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Union**" means the European Union inclusive of the United Kingdom, whether or not the United Kingdom has officially withdrawn from the European Union, as well as Switzerland.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
Amazon Web Services (AWS)	Worldwide
N/A	

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. These technical and organizational measures are documented explicitly in the provided document "Inversoft Technical and Organizational Measures" with the current version being 2.1 of September 2021.

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

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.

(a) The Parties:

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

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

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

(c) 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

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

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:

(ii) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(iii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iv) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(v) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(vi) Clause 13;

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

(viii) Clause 16(e);

(ix) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(d) 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.

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

(h) 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.

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(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.

(j) 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.

(k) 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.

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has

third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9 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.

(m) 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.

(n) 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.

(o) 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.

(p) 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) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] 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.

(q) 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.[3] 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.

(r) 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.

(s) 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.

(t) 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.

(u) 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.

(v) 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

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[4] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(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.

(w) 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.

(x) 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.

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

(z) 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.

(aa) 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.

(bb) 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

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(cc) 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.

(dd) 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.

(ee) 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.

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

Clause 13

Supervision

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

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

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(gg) 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.

(hh) 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[5];

(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.

(ii) 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

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

agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

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

(kk) 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). [For Module Three: The data exporter shall forward the notification to the controller.]

(ll) 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 [for Module Three: , if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(mm) 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.

(nn) 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.). [For Module Three: The data exporter shall forward the information to the controller.]

(oo) 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.

(pp) 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).

(qq) 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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(rr) 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.

(ss) 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).

(tt) 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 [for Module Three: and the controller] 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.

(b) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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.

(c) 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

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): 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 _____ (*specify Member State*).]

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.

(d) The Parties agree that those shall be the courts of _____ (*specify Member State*).

(e) 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.

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

APPENDIX

ANNEX I

A. LIST OF PARTIES

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

1. Name:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date: …

Role (controller/processor): Controller

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

1. Name: Inversoft, Inc, (DBA FusionAuth)

Address: 1630 Welton Street, Suite 600A, Denver, CO, USA 80202

Primary contact:

Don Bergal

Chief Executive Officer

don@fusionauth.io

Responsible for data protection:

Brian Pontarelli

Chief Security Officer

brian@fusionauth.io

Activities relevant to the data transferred under these Clauses: data processing for the performance of the Master Agreement

Signature and date: …

Role (controller/processor): Processor…

B. DESCRIPTION OF TRANSFER

See SCHEDULE 1 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 is [please include depending on where the Art. 27 Representative is located].

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

See section 4 of the DPA.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:
See section 2.3 of the DPA.