Inversoft Inc.

Data Processing Addendum

(to be attached as needed)

This Data Processing Addendum (the "**DPA**") forms a part of, and is incorporated into, the Customer License Agreement between Inversoft Inc., dba FusionAuth ("**FusionAuth**") and Customer ("**Agreement**"). All capitalized terms not defined herein shall have the meaning set forth in the Agreement. The parties agree as follows:

1. DEFINITIONS

1.1 "**Applicable Data Protection Law(s)**" means the data protection laws, rules and regulations that are applicable to FusionAuth. With respect to Personal Data from the EU, "Applicable Data Protection Law(s)" shall include, but not be limited to the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). With respect to Personal Data from California residents, as of January 1, 2020, "Applicable Data Protection Law(s)" shall include, but not be limited to the California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100-1798.199).

1.2 "**Customer Personal Data**" means Personal Data received by FusionAuth pursuant to the Agreement and pertaining to Customer's current, former, or potential customers, employees, vendors, or other individuals who are, based on information known to FusionAuth, residents of the European Union or California.

1.3 "**Data Subject**" means (i) an identified or identifiable natural person who is in the European Economic Area (EEA) or whose rights are protected by the GDPR; or (ii) a "Consumer" as the term is defined in the CCPA.

1.4 "**EU**" or "**European Union**" means the European Union inclusive of the United Kingdom, whether or not the United Kingdom has officially withdrawn from the European Union, as well as Switzerland.

1.5 "**Personal Data**" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Law(s).

1.6 "**Process**", "**Processes**", "**Processing**", "**Processed**" shall have the meanings assigned to them in the Applicable Data Protection Laws.

1.7 "**Security Incident**" means an event about which FusionAuth knows, discovers, is notified of, or reasonably suspects that, Customer Personal Data has been accessed, disclosed, acquired or used by unauthorized persons, in violation of Applicable Data Protection Law(s).

1.8 "**Sub-Processor**" means FusionAuth's contractors, agents, vendors, and third-party service providers, that Process Customer Personal Data.

2. DATA HANDLING AND ACCESS

2.1 **General Compliance**. Customer hereby authorizes and instructs FusionAuth to, and FusionAuth will, and will require Sub-Processors to, Process Customer Personal Data in compliance with the Agreement, this DPA, and all Applicable Data Protection Law(s). Customer represents and warrants that it has all authority, grounds, rights, and consents necessary to enable such processing of the Customer Personal Data pursuant to the Agreement, in accordance with the Applicable Data Protection Law(s).

2.2 FusionAuth and Sub-Processor Compliance. FusionAuth agrees to (i) enter into a written agreement with Sub-Processors regarding such Sub-Processors' Processing of Customer Personal Data that imposes on such Sub-Processors data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Law(s), and that, at a minimum, require a level of data protection and security equal to or superior to the level of data protection and security under this DPA; (ii) reasonably enforce compliance with such written agreement; and (iii) remain responsible to Customer for the actions or omissions of FusionAuth's Sub-Processors (and their sub-processors if applicable) with respect to the Processing of Customer Personal Data.

2.3 Authorization to Use Sub-Processors. Customer hereby authorizes (i) FusionAuth to engage Sub-Processors and (ii) Sub-Processors to engage sub-processors. FusionAuth will provide Customer, upon Customer's request, the name, address and role of each Sub-Processor used to Process Customer Personal Data and any other records of Processing of Customer Personal Data that Sub-Processors are required to maintain and provide under Applicable Data Protection Law(s). Customer hereby approves of the following Sub-Processors:

Name	Location
[Complete]	US
[Complete]	US

2.4 Objection Right for New Sub-Processors. FusionAuth will inform Customer of any new Sub-Processor in connection with the provision of the applicable Offerings. Customer may, on reasonable grounds, object to FusionAuth's use of a new Sub-Processor by notifying FusionAuth promptly in writing within ten (10) business days after receipt of such information, giving reasons for Customer's objection. In the event Customer objects to a new Sub-Processor, as permitted in the preceding sentence, FusionAuth may address the concerns with respect to the Sub-Processor, or recommend a commercially reasonable change to Customer's configuration or use of the Offerings to avoid Processing of Personal Data by the objected-to Sub-Processor without unreasonably burdening the Customer. If FusionAuth does not do so within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to any such Offerings which cannot be provided by FusionAuth without the use of the objected-to new Sub-Processor by providing written notice to FusionAuth. This termination right is Customer's sole and exclusive remedy to Customer's objection of any Sub-Processor appointed by FusionAuth. FusionAuth will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Order Form(s).

2.5 Following Instructions. FusionAuth will Process Customer Personal Data only in accordance with the written instructions of Customer and may process Customer Personal Data for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by users in their use of the Offerings; (iii) Processing to further develop and provide services to FusionAuth's customers, (iv) Processing to facilitate the anonymization of Personal Data, and (v) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email).

2.6 Details of the Processing. The subject matter of Processing of Personal Data by FusionAuth is the performance of the Offerings pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data

Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. COMPLIANCE

3.1 Rights of Data Subjects. FusionAuth will, to the extent legally permitted, promptly notify Customer if FusionAuth receives a request from a Data Subject to exercise the Data Subject's rights afforded to such Data Subject under Applicable Data Protection Law(s) ("**Data Subject Request**"). To the extent Customer does not have access to the applicable Customer Personal Data, FusionAuth will (i) assist Customer by appropriate technical and organizational measures for the fulfilment of Customer's obligation to respond to a Data Subject Request under Applicable Data Protection Laws, and (ii) FusionAuth will, upon Customer's request and at Customer's expense, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent FusionAuth is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws.

3.2 FusionAuth Data Transfer Mechanism. For all transfers of EU Personal Data pursuant to the Agreement, the parties hereby incorporate the Standard Contractual Clauses approved by the European Commission (the "SCCs") as Schedule 2. To the extent there is any conflict between the body of this DPA and the SCCs, the SCCs shall control.

3.3 Prior Consultation. FusionAuth agrees to provide reasonable assistance to Customer (at Customer's expense) where, in Customer's judgement, the type of Processing performed by FusionAuth is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

3.4 Demonstrable Compliance. FusionAuth agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s) and provide such records to Customer upon request. If FusionAuth is collecting Customer EU Personal Data on Customer's behalf, such records shall include but not be limited to (i) the legal basis for Processing specified by Customer or (ii) records of the verifiable consent specified by customer under Applicable Data Protection Law(s).

3.5 Sale of Personal Data. FusionAuth shall not sell Customer Personal Data as the term "sell" is defined by the CCPA. FusionAuth shall not disclose or transfer Customer Personal Data to a "third party" as the term is defined by the CCPA or other parties that would constitute "selling" as the term is defined by the CCPA. The foregoing restrictions will not apply to "aggregate consumer information" or "deidentified personal information" as each term is defined by the CCPA.

3.6 Service Provider. FusionAuth shall not retain, use, or disclose Customer Personal Data (i) for any purpose other than for the specific purpose of performing the services specified in the Agreement, or (ii) outside of the direct business relationship between Customer and FusionAuth, in each case except as otherwise permitted by the CCPA.

4. INFORMATION SECURITY

FusionAuth will maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data.

5. ASSESSMENTS, AUDITS AND REMEDIATION

5.1 Assessments. Records to demonstrate compliance with this DPA and Applicable Data Protection Law(s) will be maintained by FusionAuth and provided to Customer upon request.

FusionAuth will complete within two weeks any reasonable data protection questionnaire provided by Customer.

5.2 Audits. For the purpose of verifying FusionAuth's compliance with Applicable Data Protection Law(s) and this DPA and upon reasonable notice of no less than thirty (30) days, FusionAuth agrees to permit Customer, at Customer's cost and no more than once annually, to conduct audits through a FusionAuth-approved third-party auditor, however, if FusionAuth has completed a third-party audit within the six months prior to Customer's audit request pursuant to this Section, FusionAuth may provide the results of such third-party audit to satisfy Customer's audit request. However, FusionAuth agrees to allow audits to be conducted directly by Customer where, under Applicable Data Protection Law(s), Customer is required to conduct audits directly. FusionAuth agrees to cooperate in good faith with the audit and promptly (i) provide access to books, records (including, but not limited to, security scan records), and other information necessary for the audit, and (ii) at Customer's request enable access to FusionAuth's premises if absolutely necessary to properly conduct the audit or required under Applicable Data Protection Law(s). Notwithstanding the forgoing, Customer may not conduct any security scans or other intrusion testing on FusionAuth's systems without the express prior written consent of FusionAuth. Customer agrees to (x) schedule audits to minimize disruption to FusionAuth's business, (y) require any third party it employs to sign a non-disclosure agreement, and (z) make the results of the audit available to FusionAuth. Customer will only disclose the results of the audit to third parties to the extent such disclosure is (A) required to demonstrate Customer's own compliance, or (B) otherwise required under the Applicable Data Protection Laws.

5.3 Remediation. FusionAuth agrees to promptly take action to correct any documented material security issue affecting Customer Personal Data identified by such audit and to inform Customer of such actions. If action is not promptly taken, Customer's sole remedy will be to terminate any or all Order Forms at Customer's discretion provided that FusionAuth will incur no penalty for any such termination.

6. SECURE DISPOSAL

Customer Personal Data will be securely disposed (i) during the Term of the Agreement, upon Customer's written request if such Customer Personal Data is no longer reasonably required to perform the Offerings, (ii) at the termination of the provision of the Offerings. If instructed by Customer, a copy of such Customer Personal Data will be returned to Customer prior to disposal. FusionAuth may retain Customer Personal Data in its encrypted backups in accordance with its internal data retention policies and to the extent that it is required or permitted to do so under Applicable Data Protection law(s).

7. CHANGES TO REQUIREMENTS

FusionAuth may amend or supplement this DPA from time to time to reflect new requirements under Applicable Data Protection Law(s). In the event of any material change to this DPA, FusionAuth will provide notice to Customer in accordance with the Agreement.

8. SECURITY INCIDENT

8.1 Policy. FusionAuth will, to the extent required under Applicable Data Protection Laws, notify Customer without undue delay after becoming aware of any Security Incident. FusionAuth will make reasonable efforts to identify the cause of such Security Incident and take those steps as FusionAuth deems necessary and reasonable in order to remediate the cause of such Security Incident to the extent the remediation is within FusionAuth's reasonable control. The obligations herein shall not apply to Security Incidents that are caused by Customer or Customer's Users.

8.2 Reports. Upon request by Customer, FusionAuth will enable Customer to review the results of and reports relating to the investigation and response to a Security Incident, which Customer will treat as Confidential Information of FusionAuth.

9. TERMINATION OBLIGATIONS

Notwithstanding anything to the contrary in the Agreement or this DPA, Customer may terminate any Order Form, or any portion thereof, immediately upon written notice to FusionAuth, and without judicial notice or resolution or prejudice to any other remedies, in the event a data protection or other regulatory authority or other tribunal or court in any country finds there has been a breach of Applicable Data Protection Law(s) by virtue of Customer's or FusionAuth's Processing of Customer Personal Data in connection with the Agreement, and such breach has not been cured within sixty (60) days of FusionAuth's receiving notice thereof.

10. CONTACT INFORMATION

FusionAuth will designate a point of contact as its "Privacy and Security Coordinator". This Privacy and Security Coordinator will: (i) maintain responsibility for applying adequate protections to Customer Personal Data, including the development, implementation, and maintenance of its information security program, (ii) oversee application of FusionAuth compliance with the requirements of this DPA, and (iii) serve as a point of contact for internal communications and communications with Customer pertaining to this DPA and compliance with or any breaches thereof.

SCHEDULE 1

Nature and Purpose of Processing

FusionAuth will Process Personal Data as necessary to provide the Offerings pursuant to the Agreement, as further specified in the Order Form, and as further instructed by Customer in its use of the Offerings provided by FusionAuth.

Duration of Processing

FusionAuth will Process Personal Data for the duration of the Term, as provided in the DPA, and as otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Offerings relating to the following categories of data subjects:

- Current or potential clients, business partners and vendors of Customer (who are natural persons);
- Employees, officers, directors, contractors or contact persons of Customer's third-party suppliers, business partners and vendors;
- Customer users authorized by Customer to use the relevant Offerings.

Type of Personal Data

Customer may submit Personal Data to the Offerings, the extent of which is neither determined nor controlled by FusionAuth, and which may include, but is not limited to the following categories of Personal Data:

- Contact details (e.g. name, postal address, job title, job position, location, employer, relationship with the organization, e-mail address, password, telephone number, postal address);
- Additional content and user data that Customer submits to the Offerings;
- Information regarding a support issue relating to the Offerings;
- Information contained in employee communications related to support issues routed through the Offerings.

SCHEDULE 2

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name, Address, Tel., Fax, E-Mail of the data exporting organisation:

See ordering document or other agreement pursuant to which data exporter purchases services from data importer. (the data **exporter**)

And

Name of the data importing organisation: Inversoft Inc., dba FusionAuth

Address: 1630 Welton Street, Denver, CO 80202

Tel: N/A; fax: N/A; e-mail: support@fusionauth.io

Other information needed to identify the organisation:

("**FusionAuth**")
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data

importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Brian Pontarelli

Position: Chief Executive Officer

Address: 1630 Welton Street, Denver, CO 80202

Other information necessary in order for the contract to be binding (if any):

Signature…DocuSigned by: Brian Pontarelli D266F2CC3F354D4…….

(stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

(i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and, (ii) all affiliates of such entity established in the European Economic Area (EEA) and Switzerland that have purchased Offerings from FusionAuth.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

a provider of an authentication, authorization, and user management platform for its customers ("data exporter" or "data controller") that processes personal data upon the instruction of the data exporter pursuant to the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Employees, officers, directors, vendors, contractors, customers, and other related or third parties working with or for data exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Contact details (e.g., name, postal address, email address, password, and telephone number); comments, and other content or information data subjects may submit to data importer through the application.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Although the data importer has advised the data exporter against including any sensitive data in the personal data that is transferred, individuals entering data to the application can include any information they choose. The data exporter controls such data in its sole discretion.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Personal data may be transferred through a third party hosted cloud environment or through SFTP or API protocols. All transfers shall be in accordance with the DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See section 4 of the DPA.