DATA PROCESSING AGREEMENT

This data processing agreement (the "***DPA***") is executed upon the date of the last signature ("***DPA Effective Date***") by and between FluentPro Software Corporation ("FluentPro" or "***Service Provider***") and the customer of FluentPro ("***Customer***") to amend the FluentPro Software as a Service Subscription Agreement governing the provision of Services (the "***MSA***").

This DPA is incorporated into and subject to the MSA and reflects the parties' agreement with respect to the terms governing the processing of personal data under the MSA. If there is a conflict in terms between this DPA and the MSA, this DPA shall control. The Standard Contractual Clauses, set forth as Exhibit A, form an integral part of this DPA. Capitalized terms used but not defined in this DPA will have the meaning provided in the MSA.

1. **DEFINITIONS**

   The terms "*personal data*", "*data subject*", "*controller*", "*processing*" and "*processor*" will have the meanings ascribed to them in Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council.

2. **TERM**

   This DPA will take effect on the DPA Effective Date and automatically terminate upon the expiry or termination of the MSA.

3. **SCOPE AND ROLES**

   This DPA applies when Service Provider processes personal data on behalf of Customer. In this context, Customer is the controller and Service Provider is the processor for Customer. Personal data processed by Service Provider on behalf of Customer will be defined as "***Customer Data***".

4. **INFORMATION SECURITY**

   Service Provider shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data. Service Provider's current security program is further specified in Annex II to Exhibit A. The security program is reviewed by the Service Provider on an annual basis. Service Provider shall monitor, analyze and respond to security incidents in a timely manner in accordance with Customer's instructions.

5. **AFFECTED PERSONS/CATEGORIES OF DATA**

   The affected persons and categories of the personal data processed are specified in Annex I.B. to Exhibit A.

6. **PERSONNEL**

   Service Provider ensures (a) that its personnel with access to Customer Data are subject to written obligations to maintain the confidentiality of such data and (b) that such

personnel are adequately instructed in the appropriate handling of personal data. Service Provider shall implement measures to restrict access to personal data.

7. RECTIFICATION, RESTRICTION AND ERASURE

Service Provider may not on its own authority rectify, erase or restrict the processing of personal data, but only on documented instructions from Customer. Insofar as a data subject contacts the Service Provider directly concerning a rectification, erasure, or restriction of processing, the Service Provider will immediately forward the data subject's request to Customer. The erasure, 'right to be forgotten', rectification, data portability and access shall be ensured by the Service Provider in accordance with documented instructions from Customer without undue delay.

8. AUDIT RIGHTS

Customer has the right, after consultation with the Service Provider, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. Customer has the right to convince itself of the compliance with this DPA by the Service Provider in his business operations by means of random checks, which are ordinarily to be announced in good time.

9. SUBPROCESSING

The engagement of sub-processors is subject to Clause 9 of Exhibit A.

10. PROCESSING OF CUSTOMER DATA

Service Provider will only process Customer Data in fulfilling its obligations under the MSA. The processing of Customer Data only takes place within the framework of the MSA and according to the instructions of Customer. In particular, the collected, processed or used data may only be corrected, deleted or blocked on instructions of Customer. Backup copies are created, if they are necessary to ensure proper data processing, or reproduction processes that are necessary in order to ensure compliance with regulatory retention requirements. All instructions must be issued in writing. If this is not possible in individual cases, Customer shall instruct Service Provider verbally and confirm this instruction in writing.

11. DATA SUBJECT ACCESS REQUESTS

Service Provider will provide all required assistance to Customer in the fulfillment of Customer's obligation to respond to data subject requests for the correction, transfer or deletion of personal data, at no costs. If a data subject requests the correction or deletion of their personal data directly from Service Provider, Service Provider will promptly pass this request to Customer.

12. ASSISTANCE, REPORTING AND IMPACT ASSESSMENTS

Service Provider will provide all required assistance to Customer in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 GDPR.

13. BREACH NOTIFICATION

Service Provider shall report to Customer the unauthorized acquisition, access, use, disclosure or destruction of Customer Data ("***Breach***") promptly after a Breach has occurred. Unless prohibited by a law enforcement agency as part of the investigation efforts, Service Provider shall share information about the nature and consequences of the Breach that is reasonably requested by Customer to enable it to notify affected individuals, government agencies and/or credit bureaus.

14. RETURN AND DELETION OF CUSTOMER DATA

The return and deletion of Customer Data after the termination of the MSA shall be in accordance with Clause 8.5 of Exhibit A.

15. LIABILITY

Each party's liability arising out of or in relation to this DPA shall be subject to the Clause 12 of Exhibit A. Notwithstanding anything contained herein, FluentPro total liability arising out of or in relation to this DPA shall be subject to the 'Limitation of Liability' section of the MSA.

Exhibit A

Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

(d) The Appendix 1.2 to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

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

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e);

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Module Two: Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time,
either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses
and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 **Instructions**

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

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

8.2 **Purpose limitation**

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

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix 1.2 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 1.2 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.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data

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

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

8.7 **Sensitive data**

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

8.8 **Onward transfers**

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

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

(i) the onward transfer is to a country 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.

8.9 **Documentation and compliance**

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

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

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

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least one month in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to

exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

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

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

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

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

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

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

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

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

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to

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

MODULE TWO: Transfer controller to processor

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

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

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

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12

Liability

MODULE TWO: Transfer controller to processor

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

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

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

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim

back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

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

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

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

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

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

of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

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

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [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

MODULE TWO: Transfer controller to processor

15.1 **Notification**

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

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

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

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the

competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

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

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

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

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data

importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts in the EU Member State in which the relevant Data Exporter is established.

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

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

ANNEX I

A. **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

Data exporter(s):

The Data Exporter is a legal entity that has created an account with FluentPro for provision of the Services and has a role of the Controller.

Data importer(s):

1. Name: FLUENTPRO SOFTWARE CORPORATION

   Address: 1275 12th Ave NW, Suite 2, Issaquah, WA 98027

   Contact person's name, position and contact details: legal@fluentpro.com

   Activities relevant to the data transferred under these Clauses: The data importer will host and process Customer Data in the course of providing its Services and related software operations, support and maintenance services. In the course of the aforementioned activities, the data importer may require access to Customer Data to fulfil its obligations under the MSA.

2. Role (controller/processor): Processor

B. **DESCRIPTION OF TRANSFER**

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred
Customer may submit Customer Data to Service Provider, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Customer Data relating to the following categories of data subjects:

- Customers, resellers, business partners and vendors of Customer
- Employees, agents, contractors, freelancers of Customer
- Customer's Users authorized by Customer to use the Services

Categories of personal data transferred

Customer may submit Customer Data to Service Provider, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following categories of Customer Data:
- Personal Data (such as name, title, position, employer)
- Contact Data (such as email, phone, fax, etc.)
- Contract Billing and Payments Data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed

specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data exporter will not transfer sensitive data to the data importer.

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

Data will be transferred on a continuous basis while the MSA executed with Customer is effective.

Nature of the processing
Data is processed in the course of provision of Services and related software operations, support and maintenance services. Data is processed to identify Customer's end users, support them in software usage, and provide maintenance services. Number of software operations is based on storage, processing and structuring of Customer's data.

Purpose(s) of the data transfer and further processing
Data is transferred and further processed in the course of provision of Services to Customer for a number of purposes, including the identification of and communication with Customer's end users; effective usage and utilization of provided software products; effective usage of FluentPro websites, including websites containing software documentation, by Customer's end users; support of Customer's end users; maintenance of software operation; etc.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
The personal data is retained while the MSA executed with Customer is effective and / or Customer's end users have active software subscriptions with FluentPro. Every software product has its own data retention policy after the software subscription is suspended, the usual data retention period for suspended subscriptions is 90 calendar days.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
In usage of sub-processors, subjects and duration of the processing will be the same as stated above for data importer. The nature of the processing is storage and processing of personal data in cloud infrastructure provided by sub-processors.

C. **COMPETENT SUPERVISORY AUTHORITY**

MODULE TWO: Transfer controller to processor

The competent supervisory authority/ies in accordance with Clause 13 of is the Supervisory Authority at the location of Data Exporter.

ANNEX II

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

MODULE TWO: Transfer controller to processor

Measures of encryption of personal data

DATA WHILE STORED.

This includes any data located on company-owned or company-provided systems, devices, media, etc.

Application encryption

All data transmitted between FluentPro application components is encrypted with FIPS 140-2 compliant encryption algorithms. Protection of data at rest include minimum industry standard AES-256 encryption. The Web Apps are additionally encrypted with Azure Key Vault.

Encryption of virtual machines

All physical infrastructure is located in Microsoft Azure with a server-side encryption model currently with service managed keys. Windows virtual machines are encrypted by using Azure disk encryption, which uses Windows BitLocker technology to protect both operating system disks and data disks with full volume encryption. Encryption keys and secrets are safeguarded in Azure Key Vault. By using the Azure Backup service, encrypted virtual machines (VMs) that use Key Encryption Key (KEK) configuration can be backed up and restored.

Encryption of data storage

All information stored locally on a FluentPro owned computers or portable devices is kept to a minimum and stored on internal encrypted data storage - SharePoint Online (OneDrive, Microsoft Teams). OneDrive is used as a corporate data storage solution for internal and customer-related information. Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content. BitLocker is deployed for OneDrive for Business and SharePoint Online across the service.

DATA WHILE TRANSMITTED.

This includes any data sent across the company network or any data sent to or from a company-owned or company-provided system.

TLS/SSL encryption in Azure

The latest TLS protocol is used to protect data when it is transferred between Microsoft Cloud Services and FluentPro systems.

Communication with corporate external resources

All access to corporate external resources is protected with HTTPS with TLS 1.2.

Remote access

Remote access allows users to access data from outside of the FluentPro network. The access to the company's network is restricted to a limited number of authorized users and the rights are granted by IT Staff and Management. The network access is encrypted with L2TP/IPsec VPN protocol.

Transmitting information via emails

Microsoft Outlook is used as a corporate e-mail software. Employees use only corporate emails and are not allowed to use web email programs and chats (Yahoo, Gmail, Skype, etc.) for work-related communication. Strictly confidential information is not be sent via email and stored in one of the corporate data storages and communicated per email via link to relevant folder or file.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

FluentPro has Security Incident Response Plan, the purpose of which is to be used in the event of a detection of a security incident, as well as a guidance for preparation activities to avoid security incidents in the organization. This Plan applies to the FluentPro information systems, data, and networks and any person or device who gains access to these systems or data. The Security Incident Response Plan contains the following general flow that is used for each reported security incident:

Stage 1. Preparation

The Preparation Stage helps to identify possible security incidents, develop preventive measures and proactively detect them.

Methods of detection and prevention are kept up-to-date and renewed based on lessons learned during post-incident activity phase, as well as serve as a basis for security awareness training for all employees.

Stage 2. Detection & Diagnosis

Detection of a security incident is done in different ways depending of a type of a security incident occurred, such as:

- Detection of suspicious activities by internal monitoring and diagnostic systems (MS Azure Security Center, 24/7). These alerts come in the way of signature-based alarms such as antimalware, intrusion detection
- Detection of a suspicious activities or loss / theft of equipment or information by employees. If employees are made aware of any signs of security incidents, they promptly escalate a threat to a member of IT team.

A member of IT Team indicates an incident and makes the first investigation. During initial investigation the following main steps take place:

- Retrieval of information to confirm an incident;
- Definition of a type of incident, its severity, degree of loss/ damage;
- Assignment of a person who will handle the incident (who is free / on duty, competent in this area)
- Decision on the necessity to involve other internal teams.

If IT Team believes that customer data may have become exposed to an unlawful or unauthorized individual, parallel notification process of all involved parties begin. Customer Care Team will notify with undue delay all affected customers via email. The notification include a description of the security incident, categories of data affected, nearest measures to be taken and contact details of the responsible team. If a security incident involves a big number of customers, additional notification is posted on FluentPro Services Status Page: https://status.fluentpro.com/. Customer Care Team support customers until the incident is eradicated and inform which measures are taken or will be taken to prevent such incident type in the future.

Stage 3. Containment

The purpose of the Containment Stage is to limit any damage and prevent any further from occurring.

The emergency mitigation steps to resolve immediate security risks associated with the event are taken. The emergency steps include:

- Malware detected by antivirus software: disconnect computer from Internet / WLAN, wait for anti-virus to fix a problem.
- Physical break-in: report to security guides of the office building, call police, check video-surveillance cameras, determine if IT assets, information or resources have been damaged or stolen.
- Network attack: change firewall configurations to stop attacker;
- Compromised system: remove the system physically from the network. Remove all network cables, modem connections, and wireless network interfaces. All log files, pertaining to a compromised computer, that are stored on a secondary computer or on some type of external media should be preserved immediately.
- Compromised user credentials: determine all of the computers or mobile devices used with credentials, determine what websites have been accessed by entering the same user name and password.
- Theft or loss of equipment: check if the device was encrypted, determine if information could have been stolen/ compromised, compile the list of all user credentials, that were used on the device for immediate password change.

Stage 4. Eradication and Recovery

Once IT Team contains a security incident, it moves to Eradication and Recovery Stage, which include work towards eliminating the root cause of the security incident with a high degree of confidence and restoring operations to normal. While the exact steps involved in eradication and recovery are dependent on the incident type, the following areas and activities are considered:

- Patching and hardening of systems;
- Implementing password changes;
- Implementing changes in encryption mechanisms and algorithms;
- Improving monitoring and defenses.

Stage 5. Post-Incident Activity

The goal of a post-incident activity is to identify technical lapses, procedural failures, manual errors, process flaws and communication glitches, and/or any previously unknown attack vectors that were identified during the security incident response. The post-incident analysis is conducted by IT Team and IT Process Manager.

All key technical findings are captured in a report as well as service investments or fixes in the form of bugs or development change requests that are then followed-up with the corresponding engineering teams.

Measures for user identification and authorization

FluentPro solutions do not have an embedded password management and support a single sign-on authentication with the Microsoft Office 365 / Azure Active Directory which allows end users to apply password policy that is set in their organization. Fluentpro internal password policy has strong complexity, expiration, and lockout requirements. FluentPro grants access on a need to know on the basis of least privilege rules only after a formal approval by IT staff and management, reviews permissions quarterly, and revokes access immediately after employee termination. All employees are provided with information on a current password protection policy as a part of Security Awareness Training. The training covers password requirements set for all systems and accounts of the company.

Measures for ensuring physical security of locations at which personal data are processed

FluentPro's information systems and technical infrastructure are hosted on Microsoft Azure Cloud that provides robust physical datacenter security and environmental controls. The Microsoft Azure infrastructure is designed and managed to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. Security controls provided by our cloud provider facilities include but are not limited to:

- 24/7 Physical security guard services
- Extensive physical entry restrictions to the building, facilities and datacenter floor
- Biometric access with two-factor authentication
- Video cameras monitoring, full body metal detection screening and security scans
- Independent power, cooling, and networking for each availability zone within Azure region.

To avoid the unauthorized access to personal data stored in Cloud infrastructure through FluentPro facilities, FluentPro implemented the following measures for ensuring physical security.

Protection of FluentPro facilities

The FluentPro facilities where information systems are located are protected with strict access controls including key and biometric authentication and 24/7 surveillance cameras. Secure areas are operated and maintained to minimize the risk from theft, fire, explosion, smoke, water, electrical supply interference. Any person who does not possess a special access control key cannot access the area of the company. As a part of the onboarding training all employees are made aware that they are not allowed to borrow their access control keys to other individuals.

Visitors in FluentPro facilities

Visitors cannot access the company's facilities without an escort of an employee of the company who has an access control key. Where practical, all visitors are restricted from areas where files containing personal information and data are stored. Alternatively, if needed, visitors are escorted or accompanied by an approved employee in any area with access to information systems and internal / confidential information.

Office opening and closure procedures

Office is opened each business day by an Office Manager according to "Office opening" checklist. Office is closed by a member of IT team after the end of the second shift according to "Office Closure" checklist.

Protection of IT equipment

Access to network equipment is separately isolated and locked when left unattended. All computers that access FluentPro network have a reasonably up-to-date version of software providing virus and anti-malware protection installed and active at all times. All rooms with access to computers, laptops and any other IT equipment are closed at the end of the business day and during weekends and holidays.

Measures for ensuring limited data retention

There are company-wide data retention policies that vary depending on data types and services provided to Controller. Furthermore, FluentPro empower its customers to control the data they share through their account. As long as the end user account is active, customer have full control over the specific types of data that are stored or transferred through FluentPro services. On FluentPro side, the customer's data is retained while the company remains an active client and this data is necessary to provide the services. In any case, the Customer's data is retained for no more than 90 days after the Customer's software subscription has ended / been terminated.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

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

1. Name: Microsoft Corporation

   Address: One Microsoft Way, Redmond, state of Washington, USA, 98052

   Contact person's name, position and contact details: Attn: Chief Privacy Officer

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Storage and processing of personal data in Microsoft Azure Cloud infrastructure.

2. Name: Zendesk, Inc.,

   Address: 989 Market Street, San Francisco, CA 94103

   Contact person's name, position and contact details: privacy@zendesk.com

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): storage and processing of personal data in the course of providing its cloud-based customer services, helpdesk platform services, and its cloud-based customer support live chat platform services to Data Processor.

3. Name: Amazon Web Services Inc.

   Address: 410 Terry Avenue North, Seattle, WA 98109-5210, USA

   Contact person's name, position and contact details: Attn: Chief Privacy Officer

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Storage and processing of personal data in Amazon Web Services Cloud infrastructure.

4. Name: MongoDB, Inc.

   Address: 1633 Broadway, 38th Floor New York, NY 10019, Attention: Legal Department

   Contact person's name, position and contact details: privacy@mongodb.com; 1-866-692-1371

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Storage and processing of personal data in MongoDB Atlas Databases.

5. Name: Totango Inc., Totango Metrics Ltd.

   Address: 1 Twin Dolphin Dr, Redwood City CA, 94065

   Contact person's name, position and contact details: privacy@totango.com.
   Description of processing (including a clear delimitation of responsibilities in case

several sub-processors are authorised): Storage and processing of personal data in the course of providing its cloud-based customer relationship management services.

6. Name: Intercom, Inc.

   Address: 55 2nd Street, 4th Fl., San Francisco, CA 94105, USA

   Contact person's name, position and contact details:

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Storage and processing of personal data in the course of providing its cloud-based Conversational Relationship Platform (in-app chat).

7. Name: Momentive Global Inc.

   Address: 1 Curiosity Way San Mateo, CA 94403 United States

   Contact person's name, position and contact details:

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Storage and processing of personal data in the course of providing its cloud-based surveying platform (Wufoo forms).

8. Name: CHARGEBEE INC.

   Address: 340 S Lemon Avenue, #1537, Walnut, California 91789, USA

   Contact person's name, position and contact details: privacy@chargebee.com

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Storage and processing of personal data in the course of providing its software subscription management platform.

9. Name: Segment.io Inc.

   Address: 101 Spear Street, Fl 1 San Francisco, CA 94105 USA Attention: Data Protection Officer

   Contact person's name, position and contact details: privacy@segment.com

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Storage and processing of personal data in the course of providing its Customer Data Management Platform.

10. Name: Google LLC and its affiliates

    Address: 1600 Amphitheatre Parkway in Mountain View, California

    Contact person’s name, position and contact details: protection-office@google.com, Emil Ochotta, Google's Data Protection Officer

    Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Storage and processing of personal data in the course of providing its Google Marketing Platform.

11. Name: Pipedrive Inc

    Address: 460 Park Ave South, New York, NY, 10016, USA

    Contact person’s name, position and contact details: support@pipedrive.com

    Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Storage and processing of personal data in the course of providing its customer relationship management system.