HEXASOFT DATA PROCESSING ADDENDUM

Published: May 30, 2018

Last revised: January 10, 2019

This HEXASOFT DATA PROCESSING ADDENDUM (this "Addendum") is entered into by and between Hexasoft Development Sdn. Bhd. ("Hexasoft") and you ("You" or the "Customer") (each a "Party", and collectively the "Parties"). If You are accepting the terms of this Addendum on behalf of an entity, You represent and warrant to Hexasoft that You have the authority to bind that entity and its affiliates, where applicable, to the terms and conditions of this Addendum. You are deemed to have accepted this Addendum on the later of the date on which you have accepted the Hexasoft End User License Agreement, or the Published date indicated above (the "Addendum Date").

RECITALS

WHEREAS, the Parties have entered into a Hexasoft End User License Agreement (the "Services Agreement") involving the Processing of Personal Data (as defined below) of Data Subjects (as defined below) that the Parties now desire to amend as provided herein;

WHEREAS, in the course of performance of the Services Agreement, Hexasoft transfers, transmits, and otherwise Processes certain Personal Data of Data Subjects;

WHEREAS, in connection with receiving services under the Services Agreement and operations thereunder, the Customer transfers, transmits, and otherwise Processes certain Personal Data of Data Subjects;

WHEREAS, each of the Parties require the other Party take all necessary measures to handle any information that may be regulated by the General Data Protection Regulation of the EU (GDPR) and other applicable laws and regulations in compliance with such laws; and

WHEREAS, the Parties enter into this Addendum with the intent to comply with the principles and standards for data protection as required by the GDPR and other applicable laws and regulations, with respect to the Processing of Personal Data under the Services Agreement.

NOW, THEREFORE, in consideration of the mutual agreements set forth in this Addendum, the Parties hereby agree as follows:

1. **Definitions.** Capitalized terms used but not defined in this Addendum shall have the meanings assigned to them in the Services Agreement. For the purposes of this

Addendum, the following capitalized terms shall have the meanings ascribed to them as set forth below wherever they appear within the provisions of this Addendum:

(a) "Applicable Laws" means all laws applicable to the Processing of Personal Data, including the GDPR, laws implementing or supplementing the GDPR, EU Directive 95/46/EC, as transposed into domestic legislation of each European Union Member State ("Member State") and as amended, replaced, or superseded from time to time, other laws of the European Union (EU) or any Member State, and the laws of any other country to which the Personal Data is subject;

(b) "Customer" means the party with whom Hexasoft has executed the Services Agreement, as indicated above;

(c) "Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by European Union or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by European Union or Member State law. For the purposes of this Addendum, Data Controller or Data Controllers also refers specifically to a Party or the Parties to this Addendum;

(d) "Data Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of a Data Controller;

(e) "Data Protection Regulator" means any governmental data protection regulator(s) with valid jurisdiction over the transfer, transmission or Processing of Personal Data pursuant to this Addendum, including, but not limited to, a "supervisory authority", as defined in Article 4(21) of the GDPR.

(f) "GDPR" and "General Data Protection Regulation" means 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, and repealing Directive 95/46/EC;

(g) "Personal Data" means any information relating to an identified or identifiable natural person within the scope of this Addendum ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(h) "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed;

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

(j) "Restricted Transfer" means any transfer of Personal Data that would be prohibited by Applicable Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Applicable Laws) in the absence of the execution of the Standard Contractual Clauses or another lawful data transfer mechanism, as set out in Section 12 below.

TERMS

2. **Effective Date.** The Terms of this Addendum shall take effect on the later of the Addendum Date, or May 25, 2018 (the "Effective Date").

3. **Scope.** This Addendum serves as a framework for Personal Data Processing under the Services Agreement, as well as for the transfer of Personal Data between the Parties as Data Controllers and defines the principles and procedures that the Parties shall adhere to and the respective responsibilities of the Parties.

4. **Applicability.** This Addendum will not apply to the Processing of Personal Data, where such Processing is not regulated by the Applicable Laws.

5. **Controllership Representations and Warranties.** Each Party represents, warrants, and covenants that:

(a) with respect to the Processing of Personal Data under the Services Agreement, it is a Data Controller within the meaning of this Addendum and the GDPR;

(b) all Personal Data has been and will be collected, transferred, and otherwise Processed in compliance with the GDPR;

(c) it will independently determine its obligations under the EU Data Protection Laws;

(d) it will only conduct transfers of Personal Data, where such transfers would be subject to any transfer or export restriction under the Applicable Laws (and no

lawful exemption or derogation applies), in compliance with all applicable conditions, as laid down in the Applicable Laws; and

(e) it will, in its capacity as a "data exporter" (as defined in Section 13(b)), upon request, inform the other Party, in that other Party's capacity as a "data importer" (as defined in Section 13(b)), of all relevant data protection laws governing the receipt of data from the data exporter, including citations to and the text of such laws.

6. **Records of Processing Activities.** Each Party agrees to maintain a record of Processing activities of Personal Data under its responsibility, in accordance with Article 30 of the GDPR.

7. **Processing of Personal Data.** Processing of Personal Data by each of the Data Controllers within the scope of this Addendum is subject to the following:

   (a) Processing is limited to those services and tasks outlined in the Services Agreement and any subsequent orders, statements of work, or work orders executed between the Parties.

   (b) Each Party shall ensure that the Processing of the Personal Data for the purposes set out in the Services Agreement, is performed only on lawful grounds pursuant to Article 6 of the GDPR, and as further limited by Article 9 of the GDPR, or the equivalent provisions of any Applicable Laws, as the case may be.

   (c) Each Party must ensure that persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8. **Security Measures.** Both Parties will implement appropriate technical and organizational security measures to ensure and to be able to demonstrate that Processing is performed in accordance with the GDPR, and in particular, in accordance with Article 32 of the GDPR. Such measures shall be reviewed and updated where necessary.

9. **Data Subject Requests.** Each Party will be responsible for responding to requests it receives for the exercise of a Data Subject's rights under Chapter III of the GDPR or the equivalent provisions of other Applicable Laws, with regard to the Personal Data Processed by that Party. Each Party will designate an appropriate point of contact for Data Subject requests within its organization. Each Party will maintain a record of Data Subjects' requests to exercise their data protection rights, the decisions made, and any information that was exchanged with the Data Subject. The Parties agree to provide prompt and reasonable assistance to each other, upon the request of the other Party, to enable them to comply with Data Subject requests, as contemplated by this section.

10. **Security of Processing and Personal Data Breach Notifications.** Both Parties agree to implement and maintain technical and organizational security measures to ensure that the level of security of Personal Data Processed by them is appropriate to the risk, pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of Processing and the information available to each Party. Each Party shall provide notification of a Personal Data Breach to the applicable Data Protection Regulator and the affected Data Subject(s), as required by Articles 33 and 34 of the GDPR and any other Applicable Laws, as well as all legally required assistance to the other Party.

11. **Processors.** Each Party shall only engage a Data Processor to Process the Personal Data on its behalf if that Data Processor provides sufficient guarantees to that Party, by way of a written contract or other legal act under European Union or Member State law, that it will implement the same data protection obligations as this Addendum and the requirements of the GDPR. Such obligations shall include, in particular, the requirement that the Data Processor implements appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR, including, but not limited to, applicable requirements of Articles 28, 29, and 30 of the GDPR, and ensure the protection of the fundamental rights of the Data Subject. Where that Data Processor fails to fulfill its data protection obligations, the applicable Party shall remain fully liable to Data Subjects for the performance of that Data Processor's obligations.

12. **Restricted Transfers Mechanisms.** With regard to any Restricted Transfer from one Party to the other Party within the scope of this Addendum, one of the following data transfer mechanisms shall apply, in the following order of precedence:

    (a) The applicable data importer's self-certification under (i) the EU-U.S. Privacy Shield Framework, or (ii) the Swiss-U.S. Privacy Shield Framework (insofar as the receiving Party has such valid self-certification(s) and insofar as the prospective Restricted Transfer would be considered lawful under this mechanism); or

    (b) the Standard Contractual Clauses.

13. **Standard Contractual Clauses.**

    (a) In the event that a Restricted Transfer can be covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the order of precedence set forth in Section 12. For the avoidance of doubt, the Standard Contractual Clauses shall not apply to any Restricted Transfer covered by the applicable data importer's EU-U.S. or Swiss-U.S. Privacy Shield Framework self-certification, as described in Section 12.

    (b) Subject to the additional conditions in this Section 13, Hexasoft (as the "*data exporter*" and the "*data importer*") and the Customer (as the "*data exporter*" and

the "*data importer*") enter into the Standard Contractual Clauses (the text of which is available at https://www.fraudlabspro.com/fraudlabspro_scc.pdf) which: (i) the Parties are deemed to have accepted, executed, and signed, where necessary, in their entirety (including the appendices thereto); (ii) are incorporated by reference and constitute an integral part of this Addendum; and (iii) may be updated from time to time to reflect the latest version promulgated by the European Commission. For the purposes of clarity, as used in this Addendum and the Standard Contractual Clauses, a Party is a "data importer" where that Party is the receiving party, and a "data exporter" where it is the sending party, as applicable. Furthermore, with regards to any one particular transfer operation, a Party may only be either a "data exporter" or a "data importer".

(c) In consideration of the fact that both Parties may send or receive Personal Data to and from the other, each Party is deemed to have entered into the Standard Contractual Clauses twice, as outlined above, once as a "data exporter" with the other Party being a "data importer" and once with such roles reversed.

(d) Each Party, as a data importer, elects Clause II(h)(iii) as its choice pursuant to Clause II(h) of the Standard Contractual Clauses.

(e) In cases where the Standard Contractual Clauses apply, and there is a conflict between the terms of the Addendum and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall control. For purposes of clarity, terms in this Addendum that supplement, but do not directly contradict or frustrate the purposes of the terms of the Standard Contractual Clauses, shall not be deemed as creating a conflict.

14. Liability. Without prejudice to any form of direct liability of a Party before Data Subjects, each Party shall be liable to the other non-defaulting Party for damages the defaulting Party has caused to the non-defaulting Party by any breach of its obligations pursuant to this Addendum.

15. Contact Points for Notices and Data Protection Enquiries.

(a) Hexasoft:

VeraSafe Czech Republic s.r.o
Klimentská 46
Prague 1, 11002
Czech Republic

Contact form: https://www.verasafe.com/about-verasafe/contact-us/

(b) Customer:

The Customer shall provide without undue delay, by way of sending an e-mail to support@fraudlabspro.com, the following contact information for data protection inquiries:

- E-mail Address;
- Name;
- Title;
- Data protection registration information (if applicable).

The Customer shall promptly update, when necessary, all such information, and keep all such information complete and up to date.

(c) The Parties shall use the contact point indicated in this Section 15 for all matters related to this Addendum and the Standard Contractual Clauses, including but not limited to notices under Clause II(i) of the Standard Contractual Clauses.

16. **Evidence of Financial Resources.** When a Party exercises its rights under Clause II(f) of the Standard Contractual Clauses (the "Clause II(f) Obligee"), the other Party (the "Clause II(f) Obligor") may elect to provide the Clause II(f) Obligee with its choice of: (a) copies of recent audited financial reports that are publicly available; (b) subject to obligations of confidentiality, recent non-publicly available audited financial reports; (c) a certification by the Clause II(f) Obligor's treasurer of its financial condition; or (d) other relevant documentation or evidence. If the Clause II(f) Obligee, after having reviewed the aforementioned evidence, reasonably deems that it requires additional information, the Clause II(f) Obligor shall provide the Clause II(f) Obligee with additional evidence of financial resources sufficient to fulfill its responsibilities under Clause III of the Standard Contractual Clauses (which may include insurance coverage). The Clause II(f) Obligee agrees to pay the Clause II(f) Obligor, upon receipt of invoice, a reasonable fee based on the time spent and materials expended in relation to the Clause II(f) Obligee exercising its rights under Clause II(f) of the Standard Contractual Clauses.

17. **Auditing and Certification; Expenses.** When a Party exercises its rights under Clause II(g) of the Standard Contractual Clauses (the "Clause II(g) Obligee"), the other Party (the "Clause II(g) Obligor"), subject to obligations of confidentiality, shall provide the findings or report of any relevant third-party audit(s) to which it may have been subject. If the Clause II(g) Obligee, after having reviewed such audit report(s), reasonably deems that it requires additional information, the Clause II(g) Obligor shall submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the Clause II(g) Obligee (or any independent or impartial inspection agents or auditors, selected by the Clause II(g) Obligee and not reasonably objected to by the Clause II(g) Obligor) to ascertain compliance with the warranties and undertakings in the Standard Contractual Clauses, with reasonable notice and during regular business hours. Any such request will be subject to any necessary consent or approval from the

applicable Data Protection Regulator within the country of the Clause II(g) Obligor, which consent or approval the Clause II(g) Obligor will attempt to obtain in a timely fashion. The Clause II(g) Obligee agrees to pay the Clause II(g) Obligor, upon receipt of invoice, a reasonable fee based on the time spent and materials expended in relation to the Clause II(g) Obligee exercising its rights under Clause II(g) of the Standard Contractual Clauses.

18. **Accountability.** If either Party, acting as a data importer, determines that it can no longer meet its obligations to provide the level of protection as required by this Addendum or as required by the EU-U.S. Privacy Shield Framework or Swiss-U.S. Privacy Shield Framework, it shall: (i) promptly notify the other Party of that determination; and (ii) either cease the Processing or take other reasonable and appropriate steps to remediate the situation.

19. **Representations and Warranties of the Customer Regarding Local Laws.** The Customer represents and warrants that it has no reason to believe, at the time of entering into this Addendum, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under this Addendum or Applicable Laws, and it will inform Hexasoft if it becomes aware of any such laws.

20. **Resolution of Disputes with Data Subjects or Data Protection Regulators**

    (a) In the event of a dispute or claim brought by a Data Subject or a Data Protection Regulator concerning the Processing of the Personal Data against either or both of the Parties, the Parties will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion.

    (b) The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the applicable Data Protection Regulator. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

    (c) Each Party shall abide by a decision of a competent court of the applicable data exporter's country of establishment or of the applicable Data Protection Regulator which is final and against which no further appeal is possible.

21. **No Further Amendment.** Except as expressly provided in this Addendum, the Parties intend no amendment or modification of the Services Agreement or in any other document signed or otherwise entered into by the Parties.

22. **Primary Agreement.** The terms of the Services Agreement, together with any other addendum or supplemental agreement executed prior to this Addendum, are preserved and remain in full force and effect. To the extent that any terms of this Addendum conflict with any terms contained within the Services Agreement, the terms of this Addendum shall control with respect to the subject matter described herein.

23. Confidentiality. This Addendum is confidential information. Each Party agrees:

(a) not to disclose this Addendum to any third party except (1) to legal counsel or privacy consultants who have executed a nondisclosure agreement or who are under a statutory obligation of confidentiality; (2) as permitted or reasonably anticipated by this Addendum; or (3) as required by the GDPR or other Applicable Laws or the EU-U.S. or Swiss-U.S. Privacy Shield Frameworks (each, a "Permitted Disclosure"); and

(b) to exercise at least the same degree of care that each Party generally uses to protect its own information of similar nature, to protect this Addendum from any possession, use, or disclosure that is not a Permitted Disclosure, but in no case less than a reasonable degree of care.

* * *