DATA PROCESSING AGREEMENT

Contents

Data Processing Agreement ("DPA")

between **_____**, below referred to as "**Controller**", and **SMART Technologies ULC**, below referred to as "**Processor**".

1. Background and purpose

1.1. According to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**"), it is required to have a written agreement between the Controller and the Processor that governs the processing of personal data that the Processor shall pursue on behalf of the Controller.

1.2. This DPA between the Controller and the Processor ("**Parties**") regulates the outset obligations that the Processor shall have when processing personal data on behalf of the Controller. The purpose of this agreement is to ensure that the Processor processes personal data in accordance with the Controller's instruction and applicable law, which includes applicable law within EU/EEC, different regulations and decisions issued by authorities and recommendations from the European Data Protection Board that are applicable when processing personal data within the scope of the DPA.

1.3. No student data should be provided to Processor from the Controller.

2. Definitions

2.1. The definitions set-out in this DPA shall have the corresponding definitions as stated in the GDPR and stated herein.

3. Processing of personal data

3.1. The Parties have entered into this DPA to govern the terms and conditions for the Processor's processing of personal data pursuant to the applicable Processor's Terms of Service and Privacy Policy ("**TOSP**") which should be pursued by the Processor on behalf of the Controller.

3.2. The Processor and persons that act on behalf of the Processor may process personal data only in accordance with the DPA and any additional written instructions that the Controller may provide from time to time.

3.3. The Processor shall only process personal data in order to fulfil their obligations according to the TOSP. If the Processor has not received instructions or is uncertain of the purpose of processing that is needed in order to perform a certain task that means or could mean processing of personal data, shall that Processor, without undue delay, inform the Controller about the matter and wait until further instructions are provided from the Controller.

3.4. The Processor shall at any given time follow the Processor's obligations according to applicable law and stay informed about such obligations regarding the processing of personal data according to the DPA. The Processor shall also at any given time follow the codes of conduct or certification

that the Processor has committed to follow. The Processor shall at least, within the scope of this DPA, nominate an appropriate contact person for specific data protection issues.

3.5. The Processor commitments to follow applicable law, which shall, in all cases, be interpreted in relation to the nature of the Processor's services and typically means that the processor shall not in its sole discretion collect personal data or use personal data for any other purpose other than to fulfil the agreed delivery according to the main reseller agreement. The Processor shall not, in any event, without an order from a relevant authority or mandatory law:

a) collect or disclose personal data from or to any third party, if the Parties have not agreed anything else in writing,

b) change the method for processing personal data that would increase the risk for the data subjects fundamental freedoms and rights,

c) copy or recreate personal data for the Processor's sole use, or

d) in any other way process personal data for purposes other than the ones that are stated in the Main TOSP and appurtenant appendices.

3.6. The Processor shall take all reasonable measures that are required according to article 32 in the GDPR. The additional measurements that should be taken into account are stated in the appended instructions from the Controller.

3.7. The Processor shall assist the Controller by taking suitable technical and organisational security measures, to the extent possible, to enable the Controller to perform its obligations as a Controller and its obligations in relation to requests regarding the exercise of the data subjects rights in accordance with Chapter III of the GDPR.

3.8. The Processor shall assist the Controller in ensuring that the obligations as stated in articles 33-36 in the GDPR can be fulfilled, taking into consideration the type of processing and the information that the Processor has access to.

4. Records of processing activities

4.1. The Processor or its representative shall maintain a record regarding all categories of processing activities carried out on behalf of the Controller. The record must contain, at a minimum, the following information:

a) name and contact details of the Processor or any retained sub-processor, for the Controller and for the Controller's or the Processor's representative and the data protection officer;

b) the categories of processing which will be carried out on behalf of the Controller;

c) the categories of recipients to whom the personal data has been, or will be, disclosed, including recipients in third countries or, where applicable, international organisations;

d) documentation of suitable safeguards that have been taken, if any personal data is transferred to a third country that is not included in a decision which contains applicable provisions regarding an adequate security level or appropriate security measures, and

e) where applicable, a general description of the technical and organisational security measures taken by the Processor according to applicable law.

4.2. The Processor, shall make such records available to the Controller upon request or relevant supervisory authority containing the above content.

4.3. If a data subject, upon the exercise of their rights, requests a record over the processing of their personal data, the Processor shall, after consultation with the Controller, upon request from the data subject or the Controller make such records available regarding such processing with the contents and in a way that is in line with applicable law.

5. Confidentiality and security measures

5.1. The Processor shall implement necessary technical and organisational safeguards in accordance with applicable law and thereby establish appropriate technical and organisational measurements in order to protect personal data from unintentional or unlawful destruction, loss, or modification, from unauthorised disclosure, or from unauthorised access to the personal data which is transferred, stored, or otherwise processed mainly when the processing contains alignment or data over networks and/or any other unlawful processing. When assessing the appropriate security level, certain regards shall be taken to the risks that the processing results in, especially unintentional or unlawful destruction, loss, or modification, from unauthorised disclosure to personal data.

5.2. The Processor undertakes to process the personal data under strict confidentiality and will not disclose or make personal data accessible to any third party, if an approval has not been provided prior to this DPA or in any other way is required according to applicable law or for the execution of this DPA.

5.3. The Processor undertakes to secure that only relevant employees are allowed to gain access to the personal data the belongs to the Controller in order to fulfil the Processor's obligations under this DPA. The Processor shall ensure that the employees who are authorised to process personal data covered by this DPA are subject to confidentiality, either by law or an agreement, which should at least correspond to the confidentiality provisions in which are stipulated in this DPA. The Processor shall also ensure that the employees understand the meaning of the confidentially stipulated in this DPA. The confidentially that the Parties undertake in the DPA also applies during a period of time after this DPA has expired. However, it shall only apply to a period of time that is stated in applicable law.

5.4. The Processor may not without (i) the Controller's prior written consent, and (ii) after securing that such transfer is carried out in accordance with applicable law, transfer personal data outside

of the EU/EEA or to a country that is not included in the list of exempted countries against such transfer according to applicable law. This prohibition is also subject to technical support, maintenance and similar services.

6. Audit and request for information

6.1. The Processor shall without undue delay inform the Controller about potential contacts with relevant supervisory authority or any other authority regarding the processing of personal data. The Processor is not allowed to represent the Controller or in any way act on behalf of the Controller against relevant supervisory authority or any third party without a written consent from the Controller.

6.2. The Processor shall grant the Controller, or any third party mutually authorised by the Parties, access to all non-confidential information which is required and necessary to enable the Controller to verify and audit the Processor's compliance with the obligations that are stated in this DPA, the GDPR and any other regulation. The Processor shall also enable and assist in audits, including inspections, which are conducted by the Controller or by a third party authorised by the Controller.

6.3. The Processor is entitled to compensation from the Controller to compensate for reasonable direct cost that the Processor has suffered due to such audit or inspection.

6.4. The Processor shall grant the Controller access to all non-confidential information which is required and necessary to enable the Controller to verify compliance with the obligations that follow from this DPA and that the processing fulfils requirements according to applicable law.

6.5. In cases where a data subject, relevant supervisory authority or any other third party requests information from any of the Parties in respect of personal data, the Parties shall cooperate and exchange information in to the required extent.

6.6. The Processor may not disclose information where the Processor has not obtained a written consent from the Controller to do so, or, other than if such obligation is mandatory according to applicable law or an order from any relevant authority.

7. Sub-processor

7.1. The Processor may not retain sub-processors to process personal data on behalf of the Controller without informing the Controller in written form that the Processor will retain a sub-processor thirty (30) days prior to such engagement.

7.2. In the event that the Processor retains a sub-processor for the processing of personal data, the Processor shall impose the same undertakings and obligations which follow this DPA. The Processor shall also undertake to make sure that the sub-processor respects and follows the terms that are applicable under this Data Processor TOSP and otherwise follow by applicable law.

7.3. In the event that the Processor in accordance with this DPA, retains a sub-processor, the Processor shall ensure that the agreement between the Processor and the sub-processor is construed in such way that the sub-processor is also bound by this DPA as well as the requirements stated in this agreement and applicable law. In the event the sub-processor fails to fulfil its obligations, the

Processor shall bear full liability towards the Controller for the performance of such sub-processor's obligations. The Processor shall, from time to time, maintain an updated list of the sub-processors who may be retained. At the Controller's request, the Processor shall submit a copy of the list to the Controller.

7.4. The Controller, or any party authorised by the Controller, has the right to be assisted by the Processor when conducting an inspection or audit regarding the processing of personal data that is performed by the retained sub-processor.

8. Personal data breach

8.1. In the event that the Processor suspects or detects any type of security breach such as unauthorised access, destruction, change to personal data or anything, or if the Processor for any reason cannot fulfil the undertakings and obligations in this DPA, shall the Processor immediately investigate the incident and take appropriate measures in order to mend the incident and prevent any recurrence of such events.

8.2. The Processor shall without undue delay notify the Controller, after the Processor has learned of a personal data breach and shall after this breach provide the Controller with on-going information about the breach as information about the breach becomes accessible to the Processor.

The notification shall at least contain the following:

a) a description of the nature of the personal data breach, if possible, the categories and approximate number of affected data subjects, and the categories and approximate numbers of affected personal data records;

b) provide the name of and the contact information to the data protection officer or other contact points where more information can be found,

c) a description of the likely consequences of the personal data breach, and

d) a description of the measures that the Processor has taken or proposed in order to remediate the breach, comprised of, when appropriate, measurements in order to mitigate the potential negative effects.

8.3. The Processor shall immediately inform the Controller if;

a) the Processor retains knowledge of processing of personal data that contradicts the Controller's instruction or this DPA, and/or

b) the Processor considers that an instruction contradicts applicable law.

8.4. If a certain type of processing, especially in regard to the use of new technology and considering the type, extent, context and purpose, may probably lead to a high risk for physical persons rights and freedoms shall the Processor, before the processing is performed, assist the Controller in the assessment of the planed processed consequences for the protection of personal data.

9. Liability

9.1. Article 82 of the GDPR shall apply in case of damages awarded to a data subject, through a court decision or other decision, due to a breach of any provision in this DPA, instruction from the Controller or applicable data protection regulations.

9.2. When an administrative fine is imposed according to article 83 of GDPR or 6 chap. 2 § of the Act containing supplementary provisions to the EU General Data Protection Regulation (2018:218), the administrative fine shall be paid by the Party receiving such fine.

9.3. If either Party receives knowledge of a circumstance that can lead to a loss for the other party, that Party shall immediately inform the other party of the circumstances and actively work together with the other party in order to prevent and minimise such loss.

9.4. Despite what has been stated in the Parties TOSP and related appendices, sections 9.1 and 9.2 in the DPA shall apply before any other regulations regarding the parties cessation of obligation between them covering the processing of personal data.

10. Compensation

10.1. The Processor is not entitled to any compensation for measures which the Processor takes in respect of processing of personal data, besides otherwise stated in this DPA or the Parties reseller agreement.

11. Effective term

11.1. This DPA enters into force on the day which it is signed and applies as long as the Processor processes personal data under the Parties TOSP.

12. Termination

12.1. When the Processor discontinues processing personal data on behalf of the Controller under this DPA, the Processor shall at the choice of the Controller destroy, erase and/or return all personal data which is associated with this agreement to the Controller in accordance with the Controllers instruction and ensure that no personal data or copies of personal data are still in the Processor's possession unless required by applicable law or financial reasons, including tax.

12.2. The Processor shall once this DPA is terminated, ensure that the obligation stated in section 12.1 of the DPA also applies to any sub-processor.

13. Amendments

13.1. The Controller may due to necessary compliance with applicable law, amend the contents of this this DPA. An amendment may enter into force thirty (30) days after the Controller has sent a notice to the Processor regarding the amendment. In the event that the Processor does not accept the relevant amendment, the Controller shall have the right to terminate all agreements with the Processor under which the Processor shall process personal data.

13.2. Amendments to this DPA shall be made in writing and signed by both Parties in order to legally binding.

14. Standard contractual clauses

14.1. Within the scope of the COMMISSION 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 the standard contractual clauses ("**SCC**") attached in Annex 1 shall apply.

15. Applicable provisions and order of precedence

15.1. The agreements between the parties apply in the following order, whereby, in case of contradictions, provisions of the documents first mentioned shall prevail over the provisions in the documents mentioned thereafter:

a) SCC subject to this DPA in Annex 1;

b) the provisions of this DPA and

c) the provisions of the TOSP.

16. Governing law and jurisdiction

16.1. This DPA shall be governed by the substantive law of _____. Any dispute, controversy or claim arising out of or in connection with this DPA, shall be finally settled in the general courts of _____ with the district court of _____ as the first instance.

This DPA may be executed, including electronically, in any number of counterparts.

_____	_____
Date	Date
_____	_____
Controller's signature	**Processor's signature**
_____	_____
Name and Title in print	Name and Title in print

ANNEX 1: STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer Controller to Processor

SECTION I

1. Clause 1 – Purpose and scope

1.1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)[1] for the transfer of data to a third country.

1.2. The Parties:

1.2.1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

1.2.2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

1.3. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B

1.4. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

2. Clause 2 – Effect and invariability of the Clauses

2.1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

2.2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

3. Clause 3 – Third-party beneficiaries

3.1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

3.2. Clause 1, Clause 2, Clause 3, Clause 6; Clause 7;

3.3. Clause 8.1.2, 8.9.1, 8.9.3, 8.9.4 and 8.9.5;

3.4. Clause 9.1, 9.3, 9.4 and 9.5;

3.5. Clause 12.1, 12.4 and 12.6;

3.6. Clause 13;

3.7. Clause 15.1.3, 15.1.4 and 15.1.5;

3.8. Clause 16.5;

3.9. Clause 18.1 and 18.2.

3.10. Paragraph 3.1 is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

4. Clause 4 – Interpretation

4.1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

4.2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

4.3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

5. Clause 5 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

6. Clause 6 – Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

7. Clause 7 – Docking clause

7.1. [*Intentionally deleted*]

SECTION II – OBLIGATIONS OF THE PARTIES

8. Clause 8 – Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1. Instructions

8.1.1. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

8.1.2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14.5 to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14.1.

8.6. Security of processing

8.6.1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.6.2. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.6.3. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

8.6.4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

8.8.1. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

8.8.2. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

8.8.3. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

8.8.4. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

8.9.1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9.2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

8.9.3. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

8.9.4. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

8.9.5. The Parties shall make the information referred to in paragraphs 8.9.2 and 8.9.3, including the results of any audits, available to the competent supervisory authority on request.

9. Clause 9 – Use of sub-processors

9.1. GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

9.2. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

9.3. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

9.4. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

9.5. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

10. Clause 10 – Data subject rights

10.1. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

10.2. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

10.3. In fulfilling its obligations under paragraphs 10.1 and 10.2, the data importer shall comply with the instructions from the data exporter.

11. Clause 11 – Redress

11.1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

11.2. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

11.3. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

11.3.1. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

11.3.2. refer the dispute to the competent courts within the meaning of Clause 18.

11.4. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

11.5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

11.6. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

12. Clause 12 – Liability

12.1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

12.2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

12.3. Notwithstanding paragraph 12.2, the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

12.4. The Parties agree that if the data exporter is held liable under paragraph 12.3 for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

12.5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

12.6. The Parties agree that if one Party is held liable under paragraph 12.5, it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

12.7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

13. Clause 13 – Supervision

13.1. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States 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 behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

13.2. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the

measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

14. Clause 14 – Local laws and practices affecting compliance with the Clauses

14.1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

14.2. The Parties declare that in providing the warranty in paragraph 14.1, they have taken due account in particular of the following elements:

14.2.1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

14.2.2. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards3;

14.2.3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

14.3. The data importer warrants that, in carrying out the assessment under paragraph 14.2, it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

14.4. The Parties agree to document the assessment under paragraph 14.2 and make it available to the competent supervisory authority on request.

14.5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph 14.1, including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph 14.1.

14.6. Following a notification pursuant to paragraph 14.5, or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16.4 and 16.5 shall apply.

15. Clause 15 – Obligations of the data importer in case of access by public authorities

15.1. Notification

15.1.1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

15.1.1.1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

15.1.1.2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

15.1.2. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to 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. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

15.1.3. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests,

type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

15.1.4. The data importer agrees to preserve the information pursuant to paragraphs 15.1.1 to 15.1.3 for the duration of the contract and make it available to the competent supervisory authority on request.

15.1.5. Paragraphs 15.1.1 to 15.1.3 are without prejudice to the obligation of the data importer pursuant to Clause 14.5 and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2. Review of legality and data minimisation

15.2.1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14.5.

15.2.2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

15.2.3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

16. Clause 16 – Non-compliance with the Clauses and termination

16.1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

16.2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14.6.

16.3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

16.3.1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph 16.2 and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

16.3.2. the data importer is in substantial or persistent breach of these Clauses; or

16.3.3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

16.4. Personal data that has been transferred prior to the termination of the contract pursuant to 16.3 shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

16.5. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

17. **Clause 17 – Governing law**

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____.

18. Clause 18 – Choice of forum and jurisdiction

18.1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

18.2. The Parties agree that those shall be the courts of _____.

18.3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

18.4. The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX to the Standard Contractual Clauses

ANNEX I

A. LIST OF PARTIES

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

Name:	
Address:	
Contact person's name, position and contact details:	
Activities relevant to the data transferred under these Clauses:	
Signature and date:	
Role (controller/processor):	

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

Name:	SMART Technologies ULC
Address:	3636 Research Road NW, Calgary AB, T2L 1Y1

Contact person's name, position and contact details:	Glenn Carbol, Data Protection Officer
Activities relevant to the data transferred under these Clauses:	Processing of data for SMART Learning Suite
Signature and date:	
Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data are transmitted

- **User**
- **Customer**

Categories of Data Subjects for Users:

User

- Direct identifying information (e.g. name, email address)
- Any personal data supplied by end users of the Service
- Application Technology Meta Data
  - IP addresses, use of cookies, etc.
- Application Use Statistics
  - Meta data on user interaction with application
  - Other assessment data – determined by teacher running the class
- Online communications captured (emails, blog entries)
- Provder/App assigned student ID number
- Student app username
- Student responses to surveys or questionnaires
- Student generated content; writing, pictures, etc. – anything stored in teacher's lesson file
- Microsoft Single Sign-On
- Google Single Sign-On
- Region for data storage (USA or EU)
- Google Anyalytics (anonymous)

- MixPanel Analytics (anonymous)

Categories of Data Subjects for Customers:

- Organization name
- E-mail
- Phone
- Address
- Required order information: product, quantity, price and tax, delivery

Sensitive Data: The Processor hereby expressly prohibits the Controller from transferring any special categories of personal data to it.

Frequency of the Transfer: Continuous during the Service.

Nature of the Processing:

Processor will perform the following basic processing activities:

- processing to provide the Service in accordance with the TOSP;
- processing to perform any steps necessary for the performance of the Service; and
- processing to comply with other reasonable instructions provided by Controller (e.g. via email) that are consistent with the terms of the TOSP.

Period for which the personal data will be retained: Throughout the Term of the TOSP plus the period from expiry of the Term until deletion of Personal Data by the Processor in accordance with applicable law or as requested by Controller (Data Erasure Request).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

Controller please enter your country's supervisory authority here:_____
_____

**Note - where the Controller acts as the data exporter and is established in an EU Member State the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated here, shall act as competent supervisory authority.*

ANNEX II – TECHNICAL AND ORGANIZATIONAL MEASURES

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

The Parties shall agree the following categories of measures will be implemented. The details of each measure is available upon request.

1. The Processor should have a structured organisation where different employees have roles and responsibilities regarding security information that are clearly defined.

2. The Processor shall on a regular basis provide courses to increase awareness regarding information systems built to resist.

3. The Processor should have routines and functions in order to permanently delete and erase information that is related to the delivery.

4. The Processor has performed a risk evaluation of the system and preformed measurements to identify any faults in such system.

5. The Controler's requirements regarding processing of information shall be adopted. In case such requirements are not expressed, the Processor shall be able to present the routines that apply to the Processor.

6. The users are to be provided personal and unique user identities to the extent that anonymous guest accounts are to not used. For more information, see Guidance for trust level 1 (LoA1).

7. The Processor shall follow an agreed upon routine that enables the Controller to approve certain selected authorities.

8. The Processor shall use personal and traceable user identities for high level authorities that are used to administrate the system.

9. The Processor shall have a system that distributes and resets passwords without disclosing the password to unauthorised persons. For more information, see Guidance for trust level 1 (LoA1).

10. The authorisation system shall log information of when a user is created or removed.

11. The Processor shall have a routine for removing user identities form the system.

12. The Processor shall have established rules regarding the person responsible for handling authentication information.

13. Only information or services that are public shall be available in the system and any other related infrastructure that has not been subject to authentication.

14. The system shall use passwords or anything that holds a better security level for authentication. There should be provided rules for how a password is allowed to be handled in the system and by a user. For more information, see Guidance for trust level 1 (LoA1).

15. The so called data hall shall fulfil at least protection level 2 (according to "data room", stated in the Swedish Civil Contingencies Agencies "Guidance for physical security information in the it-room").

16. The Processor shall have routines in which secure that only authorised personal have physical access to the so called data hall.

17. The Processor should have different functions, processes and routines to monitor and create prognoses regarding performance.

18. The Processor should provide protection against damaging code for the parts that are included in the delivery.

19. The Processor should have routines and functions for backups and restoration of information according to the agreed upon accessibility requirements with the Controller. Backups should be protected in the same way as the original information and stored separately.

20. Log-in functions should be available for security related events, especially regarding incorrect log-ins, any change to an authorisation, unauthorised connections and infringements of authorisations.

21. The Processor shall protect log-in functions and log tools against manipulation and unauthorised access, which also includes the Processor’s employees.

22. The system and related infrastructure should use the same time synchronisation as the time source, which is UTC+0.

23. The Processor shall without delay inform the Controller about technical vulnerabilities in the delivered components. Found vulnerabilities should be amended immediately.

24. The Controller shall upon request be informed about every exchange of information that occurs with other systems outside the Controller’s environment.

25. The Processor has established and documented principles and methods for the development of secure systems and present these to the Controller.

26. The Processor has guidelines for an information system to resist within their development processes.

27. The Processor’s responsibilities as stated herein will apply to any sub-processors. The Controller shall upon request be informed of which sub-processor is used.

28. The Processor should have routines for reporting, escalation, and the handling of any security events or incidents.

29. The Processor shall together with an appointed roll within the Controller, cooperate when handling any vulnerabilities, security events or incidents.

30. The Processor shall together with the Controller continuously strive for the delivery to follow all relevant law, regulations and rules which apply to the Controller’s business.

31. When processing personal data, the Controller shall establish a processor agreement with the Processor regarding the processor before the agreement is effective.

32. The Processor shall ask for an approval before the information in the system is reused (text, pictures etc.) in any other context.

ANNEX III – SUB-PROCESSORS

LIST OF SUB-PROCESSORS (*Source: https://www.smarttech.com/legal/lumio-privacy*)

The controller has authorised the use of the following sub-processors:

GUESTS

Self-Chosen Display Name for Guests

Type: **Anonymous**

Where	Who	Data & Purpose
Canada	SMART Technologies ULC	Required for basic functionality. Display name is recorded inside of a teacher's lesson or activity when the user participates. SLS Terms GDPR - EC Adequacy Decision
USA/ Germany	Amazon Web Services, Inc.	Required for storage. We offer both an American and European data storage option. AWS Privacy AWS GDPR
USA/ Belgium	Firebase (Google LLC)	Required for basic functionality (Firebase is a Backend-as-a-Service (BaaS) cloud-computing solution we use for real time (temporary) automated computer processing). Firebase Privacy Firebase GDPR

Guest Created Content

Type:	**Anonymous**	
Where	**Who**	**Data & Purpose**
Canada	SMART Technologies ULC	Optional *(stored inside a teacher's lesson).* SLS Terms GDPR - EC Adequacy Decision
USA/ Germany	Amazon Web Services, Inc.	Required for storage. We offer both an American and European data storage option. AWS Privacy AWS GDPR
USA/ Belgium	Firebase (Google LLC)	Required for basic functionality (Firebase is a Backend-as-a-Service (BaaS) cloud-computing solution we use for real time (temporary) automated computer processing). Firebase Privacy Firebase GDPR

Guest Analytics

Type:	**Anonymous**	
Where	**Who**	**Data & Purpose**
Canada	SMART Technologies ULC	Required for product improvement and service monitoring. We use Mixpanel as our processor for this. SLS Terms GDPR - EC Adequacy Decision
USA	Mixpanel, Inc.	Required for product improvement and service monitoring. Mixpanel allows us to analyze how our de-identified users interact with Lumio. It is designed to identify trends, understand common aggregated usage

		behavior, and helps us make better decisions on how to improve the usability and features of our product. This data is also used to track how long it takes our servers to complete actions like open files, which helps us measure service health and up/downtime. Mixpanel Privacy Mixpanel GDPR
N/A	Third-party content providers	Optional content or activity a teacher may add to a lesson such as a YouTube or other embedded content a user voluntarily adds. We cannot control what data a third party directly collects when a teacher or student decides to include it in a lesson. For premium content that SMART provides however, we only report anonymous usage to the third-party publisher.
USA	Sentry.io	• Lesson ID (no PII) • User ID and Session IDs (hashed and salted to maintain anonymity) • request header (application and version, platform, operating system, browser, language, date and time) • bread crumbs (last pages visited and links clicked) Optional User Error Reporting: After automatic error reporting is complete, users are given the option to provide their name, email address, and additional information about the error. Users are also asked if they wish SMART to follow up with them. This optional personal information is stored in Salesforce (located in the United States) and shared with our customer support team.

STUDENTS / MINORS, SIGNED-IN

Student Account

Type:	**Identifiable**	
Where	**Who**	**Data & Purpose**
Canada	SMART Technologies ULC	Required account details for product functionality: display name, full name, email, public profile picture. language preference. SLS Terms GDPR - EC Adequacy Decision

Global	Microsoft, Inc.	Required if you use Microsoft as your single-sign-on (SSO) provider to access Lumio. Microsoft provides SMART with required account details. Microsoft SSO Microsoft Privacy Microsoft GDPR
Global	Google LLC	Required if you use Google as your single-sign-on (SSO) provider to access Lumio. Google provides SMART with required account details. Google SSO Google Privacy Google GDPR
USA/ Germany	Amazon Web Services, Inc.	Required for storage. We offer both an American and European data storage option. AWS Privacy AWS GDPR

Using Lumio as a Signed-In Student (student created content)

Type:	**Pseudonymized**	
Where	**Who**	**Data & Purpose**
Canada	SMART Technologies ULC	Optional. If students participate in live activities where they provide responses or they upload content they created, it will be attributed to their account. SLS Terms GDPR - EC Adequacy Decision
USA/ Germany	Amazon Web Services, Inc.	Required for storage. We offer both an American and European data storage option. AWS Privacy AWS GDPR

USA/ Belgium	Firebase (Google LLC)	Required for basic functionality (Firebase is a Backend-as-a-Service (BaaS) cloud-computing solution we use for real time (temporary) automated computer processing). Firebase Privacy Firebase GDPR

Signed-In Student Analytics

Type: **Pseudonymized**

Where	**Who**	**Data & Purpose**
Canada	SMART Technologies ULC	Required for product improvement and service monitoring. We use Mixpanel as our processor for this. SLS Terms GDPR - EC Adequacy Decision
USA	Mixpanel, Inc.	Required for product improvement and service monitoring. Mixpanel allows us to analyze how our de-identified users interact with Lumio. It is designed to identify trends, understand common aggregated usage behavior, and helps us make better decisions on how to improve the usability and features of our product. This data is also used to track how long it takes our servers to complete actions like open files, which helps us measure service health and up/downtime. Mixpanel Privacy Mixpanel GDPR
N/A	Third-party content providers	Optional content or activity a teacher may add to a lesson such as a YouTube or other embedded content a user voluntarily adds. We cannot control what data a third party directly collects via the content when a teacher or student decides to include it in a lesson. For premium content that SMART provides however, we only report anonymous usage to the third-party publisher.
USA	Sentry.io	• Lesson ID (no PII)

- User ID and Session IDs (hashed and salted to maintain anonymity)
- request header (application and version, platform, operating system, browser, language, date and time)
- bread crumbs (last pages visited and links clicked)

Optional User Error Reporting: After automatic error reporting is complete, users are given the option to provide their name, email address, and additional information about the error. Users are also asked if they wish SMART to follow up with them. This optional personal information is stored in Salesforce (located in the United States) and shared with our customer support team.

TEACHERS / ADULTS, SIGNED-IN

Teacher Account

Type: **Identifiable**

Where	Who	Data & Purpose
Canada	SMART Technologies ULC	Required account details: display name, name, email, public profile picture. language preference. Required account profile settings: opt-ins, user type, location. SLS Terms GDPR - EC Adequacy Decision
Global	Microsoft, Inc.	Required if you use Microsoft as your single-sign-on (SSO) provider to access Lumio. Microsoft provides SMART with required account details. Microsoft SSO Microsoft Privacy Microsoft GDPR
Global	Google LLC	Required if you use Google as your single-sign-on (SSO) provider to access Lumio. Microsoft provides SMART with required account details. Google SSO Google Privacy Google GDPR

USA/ Germany	Amazon Web Services, Inc.	Required for storage. We offer both an American and European data storage option. AWS Privacy AWS GDPR

Using Lumio as a Signed-In Teacher (teacher created content)

Type: **Identifiable**

Where	Who	Data & Purpose
Canada	SMART Technologies ULC	Generated Content (lessons and activities created by a teacher). Self-chosen class names. SLS Terms GDPR - EC Adequacy Decision
USA/ Germany	Amazon Web Services, Inc.	Required for storage. We offer both an American and European data storage option. AWS Privacy AWS GDPR
USA/ Belgium	Firebase (Google LLC)	Required for basic functionality (Firebase is a Backend-as-a-Service (BaaS) cloud-computing solution we use for real time (temporary) automated computer processing). Firebase Privacy Firebase GDPR

Signed-In Teacher Analytics

Type: **Pseudonymized**

Where	Who	Data & Purpose
Canada	SMART Technologies ULC	Required for product improvement and service monitoring. We use Mixpanel as our processor for this. SLS Terms GDPR - EC Adequacy Decision
USA	Mixpanel, Inc.	Required for product improvement and service monitoring. Mixpanel allows us to analyze how our de-identified users interact with Lumio. It is designed to identify trends, understand common aggregated usage behavior, and helps us make better decisions on how to improve the usability and features of our product. This data is also used to track how long it takes our servers to complete actions like open files, which helps us measure service health and up/downtime. Mixpanel Privacy Mixpanel GDPR
N/A	Third-party content providers	Optional content or activity a teacher may add to a lesson such as a YouTube or other embedded content a user voluntarily adds. We cannot control what data a third party directly collects via the content when a teacher or student decides to include it in a lesson. For premium content that SMART provides however, we only report anonymous usage to the third-party publisher.
USA	Sentry.io	• Lesson ID (no PII) • User ID and Session IDs (hashed and salted to maintain anonymity) • request header (application and version, platform, operating system, browser, language, date and time) • bread crumbs (last pages visited and links clicked) Optional User Error Reporting: After automatic error reporting is complete, users are given the option to provide their name, email address, and additional information about the error. Users are also asked if they wish SMART to follow up with them. This optional personal information is stored in Salesforce (located in the United States) and shared with our customer support team.

CUSTOMER DATA COLLECTED AND PROCESSED

This section outlines what data is collected, processed, and disclosed from customers (purchasers, prospects, and SMART's authorized channel partners). You can request, through our Customer Support, data and account deletion at any time, but we must retain all data relevant to purchases and financial transactions until it is no longer required by applicable law. The term "identifiable" used in the below chart does not necessarily mean personally identifiable information.

Where	Who	Role	Data & Purpose	Type
N/A	Reseller & SMART's Regional Office	Seller	Required contact information: organization name, e-mail, title, phone, address. Required order information: product, quantity, price and tax, delivery. Ask your local regional reseller about their privacy policies.	Identifiable
Canada	SMART Technologies ULC	Manufacturer	Required account information: organization name, e-mail, title, phone, address, reseller, current subscriptions. Required order information: product, quantity, price and tax, delivery. Required admin portal information for license provisioning: licenses and activations, teachers', and admins' first and last names (can provide non-PII version to comply with GDPR) and e-mail address, and class names (can be non-PII version to comply with GDPR). SLS Terms GDPR - EC Adequacy Decision	Identifiable
Canada	Blue Ocean Contact Centers, Inc.	Support	Optional. Blue Ocean is a subcontractor providing live (telephone, e-mail, and web) support. Information collected includes organization name, caller name (can use company title only if preferred for GDPR reasons), e-mail (can provide non-PII version to comply with GDPR), title, phone, address and a description of the issue and any shared details to help solve the problem. Calls are recorded. Blue Ocean Privacy GDPR - EC Adequacy Decision	Identifiable

Where	Who	Role	Data & Purpose	Type
USA/ Germany	Amazon Web Services, Inc.	Processing, Back-Office	Required for product infrastructure including the hosting of support call recordings. AWS Privacy AWS GDPR	Identifiable
USA	Google, LLC.	Processing, Back-Office.	Optional. Only used for processing of support forms. Google Forms are used when a purchaser is engaged with our Field Services (i.e., onsite support). Google Privacy Google GDPR	Identifiable
USA	Microsoft, Inc.	Processing, Back-Office	Required for our enterprise resource planning (ERP) system, which is software to manage the day-to-day business activities such as accounting, procurement, project management and supply chain operations, as well as our e-mail, PowerBI® (data visitation) and SharePoint® (document management), as well as all the other standard Microsoft Office software titles, like Word, Excel, etc. Microsoft Privacy Microsoft GDPR	Identifiable
USA	BigCommerce, Inc.	Ordering	Optional. Only used when a customer purchases through our e-commerce store: customer name, e-mail, title, phone, address, product, or service purchased and whether payment is received. BigCommerce Privacy BigCommerce GDPR	Identifiable
USA	Stripe, Inc. and Stripe Payments Europe, Ltd.	Ordering	Optional. Only used when a customer purchases through our e-commerce store using a credit card: customer name, e-mail, title, phone, address, product, or service purchased, credit card details. Residents of the European	Identifiable

Where	Who	Role	Data & Purpose	Type
			Economic Area (EEA), the UK and Switzerland. The entity responsible for the collection and processing of credit card personal data for residents of the EEA, the UK and Switzerland is Stripe Payments Europe, Ltd., a company incorporated in Ireland and with offices at 1 Grand Canal Street Lower, Grand Canal Dock, Dublin. To exercise your rights, the Data Protection Officer may be contacted via dpo@stripe.com. Stripe Privacy Stripe GDPR	
USA	Salesforce.com, Inc	Ordering, Marketing, Channel Support	Required order information (product, quantity, price and tax, delivery). Required for our customer relationship management (CRM). Required to allow our authorized distributors and resellers to work together with SMART. Basic customer and purchase information is shared between SMART and its authorized distributors and resellers. Salesforce Privacy Salesforce GDPR	Identifiable
USA	HubSpot, Inc.	Marketing	Optional. We use HubSpot, which is a customer relationship management (CRM), for individuals that have expressly opted in to receive certain communications, such as marketing, training, news, and offers from us. Hubspot Privacy Hubspot GDPR	Identifiable
USA	Mixpanel, Inc.	Monitoring	Required for product improvement and service monitoring. Mixpanel allows us to analyze how our de-identified users interact with Notebook. It is designed to identify trends, understand common aggregated usage behavior, and helps us make better decisions on how to improve the usability and features of	Pseudonymized

Where	Who	Role	Data & Purpose	Type
			our product. This data is also used to track how long it takes our servers to complete actions like open files, which helps us measure service health and up/downtime. Mixpanel Privacy Mixpanel GDPR	
USA	Gainsight, Inc.	Marketing	Applicable only to USA customers. We use Gainsight, which is a customer relationship management (CRM) tool, for e-mail (name, e-mail address, company information) marketing to individuals and organizations. Gainsight Privacy	Identifiable