as applicable; (g) patching of software; (h) testing object code and source code for common coding errors and vulnerabilities using code analysis tools; (i) testing of web applications for vulnerabilities using web application scanners; and (j) testing software for performance under denial of service and other resource exhaustion attacks.

11. Physical Safeguards. Company will maintain physical access controls that secure relevant Company Systems used to Process any Customer's Confidential Information, including an access control system that enables Company to monitor

and control physical access to each Company facility, which includes 24x7 physical security monitoring systems and the use of trained and experienced security guards.

12. Administrative Safeguards. Prior to providing access to Customer's Confidential Information to any of its personnel, Company will: (a) ensure the reliability of such personnel, including by performing background screening (to the extent permitted by Data Protection Law); and (b) provide appropriate security training to such personnel to ensure such personnel can comply with the obligations under this Exhibit C1. Company will periodically provide additional training to its personnel as may be appropriate to help ensure that Company's Information Security Program meets or exceeds prevailing industry standards.

Exhibit F

PIPEDA Data Protection Schedule

1. **Context.** The terms and conditions included in this Exhibit F shall apply to the extent that the Company has access to, collects, uses or discloses any Canadian Personal Information (as defined below) while performing the Services under the Agreement. The obligations under this Exhibit F shall survive the termination or expiration of the DPA or any renewal or extension thereof.

2. **Definitions.** For the purposes of this exhibit:

(a) **"Canadian Personal Information"** means information about an identifiable individual or personal health information that is regulated by any Privacy Laws that is transferred to, collected by, compiled, stored, or otherwise under the control or custody of the Company pursuant to the Agreement and solely to perform the Services, and that is: (i) used to provide the Services; (ii) is about the Customer's Customers, employees, past employees, or other individuals to whom the Customer is under an obligation to comply with Privacy Laws; or, (iii) is otherwise held by the Company on behalf of the Customer; and

(b) **"Privacy Laws"** means any applicable Canadian privacy laws including, without limitation, the *Personal Information Protection and Electronic Documents Act* (Canada), or any substantially similar provincial laws, and any regulations, policies, requirements guidelines, or standards established, formulated or otherwise made pursuant thereto or in accordance therewith.

3. **Control of and Rights in Canadian Personal Information.** As between the Company and the Customer, control of Canadian Personal Information shall always remain with the Customer. The Company acknowledges and agrees that nothing gives the Company any right, title or interest in any Canadian Personal Information.

4. **Access to and Use of Canadian Personal Information**. The Company may access and use Canadian Personal Information on a need-to-know basis as expressly authorized by the Customer for the sole and express purpose of fulfilling its obligations under the Agreement. Any such access or use of Canadian Personal Information by the Company shall be to the minimum extent necessary for the Company to fulfill its obligations under the Agreement.

5. **Return or Destruction of Canadian Personal Information.** At the choice of Customer, Company will delete or return all Canadian Personal Information to Customer within ninety (90) days after the end of the provision of the Service to Customer and delete existing copies unless applicable law requires retention of Canadian Personal Information.

6. **Location of the Canadian Personal Information**. Unless the Customer has given its prior written consent, the Company may possess and maintain the Canadian Personal Information only in Canada, the United States, and India.

7. **Security of Canadian Personal Information.** Without limiting any other provision in this Schedule or the Agreement with regard to the security of information, the Company shall have in place reasonable policies, procedures and safeguards to protect the confidentiality and security of the Canadian Personal Information. The Company shall ensure the physical security of the Canadian Personal Information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, disposal, loss or modification.

   The Company will protect the security and confidentiality of the Canadian Personal Information to at least the same standard as the Company protects its own confidential information of a similar nature and, in any event, to at least the standard required by applicable Privacy Laws.

8. **Audit.** The Company will provide (a) the Customer's internal auditor; and/or (b) a nationally recognized audit firm appointed by the Company, with reasonable access to relevant books, records and facilities under the control of Company in order to conduct appropriate audits, examinations and inspections to ensure the Company's compliance with this Exhibit. Such audits shall be conducted on reasonable notice and shall not unreasonably interfere with the Company's operations. Notwithstanding the foregoing, in no event shall Customer have access to the information of any other Customer of the Company and the disclosures made pursuant to this Section 8 ("Canadian Audit Information") shall be held in confidence as the Company's Confidential Information and subject to any confidentiality obligations in the Agreement. Without limiting the generality of any provision in the Agreement, Customer shall employ the same degree of care to safeguard Canadian Audit Information that it uses to protect its own confidential and proprietary information and in any event, not less than a reasonable degree of care under the circumstances, and Customer shall be liable for any improper disclosure or use of Canadian Audit Information by Customer or its agents.

9. **Breach Notification.** The Company shall promptly notify the Customer in writing in the event the Company becomes aware of, or reasonably suspects, any unauthorized or improper access to, use of or disclosure of any Canadian Personal Information. The Company agrees to take all reasonable steps to cooperate with the Customer in relation to, and (to the extent such authorized access to, use or disclosure of Canadian Personal Information is caused by the negligent acts or

omissions of the Company) to mitigate any harmful effect resulting from, any such unauthorized access to, use or disclosure of Canadian Personal Information.