QWICKLY GDPR DATA PROCESSING ADDENDUM

This Addendum, including its Appendix and Annexes, (collectively, the "Addendum") forms part of the Master Services Agreement ("Master Agreement") between Qwickly, a corporation with an address at 2019 Center Street, Cleveland, OH 44113, USA (hereinafter, "Processor") and the institution licensing Qwickly Products (hereinafter "Controller") (collectively, "the parties" or individually, "a/the party").

In the event of a conflict between the terms and conditions of this Addendum and the Master Agreement, the terms and conditions of this Addendum shall supersede and control.

---

1. DEFINITIONS

1.1 "**Applicable Data Protection Law**" means the General Data Protection Regulation (as implemented in the relevant European Union Member State) and all applicable data protection legislation and regulations.

1.2 "**Business Days**" means Monday through Friday, except for Federal legal public holidays as defined by 5 U.S.C. § 1603(a).

1.3 "**Consent**" of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

1.4 "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by European Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by European Union or Member State law.

1.5 "**Data Exporter**" means the Controller who transfers Personal Data to a Processor.

1.6 "**Data Importer**" means the Processor who agrees to receive from the Data Exporter any Personal Data intended for Processing on its behalf after the transfer in accordance with the terms and conditions defined in this Agreement and who is not subject to a third country's system ensuring adequate protection within the meaning of the GDPR.

1.7 "**General Data Protection Regulation**" or "**GDPR**" means Regulation 2016/679, adopted by the European Parliament on April 27, 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 the 1995 Data Protection Directive (95/46/EC).

1.8 "**Personal Data**" means any information provided to or accessed by Controller in connection with the performance of the Master Agreement and/or this Addendum and that relates to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the

physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.9 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

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

1.11 "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.12 "**Special Categories of Data**" means information related to a Data Subject's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (when used for identification purposes), health, sex life, or sexual orientation.

1.13 "**Sub-Processor**" means any Processor engaged by the Data Importer or by any other Sub-Processor of the Data Importer who agrees to receive from the Data Importer or from any other Sub-Processor of the Data Importer Personal Data exclusively intended for Processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with this Addendum.

1.14 "**Supervisory Authority**" means an independent public authority which is established pursuant to Article 51 of the GDPR.

1.15 "**Technical and Organizational Security Measures**" means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

2. DATA CONTROLLER ACTIVITIES AND DATA PROTECTIONS

2.1. Controller agrees that at any and all times that it is serving as a Controller for the purposes of satisfying the terms and conditions of the Master Agreement and/or this Addendum, it will undertake or adhere to the following:

a. Provide the Data Subject, in writing and at the time that Personal Data is collected, the information set forth in Articles 13 and 14 of the GDPR in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

b. Where Processing is based on the Data Subject's consent, implement all necessary measures to ensure that Data Subjects have been notified and appropriately consented (in accordance with the terms and conditions of the GDPR) to their Personal Data being collected, retained, stored, disclosed, or otherwise disseminated.

c. Respond to any communication or correspondence from a Data Subject, or a third party acting on the Data Subject's behalf, regarding the invocation of any rights set forth in the GDPR, including those in Articles 15 to 22.

3. DATA PROCESSOR ACTIVITIES AND DATA PROTECTIONS

3.1. Processor agrees that at any and all times that is it serving as a Processor for the purposes of satisfying the terms and conditions of the Master Agreement and/or this Addendum, it (and any individual or entity acting on its behalf) will undertake and/or adhere to the following:

a. Process any Personal Data provided to it by Controller only in accordance with the terms and conditions set forth in the Master Agreement and/or this Addendum, or on the documented instructions from Controller, unless otherwise required to do so by law. In the event Processor is compelled by law to Process Personal Data provided to it by Controller in a manner beyond or in contrast to the terms and conditions set forth in the Master Agreement and/or this Addendum, or the documented instructions from Controller, it shall notify Controller of that legal requirement prior to Processing, unless such notification is expressly prohibited by law.

b. Maintain confidentiality of all Personal Data and ensure that individuals who are authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. Implement appropriate technical and organizational security measures to ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, and by taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing.

d. Provide Controller, in accordance with the Master Agreement, access to Personal Data to enable Controller to comply with its legal obligations with regard to Data Subjects invoking their rights under the GDPR. Processor shall, at the request of Controller and without delay, amend, correct, delete, cease using, or restrict the use of Personal Data. Processor shall refer immediately and without delay, any correspondence it receives from a Data Subject seeking to invoke his/her rights under the GDPR to Controller.

e. Notify Controller, immediately and without delay, of any actual or reasonably suspected Personal Data Breach or other breach affecting Personal Data after Processor becomes aware of the incident. Processor shall, taking into account the nature of the Processing and the information available to Processor, provide, to the greatest extent possible, assistance to Controller to enable Controller to meet its legal obligations to notify any Supervisory Authority, regulatory or governmental authority, Data Subject, or any other individual of the incident.

f. Assist, to the greatest extent possible, Controller in relation to any privacy impact assessments or consultations with Supervisory Authorities concerning the Processing of Personal Data within the scope of the Master Agreement and/or this Addendum.

g. Assist, to the greatest extent possible, Controller in relation to any inquiry, complaint, or claim in relation to the Processing of Personal Data within the scope of the Master Agreement and/or this Addendum.

h. After completing all necessary Processing, at the choice of Controller, either return all Personal Data and the copies thereof to Controller, or destroy, and certify the destruction of, all Personal Data, unless otherwise prohibited by law.

i. Audit, on a periodic basis, the adequacy of its technical and organizational security measures used to Process Personal Data on behalf of Controller, in accordance with industry standards or such alternative standards that are substantially equivalent. The audit described herein may be performed by Processor or a third party at Processor's selection and expense.

j. Undertake good faith efforts to allow for and contribute to audits (including inspections) undertaken by Controller or by an auditor designated by Controller by providing reports on or another confidential summary of its technical and organizational security measures so that Controller can reasonably verify Processor's compliance with its legal and/or contractual obligations.

k. Implement appropriate technical and organizational security measures to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, including when necessary to assist Controller in satisfying the terms and conditions of the Master Agreement and/or this Addendum.

3.2. Controller acknowledges and agrees that in order to satisfy to the terms and conditions of the Master Agreement and/or this Addendum, Processor may subcontract to third party vendors, subject to the following terms and conditions:

a. Processor shall inform Controller of any intended changes concerning the addition or replacement of other subcontractors, thereby giving Controller the opportunity to object to such changes.

b. Processor will ensure that any such third-party vendor agrees, in writing, not disclose to any other party not privy to this Addendum the content of any information, including any Personal Data, provided to or accessed by the third party vendor in connection with the performance of the Master Agreement and/or this Addendum.

c. Processor will ensure that any third party that performs Processing activities concerning Personal Data on its behalf will be subject to any and all applicable obligations and conditions set forth in the GDPR, and the same contractual requirements set forth in the Master Agreement and/or this Addendum.

d. Processor shall remain liable to Controller for any breaches caused by third parties performing sub-Processing activities.

4. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

4.1. The parties agree to transfer Personal Data to any non-European Economic Area country or to an international organization only in accordance with applicable law, including the GDPR.

4.2. In the event that Processor is undertaking or intends to undertake the Processing of Personal Data on the behalf of Controller that involves the transfer of Personal Data to any non-European Economic Area country or to an international organization, both parties shall comply with the terms of the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries approved by the European Commission Decision of June 4, 2021 and reproduced in Appendix A.

4.3. In the event that Appendix A is amended, replaced, or repealed by government authorities, the parties will adhere, to the greatest extent possible, to any new provisions or obligations set forth by the government authorities, until such time that both parties can agree to new terms and conditions governing the transfer of Personal Data to any non-European Economic Area country or international organization.

4.4. The parties shall also comply with the terms and conditions set forth in Appendix A in all cases where Personal Data that was originally exported in the circumstances described in Section 4.2 of this Addendum is subsequently transferred to another country. If required by law, the Parties shall execute or re-execute the terms and conditions set forth in Appendix A as separate documents setting out the proposed transfers of Personal Data in any such manner as may be required by the GDPR or other applicable law.

4.5. In case of any conflict between the terms and conditions set forth in Appendix A and any other part of this Addendum, the terms and conditions set forth in Appendix A shall prevail.

4.6. The parties' signature to this Addendum shall be considered as signature to the terms and conditions set forth in Appendix A.

5. LAWFUL ACTIVITIES AND COMPLIANCE

5.1. Processor and Controller shall perform all activities related to this Addendum in accordance with all relevant terms and conditions set forth in the GDPR.

5.2. In the event that either party cannot, for whatever reason, comply with the GDPR, it will promptly notify the other of this situation and provide reason(s) for noncompliance. Upon request by Processor or Controller, the other party shall, as soon as reasonably practicable, but in no case more than fourteen (14) business day, make available to it all information necessary to demonstrate compliance with this Addendum and the GDPR's terms, conditions, obligations, and requirements.

6. DISPUTES AND GOVERNING LAW

6.1. Any action, suit, or proceeding arising under or in connection with this Addendum must be commenced within one year after the claim or cause of action accrued. The prevailing party in any action, suit or proceeding shall be entitled to recover, in addition to any other remedy under this Addendum, reasonable attorney fees and costs.

6.2. Except as provided for in Clause 17 (Governing Law) of Appendix A, any action, suit, or proceeding arising under or in connection with this Addendum shall be governed in all respects by the laws stipulated to in the Master Agreement.

7. THIRD PARTY RIGHTS

7.1. Unless expressly provided for in this Addendum, including in the terms and conditions set forth in Appendix A, or provided for in law, including the GDPR, a person who is not a party to this Addendum has no right to enforce any term of this Addendum.

7.2. Unless required by law or by the terms and conditions provided for in this Addendum, the parties do not require the consent of any third party to terminate, rescind, amend, or otherwise alter this Addendum at any time.

Accepted and agreed to by each party's authorized signatory:

Signed:	Signed:
Printed:	Printed:
Title:	Title:
Date:	Date:

Appendix A

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

(a) 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) for the transfer of personal data to a third country.

(b) The Parties: (i) 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 (ii) 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").

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

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

Clause 2
Effect and invariability of the Clauses

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

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

Clause 3
Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e)
(iii) Clause 9(a), (c), (d) and (e)
(iv) Clause 12(a), (d) and (e);
(v) Clause 13
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16 (e);
(viii) Clause 18(a) and (b).

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

Clause 4
Interpretation

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

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

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

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.

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.

Clause 7 - Optional
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

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 organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) 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.
(b) 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 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(e) 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(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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.

(b) 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 authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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.

(d) 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 (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:

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

(ii) 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.

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) 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

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

(b) 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.

(c) 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 noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) 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.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorization. The data importer shall submit the request for specific authorization at least one (1) month prior to the engagement of the subprocessor, together with the information necessary to enable the data exporter to decide on the authorization. The list of sub-processors already authorized by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) 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 fulfills 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.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor 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.

(d) 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 subprocessor to fulfill its obligations under that contract.

(e) 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.

Clause 10
Data subject rights

(a) 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 authorized to do so by the data exporter.

(b) 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 organizational 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.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) 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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) 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.

(c) 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: (i) 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; (ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

(f) 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.

Clause 12
Liability

(a) 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.

(b) 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.

(c) Notwithstanding paragraph (b), 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.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) 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.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13
Supervision

(a) 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.

(b) 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

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) 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 authorizing 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.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

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

- any relevant contractual, technical or organizational 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.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), 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.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) 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 (a), 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 (a).

(f) Following a notification pursuant to paragraph (e), 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 organizational 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(d) and (e) shall apply.

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

15.1 Notification

(a) 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:

i. 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

ii. 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.

(b) 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.

(c) 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.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) 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 minimization

(a) 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(e).

(b) 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.

(c) 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

Clause 16
Non-compliance with the Clauses and termination

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

(b) 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(f).

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

- The data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension.

- The data importer is in substantial or persistent breach of these Clauses; or

- 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.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph c) 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.

(e) 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.

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 applicable country.

Clause 18
Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of applicable country.

(c) 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.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The Data Exporter is a customer of the Data Importer, which it has engaged to provide certain data and software services. In the course of receiving these services and related support, the Data Exporter will transfer Personal Data to the Data Importer for Processing, the nature of which and the purposes for which are specified the Master Agreement, the Addendum, and this Annex 1.

Data importers(s): The Data Importer is a provider of information and content, software and technology that allows customers to manage their classroom metrics.

B.DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Qwickly Attendance

- Data Exporter's students and school employees.

Qwickly Course Tools

- None (No Personal Data is transferred by Qwickly Course Tools).

Categories of personal data transferred:

Qwickly Attendance

- Student Name
- Instructor Name
- Student Email Address
- Instructor Email Address
- Student ID Number
- Learning System (VLE) Student Database ID
- Learning System (VLE) Instructor Database ID

Qwickly Course Tools

- None (No Personal Data is transferred by Qwickly Course Tools)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

The data is transferred on a continuous basis.

Nature and purpose of the processing

The Data Importer will Process the Personal Data in order to provide the contracted services, as defined in the Master Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Throughout the contractual relationship.

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

A description of the technical and organizational security measures implemented by the Data Importer in accordance with Sections 4(d) and 5(c) of Appendix A is provided as follows:

By design, Qwickly products do not store or cache personally identifiable information. When personally identifiable information can be used to enhance the use of a product, the goal is to keep its impact at a minimum.

Institutions that license Qwickly Attendance first need to opt-in to have this type of information cached with Qwickly and individual users have the right to opt-out at any point.

Qwickly Course Tools requests all of its information directly from the learning system (LMS/VLE) on a per use basis. The actions performed by Qwickly Course Tools work within the confines of the learning system and do not require Qwickly to store or cache any personal data.

The most current and updated information is available at https://www.goqwickly.com/privacy/.

ANNEX III – LIST OF SUB-PROCESSORS

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

None.