DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) reflects the parties’ agreement with respect to the processing of personal data pursuant to either Jotform’s Terms of Use that apply to Jotform's Starter, Bronze, Silver, and Gold customers (the "Terms"), or for our Enterprise customers, the Master Subscription Agreement ("MSA") between the parties, as applicable.

The term of this DPA shall follow the term of Controller’s Jotform subscription. Terms not otherwise defined herein shall have the meaning as set forth in the Terms or MSA, as applicable per the above.

Additional Definitions

“Controller” means the Jotform customer that has a Jotform subscription.

“Data Protection Law” means all applicable legislation relating to data protection and privacy including without limitation the the GDPR, supplementary laws and regulations to the GDPR and rules, regulations and binding decisions adopted by competent data protection supervisory authorities, UK GDPR, the UK Data Protection Act 2018 (and regulations made thereunder), the UK Privacy and Electronic Communications Regulations 2003, and the Swiss Data Protection Act (revFADP), together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms “process”, “processes” and “processed” will be construed accordingly.

“Data Subject” means the individual to whom Personal Data relates.

“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.

“GDPR” means the General Data Protection 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.

“Instructions” means the written directions from Controller to Processor that Processor shall process Personal Data as needed to provide Controller with access to and use of the Platform.

“Personal Data” means any personally identifiable information under applicable Data Protection Law.

“Platform” means Jotform’s form-building platform.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

"Processor" means Jotform Inc. or, if you are located in a jurisdiction where the contracting entity is a different Jotform entity, as set forth in our Terms of Use here or in our Enterprise contract with you, "Processor" means the applicable Jotform entity.

“Service” means the Jotform service as described in the Agreement.

“Standard Contractual Clauses” means the clauses attached hereto as Exhibit 1, set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as well as any modified clauses, described in the UK Addendum, attached hereto as Exhibit 2, set out by the United Kingdom pursuant to UK GDPR, the UK Data Protection Act 2018 (and regulations made thereunder), the UK Privacy and Electronic Communications Regulations 2003.

Details of the Processing

1. Categories of Data Subjects: (a) Parties who submit filled-in forms containing Personal Data to Controller pursuant to Controller’s use of the Platform, and (b) Controller and those acting on Controller’s behalf who provide Processor with their Personal Data pursuant to Controller’s use of the Platform.

2. Types of Personal Data. Personal data as defined in Article 4 of the GDPR.

3. Subject-Matter and Nature of the Processing. The subject-matter of Processing of Personal Data by Processor is the provision of the Platform to the Controller that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as specified herein.

4. Purpose of the Processing. Personal Data will be Processed for purposes of providing the Platform.

5. Duration of the Processing. Personal Data will be Processed for the duration of the applicable Platform subscription.

Controller Responsibility

Within the scope of the Terms, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy applicable to Controller, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data.

Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

Obligations of Processor

1. Compliance with Instructions. Controller acknowledges and agrees that they are the Controller of Personal Data and Jotform is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of the Instructions and within the scope of the applicable Data Protection Laws.

2. Security. Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, described in Appendix 2 to the Standard Contractual Clauses. Such measures include, but are not be limited to:

i. the prevention of unauthorized persons from gaining access to Personal Data processing systems (physical access control),

ii. the prevention of Personal Data processing systems from being used without authorization (logical access control),

iii. ensuring that persons entitled to use a Personal Data processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control),

iv. ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),

v. ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into or modified in, Personal Data processing systems (entry control),

vi. ensuring that Personal Data is Processed solely in accordance with the Instructions,

vii. ensuring that Personal Data is protected against accidental destruction or loss (availability control).

Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 inclusive of the GDPR), by (i) implementing and maintaining the security measures described under Annex II, (ii) complying with the terms of Section 4 of this DPA (Data Breaches); and (iii) providing the Controller with information in relation to the Processing in the event of a data security breach.

3. Confidentiality. Processor shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to the handling and processing of Personal Data.

4. Data Breaches. Processor will notify the Controller of a Data Breach affecting any Personal Data as described under all applicable Data Protection Laws. At the Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify affected data subjects of any Data Breaches and, if required under applicable law, to notify competent authorities.

5. Data Subject Requests. Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under applicable Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests.

6. Sub-Processors. Processor shall be entitled to engage Google Cloud and/or Amazon Web Services as Sub-Processors to fulfill Processor's obligations in providing storage for the Platform. If Processor intends to instruct other Sub-Processors, Processor will notify the Controller thereof in writing and will give the Controller the opportunity to object to the engagement of the new Sub-Processors within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the Controller proves that the use of such Sub-Processor would present

significant risks for the protection of its Personal Data). If the Processor and Controller are unable to resolve such objection, Controller may terminate its subscription by providing written notice to Processor.

Where Processor engages Sub-Processors, Processor will ensure that a contract is in place between Processor and each Sub-Processor that imposes on the Sub-Processor substantially the same obligations that apply to Processor under this DPA. Where the Sub-Processor fails to fulfill its data protection obligations, Processor will be responsible to the Controller for such failures. Controller shall have the right to obtain from Processor information reasonably necessary to confirm that the Sub-Processor is complying with its obligations to Processor to process Personal Data consistent with applicable data protection laws.

The provisions of this Section shall mutually apply if the Processor engages a Sub-Processor in a country outside the European Economic Area ("EEA") not recognized by the European Commission as providing an adequate level of protection for personal data. If, in the performance of this DPA, Processor transfers any Personal Data to a new sub-processor located outside of the EEA, Jotform shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

7. Data Transfers.

To the US: Controller acknowledges and agrees that, notwithstanding that Controller may have elected to have Personal Data stored in the EU, Personal Data could in very rare cases be transferred to the United States if Processor were to receive a demand for the data in connection with a judicial proceeding or a law enforcement request and where Processor believes that it has to produce the data. In such cases, the Data Privacy Framework (DPF / Privacy Shield) shall apply and the Standard Contractual Clauses shall not apply. Jotform Inc. is self-certified to the DPF. In cases of a transfer from the UK to the US, the UK-US Data Bridge shall apply.

Outside the US or to another country without a European Commission adequacy decision: The Standard Contractual Clauses at Exhibit 1 will apply with respect to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the Data Protection Law), with the exception of Personal Data that is transferred outside the UK, which is governed by the UK Addendum, attached hereto as Exhibit 2.

8. Deletion or Retrieval of Personal Data. Other than to the extent required to comply with Data Protection Law, following termination or expiry of Controller's subscription, Processor will delete all Personal Data (including copies thereof) in its possession processed pursuant to this DPA. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.

9. Other Stipulations. If and to the extent that any of the requirements of GDPR Section 28(a)-(h) are not explicitly addressed herein, this DPA is hereby deemed to include those requirements as

stipulations agreed to by the parties.

Audits

Controller may, once every year during the Term of its subscription, obtain information from Jotform necessary to demonstrate compliance with its obligations under GDPR Article 28, and Processor shall cooperate with Controller with regard to such audits. Processor shall not be required to provide or disclose information that would violate applicable law, a duty of confidentiality, or any other obligation owed to a third party.

FERPA

If, when, and to the extent that Jotform, in the processing of student records or data on behalf of a LEA (Local Educational Agency), (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and re-disclosure of personally identifiable information from education records, Jotform agrees to fully comply with all of its related obligations under FERPA.

CCPA

Jotform agrees that it shall not discriminate against any consumers for exercising their rights under the California Consumer Privacy Act, and that it shall not sell personal information of consumers. Jotform agrees to comply with its obligations under the CCPA, including complying with consumer requests for access, deletion, or opting out of the sale of their data.

General Provisions

In case of any conflict, this DPA shall take precedence over the Terms. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

Unless otherwise indicated by the UK Addendum, the parties indicated in the Section below entitled “Parties to this DPA” are agreeing to the Standard Contractual Clauses (where and as applicable) attached as Exhibit 1, the UK Addendum attached as Exhibit 2 to the extent legally applicable, and to all appendixes attached thereto. In the event of any conflict or inconsistency between this DPA, the Standard Contractual Clauses in Exhibit 1, and the UK Addendum in Exhibit 2, the Standard Contractual Clauses shall prevail where the EU GDPR governs and the UK Addendum will prevail where the UK GDPR governs. Effective 25 May 2018, Jotform will process Personal Data in accordance with the Data Protection Law requirements contained herein which are directly applicable to Processor’s provision of the Platform.

If Controller is located in the US, the Jotform entity that is a party to this DPA is Jotform Inc. If

Controller is located in the UK or the EU, the Jotform entity that is a party to this DPA is Jotform Ltd. If Controller is located in Australia, New Zealand, or Asia, the Jotform entity that is a party to this DPA is Jotform Pty Ltd. If Controller is located in any other place than those cited in this paragraph, the Jotform entity that is a party to this DPA is the Jotform company through which Controller obtained a subscription to use the Jotform platform.The terms of this DPA shall, upon the customer signing, be deemed to have been agreed to by Jotform without the need for a Jotform signature.

Controller shall electronically sign this DPA.

The parties hereby agree to the terms of this DPA.

EXHIBIT 1

The parties agree that the following Standard Contractual Clauses - as updated by the EU in June 2021, together with the annexes thereto, shall apply as to all transfers of personal data to countries outside the EEA without an adequacy decision.

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) (1) 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 (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 (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.

(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 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – 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.

Clause 7

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.

(b) Once it has completed the Appendix and signed Annex I, 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.

(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 organisational 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, 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. 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 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.

(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 authorised 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.

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 (4) (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:

(a) 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;

(b) 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;

(c) 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

(d) 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 non-compliance. 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 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 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.

(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. (8) 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.

(c) 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.

(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 sub-processor to fulfil 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 authorised 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 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.

(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 authorised 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, organisation 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 parties agree that the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall be the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), which shall act as competent supervisory authority. Where the Controller is in the UK, the supervising authority shall be the UK ICO.

(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 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.

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

(i) 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;

(ii) 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 safeguards (12);

(iii) 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.

(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 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(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 minimisation

(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:

(i) 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;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) 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 the Republic of Ireland.

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 the Republic of Ireland.

(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 - Parties; Details of the Processing

The data exporter is the Customer/Controller as identified in the DPA.

The data importer is Jotform Inc.

Data subjects include: Parties who submit filled-in forms (which forms have been provided to Controller by Jotform or which Controller has created using the Service) to Controller; and Controller's employees, staff, and contractors whose Personal Data has been provided by such parties to Jotform in connection with the Agreement.

The personal data transferred concern the following categories of data subjects: The data exporter may submit Personal Data to JotForm and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

• Prospective customers, customers, resellers, referrers, business partners, and vendors of the data exporter (who are natural persons);

• Employees or contact persons of the data exporter's prospective customers, customers, resellers, referrers, subcontractors, business partners, and vendors (who are natural persons);

• Employees, agents, advisors, and freelancers of the data exporter (who are natural persons); and/or

• Natural persons authorized by the data exporter to use the services provided by Jotform Inc. to the data exporter.

Categories of data: The personal data transferred concern the following categories of data may include, but is not limited to, the following categories of Personal Data: Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localization data (including IP addresses).

Special categories of data (if appropriate): The personal data transferred concern the following special categories of data: The data exporter may submit special categories of data to JotForm and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sexual and gender orientation.

Processing operations: The personal data transferred will be subject to the following basic

processing activities: Processing of the data in order for JotForm to provide the Service to the Customer.

Processing locations: Data is processed by Jotform in the US, by our subprocessors (see below), and occasionally as needed by Jotform to provide the Service and to comply with Jotform's legal obligations, at locations such as the UK and Turkey.

Subprocessors: See https://www.jotform.com/subprocessors/ for a list of the same. Data is not typically transferred to subprocessors. Any such transfers would be for the purpose of providing the Service to the customer.

Period of processing upon transfer: Usually in one day or less. The data is retained for as long as necessary to provide the Service to the customer, i.e., as set forth in the contract or terms of use applicable to the customer.

Annex II - Security Measures

Processor agrees to implement the following security measures to protect Personal Data

Access Control of Processing Areas

Data importer/subprocessor implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- establishing security areas;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data center where personal data are hosted is logged, monitored, and tracked; and
- the data center where personal data are hosted is secured by appropriate security measures.

Access Control to Data Processing Systems

Data importer/subprocessor implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- use of adequate encryption technologies;
- identification of the terminal and/or the terminal user to the data importer/subprocessor and processing systems;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- all access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer/subprocessor commits that the persons entitled to use their data processing

system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the personal data;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of adequate encryption technologies;
- control of files, controlled and documented destruction of data.

Availability Control

Data importer/subprocessor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy;
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data importer/subprocessor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- certain highly confidential employee data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system;
- providing user alert upon incomplete transfer of data (end to end check); and
- as far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Data importer/subprocessor implements suitable input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time;
- proof established within data importer/subprocessor’s organization of the input authorization; and
- electronic recording of entries.

Separation of Processing for different Purposes

Data importer/subprocessor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- modules within the data importer/subprocessor’s database separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data is stored in different normalized tables, separated per module, per Controller Customer or function they support;
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data importer/subprocessor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/subprocessor shall take reasonable steps to

ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Annex II.

Monitoring

Data importer/subprocessor shall implement suitable measures to monitor access restrictions to data importer/subprocessor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;

- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;

- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/subprocessor and applicable laws;

- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.

UK Addendum to Standard Contractual Clauses

International Transfer Agreement

This UK Addendum to Standard Contractual Clauses International Transfer Agreement ("**Addendum**") has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Table 1: Parties

Start Date	The Effective Date of the Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' Details	Customer	Jotform Inc. (US) or Jotform Ltd (UK)
Key Contact	Attn: Customer email: electronic mail address provided for Customer's account owner	Attn: General Counsel email: legal@jotform.com

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs:	The version of the Approved EU SCCs which this Addendum is appended to, detailed below: Module 2, as set out in Schedule 2 to the DPA.
Module:	Module 2, as set out in Schedule 2 to the DPA.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendices of the Approved EU SCCs as incorporated by reference into the DPA and set forth in Schedule 2 of the DPA.

Annex I: List of Parties: As set out in the Agreement.

Annex I: Description of Transfer: As set out in the DPA and/or the terms of use or master service agreement.

Annex II: Technical and organizational measures including technical and organisational measures to ensure the security of the terms of use, or at https://www.jotform.com/security/.

Annex III: List of sub-processors: As set out in https://www.jotform.com/subprocessors/.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum Changes	Which Parties may end this Addendum as set out in Section 19: Importer (yes) Exporter (yes) neither Party (no)

Part 2: Mandatory Clauses. Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.