GDPR DATA PROTECTION ADDENDUM

This GDPR Data Protection Addendum ("**Addendum**") is made by and between Statsbot, Inc. ("**Statsbot**") and Statsbot's customer ("**Client**") as of the date of acceptance of the Statabot Terms of Service. Statsbot and Client are each referred to as a "**Party**" and collectively the "**Parties**" hereinafter.

WHEREAS:

(A) Statsbot provides an analytics platform to Client (collectively, the **"Services")**.

(B) The Services are provided according to a certain services agreement or terms of service (including the *Statsbot Terms of Service*) and any amendments thereto, between Statsbot and Client ("**Services Agreement**") and this Addendum is an addendum to and modifies the Services Agreement.

(C) The Parties acknowledge that the provision by Statsbot of the Services under the Services Agreement may require the transfer of Personal Data (as defined below) of Client and third parties.

(D) This Addendum specifies the data protection obligations of the Parties, their staff and any third parties acting on their behalf, and applies to all Personal Data transferred between the Parties in connection with the provision of the Services under the Services Agreement.

(E) As to certain Personal Data or Processing Activities, Statsbot and Client each act as a Data Controller and, as to certain other Personal Data, Statsbot acts as a Data Processor to Client who acts as a Data Controller.

THE PARTIES HAVE AGREED:

1. DEFINITIONS

1.1 For the purpose of this Addendum and all Exhibits and attachments hereto, the defined terms shall have the following meaning:

(a) **"Data Protection Legislation"** shall mean the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**"), the European Directives 95/46 and 2002/58/EC (as amended by Directive 2009/136/EC) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including but not limited to the Privacy and Electronic Communication (EC Directive) Regulations 2003), and all other applicable laws relating to the processing of Personal Data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by the relevant supervisory authorities); and

(b) **"Data Controller"**, **"Data Processor"**, **"Third Party Processor"**, **"Data Subject"**, **"Personal Data"** and **"Processing"** shall have the meanings given in the GDPR, first and foremost, and then any related Data Protection Legislation where applicable.

(c) "**EU**" and "**EEA**" shall respectively mean the European Union and the European Economic Area.

2. **ROLES**

2.1 The terms of **Exhibit 1** ("**Data Sharing Terms and Conditions**") shall apply when Statsbot and Client each act as a Data Controller with respect to the Processing activities undertaken ("**C2C"**).

2.2 The terms of **Exhibit 2** ("**Processor Addendum**") shall apply when Statsbot acts as a Data Processor and Client acts as the Data Controller with respect to the Processing activities undertaken ("**C2P**").

2.3 Where Data Protection Legislation applies, neither Party shall transfer or permit any Personal Data shared by the other Party to be transferred to a territory outside of the EEA unless it has taken such measures as are necessary to ensure the transfer is in compliance with Data Protection Legislation. Such measures may include (without limitation) transferring the Personal Data to a recipient in a country that the European Commission has decided provides adequate protection for Personal Data or to a recipient in the United States that has certified compliance with the EU-US Privacy Shield framework

2.4 **C2C Transfers**. Where each Party is a separate Data Controller, the following terms apply, subject to Section 4 of the Data Sharing Terms and Conditions (**Exhibit 1**). Except with regard to Personal Data transferred from one Party to the other Party in reliance on the receiving Party's Privacy Shield certification or other appropriate transfer mechanism specified in Section 2.3 above, the '*EU Controller to Controller Standard Clause Agreement*' (as further described in Section 4 of **Exhibit 1**) shall apply to the receiving Party's Processing of the Personal Data in countries outside the EEA that do not provide an adequate level of data protection. To the extent that the Parties transfer Personal Data in reliance on the *EU Controller to Controller Standard Clause Agreement*, the *EU Controller to Controller Standard Clause Agreement* shall be incorporated herein upon execution of this Agreement by the Parties.

2.5 **C2P Transfers**. Where Statsbot is the other Party's Data Processor, the following terms apply, subject to § 5 of the Processor Addendum (**Exhibit 2**). Unless the Data Processor receives Personal Data pursuant to a transfer mechanism specified in Section 2.3 above, the Parties shall execute and abide by the '*EU Controller to Processor Standard Clause Agreement*' (as further described in § 5 of **Exhibit 2**), which shall apply to Processing of Personal Data in countries outside the EEA that do not provide an adequate level of data protection. To the extent that the Parties transfer Personal Data in reliance on the *EU Controller to Processor Standard Clause Agreement*, the *EU Controller to Processor Standard Clause Agreement* shall be incorporated herein upon execution of this Agreement by the Parties and Statsbot will be considered the data importer and Client will be considered the data exporter.

3. GENERAL

3.1 For purposes of this Addendum, including any attachments hereto, the Parties agree that the types and categories of Personal Data needed for Processing in connection with the Services may include the following without limitation:

- Identity Data: such as company of employment and title, first name, last name, username or similar identifier and an encrypted version of Client's login/password. If Client interacts with Statsbot through social media, such as a login through Slack or GSuite, this may include Client's social media user name.
- Contact Data: includes billing address, email address and telephone numbers.

- Profile Data: includes Client's username and password, preferences, feedback and survey responses, as well as any profile data which we have added (for example, using analytics and profiling).
- Financial Data: such as payment card details, and tax ID numbers.
- Transaction Data: includes details about purchases and payments to and from Client and other details relating to your activity on the Services.
- Technical Data: such as internet protocol (IP) address, your login data, browser type and version, location, and other technology on the devices Client uses to access the Services.
- Usage Data: includes information about how Client uses our Services, products and services.
- Tracking Data: this is information Statsbot or others collect about Client from cookies and similar tracking technologies.
- Marketing and Communications Data: includes your preferences in receiving direct marketing from us, as well as Client's communication preferences.
- Other Data: includes other Personal Data that Client may upload to the Services.

3.2 This Addendum only applies to the extent that the Data Protection Legislation applies to the Processing of Personal Data under the Services Agreement, including if (a) the Processing is in the context of the activities of an establishment of either Party in the EU/EEA and/or (b) the Personal Data relates to Data Subjects who are in the EU/EEA and the Processing relates to the offering to them of goods or services or the monitoring of their behavior in the EU/EEA by or on behalf of a Party.

3.3 This Addendum shall become effective after it has been signed by both Parties and shall continue to apply until the expiration or termination of the Services Agreement; *provided, however*, that the Parties agree that given the uncertainty with respect to the lack of interpretive decisions relating to GDPR, including as to the allocation of "controller" and "processor" responsibilities, each Party reserves the right to further amend or clarify this Addendum in writing, upon good faith negotiations with the other Party, in order to ensure compliance with Data Protection Legislation. If the Parties cannot agree on any such subsequent amendments such that one or the other determines that it cannot be in compliance with applicable Data Protection Legislation, the Parties shall each have the right to immediately terminate this Addendum. In the event of such termination, the Parties agree to immediately cease any further processing of Personal Data, or to fully anonymize any Personal Data (as such term is defined under GDPR) if such further processing is contemplated. Each Party's obligation to handle any Personal Data obtained prior to such termination in accordance with any applicable Data Protection Legislation, as well as indemnification obligations set forth herein, shall survive this Addendum indefinitely upon termination.

3.4 The stipulations on choice of law and venue of jurisdiction of the Services Agreement apply to this Addendum as well.

3.5 In the event of any conflicting stipulations between this Addendum and other agreements in place between the Parties, the stipulations within this Addendum (and all of its exhibits incorporated herein) shall prevail.

3.6 No change of, or amendment to, this Addendum shall be valid and binding unless made in writing (including electronic copies) signed by or on behalf of the Parties. If one or more stipulations of this Addendum are deemed void, this shall not affect validity of the other stipulations of this

Addendum. In the event of invalidity of one or more stipulations of this Addendum, the Parties shall negotiate a legally effective provision commercially close to the invalid stipulation.

3.7 Except as provided for in this Addendum, all other terms and conditions of the Services Agreement shall remain in full force and effect, but in the event of a contradiction between the Services Agreement and this Addendum, this Addendum shall prevail. Notwithstanding the foregoing, each Party's aggregate liability with respect to the the obligations hereunder only shall be capped at Twenty Thousand Dollars ($20,000).

3.8 This Addendum may be signed in separate counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

EXHIBIT 1

DATA SHARING TERMS AND CONDITIONS

(Controller to Controller)

1. RELEVANT DATA AND DATA SHARING

1.1 Each Party, in accordance with its privacy policy may collect certain Personal Data as defined in Section 3.1 of the Addendum ("**Relevant Data**"). When Client is the Controller, Client collects such Personal Data from Client's customers or other third parties. When Statsbot is the Controller, Statsbot collects such Personal Data from Client.

1.2 It is acknowledged that for the Relevant Data held by either Client and Statsbot (whether such Personal Data is collected from a third party directly, or passed to one Party by the other Party), each Party holds such Personal Data at all times as Data Controller subject to the terms of this **Exhibit 1**; *provided, however,* that the Parties' determination that they each act as a separate Data Controller may be affected by interpretations of, updates to and guidance under the Data Protection Legislation, or by a change in their respective Processing activities, in which case the Parties agree to amend this **Exhibit 1** in good faith as needed in order to comply with Data Protection Legislation, or terminate this **Exhibit 1** if the Parties cannot agree in good faith.

1.3 It is further acknowledged that in respect of any Personal Data held or shared pursuant to Clause 1.2 above, under no circumstances shall either Party be a Joint Controller as described in Article 26 of the GDPR. Notwithstanding the foregoing, to the extent that either Party collects Personal Data concerning a third party from the other Party and does not solely process such Personal Data for the purpose of providing or receiving the Services contemplated under the Services Agreement (the "**Additional Processing Activities**") and such Additional Processing Activities may adversely impact the rights and freedoms of the Data Subjects concerned, such Party shall promptly inform the other Party of its Additional Processing Activities such that the Parties may amend or supplement this **Exhibit 1**, and such Party arty shall be solely responsible for complying with applicable law, (including but not limited to Data Protection Legislation) with respect to its Additional Processing Activities. In no event shall the other Party be liable for any of the Additional Processing Activities, including with respect to any third-party claims from Data Subjects or data protection authorities.

2. DATA PROTECTION OBLIGATIONS

2.1 Each Party shall, in relation to the sharing of any Personal Data or the Processing of Relevant Data in connection with the performance of its obligations under this **Exhibit 1** (including and any attachments) and the Services Agreement:

(a) comply with the Data Protection Legislation (including without limitation ensuring that (i) it has a lawful basis for sharing or processing contemplated by this **Exhibit 1**, (ii) its processing activities are transparent as required under GDPR, and (iii) it complies in every respect with Data Subject rights under GDPR);

(b) update its end user agreements and privacy policy as necessary to comply with the Data Protection Legislation relating to, without limitation, the Personal Data that it receives from or transfers to, the other Party under the Services Agreement or this **Exhibit 1**;

(c) provide such assistance to the other Party (at its own cost) to respond to any mandatory request from a Data Subject according to the Data Protection Legislation (including access requests, and requests for erasure, rectification or to cease processing activities);

(d) immediately (and no later than 48 hours) notify the other Party on becoming aware of any breach (as it is defined in the GDPR) of Personal Data contemplated by this **Exhibit 1**;

(e) adhere in all material respects with its end user agreements and privacy policy;

(f) implement any and all appropriate technical and organizational measures to ensure a level of security appropriate to the risk as per Article 32 of the GDPR; and

(g) ensure that any contracts with sub-processors comply with the Data Protection Legislation.

3. LIABILITY

3.1 Each Party shall indemnify (the "**Indemnifying Party**") the other Party, including its subsidiaries, affiliates, officers, directors, agents, or employees (the "**Indemnified Party**"), from any and all third party claims and resulting fines, sanctions, claims, losses, liabilities, damages, costs and expenses demands, reasonable attorneys' fees, consultants' fees and court costs (collectively, "**Claims**") to the extent that such Claims arise from, or may be in any way attributable to (i) any violation by the Indemnifying Party of its obligations under this **Exhibit 1**; and (ii) the negligence, gross negligence, bad faith, or intentional or willful misconduct of the Indemnifying Party or its personnel in connection with obligations set forth in this **Exhibit 1**. The Parties agree that the foregoing indemnification obligations shall (a) amend and replace any existing indemnification obligations under the Services Agreement (and any amendments thereto) with respect to the protection of Personal Data; and (b) apply irrespective of the location where such Claim is made, filed or adjudicated, whether in the United States or abroad, and irrespective of any choice of law/forum language in the Services Agreement.

4. INTERNATIONAL TRANSFERS OF PERSONAL DATA

4.1 As may be applicable under the Data Protection Legislation, with respect to "Cross-Border Transfers" of Personal Data (as set forth in Article 44 of the GDPR), the Parties agree to be bound by the *EU Controller to Controller Standard Contractual Clause Agreement* as approved by the European Commission from time to time, the approved version of which in force at present is that set out in the European Commission's Decision 2004/915/EC of 27 December 2004, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004D0915. **Schedule 1** to this **Exhibit 1** shall apply as **Annex B** of the *EU Controller to Controller Standard Contractual Clause Agreement*. To the extent that certain portions or annexes of the *EU Controller to Controller Standard Contractual Clause Agreement* must be signed by the Parties, the Parties agree that the agreement to this Addendum shall be binding with respect to such portions or annexes.

4.2 The Parties agree that any disputes arising under a *EU Controller to Controller Standard Contractual Clause Agreement* shall be treated as if they had arisen under the Services Agreement. To the extent that either Party works with a sub-processor to for the Processing of the Personal Data, it shall ensure that a sub-processor complies with the *EU Controller to Controller Standard Contractual Clause Agreement* included herein. The Parties recognize that the EU governing authorities may supplement or otherwise amend any requirements that must be set forth in the *EU Controller to Controller Standard Contractual Clause Agreement* under Article 46(c) of the

GDPR and agree to modify the *EU Controller to Controller Standard Contractual Clause Agreement* accordingly.

Schedule 1

ANNEX B

(to *EU Controller to Controller Standard Contractual Clause Agreement)*

DESCRIPTION OF THE TRANSFER

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects: Clients users that use the Services

Purposes of the transfer

The transfer is made for the purpose of allowing the provision of the Services

Categories of Personal Data

Relevant Data, as defined in Section 1 of the Data Sharing Terms and Conditions.

Recipients

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:

Employees, vendors and other representatives of the data importer who have a legitimate business purpose for the Processing of such Personal Data.

Sensitive Data (if appropriate)

The Personal Data transferred concern the following categories of sensitive data: none.

Data Protection Registration Information of Data Exporter (where applicable)

None.

Additional Useful Information (storage limits and other relevant information)

The Personal Data transferred between the Parties may only be retained for the period of time permitted under the Services Agreement.

Contact Information.

See above or the Services Agreement.

EXHIBIT 2
DATA PROCESSOR AGREEMENT

Client is referred to hereinafter referred to as "**Data Controller**"–

and

Statsbot is referred to hereinafter referred to as "**Data Processor**"–

Data Controller and Data Processor (as each are further defined in § 1) are hereinafter jointly referred to as the "**Parties**" and each of the Parties individually also as a "**Party**". For purposes of this **Exhibit 2**, this shall be hereinafter referred to as the "**Processor Addendum**".

Recitals

All capitalized terms shall have the meanings set forth herein. In the course of its business activities and under a separate commercial agreement for the provision by Statsbot of the analytics platform (the "**Services Agreement**"), Data Processor receives from Data Controller access to certain Personal Data controlled by the Data Controller. This Processor Addendum is concluded in order to ensure that Data Controller may meet its data protection obligations under Data Protection Law as defined below and with respect to the Commissioned Processing as also defined hereinafter. This Processor Addendum only applies to the extent that the Data Protection Legislation applies to the Processing of Personal Data under the Services Agreement, including if (a) the Processing is in the context of the activities of an establishment of either Party in the EU/EEA and/or (b) the Personal Data relates to Data Subjects who are in the EU/EEA and the Processing relates to the offering to them of goods or services or the monitoring of their behavior in the EU/EEA by or on behalf of a Party. The Parties shall ensure that they will Process Personal Data solely for the purposes contemplated in the Services Agreement or as otherwise agreed to in writing by the Parties. For the avoidance of doubt, this Processor Addendum and the obligations hereunder do not apply to Data Processor's use (1) of aggregated reporting or anonymized statistics; or (2) for compliance with legal and regulatory obligations.

§ 1 Definitions

All capitalized terms herein shall have the meaning set forth in the Addendum to which this **Exhibit 2** is attached. The following additional terms shall be defined as follows:

1. "**Commissioned Processing**" shall mean Processing of Personal Data that is carried out by Data Processor on behalf of Data Controller, in accordance with the instructions of Data Controller and the terms of this Processor Addendum.

§ 2 Details of the Processing

1. Subject and Duration of the Services to be Carried Out

The subject of the Commissioned Processing is Personal Data as necessary to carry out the Services Agreement. The duration of the Commissioned Processing is determined by Data Controller or for the duration of the Services Agreement.

2. Types of Personal Data

Personal Data and/or Personal Data categories that are the subject of the Commissioned Processing include the "Other Data" category of Personal Data listed in Section 3.1 of the Addendum to which this **Exhibit 2** is attached. The Parties agree that such list is non-exhaustive and may include additional types of Personal Data but only to the extent required to perform the Services.

3. Purpose of the Commissioned Processing

The purpose of the Commissioned Processing is the provision by Data Processor of the Services.

4. Type and Extent of the Commissioned Processing

Data Processor shall process Personal Data only as necessary to deliver the Services according to the Services Agreement to Data Controller.

5. Categories of Data Subjects

The Data Subjects that will be impacted by the Commissioned Processing are Data Controller's users and/or third parties, whose data Data Controller uploads to the Services.

6. Technical and Organizational Measures

"**Technical and Organizational Measures**" (as that term is defined in GDPR) to be implemented by Data Processor are stipulated in Annex 1 to this Processor Addendum.

7. Rectification, Erasure, and Blocking of Personal Data, Portability Requests and Objection

Data Processor shall promptly (and in no event within more than three (3) business days transmit to Data Controller any claim or request of a Data Subject arising out of the Commissioned Processing of the Personal Data by Data Processor, including but not limited to rectification, erasure, and blocking of Personal Data, portability requests and objection. Data Processor shall not be entitled to act in its own discretion with respect to any claim or request without consultation of Data Controller

Data Processor shall rectify, erase, and block Personal Data as ordered by Data Controller unless prohibited by law from doing so.

8. Obligations of Data Processor

Data Processor shall perform the Commissioned Processing by Processing all Personal Data only within the scope of the work to be carried out and according to documented instructions of Data Controller.

Data Processor shall supervise and keep records on any Technical and Organizational Measures with respect to § 2.6 of this Processor Addendum on a regular basis. Data Processor shall provide Data Controller with respective records upon request of Data Controller, as set forth in § 10 hereof.

Data Processor has appointed the person listed below as a contact person for data protection purposes:

Pavel Tiunov <pavel@statsbot.co>

Any change in this contact person shall be disclosed promptly to Data Controller.

Data Processor shall be liable with regard to ensuring confidentiality of the Personal Data that it has received from Data Controller. All persons, including employees, officers, agents, and contractors, of Data Processor who may access the Personal Data shall be pledged in writing to confidentiality, and shall be notified of the data protection obligations specifically arising from the work to be carried out, and any order or appropriation hereof.

9. Sub-Processing

Data Controller hereby provides Data Processor with a general written authorization to employ sub-processors under this Processor Addendum for the Commissioned Processing. Data Processor shall inform Data Controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving Data Controller the opportunity to object to such changes. In the event that Data Controller objects, Data Processor shall use reasonably commercial efforts to secure another sub-processor, to which Data Controller shall also have the right to object. If Data Processor is unable to secure a satisfactory sub-processor, Data Processor shall be entitled to terminate the Services to be provided hereunder without any additional obligations to Data Controller.

Where Data Processor subcontracts its obligations under the Processor Addendum to a sub-processor, Data Processor shall ensure that the written subcontract imposes substantially the same obligations on the sub-processor as are imposed on Data Processor under this Processor Addendum, including compliance with § 5 hereunder.

Data Processor shall, prior to and regularly during the term of the subcontract, supervise the Technical and Organizational Measures that are necessary to protect the Personal Data and were implemented by the subcontractor. The transmission of Personal Data is only permitted if the subcontractor has implemented Technical and Organizational Measures comparable to the ones agreed upon in this Processor Addendum and complies with the obligations in its written contract with Data Processor.

10. Rights of Data Controller to Monitor and Audit

Data Processor agrees that Data Controller is entitled to monitor its compliance with Data Protection Legislation and this Addendum during its regular business hours. Data Processor covenants to provide Data Controller with all information that is reasonably necessary to conduct these monitoring procedures within an appropriate time period, at Data Controller's expense and subject to any confidentiality or nondisclosure agreement at the discretion of Data Processor. If Data Controller is convinced that an audit on-site at Data Processor's headquarters (or relevant office location(s)) is necessary, Data Processor shall

allow Data Controller access to the offices of Data Processor and to the stored Personal Data and data processing programs on-site, subject to good faith negotiations between the Parties as to how and when such audit will be carried out. Data Processor shall be entitled to put in place any confidentiality or nondisclosure agreement in order to protect its proprietary information, as well as the conditions under which such on-premise audit will be carried out. Data Controller is entitled to have the audit carried out by a third party (auditor) that is to be appointed on an individual basis, unless the Data Processor can identify a reasonable conflict of interest with such third party, in which case Data Controller shall appoint another. Data Controller shall announce such an audit in writing at least five (5) business days in advance. Any and all monitoring and/or audit carried out by Data Controller shall be at Data Controller's sole expense. Data Controller shall reimburse Data Processor reimburse Data Processor for its reasonable expenses and time spent and incurred in connection with an audit under this section.

11. Notification of Violations of Data Processor

Data Processor will notify Data Controller immediately about any case in which Data Processor or one of its employees breaches any provision regarding the protection of the Personal Data of Data Controller or the obligations under this Processor Addendum.

Data Controller shall be notified about any loss, illegal transmission, or third-party acquisition of the Personal Data irrespective of causation. Data Processor shall take appropriate measures in consultation with Data Controller regarding the security of the Personal Data, as well as the reduction of possible disadvantageous consequences for the Data Subjects. Insofar as notification obligations apply to Data Controller, and to the extent applicable, and subject to the limitations in Article 28(3)(f) of the GDPR, Data Processor must assist Data Controller in fulfilling these obligations.

12. Orders by Data Controller

The Commissioned Processing of Data Controller's Personal Data by Data Processor is solely carried out within the framework of the Processor Addendum and the specific individual instructions by Data Controller entered into the Services which will be documented by Data Processor.

Data Processor shall comply with (individual) instructions regarding the type, extent and procedure of Commissioned Processing.

Data Processor shall promptly notify Data Controller if Data Processor assumes that a given instruction by Data Controller may violate Data Protection Legislation. Data Processor is entitled to suspend the Commissioned Processing of the respective instruction until it has been confirmed or amended by an authorized employee of Data Controller.

13. Erasure of Personal Data after the Commissioned Processing has been Carried Out

After the Commissioned Processing has been carried out, Data Processor shall hand over, or upon prior consent of Data Controller only, destroy in a secure and data protective manner, or safely erase according to the state of the art, all Personal Data processed for Data Controller within ninety (90) days of the termination of the Commissioned Processing hereunder. Any right of retention regarding the documentation, Personal Data, processing and utilization results and the correspondent Personal Data carrier is hereby excluded, unless (a) such Personal Data is anonymized as defined under the GDPR, in

which case Data Processor shall be entitled to retain the anonymized data, or (b) European Union or EU Member State law requires additional retention or storage of the Personal Data.

§ 3 Further Obligations of Data Processor

1. Data Processor shall not use the transmitted Personal Data for any other purposes than the Commissioned Processing or other than as set forth in the Recitals. Copies or duplicates must not be created without knowledge of Data Controller, provided that this is not part of the work to be carried out as set forth in this Addendum. Data Processor warrants that the Personal Data processed for Data Controller will be held separately and segregated from any other data set.

2. Data Processor shall support Data Controller to the appropriate extent in defending against claims arising from alleged or actual violation of data protection requirements, at Data Controller's sole expense. Data Controller shall pursue complaints issued by Data Subjects within the framework of its data protection liability to an appropriate extent and shall deal with such complaints.

3. Data Processor acknowledges that information due in response to a Data Subject's request shall be given exclusively by Data Controller or by an authorized representative of Data Controller. To the extent that such request is impacted by the Commissioned Processing, Data Processor shall be obliged to promptly provide Data Controller with the relevant information and support Data Controller with respect to its obligations, at Data Controller's sole expense.

4. Data Processor shall assist Data Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to Data Processor.

5. Data Processor shall notify Data Controller about the results of the inspections of any data protection supervisory authorities, to the extent that they are associated with the Commissioned Processing and this Addendum. Data Processor shall notify Data Controller about objections issued by the supervisory authorities that refer to Data Processor's area of accountability, and shall amend ascertained objections to the extent legally required.

§ 4 Obligations of Data Controller

1. Data Controller shall be solely liable for the material legality of the Commissioned Processing, and safeguarding the rights of its Data Subjects, subject to § 6 below, including without limitation ensuring that it has provided Data Subjects with the mandated transparency associated with the Commissioned Processing under GDPR, and establishing all legal bases (and obtaining consent where consent is required) for the Processing contemplated hereunder.

2. Data Controller shall inform Data Processor of any faults, changes or irregularities (per the above paragraph regarding Data Controller's obligations) in the Personal Data processed by Data Processor promptly upon discovery by Data Controller.

§ 5 International Transfers of Personal Data

1. With respect to any Personal Data originating from, or processed on behalf of, Data Controller within EU/EEA and transferred to Data Processor's sub-processors within the EU/EEA, what is set out in § 2.9 regarding sub-processors shall apply hereinafter.

2. With respect to Personal Data originating from, or processed on behalf of, the Data Controller within EU/EEA, but accessed or otherwise processed by Data Processor (and/or its sub-processors) in jurisdictions outside the EU/EEA, and to the extent that no adequate safeguards are otherwise available (as defined in the Data Protection Legislation), the Parties agree to be bound by the *EU Controller to Processor Standard Contractual Clause Agreement* as approved by the European Commission from time to time, the approved version of which in force at present is that set out in the European Commission's Decision 2010/87/EU of 5 February 2010, available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087. Annex 1 of this Exhibit 2 shall apply as Appendix 2 of the *EU Controller to Processor Standard Contractual Clause Agreement***,** and **Annex 2** to this **Exhibit 2** shall apply as Appendix 1 of the *EU Controller to Processor Standard Contractual Clause Agreement*. To the extent that certain portions or appendixes of the *EU Controller to Processor Standard Contractual Clause Agreement* must be signed by the Parties, the Parties agree that the agreement to this Addendum shall be binding with respect to such portions or appendixes. The Parties agree that any disputes arising under an *EU Controller to Processor Standard Contractual Clause Agreement* shall be treated as if they had arisen under the Services Agreement. Notwithstanding the foregoing, the *EU Controller to Processor Standard Contractual Clause Agreement* shall not apply if the jurisdiction in which the Data Processor is established has been deemed by the EU as a jurisdiction with adequate protection for personal data or if the Data Processor and/or its sub-processors located in the U.S. has received Privacy Shield certification, *provided, however*, that if the EU deems Privacy Shield inadequate during the term of the Agreement and this Addendum, the Parties shall promptly ensure compliance with the *EU Controller to Processor Standard Contractual Clause Agreement* as set forth above To the extent that either Party works with a sub-processor for the Processing of the Personal Data, it shall ensure that a sub-processor complies with the *EU Controller to Processor Standard Contractual Clause Agreement* included herein. The Parties further recognize that the EU governing authorities may supplement or otherwise amend any requirements that must be set forth in the *EU Controller to Processor Standard Contractual Clause Agreement* under Article 46(c) of the GDPR and agree to modify the *EU Controller to Processor Standard Contractual Clause Agreement* accordingly.

3. With respect to Personal Data originating from, or processed on behalf of, Data Controller outside the EU/EEA, where the Processing of Personal Data is subject to any applicable regulatory requirement (other than the Data Protection Legislation) that prohibits or restricts (i) the transfer of Personal Data to any jurisdiction, or (ii) the Processing of Personal Data in any jurisdiction (including remote access to that Personal Data from any country or territory and through the use of cloud based IT solutions), Data Processor shall not transfer or process the Personal Data in contravention of any such prohibition or restriction. In such event, the Parties shall collaborate in good faith to find a feasible solution.

§ 6 Final Provisions

1. If any of the Personal Data of Data Controller in the possession of Data Processor may be affected by seizure or confiscation, insolvency proceedings, or any other events or measures taken by a third party, Data Processor shall inform Data Controller hereof. In addition, Data Processor shall inform

any such third party that sovereignty and ownership of the Personal Data belong solely to Data Controller.

2. Data Controller shall indemnify Data Processor, including its subsidiaries, affiliates, officers, directors, agents, or employees, from any and all fines, sanctions, claims, losses, liabilities, damages, costs and expenses, demands, reasonable attorneys' fees, consultants' fees and court costs, including third-party claims, (collectively, "**Claims**") to the extent that such Claims arise from, or may be in any way attributable to (i) any failure by Data Controller to establish (and obtain) the proper legal bases for Processing the Personal Data that falls within the Commissioned Processing, or to properly communicate to Data Processor any changes in such legal bases (such as, without limitation, withdrawal of consent or exercise of the right to be forgotten by a Data Subject under GDPR); and (ii) the negligence, gross negligence, bad faith, or intentional or willful misconduct of Data Controller or its personnel in connection with obligations set forth in this **Exhibit 2**. Data Controller's indemnification obligations shall not apply in the event of gross negligence or wilfiull misconduct of Data Processor that materially contributes to the facts and circumstances upon which the Claims are based. The Parties agree that the foregoing indemnification obligations shall (a) amend and replace any existing indemnification obligations under the Services Agreement (and any amendments thereto) with respect to the protection of Personal Data; and (b) apply irrespective of the location where such Claim is made, filed or adjudicated, whether in the United States or abroad, and irrespective of any choice of law/forum language in the Services Agreement.

3. If one or more stipulations of this Processor Addendum are deemed void, this shall not affect validity of the other stipulations of this Processor Addendum In the event of invalidity of one or more stipulations of this Processor Addendum, the Parties shall negotiate a legally effective provision commercially close to the invalid stipulation. The same shall apply in the event of a regulatory gap. In case a change in applicable law makes an amendment of this Addendum necessary, the parties will discuss and agree such required change in good faith.

4. The stipulations on choice of law and venue of jurisdiction of the Services Agreement apply to this Addendum as well.

5. In the event of any conflicting stipulations between this Processor Addendum and other agreements in place between the Parties, the stipulations within this Processor Addendum shall prevail.

Annex 1

(to the EU Controller to Processor Standard Contractual Clause Agreement)

Description of the technical and organizational security measures implemented by the Data Processor / data importer in accordance with Clauses 4(d) and 5(c) of the EU Controller to Processor Standard Contractual Clause Agreement.

"**Technical and Organizational Measures**" shall be defined as:

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, the Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia 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;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In furtherance of the above definition, Data Processor shall take the following specific measures shall to ensure that it meets the Technical and Organizational Measures prescribed in the Addendum with respect to the Commissioned Processing:

firewalls, password protection, secure socket layer, encryption

Annex 2

Appendix 1 to EU Controller to Processor Standard Contractual Clause Agreement

This Appendix forms part of the Clauses and shall be deemed signed by the Parties via Statsbot's GDPR registration portal. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is:

Client

Data importer

The data importer is:

Statsbot

Data subjects

Data Subjects are defined in Section 2 of the Processor Addendum.

Categories of data

Personal Data and/or Personal Data categories that are the subject of the Commissioned Processing include the "Other Data" category of Personal Data listed in Section 3.1 of the Addendum. The Parties agree that such list is non-exhaustive and may include additional types of Personal Data but only to the extent required to perform the Services.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data: none

Processing operations

The Personal Data transferred will be subject to the following basic processing activities: Data Processor shall process Personal Data only as necessary to deliver the Services according to the Services Agreement to Data Controller.