SnatchBot

Data Processing Addendum Agreement to the SnatchBot Terms of Use Regarding the Processing of Personal Data of EU Customers

(hereafter referred to as "SnatchBot DPA")

Table of contents

Data Processing Addendum Agreement to the SnatchBot Terms of Use Regarding the Processing of Personal Data of EU Customers

(hereafter referred to as "SnatchBot DPA")

1. Snatch Group Limited, All rights reserved. 8 Abba Eban Blvd, Herzliya Pituach, Israel,

- hereafter referred to as "**SnatchBot**" -

And

2. SnatchBot's customers being subject to the rules under the European General Data Protection Regulation or the Standard Contractual Clauses for Processors pursuant to European Commission Decision of 5 February 2010.

- hereafter referred to as "**the Customer**" –

SnatchBot and the Customer are hereafter referred to as the "**Parties**" and each individually as "**Party**"

PREAMBLE

SnatchBot performs cloud based analytics services for Customer ("**Services**") as agreed between the Parties in the SnatchBot Terms of Use entered into between the Customer and SnatchBot ("**SnatchBot Terms and Conditions**"). In the course of providing the Services, SnatchBot will process personal data for which, pursuant to EU data privacy laws, Customers or Customer's Customers located in the European Union and/or European Economic Area are responsible ("**Customer's Customers**") as provided under Art. 4 no 7 GDPR ("**Customer's personal data**"), or where Customers are, for contractual reasons, obliged to subject the data processing to principles applicable to a person within the EU. The Customer's Customers are companies that render services to their end-customers and who engage SnatchBot as sub-processor.

This SnatchBot DPA regulates the data protection obligations of the Parties when processing the Customer's personal data. This is done under the SnatchBot Terms of Use and will reasonably ensure that such processing will only take place on behalf of and under the Instructions of the Customer or the Customer's Customers and in accordance with the EU Standard Contractual Clauses for Processors pursuant to European Commission Decision of 5 February 2010 ("**SCC**") and Art. 28 et seq. of the General Data Protection Regulation ("**GDPR**").

SPECIFICATIONS OF PROCESSING

SnatchBot will, in the course of providing Services under the SnatchBot Terms of Use, process the Customer's personal data, which shall be subject to the following provisions contained in this SnatchBot DPA.

When performing Services, SnatchBot will act either as processor or sub-processor. SnatchBot's function as processor or sub-processor will be determined by the function of SnatchBot's Customer. If the Customer is the data controller, then SnatchBot shall be the processor. If the Customer is processor on behalf of its Customer's Customers, then SnatchBot shall be the sub-processor and the Customer and any of the Customer's Customers shall be entitled to issue Instructions under this SnatchBot DPA.

The categories of data and data subjects which may be affected by the processing are listed in Exhibit, Appendix 1.

This SnatchBot DPA amends the SnatchBot Terms of Use with respect to any processing of personal data by SnatchBot as a processor for and as provided by the Customer or the Customer's Customers as amended from time to time by written agreement between both Parties.

The Customer enters into this SnatchBot DPA on its own behalf and on behalf of each of the Customer's Customers and confirms of being authorized to do so. Alternatively, EU Customer's Customers can co-sign this SnatchBot DPA. This SnatchBot DPA is by way of reference an integral part of any agreement entered into between SnatchBot and SnatchBot's Customers

STANDARD CONTRACTUAL CLAUSES (SCC)

Any processing operation as described above shall also be subject to the SCC as contained in Exhibit, which shall prevail over any conflicting clauses in the SnatchBot Terms of Use or the SnatchBot DPA. The Parties agree that the SCC shall be directly binding between SnatchBot as Data Importer, the Customer and each of the Customer's Customers, each acting as Data Exporter (as defined therein) in relation to the personal data provided by the Customer or the respective Customer's Customer.

SNATCHBOT'S OBLIGATIONS

In addition to Clause 5 (a) SCC, SnatchBot shall in the course of providing Services — including in regard to transfers of personal data to a third country — process the Customer's personal data only on behalf of and under the documented Instructions of the Customer unless required to do so otherwise under EU or Member State law; in such a case, SnatchBot shall inform the Customer of that legal requirement before processing, unless that law prohibits communicating such information on important grounds of public interest.

SnatchBot shall take all reasonable steps necessary to ensure that any natural person acting under its authority who has access to personal data does not process such personal data except on Instructions from the Customer, unless he or she is otherwise required to do so by EU or Member State law.

SnatchBot ensures that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that the obligation will remain after termination of this SnatchBot DPA.

Technical and Organizational Data Security Measures

In addition to Clause 5 (c) SCC, the measures specified in Exhibit, Appendix 2 are subject to technical advancements and development.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, SnatchBot shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Art. 32 GDPR. This may include (as appropriate) :

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

If SnatchBot significantly modifies measures specified in Exhibit, Appendix 2, such modifications have to meet the obligations pursuant to Sect. 4.4.2 and 4.4.3. If SnatchBot significantly modifies measures SnatchBot shall make available to the Customer a description of such measures sufficient to enable the Customer to assess compliance with Art. 32 GDPR and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer as permitted by Clause 5 (f) SCC. SnatchBot and the Customer shall agree on such significant modifications by accepting the modified Exhibit, Appendix 2. The Customer shall not refuse to accept any modification that meets the requirements pursuant of this SnatchBot DPA.

SnatchBot shall implement a data protection management procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to appropriately ensure the security of the processing. SnatchBot will further, by way of regular self-audits, reasonably ensure that the processing of the Customer's personal data conforms with the provisions as agreed with the Customer or to the Customer's Instructions.

SnatchBot shall, while taking into account the nature of the processing, assist the Customer through appropriate technical and organizational measures, in the fulfilment of the Customer's obligations to

respond to requests exercising the rights of data subjects in accordance with Applicable Law, in particular Art. 15 through 18 and 21 GDPR.

Taking into account the nature of the processing and the information available to SnatchBot, SnatchBot shall assist the Customer in ensuring compliance with the obligations pursuant to Art. 33 through 36 GDPR (Data Security Breach Notification, Data Protection Impact Assessment, Consultation with Data Protection Supervisory Authorities).

Documentation and Audit Rights

SnatchBot may, at its discretion, provide data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, by a publically certified auditing company or by another customer of SnatchBot.

Notification Duties

In addition to Clause 5 (d) SCC, SnatchBot shall inform the Customer in text form (e.g. letter, fax or e-mail) without undue delay of the events listed in Clause 5 (d) SCC and the following events:

- Requests from third parties including from a data protection supervisory authority regarding the Customer's personal data;
- Threats to the Customer's personal data in possession of SnatchBot by garnishment, confiscation, insolvency and settlement proceedings or other incidents or measures by third parties. In such cases, SnatchBot shall immediately inform the respective responsible person/entity that the Customer holds the sovereignty and ownership of the personal data.

Rectification, Erasure (Deletion), Restriction

- If legally required and the Customer is unable to perform the applicable task itself or if provided so in the services description contained in the SnatchBot Terms of Use, SnatchBot shall rectify, erase (delete) or restrict (block) the Customer's personal data upon the Customer's request. Any deletion of the Customer's personal data pursuant to this Sect. 4.9 shall be executed in such a manner that restoring or recovering such data is rendered impossible.

- At the Customer's request, SnatchBot shall conduct a data protection-compliant destruction of data media and other material if so provided by the Customer. Alternatively, at the request of the Customer, SnatchBot shall provide the data media and other material to the Customer or store it on the Customer's behalf.

- SnatchBot will inform the Customer of the name and the official contact details of its data protection officer if SnatchBot is, by Applicable Law, required to appoint a data protection officer. If SnatchBot is not required to appoint a data protection officer, SnatchBot shall name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing this SnatchBot DPA.

- In the case that claims based on Art. 82 GDPR are raised against the Customer, SnatchBot shall reasonably support the Customer with its defense to the extent the claim arises in connection

with the processing of personal data by SnatchBot in connection with performing the Services to the Customer.

THE CUSTOMER'S OBLIGATIONS

In addition to Clause 4 (b) SCC, the Customer shall provide all Instructions pursuant to this SnatchBot DPA to SnatchBot in written or electronic form.

The Customer shall inform SnatchBot immediately if processing by SnatchBot might lead to a violation of data protection regulations.

In the case that claims based on Art. 82 GDPR are raised against SnatchBot, the Customer shall reasonably support SnatchBot with its defense to the extent that the claim arises in connection with the processing of personal data by SnatchBot in connection with performing the Services to the Customer.

The Customer shall name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing this SnatchBot DPA.

SUBPROCESSING

In addition to the provisions contained in Clause 11 SCC, any sub-processor is obliged, before initiating processing, to commit itself in writing — for the benefit of the Customer and the Customer's Customers — to comply with the same data protection obligations as the ones under this SnatchBot DPA or legal Act within the meaning of Art. 28 para 3, 4 and 6 GDPR vis-à-vis the Customer (the sub-processing agreement must provide at least the same level of data protection as required under this SnatchBot DPA). Where the subprocessor fails to fulfil its data protection obligations, SnatchBot shall remain fully liable to the Customer for the performance of the subprocessor's obligations.

Where a subprocessor refuses to be bound by the same data protection obligations as the ones under this SnatchBot DPA, the Customer may consent thereto whereby such consent shall not be unreasonably withheld.

6.4 Subject to SnatchBot complying with the obligations under Clause 11 SCC and Art. 28 para 2 GDPR, the Customer herewith agrees to the following subprocessors:

- Amazon Web Services (AWS) located in the USA using the cloud based service AWS for hosting the Data Importer's cloud database and cloud services. The location of the data services is restricted to the USA. The Customer confirms that AWS provides its services the basis of its own on standardized terms and conditions which are similar but not identical to the ones under this agreement. The terms and conditions of AWS are also based on the SCC. Customer can view such terms and condition at: https://aws.amazon.com/compliance/gdpr-center/

LIABILITY

The Customer and SnatchBot shall be each liable for the damages of concerned data subjects according to Art. 82 GDPR (external liability):

- The Customer and SnatchBot shall be liable for all the damage caused by processing which infringes the GDPR.
- SnatchBot's liability shall be limited to the damage caused by processing where it has not complied with obligations of the GDPR specifically directed to SnatchBot or where it has acted outside or contrary to the lawful Instructions of the Customer.
- The Customer and SnatchBot shall be exempt from liability if they prove to not be in any way responsible for the event giving rise to the damage.
- Where more than one Customer and SnatchBot, or both the Customer and SnatchBot, are involved in the same processing are responsible for any damage caused by processing, each Customer or SnatchBot shall be held liable for the entire damage.
- The above shall apply only where more beneficial for data subjects in comparison with Clause 3 and 6 SCC. In any other case, Clauses 3 and 6 SCC shall prevail.
- The Customer and SnatchBot shall be entitled to claim back from the other, SnatchBot or the Customer, that part of the compensation corresponding to their part of responsibility for the damage.

As regards internal liability and without any effect as regards external liability towards data subjects, the Parties agree that notwithstanding anything contained hereunder, when providing the Services, SnatchBot's liability for the breach of any terms and conditions under this SnatchBot DPA shall be subject to the liability limitations agreed in the SnatchBot Terms of Use. Further, no EU Customer Affiliate shall become a beneficiary of the SnatchBot DPA without being bound by this SnatchBot DPA and without accepting this liability limitation. The Customer will indemnify SnatchBot against any losses that exceed the liability limitations in the SnatchBot Terms of Use suffered by SnatchBot in connection with any claims of the Customer's EU Customer Affiliates or data subjects who claim rights based on alleged violation of this SnatchBot DPA including the SCC.

CONTRACT PERIOD

The subject matter, duration, nature and purpose of the processing and the rights, benefits and obligations of this SnatchBot DPA shall commence with the initiation of the Services and shall terminate with termination of the agreed Services under the SnatchBot Terms of Use. The rights, benefits and obligations of this SnatchBot DPA shall commence with the initiation of the Services and shall terminate with termination of the agreed Services under the SnatchBot Terms of Use.

MODIFICATIONS

SnatchBot may modify or supplement this SnatchBot DPA, with notice to the Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the GDPR. The Customer shall notify SnatchBot if it does not agree to a modification, in which case SnatchBot may terminate the DP Amendment Agreement with two (2) months' prior written notice.

WRITTEN FORM

Any side agreements to this SnatchBot DPA as well as changes and amendments of this SnatchBot DPA, shall be in writing (text form being sufficient).

CHOICE OF LAW

This SnatchBot DPA is governed by, and shall be interpreted in accordance with, the law of the EU Member State in which the Customer or, if the Customer is not controller, the Customer's Customer resides, excluding its conflict of law provisions, to the extent not otherwise provided by Clause 7 SCC.

MISCELLANEOUS

For the determination of data protection obligations, entitlement to provide orders and control, responsibilities, liabilities and consequences of objectives, the SnatchBot DPA shall prevail over all other agreements between the Parties.

This SnatchBot DPA may only be amended, supplemented or changed upon the written agreement of the Parties.

In the event that a clause under the SnatchBot Terms of Use has been found to violate the GDPR including all other Applicable Laws, the Parties will mutually agree on modifications to the SnatchBot Terms of Use to the extent necessary to ensure data privacy-law compliant processing.

Exhibit– Standard Contractual Clauses for Processors

Standard Contractual Clauses for Processors

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

The Customer and each Customer's Customer are hereafter referred to as the "Data Exporter" with respect to the personal data provided by that Data Exporter.

SnatchBot, as defined in the SnatchBot DPA, is hereafter referred to as the "Data Importer".

The Data Exporter(s) and the Data Importer, each a "party" and collectively "the parties" HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

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

b. 'the Data Exporter' means the controller who transfers the personal data;

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

d. 'the subprocessor' means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

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

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

11

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

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

2. that it has instructed — and throughout the duration of the personal data processing services will instruct — the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;

3. that the Data Importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

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

5. that it will ensure compliance with the security measures;

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

7. to forward any notification received from the Data Importer or any subprocessor pursuant to Clause

8. 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;

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

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

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

Clause 5

Obligations of the Data Importer

The Data Importer agrees and warrants:

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

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

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

D. that it will promptly notify the Data Exporter about:

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

F. (ii) any accidental or unauthorised access, and

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

H. to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

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

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

K. that, in the event of subprocessing, it has previously informed the Data Exporter and obtained its prior written consent;

L. that the processing services by the subprocessor will be carried out in accordance with Clause 11;

M. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

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

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

If a data subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The Data Importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the data subject:
   a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the Data Importer under the Clauses (This requirement may be satisfied by the subprocessor co-signing the contract entered into between the Data Exporter and the Data Importer which is based on the terms and conditions of this Agreement.). Where the subprocessor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the subprocessor's obligations under such agreement.

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

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

Clause 12

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter

EU-based creators of chatbots using SnatchBot's bot-building platform

Data Importer

Snatchbot is engaged in providing a platform-as-a-service-solution to individuals, companies, and agencies to build, host, and manage chatbots for Facebook Messenger. SnatchBot is a platform that allows its clients' customers to get in contact with the client by communicating with the provided chatbots via Facebook Messenger, Skype, Slack, LINE, etc.

Data subjects

The Data subjects are individual online consumers of Data Exporter.

Categories of data

The personal data transferred concern the following categories of data:

- The Customer's client's bot users' first name, last name, Facebook, Skype, Slack etc. avatar photo, time zone, language settings and gender, as long as those pieces of information are available in the public channel profiles.

- On request of the Customer to its clients, while using the chatbot indefinite categories of data can be transferred, such as location information, phone number, and email address.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

- N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities: SnatchBot uses personal data to enable bot admins to customize and improve bot experiences.

Retention

At all times during the term of the Customer's subscription, the Customer will have the ability to access and extract Customer personal data stored by Snatchbot. Snatchbot will retain Customer personal data stored in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Snatchbot will disable Customer's account and delete the personal data.

The Services may not support retention or extraction of software provided by Customer. Snatchbot has no liability for the deletion of personal data as described in this section.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

A description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Sub-Processors will be bound to adhere to similar but not identical organizational security measures which shall not fall below the level of data security as agreed herein. Any organizational security measures are subject to change as technical standards evolve and such changes can be implemented by the Data Importer. If so requested, the Data Importer will provide the Data Exporter with a description of the then current measures.

1. Access control to premises and facilities:

Only authorized representatives have access to Snatchbot's premises and facilities. Measures include:

- Snatchbot has physical offices in office buildings located in Herzliya Pituach, Israel.
- Keys to the office locations are issued to all employees in accordance with their need to have access. The distribution and usage of keys are managed and monitored by the Office Manager.
- The office is secured and monitored on a 24/7 basis. Key points within the office building are monitored by security cameras.

2. Physical access:

Snatchbot ensures physical access to Personal Data is protected. Measures include:

- Snatchbot runs its services from professional, third-party production data centers that meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, verify adherence to the strict security controls these standards mandate.
- Power and telecommunications cabling carrying Personal Data or supporting information services at the production data center are protected from interception, interference and damage.
- Production data centers and their equipment are physically protected against natural disasters, malicious attacks and accidents.
- Equipment at production data centers is protected from power failures and other disruptions caused by failures in supporting utilities, and is correctly maintained.

3. Access control to systems:

Snatchbot's data processing systems are used only by approved, authenticated users. Measures include:

- Access to Snatchbot internal systems is granted only to Snatchbot Personnel and/or to permitted employees of Snatchbot's subcontractors and access is strictly limited as required for those persons to fulfill their function.
- Access to production servers is secured against unauthorized use through the encrypted data transmission over SSL/SSH.
- All users access Snatchbot systems with a unique identifier (user ID).

- Each computer has a password-protected screensaver.
- Snatchbot has a thorough procedure to deactivate users and their access when a user leaves the company or a function.

4. Access control to data:

Persons entitled to use data processing systems gain access only to the Personal Data that they are authorized to access.

Measures include:

- Snatchbot restricts Personnel access to files and programs on a "need-to-know" basis.
- The production environment is separate from the development and testing environment.
- Snatchbot uses well-configured firewalls for their backend infrastructure.
- Snatchbot Platform contains capabilities to set roles and permissions to let Customers manage authorizations to set that Personal Data is only made available to appropriate users when needed.

5. Data Transmission:

Snatchbot takes steps to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during transfer.

Measures include:

- All Personal Data that is coming to Snatchbot Platform from the channels we support on the platform is transmitted in encrypted form over HTTPS protocol.
- The Snatchbot Platform supports integrations with third-party services over HTTPS protocol.
- The Customer is responsible for the security of Personal Data once it has been transmitted from SnatchBot to the Customer including when downloaded or accessed by Customer users.

6. Confidentiality and Integrity:

Personal Data remains confidential throughout processing and remains intact, complete and current during processing activities.

Measures include:

- Snatchbot has a central, secured repository of product source code, which is accessible only to authorized Personnel.
- All changes to Snatchbot Platform's source code are being tracked, thoroughly reviewed, and tested in an isolated environment before being accepted.
- All releases to production environment are additionally tested in an isolated staging environment, reviewed and approved before being deployed.

7. Availability:

Personal Data is protected from accidental destruction or loss, and there is timely access, restoration or availability to Personal Data in the event of an incident.

Measures include:

- Snatchbot uses a high level of redundancy at the production data center so that an availability failure of a single system or component is unlikely to impact general availability.
- Snatchbot deploys its infrastructure only on reliable cloud providers whose data centers have multiple power supplies, generators on-site and with battery backup to safeguard power availability to the data center, and multiple access points to the Internet to safeguard connectivity.
- Snatchbot uses commercially reasonable efforts to create frequent backup copies of Personal Data.
- Snatchbot has a system in place to ensure that any failures of backup to operate correctly are flagged and dealt with.
- Snatchbot's infrastructure and services are monitored 24x7x365 for availability and technical issues

8. Job Control:

Personal Data processed on a Customer's behalf is processed solely in accordance with the relevant agreement and related instructions of the Customer including in the use of sub-processors.

Measures include:

- Snatchbot acts as data processor with respect to Personal Data and stores and processes Personal Data in order to operate the Snatchbot Platform.

- Snatchbot does not access Customer Personal Data, except to provide services to the Customer which Snatchbot is obligated to perform in support of the Customer experience including for general operation and monitoring of Snatchbot Platform, troubleshooting and maintenance purposes, for security reasons, as required by law, or on request by Customer.

- Snatchbot uses a limited number of sub-processors to help it provide the Service including a small number of third party companies and some individual (natural person) subcontractors. A list of individual (natural person) subcontractors as well as a list of third party companies used as sub-processors is available on request.

Snatchbot has contracts in place directly or via affiliates with all sub-processors that provide for confidentiality of Personal Data and agreements incorporating the EU Standard Contractual Clauses (Processors) in place with all sub-processors that process relevant Personal Data outside of the European Economic Area.