Privacy Policy

All capitalized terms used in this privacy policy (the "**Privacy Policy**") and not otherwise defined shall have the meaning ascribed to them in the General Terms and Conditions of Use, which govern all use of the www.sayatalabs.com website, owned and operated by Sayata Labs Ltd. and the software available at such site (the "**Terms and Conditions**").

In order to assess your organization's cyber risk we will analyze various parameters we believe can give visibility into such risk (the "**Service**"). Those parameters may include the following, as well as additional parameters we will deem necessary for the purposes of provision of the Service (the "**Parameters**"): (i) alerts concerning suspicious activity; (ii) security measures taken to protect user accounts; (iii) inbound activity from malicious domains; (iv) overall exposure to third parties; and (v) adherence to general cyber security best policies.

By using the Service, you agree to the information collection, use and disclosure practices described in this Privacy policy, as set forth below, and as may be amended from time to time in accordance with the terms of the Terms and Conditions, and you further agree that you read, understood and agree to be bound by the Terms and Conditions, and you represent that you have the authority to bind to the Privacy Policy and to the Terms and Conditions any person or other entity on whose behalf you are acting in connection with the Service hereunder and thereunder:

1. We may collect the following types of information when you use or access the Service (the "**Information**"): (i) the Parameters; (ii) the Registration Data and other information that you and/or third parties provide us, such as your name, address, email, annual turnover, number of employees and/or customer characteristics; (iii) details about your usage of the Service; and (iv) details about your IT and security systems.

2. Without derogating from any other provision contained herein or from any right afforded to us by any law, we may use the Information, in our discretion, for any or all of the following purposes: (i) establishing, authenticating or confirming your identity and securing the protection of the Information; (ii) offering, providing, administering or marketing any service we provide, or may provide in the future; (iii) improving, modifying, cancelling and monitoring any services or applications offered through the Service; (iv) auditing, reporting or accounting purposes; (v) safeguarding, enforcing or defending legal rights and enforcing, defending against or managing legal claims; (vi) delivering to you advertising and promotional content; (vii) safeguarding the privacy, safety or property of any party; (viii) monitoring or enforcing compliance with any of our policies; and (ix) to comply with applicable law and orders or requests of any court or other governmental body.

3. We will not share the Information with other parties without your consent except as provided below or as required or permitted by law:

    3.1 We may share the Information to the extent we deem required by applicable law or to the extent we deem necessary in connection with any action, suit, litigation, arbitration, proceeding (including any civil,

criminal, administrative, investigative or appellate proceeding), hearing, inquiry, audit, examination or investigation commenced, brought, conducted or heard by or before, or otherwise involving, any court or other governmental body or any arbitrator or arbitration panel in any jurisdiction.

3.2 We may share the Information with third parties in order to investigate, prevent or take action regarding any illegal activity or what we suspect to be an illegal activity, actual or perceived threats to our property or to the physical safety of any person, violations of any of our terms of use, terms and conditions or other rules or policies, or as otherwise permitted by law.

3.3 We may share the Information with our directors, officers, employees, consultants, agents, shareholders, affiliates, service providers, third parties to whom we provide services, business partners, and other third parties who are, directly or indirectly, involved in the operation of our business and/or in the delivery of the Service.

3.4 We may share the Information to a third party as part of a purchase of Sayata, whether by acquisition, merger, sale, reorganization, consolidation or liquidation, purchase of all or substantially all of our assets, the transfer or grant of an exclusive license to all or substantially all of our intellectual property or, or by any other way. It is hereby expressly clarified that the Information may be one of the transferred assets and we will be entitled to transfer the Information to such acquiring third party, at our discretion. Without derogating from the aforesaid, we shall have the right to disclose the Information to any third party or its legal councils as part of due diligence in anticipation of the consummation or occurrence of any of the events in this Section 3.4 above.

4. Your privacy is important to us. For such purposes, we shall take the following measures to secure and protect the Information (the "**Security Measures**"):

4.1 Access Control to Premises and Facilities. Sayata shall take measures of door locking and surveillance of the facilities to control access to premises and facilities, particularly to check authorization.

4.2 Access Control to Systems. Sayata shall take reasonable measures to prevent unauthorized access to IT systems. Sayata shall further take technical (ID/password security) and organizational (user master data) measures for user identification and authentication, of password procedures (minimum length, change of password) and encryption of data media.

4.3 Access Control to Data. Sayata shall take measures to prevent activities in IT systems not covered by the allocated access rights, as follows: (i) requirements-driven definition of the authorization scheme and access rights; (ii) monitoring and logging of accesses; (iii) differentiated

access rights (profiles, roles, transactions and objects) of the personnel on Sayata's behalf; and (iv) revoking user access to data upon termination of an authorized personnel's engagement with Sayata.

4.4 Disclosure Control. Sayata shall take reasonable measures to control the following aspects of the disclosure of personal data: electronic transfer, data transport, transmission control. Sayata shall further take measures of encryption for the transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking.

4.5 Input Control. Sayata shall maintain the documentation of data management and maintenance. Sayata shall take measures of maintain logging and reporting systems for subsequent checking whether data have been entered, changed or removed (deleted), and by whom.

4.6 Job Control. Sayata shall take reasonable measures to procure that commissioned data processing shall be carried out according to instructions. Sayata shall take the following measures (technical/organizational) to segregate the responsibilities between Sayata and sub processors on its behalf (if any): (i) unambiguous wording of the contract between Sayata and the sub processors, with respect to the processing of the data; (ii) criteria for engaging with the sub processors; and (iii) monitoring of contract performance by the sub processors.

4.7 Availability Control. Sayata shall take reasonable measures to protect the data against accidental destruction or loss. Sayata shall take the following measures to assure data security (physical/logical): (i) backup procedures; (ii) anti-virus/firewall systems; and (iii) disaster recovery plan.

4.8 Segregation Control. Sayata shall process separately data collected for different purposes. Sayata shall take measures of segregation of functions (production/testing) to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes.

By using the Service, you instruct Sayata, within your area of responsibility, to take the Security Measures and to structure its internal corporate organization to ensure compliance with the specific requirements of the protection of personal data, to take the Security Measures to adequately protect your Information against misuse and loss, and you acknowledge that the Security Measures, implemented by Sayata, are appropriate.