DATA PROCESSING AGREEMENT

concluded ... ...

between:

....., a company having its principle place of business in ....., registered with the Chamber of Commerce under number....., hereby duly represented by ....., (hereinafter: 'the Controller')

and

SURVICATE SP. Z O.O., a company having its principle place of business in Warsaw, Poland, 8 Zamiany St. LU 2, ZIP code: 02-7876, registered with the Chamber of Commerce under number 0000551025, hereby duly represented by Marcin Przybył, VP, Chief Operating Officer, (hereinafter: 'the Processor');

hereinafter collectively referred to as 'Parties' and individually 'Party',

ARTICLE 1.
PROCESSING OBJECTIVES

1.1. The Processor undertakes to process personal data on behalf of the Controller in accordance with the conditions laid down in this Agreement. The processing will be executed exclusively within the framework of this Agreement, and for all such purposes as may be agreed to subsequently.
1.2. The scope and type of personal data includes data visible after logging in to the Survicate account. The account shows the personal details of the Controller's clients or potential customers (Categories of data subjects).
1.3. The purpose of data processing includes displaying and grouping of personal data in the application and making backup copies by the Processor.
1.4. All personal data processed on behalf of the Controller shall remain the property of the Controller and/or the relevant Data subjects.
1.5. The Controller entrusts the Processor to process personal data for the duration of the Agreement for the purpose of performing this Agreement and services in the Survicate application.
1.6. The Processor shall take no unilateral decisions regarding the processing of the personal data for other purposes, including decisions regarding the provision thereof to third parties and the storage duration of the data.

ARTICLE 2.
STATEMENTS

2.1. The Controller declares that he is the administrator and the Processor that he is the processor, within the meaning of Regulation of European Parliament and Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement such data and the repeal of Directive 95/46 / EC (hereinafter referred to as "GDPR").
2.2. The Controller also declares that the consultants he has added are authorized by him to process personal data.

2.3. The Controller undertakes that the personal data visible within the account he or she manages is processed in accordance with the law and with respect for the rights and freedoms of the data subjects.

2.4. The Processor declares that it provides sufficient guarantees to implement the appropriate technical and organizational measures as detailed in Appendix 1 so that the processing meets the requirements of the GDPR and protects the rights of the data subjects.

ARTICLE 3.
TRANSMISSION OF PERSONAL DATA

3.1. The Controller consents to the provision of personal data by the Processor in the scope and purpose consistent with the Agreement to the companies cooperating with the Processor in the European Economic Area in the field of IT services and respectively outside the European Economic Area to Amazon provided that Processor ensures that specific conditions of Article 44 et seq. GDPR have been fulfilled.

3.2. The Processor is authorised within the framework of this Agreement to engage third parties within the EU/EEA, without the prior approval of the Controller being required. Upon request of the Controller, the Processor shall inform the Controller about the third party/parties engaged. Each and every transfer of data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of mySugr and shall only occur if the specific conditions of Article 44 et seq. GDPR have been fulfilled.

3.3. The Processor shall in any event ensure that such third parties will be obliged to agree in writing to the same duties that are agreed between the Controller and the Processor.

ARTICLE 4.
DUTIES – THE PROCESSOR

4.1. The Processor undertakes that:

(a) processes the personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32 od GDPR;

(d) respects the conditions referred to in Article 28 paragraphs 2 and 4 of GDPR for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR - functionality in the application;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the Processor - functionality in the application;

(g) at the choice of the Controller, deletes or returns all the personal data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

4.2. The Processor shall promptly inform the Controller if, in his opinion, the instruction given to him is in breach of the GDPR or other provisions of the Union or of a Member State for data protection due to the location of the Recipient.

4.3. The Processor agrees that during the term of the Agreement, as part of its organization, it will process the personal data entrusted to it in accordance with the provisions of the law on personal data protection (GDPR and the regulations of the Member State due to its registered office), including, but not limited to, processing By using appropriate technical and organizational measures to ensure protection of personal data processing adequate to the risks and categories of data protected and to make them available to unauthorized persons, it will keep records of persons authorized to process entrusted personal data and oblige them to keep confidential.

ARTICLE 5.
RESPONSIBILITY

5.1. The Processor shall only be responsible for processing the personal data under this Agreement. The Processor is explicitly not responsible for other processing of personal data, including but not limited to processing for purposes that are not reported by the Controller to the Processor, and processing by third parties that are not performing on behalf of the Processor.

5.2. Controller represents and warrants that it has express consent and/or a legal basis to process the relevant personal data. Furthermore, the Controller represents and warrants that the consents are not unlawful and do not infringe any rights of a third party. In this context, the Controller indemnifies the Processor of all claims and actions of third parties related to the processing of personal data without express consent and/or legal basis under this Agreement.

ARTICLE 6.
DUTY TO REPORT

6.1. In the event of a security leak and/or data protection breach, as referred to in Article 4.12 of GDPR, the Processor shall, to the best of its ability, notify the Controller thereof with undue delay, after which the Controller shall determine whether or not to inform the Data subjects and/or the relevant regulatory authority(ies). This duty to report applies irrespective of the impact of the leak. The Processor will endeavour that the furnished information is complete, correct and accurate.

6.2. If required by law and/or regulation, the Processor shall cooperate in notifying the relevant authorities and/or Data subjects. The Controller remains the responsible party for any statutory obligations in respect thereof.

ARTICLE 7.
SECURITY

7.1. The Processor will endeavour to take adequate technical and organisational measures against loss or any form of unlawful processing (such as unauthorised disclosure, deterioration, alteration or disclosure of personal data) in connection with the performance of processing personal data under this Data Processing Agreement.

7.2. The Processor does not guarantee that the security measures are effective under all circumstances. The Processor will endeavour to ensure that the security measures are of a reasonable level, having regard to the state of the art, the sensitivity of the personal data and the costs related to the security measures.

7.3. The Controller will only make the personal data available to the Processor if it is assured that the necessary security measures have been taken. The Controller is responsible for ensuring compliance with the measures agreed by and between the Parties.

ARTICLE 8.

NON DISCLOSURE AND CONFIDENTIALITY

8.1. All personal data received by the Processor from the Controller and/or compiled by the Processor within the framework of this Agreement is subject to a duty of confidentiality vis-à-vis third parties.
8.2. This duty of confidentiality will not apply in the event that the Controller has expressly authorised the furnishing of such information to third parties, where the furnishing of the information to third parties is reasonably necessary in view of the nature of the Survicate application, or if there is a legal obligation to make the information available to a third party.

ARTICLE 9.
AUDIT

9.1. In order to confirm compliance with this Data Processing Agreement, the Controller shall be at liberty to conduct an audit by assigning an independent third party who shall be obliged to observe confidentiality in this regard. Any such audit will follow the Processor's reasonable security requirements, and will not interfere unreasonably with the Processor's business activities.
9.2. The audit may only be undertaken no earlier than two weeks after the Controller has provided written notice to the Processor.
9.3. The findings in respect of the performed audit will be discussed and evaluated by the Parties and, where applicable, implemented accordingly as the case may be by one of the Parties or jointly by both Parties.
9.4. The costs of the audit will be borne by the Controller.

ARTICLE 10.
DURATION AND TERMINATION

10.1. This Data Processing Agreement is entered into for the duration set out in the Agreement, and in the absence thereof, for the duration of the cooperation between the Parties.
10.2. The Data Processing Agreement may not be terminated in the interim.
10.3. This Data Processing Agreement may only be amended by the Parties subject to mutual consent.
10.4. The Processor shall provide its full cooperation in amending and adjusting this Data Processing Agreement in the event of new privacy legislation.

ARTICLE 11.
MISCELLANEOUS

11.1. This Agreement and the implementation thereof will be governed by Polish law.
11.2. Any dispute arising between the Parties in connection with and/or arising from this Agreement will be referred to the competent Polish court in the district where the Processor has its registered office.
11.3. The contact person in the implementation of the Agreement is:
   a) on the part of the Processor: Marcin Przybył, VP, Chief Operating Officer, gdpr@survicate.com;
   b) on the part of the Controller: .....
11.4. Logs and measurements taken by the Processor shall be deemed to be authentic, unless the Controller supplies convincing proof to the contrary.
11.5. After completing the processing services, the processor removes all personal data and removes all existing copies of these services that relate to the category of persons. With regard to Users' personal data, these data are processed for a period of 10 years from the termination of the Agreement for the purpose of settling potential claims. The types of operations performed on data are also preserved (performed actions in the application), however without any personal data of clients or potential clients of the Controller.
11.6. The Processor is responsible for the amount of application fees paid by the Controller.

11.7. If any provisions of this Agreement prove to be invalid, this shall not prejudice the remaining power, and the Parties shall endeavor to replace the invalid provision with a valid provision reflecting the original will of the Parties.

MARCIN PRZYBYŁ	
Name	*Name*
Signature	*Signature*
The Processor	The Controler

Appendix 1 - Technical and Organisational Measures

1. **Confidentiality (Article 32 Paragraph 1 Point b GDPR)**
   - Physical access control
     No unauthorised access to data processing facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
   - Electronic access control
     No unauthorised use of the data processing and data storage systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
   - Internal access control (permissions for user rights of access to and amendment of data)
     No unauthorised reading, copying, changes or deletions of data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events
   - Isolation control
     The isolated processing of data, which is collected for differing purposes, e.g. multiple client support, sandboxing;
   - Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
     The processing of personal data in such a method/way, that the data cannot be associated with a specific data subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

2. **Integrity (Article 32 Paragraph 1 Point b GDPR)**
   - Data transfer control
     No unauthorised reading, copying, changes or deletions of data with electronic transfer or transport, e.g.: encryption, virtual private networks (VPN), electronic signature;
   - Data entry control
     Verification, whether and by whom personal data is entered into a data processing system, is changed or deleted, e.g.: logging, document management.

3. **Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)**
   - Availability control
     Prevention of accidental or wilful destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting procedures and contingency planning
   - Rapid recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);

4. **Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)**
   - Data protection management;
   - Incident response management;
   - Data protection by design and default (Article 25 Paragraph 2 GDPR);
   - No third party data processing as per Article 28 GDPR without corresponding instructions from mySugr, e.g.: clear and unambiguous contractual arrangements, formalised order management, strict controls on the selection of the service provider, duty of pre-evaluation, supervisory follow-up checks.