1470 Peel Street, Suite 500
Montreal, QC, H3A 1T1, Canada

Explorance

Data Processing Agreement

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Master Services Agreement**")

between

Customer Name

(Data Controller)

and

Explorance Inc.

(Data Processor)

This Data Processing Agreement ("Agreement") is entered into on ("Effective Date" noted in the Master Services Agreement) by and between:

[Customer], an entity incorporated and registered in [Customer Country] and having its registered office at [Customer Address] ("Data Controller")

and

Explorance Inc., a company incorporated and registered in Canada and having its registered office at 1470 rue Peel #500, Montreal, QC H3A 1T1 ("Data Processor").

RECITALS

WHEREAS, the Data Processor agrees to provide data processing services selected in Table 1 below ("the Services") to the Data Controller in accordance with the terms and conditions of this Agreement.

Table 1

☐	**Blue** - Explorance Canada Hosted
☐	**BlueX** - Explorance Canada Hosted
☐	**Blue** - Azure Netherlands
☐	**Blue** - Azure Australia
☐	**MLY** - Azure USA **Optional Modules:** Redaction ☐ Translation ☐ Summarization ☐
☐	**MLY** - Azure Netherlands **Optional Modules:** Redaction ☐ Translation ☐ Summarization ☐
☐	**MLY -** Azure Australia **Optional Modules:** Redaction ☐ Translation ☐ Summarization ☐
☐	**Metrics That Matter (MTM)** - Azure USA

WHEREAS, the Data Controller and the Data Processor (together "the Parties") wish to lay down their rights and obligations concerning the processing of personal data in accordance with the applicable data protection laws.

WHEREAS, the parties acknowledge that the attached Schedules, listed and referred to herein, are an integral part of this Agreement and are incorporated by reference.

NOW, THEREFORE, in consideration of the mutual covenants herein contained, the Parties hereby agree as follows:

1. Definitions and Interpretation

1.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1. "Data Protection Laws" means all applicable laws relating to data protection, privacy, and the processing of personal data, including, but not limited to, where applicable, the General Data Protection Regulation (EU) 2016/679 ("GDPR"), and the UK Data Protection Act 2018 and its attendant amendments.

1.1.2. "Personal Data" means any information relating to an identified or identifiable natural person as defined in the Data Protection Laws.

1.1.3. "Processing" means any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

1.1.4. The terms, “Controller”, “Data Subject”, “Personal Data”, “Personal Data Breach”, and “Processing” shall have the same meaning as in the Data Protection Laws, and their cognate terms shall be construed accordingly.

2. Subject Matter of the Agreement

2.1. The Data Controller hereby appoints the Data Processor to process Personal Data on behalf of the Data Controller in accordance with the terms and conditions set out in this Agreement.

3. Duration

3.1. This Agreement shall commence on the Effective Date and shall continue until terminated by either party in accordance with Section 14 of this Agreement.

4. The Services

4.1. The scope of the data processing services heretofore referenced here and in the Master Services Agreement as "Blue" which are curated by the Data Processor, are detailed in Schedule 1.

5. Nature and Purpose of Processing

5.1. The Data Processor shall process Personal Data solely for the purposes detailed in Schedule 3 of this Agreement and in accordance with the documented instructions of the Data Controller.

6. Categories of Data Subjects

6.1. The categories of data subjects whose Personal Data will be processed under this Agreement as defined by the Data Controller include but are not limited to, at the sole discretion of the Data Controller, the categories detailed in Schedule 5 of this Agreement.

7. Categories of Personal Data

7.1. The categories of Personal Data to be processed under this Agreement include but are not limited, at the sole discretion of the Data Controller, to what is detailed in Schedule 2 of this Agreement.

8. Obligations of the Data Controller

8.1. The Data Controller shall ensure that all processing instructions provided to the Data Processor are lawful, documented, and comply with applicable Data Protection Laws.

8.2. The Data Controller shall be responsible for establishing and maintaining a valid legal basis for the processing of Personal Data, including obtaining any required consents.

8.3. The Data Controller shall ensure that Personal Data provided to the Data Processor is accurate, relevant, and limited to what is necessary for the purposes of processing.

8.4. The Data Controller shall be responsible for providing all required notices to Data Subjects and for fulfilling transparency obligations under applicable Data Protection Laws.

8.5. The Data Controller shall respond to and manage Data Subject rights requests and shall instruct the Data Processor as necessary to support such requests.

8.6. The Data Controller shall ensure appropriate technical and organizational measures are in place on its own systems and shall assess whether the Data Processor's measures are adequate for the intended processing.

8.7. The Data Controller shall be responsible for determining retention periods and for instructing the Data Processor regarding deletion or return of Personal Data at the end of processing.

8.8. The Data Controller shall be responsible for conducting any required data protection impact assessments and for consulting supervisory authorities where required by law.

9. Obligations of the Data Processor

9.1. The Data Processor shall process Personal Data only on documented instructions from the Data Controller, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by applicable law.

9.2. The Data Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9.3. The Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including measures to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Further details on such measures are listed in Schedule 4.

9.4. The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Data Protection Laws, taking into account the nature of processing and the information available to the Data Processor.

9.5. The Data Processor shall, at the choice of the Data Controller, delete or return all Personal Data to the Data Controller after the end of the provision of services relating to processing, and delete existing copies unless applicable law requires storage of the Personal Data. Until the

data is deleted or returned, the Data Processor shall continue to ensure compliance with this Agreement.

9.6. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Data Controller or another audit or mandated by the Data Controller at the Data Controller's own cost.

10. Sub-Processors

10.1. The Data Processor engages the Sub-Processors specified in Schedule 6.

10.2. The Data Processor shall not engage another processor ("Sub-Processor") without prior specific or general written authorization of the Data Controller. In the case of general written authorization, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of Sub-Processors, thereby giving the Data Controller the opportunity to object to such changes.

10.3. Where the Data Processor engages a Sub-Processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in this Agreement shall be imposed on that Sub-Processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Data Protection Laws.

11. Data Subject Rights

11.1. Taking into account the nature of the Processing, the Data Processor shall assist the Data Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligations, to respond to requests to exercise a Data Subject's rights under the Data Protection Laws.

11.2. The Data Processor shall:

11.2.1. Promptly notify the Data Controller if it receives a request from a Data Subject under any Data Protection Law in respect of the Data Controller's Personal Data; and

11.2.2. Ensure that it does not respond to such request except on the documented instructions of the Data Controller or as required by applicable laws to which the Data

Processor is subject, in which case the Data Processor shall to the extent permitted by applicable laws inform the Data Controller of that legal requirement before the Data Processor responds to the request.

12. Personal Data Breach

12.1. In the event of a breach of Personal Data within the Data Processor's information systems that has been found to affect the Data Controller's Personal Data, the Data Processor shall notify the Data Controller without undue delay. The Data Processor will provide the Data Controller with sufficient information to allow the Data Controller to meet any obligations to report or inform the affected Data Subjects of the Personal Data Breach under the Data Protection Laws.

12.2. The Data Processor shall co-operate with the Data Controller and take reasonable commercial steps to assist the Data Controller in the investigation, mitigation and remediation of each such Personal Data Breach.

13. Audit Rights

13.1. During the life of this Agreement, upon written request, the Data Processor shall make available to the Data Controller, the Data Processor's annual SOC 2 Type 2 attestation report or other industry equivalent report or certification.

14. Data Transfer

14.1. The Data Processor may not transfer or authorize the transfer of Personal Data to entities other than the Data Controller or those listed in Schedule 6, or to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Data Controller. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the Personal Data are adequately protected. To achieve this, the Parties shall, in the absence of an adequacy decision, rely on EU or UK approved additional safeguards.

15. Termination

15.1. Either party may terminate this Data Processing Agreement for any reason by providing 30 days' written notice to the other party.

16. General Terms

16.1. Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

16.2. Notices. All notices and communications given under this Agreement must be in writing and will be delivered either personally, sent by post, or sent by email to the address or email address set out in the heading of this Agreement or at such other addresses as notified from time to time by the Parties changing the notification address.

16.3. The Parties agree that the Data Processing Agreement (DPA) forms an integral part of the Master Services Agreement (MSA) with which this DPA is associated. The terms and conditions set forth in the DPA shall apply to all processing of Personal Data carried out under the MSA. In the event of any conflict between the terms of this MSA and the DPA, the terms of the DPA shall prevail with respect to data protection and processing matters.

17. Governing Law and Jurisdiction

17.1. This Agreement is governed by the laws of _____.

17.2. Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of _____, subject to possible appeal to _____.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

On behalf of the Data Controller:

Company Name:

Signature: _____

Name: _____

Title: _____

Date Signed: _____

On behalf of the Data Processor:

Company Name: Explorance Inc.

Signature: _____

Name: Sophiann Hayet

Title: Interim Data Protection and Risk Officer

Date Signed: _____

Schedule 1

Data Processing Activities

1. Description of the data processing carried out on behalf of the Data Controller

In addition to the information provided elsewhere in the Agreement, the Parties wish to document the following information in relation to the data processing activities. The data processing details, and Privacy Policy can be found on the Explorance website at: https://explorance.com

For Blue Services:

The personal data transferred will be subject to the following basic processing activities:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organisation, and structuring
- Protecting data, including restricting, encrypting, and security testing
- Returning data to the Data Controller
- Erasing data, including destruction and deletion

For MLY Services:

The data processing performed by the Data Processor on behalf of the Data Controller relates to the Data Controller leveraging specialized models that accurately consume, analyze, and categorize comments, tying them with context-specific insights.

For Metrics That Matter (MTM) Services:

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is to provide services to the Data Controller to measure the effectiveness of their learning and development process.

2. Frequency of data transfer

The transfer will be performed on a continuous basis.

Schedule 2

Categories of Personal Data

For Blue & BlueX Services:

The Personal Data transferred may include the following categories of data:

- Name
- Email
- Username
- IP Address
- For Higher Ed: Enrollment data, including connections to courses, study programs, and tenure
- End-user responses to the evaluation or survey

For MLY Services:

- Name
- Email
- Comments from end-user responses to the evaluation or survey

For MTM Services:

- Name
- Email
- Username
- IP Address
- Department demographics, including role/title, department name, and connections to peers, direct reports, tenure, and manager
- End-user responses to the evaluation or survey

Special Categories of Personal Data

None

Schedule 3

Purpose of processing

For Blue & BlueX Services: The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is to provide services to the Data Controller to perform online course evaluations, surveys, and/or 360 feedback assessments.

For MLY Services: The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is to provide quantitative feedback and insights to the Data Controller through comment analysis.

For MTM Services: The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is to provide services to the Data Controller to measure the effectiveness of their learning and development process.

Personal data that the Data Processor processes on behalf of the Data Controller may not be used for any other purpose without the prior approval of the Data Controller.

Schedule 4

Organisational Security Measures

Explorance secures client data by, but not limited to:

- Setting the tone of IT infrastructure and data governance at the top of the organization.
- Establishing clear roles and responsibilities.
- Mandating InfoSec training at new-hire and on an annual basis.
- Granting access to key systems on a least privilege basis.
- Performing third-party vendor security risk assessments.
- Employing security practices from established frameworks such as OWASP, ISO-27001, and NIST.
- Recording and managing its information assets (physical and logical).
- Encrypting data in transit and at rest.
- Centrally managing infrastructure and anti malware (servers and laptops).
- Monitoring and logging all systems and events.
- Managing changes to the environments.
- Performing regular backups of all key systems.

Schedule 5

Categories of Data Subjects

The categories of data subjects whose personal data is transferred:

- Students and pupils

Each category includes current, past, and prospective Data Subjects. Where any of the following is itself a business or organisation, it includes their staff.

Schedule 6

List of Sub-processors by Service Type

Blue & BlueX Explorance Canada Hosted			
Sub-Processor	**Purpose**	**Country**	**Address**
SendGrid	Email SMTP / SMS Provider	USA	1801 California St, Denver CO 80202 / legal@sendgrid.com

Blue Azure Netherlands			
Sub-Processor	**Purpose**	**Country**	**Address**
Microsoft Azure	Infrastructure as a Service	Netherlands (Production) Ireland (Offsite backup)	Evert van de Beekstraat 354 1118 CZ Schiphol, Nederland
SendGrid	Email SMTP / SMS Provider	USA	1801 California St, Denver CO 80202 / legal@sendgrid.com

Blue Azure Australia			
Sub-Processor	**Purpose**	**Country**	**Address**
Microsoft Azure	Infrastructure as a Service	Australia (Production and offsite backup)	Level 24-30, 1 Denison Street, North Sydney, NSW, 2060
SendGrid	Email SMTP / SMS Provider	USA	1801 California St, Denver CO 80202 / legal@sendgrid.com

MLY Azure USA			
Sub-Processor	**Purpose**	**Country**	**Address**
Microsoft Azure	**MLY Portal and Data Controller Database** - Infrastructure as a Service	USA	One Microsoft Way Redmond, WA 98052 +1 (425) 882 8080
Microsoft Azure	**Comment Analysis** - Infrastructure as a Service	USA	One Microsoft Way Redmond, WA 98052 +1 (425) 882 8080
SendGrid	Email SMTP / SMS Provider	USA	1801 California St, Denver CO 80202 / legal@sendgrid.com

MLY Azure Netherlands			
Sub-Processor	**Purpose**	**Country**	**Address**
Microsoft Azure	**MLY Portal and Data Controller Database** - Infrastructure as a Service	Netherlands (Production) Ireland (Offsite backup)	Evert van de Beekstraat 354 1118 CZ Schiphol, Nederland
Microsoft Azure	**Comment Analysis** - Infrastructure as a Service	USA	One Microsoft Way Redmond, WA 98052 +1 (425) 882 8080
SendGrid	Email SMTP / SMS Provider	USA	1801 California St, Denver CO 80202 / legal@sendgrid.com

MLY Azure Australia			
Sub-Processor	**Purpose**	**Country**	**Address**
Microsoft Azure	**MLY Portal and Data Controller Database** - Infrastructure as a Service	Australia (Production and offsite backup)	Level 24-30, 1 Denison Street, North Sydney, NSW, 2060
Microsoft Azure	**Comment Analysis** - Infrastructure as a Service	USA	One Microsoft Way Redmond, WA 98052 +1 (425) 882 8080
SendGrid	Email SMTP / SMS Provider	USA	1801 California St, Denver CO 80202 / legal@sendgrid.com

Metrics That Matter (MTM) Azure USA			
Sub-Processor	**Purpose**	**Country**	**Address**
Microsoft Azure	Infrastructure as a Service	USA	One Microsoft Way Redmond, WA 98052 / +1 (425) 882 8080
SendGrid	Email SMTP / SMS Provider	USA	1801 California St, Denver CO 80202 / legal@sendgrid.com

Schedule 7

Generative AI Usage

1. **Supervised Learning Deep Neural Network**
    - MLY's core functionality is driven by a supervised learning model implemented using deep neural network architecture focused on classification or regression tasks to map inputs to outputs. By contrast, GPT models are trained to model the distribution of input data and generate new similar data, such as natural language generation. In terms of data privacy, a key distinction is that the DNN does not generate text, thus obviating the potential for privacy leakage in its output versus the potential for privacy leakage inherent when training GPT models.
2. **Use of Generative Artificial Intelligence**
    - The MLY platform offers optional Generative Pre-trained Transformer (GPT) modules to provide a) language translation service and/or b) redaction suggestions and/or c) summarization services.
3. **Data Input and Processing**
    - The GPT modules process the data input by the Controller (customer) exclusively for the purpose of providing the requested service functionality. No personal data or other input provided by the Controller is stored, retained, or used by the GPT modules beyond the duration of the specific processing request. The GPT modules operate in a stateless manner, meaning that data input does not persist beyond the immediate processing required to deliver results.
4. **No Use for Training or Model Improvement**
    - The Processor (Explorance) confirms that any data input by the Controller or processed through the GPT modules is not used to train, improve, or otherwise modify the respective GPT LLMs. The optional GPT modules used by the Processor are pre-trained, and no further training is conducted using the Controller's data.
5. **Compliance with Applicable Laws**
    - The Processor ensures that the use of GPT modules is compliant with applicable data protection laws, including but not limited to the General Data Protection Regulation (GDPR). The Processor shall not engage in any processing activities with the GPT modules that contravene the Controller's instructions or violate applicable data protection regulations.