Data Protection Agreement

The Customer shall make available to the Company and the Customer authorizes the Company to process information including Personal Data for the provision of the Services under the Agreement. The parties have agreed to enter into this DPA to confirm the data protection provisions relating to their relationship and so as to meet the requirements of the applicable Data Protection Law.

1. Definitions

1.1. For the purposes of this DPA:

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

"**Data Protection Law**" mean all applicable laws, regulations, and other legal requirements relating to (a) privacy, data security, consumer protection, marketing, promotion, and text messaging, email, and other communications; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.;

"**the Company Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Company. "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity;

"**Services**" means any of the following services provided by the Company: (a) Company-branded product offerings made available via the website of the Company, (b) consulting or training services provided by the Company either remotely via the Internet or in person, and (c) any support services provided by the Company, including access to Company's help desk;

the terms "**data controller**", "**data processor**", "**data subject**", "**personal data**", "**processing**" and "**appropriate technical and organisational measures**" shall have the meanings given to them under applicable Data Protection Law.

2. Subject Matter, Nature and Purpose of Company's Processing of Personal Data

2.1. The subject matter, nature and purpose of the processing of Personal Data under this DPA is Company performance of the Services as further instructed in writing by the Customer in its use of the Services, unless required to do so otherwise by the Data Protection Law, in which case to the extent permitted by the Data Protection Law, the Company shall inform the Customer of this legal requirement prior to carrying out the processing. The Company shall only collect or process Personal Data for the period of rendering of the Services to the extent, and in such a manner, as is necessary for provision of the Services and in accordance with the DPA and the Data Protection Law applicable to the Company.

3. Duration

3.1. The processing of Personal Data will be carried out by the Company while Services Account of the Customer is in existence or as needed for the performance of the obligations and rights between the Company and the Customer unless otherwise agreed upon in writing.

4. Type of Personal Data Processed

4.1. The Customer may submit Customer Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- **Account Information.** When the Customer signs up for a Services Account, it is required certain information such as the name and email. The Customer may update or correct its information and email preferences at any time by visiting the Services Account. The Company can provide the Customer with additional support to access, correct, delete, or modify the information the Customer

provided to the Company and associated with the Customer's Services Account. To protect the security, the Company takes reasonable steps (such as requesting any legal information) to verify the identity of the Customer before making corrections. The Customer is responsible for maintaining the secrecy of the password and information of the Customer's Services Account at all times.

- Additional Profile Information. The Customer may choose to provide additional information as part of its profile. Profile information helps the Customer to get more from the Services. It's the Customer's choice whether to include sensitive information on its profile.

- Other Information. The Customer may otherwise choose to provide the Company information when the Customer fills in a form, conducts a search, updates or adds information to its Services Account, responds to surveys, posts to community forums, participates in promotions, or uses other features of the Services platform.

3. Company Obligations

3.1. The Company agrees and/or warrants:

(a) to process the Personal Data only on behalf of the Customer and in compliance with its instructions and the DPA; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Customer of its inability to comply, in which case the Customer is entitled to suspend the transfer of data and/or terminate the Services;

(b) that all Personal Data processed on behalf of the Customer remains the property of the Customer and/or the relevant Data subjects;

(c) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Customer and its obligations under the DPA 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 DPA, it will promptly notify the change to the Customer as soon as it is aware, in which case the Customer is entitled to suspend the transfer of data and/or terminate the Services;

(d) that it has implemented the technical and organizational security measures specified in Appendix 1 before processing the Personal Data transferred;

(e) that it will promptly notify the Customer about:

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;

ii. any accidental or unauthorized access; and

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

(f) to deal promptly and properly with all inquiries from the Customer 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;

(g) at the request of the Customer to submit its data-processing facilities for audit of the processing activities covered by the DPA;

(h) that, in the event of sub-processing, it has previously informed the Customer and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Section 7;

(j) to appoint a data protection officer, who performs his/her duties in compliance with the Data Protection Law. The data protection officers contact details are available at the Company web page.

(k) to entrust only such employees with the data processing outlined in this DPA who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Company and any person acting under its authority who has access to Personal Data, shall not

process that data unless on instructions from the Customer, unless required to do so by the Data Protection Law;

(l) to monitor periodically the internal processes to ensure that processing within Company area of responsibility is in accordance with the requirements of the Data Protection Law and the protection of the rights of the data subject.

5. Customer Obligations

5.1. The Customer agrees and/or warrants:

(a) 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 Data Protection Law and does not violate the relevant provisions;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the Company to process the Personal Data transferred only on the Customer's behalf and in accordance with the Data Protection Law and the DPA;

(c) that the Company will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 1 to this DPA;

(d) that after assessment of the requirements of the Data Protection Law, the security measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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;

(e) that it will ensure compliance with the security measures;

(f) to access and use the Services only for legal, authorized, and acceptable purposes. The Customer will not use (or assist others in using) the Services in ways that: (a) violate, misappropriate, or infringe the rights of the Company, its users, or others, including privacy, publicity, intellectual property, or other proprietary rights; (b) are illegal, obscene, defamatory, threatening, intimidating, harassing, hateful, racially, or ethnically offensive, or instigate or encourage conduct that would be illegal, or otherwise inappropriate; (c) involve publishing falsehoods, misrepresentations, or misleading statements; (d) impersonate someone; (e) involve sending illegal or impermissible communications such as bulk messaging, auto-messaging, auto-dialing, and the like; or (f) involve any other use of the Services prescribed in this DPA unless otherwise authorized by the Company;

(g) do not to (or assist others to) access, use, copy, adapt, modify, prepare derivative works based upon, distribute, license, sublicense, transfer, display, perform, or otherwise exploit the Services platform in impermissible or unauthorized manners, or in ways that burden, impair, or harm the Company, the Services platform, systems, other users, or others, including that the Customer will not directly or through automated means: (a) reverse engineer, alter, modify, create derivative works from, decompile, or extract code from the Services platform; (b) send, store, or transmit viruses or other harmful computer code through or onto the Services platform; (c) gain or attempt to gain unauthorized access to the Services platform or systems; (d) interfere with or disrupt the integrity or performance of the Services platform; (e) create accounts for the Services platform through unauthorized or automated means; (f) collect the information of or about other users in any impermissible or unauthorized manner; (g) sell, resell, rent, or charge for the Services platform; or (h) distribute or make the Services platform available over a network where it could be used by multiple devices at the same time;

(h) that the Customer is responsible for keeping the Customer's Services Account safe and secure, and the Customer will notify the Company promptly of any unauthorized use or security breach of the Customer's Account or the Services platform;

(i) that the Company grants the Customer a limited, revocable, non-exclusive, non-sublicensable, and non-transferable license to use the Services platform. This license is for the sole purpose of enabling the Customer to use the Services platform, in the manner permitted by this DPA. No licenses or rights are

granted to the Customer by implication or otherwise, except for the licenses and rights expressly granted to the Customer.

6. Technical and Organizational Measures

6.1. The Company shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, described under Appendix 1. Such measures include but not limited to physical and IT measures, and organizational measures to:

(a) the prevention of unauthorized persons from gaining access to Personal Data processing systems (physical access control),

(b) the prevention of Personal Data processing systems from being used without authorization (logical access control),

(c) ensuring that persons entitled to use a Personal Data processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control),

(d) ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),

(e) ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data processing systems (entry control),

(f) ensuring that Personal Data is protected against accidental destruction or loss (availability control).

6.2. The technical and organizational measures are subject to technical progress and further development. In this respect the Company may implement alternative adequate measure, however, the security level of the defined measures must never be reduced. Major changes must be documented.

7. Sub-Processors

7.1. The Customer agrees that the Company may engage Company Affiliate or third parties to process Personal Data in order to assist the Company to deliver the Services on behalf of the Customer (**"Sub-processors"**). The Company has or will enter into written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA to the extent applicable to the nature of the Services provided by such Sub-processor. If the Sub-processor processes the Services outside the EU/EEA, the Company shall ensure that the transfer is made pursuant to European Commission approved standard contractual clauses for the transfer of Personal Data which the Customer authorizes the Company to enter into on its behalf, or that other appropriate legal data transfer mechanisms are used.

7.2. The current Sub-processors for the Services are set out at website of the Company ("Sub-processor List") and the Customer agrees and approves that the Company has engaged such Sub-processors to process Personal Data as set out in the list. The Company shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to process Personal Data in connection with the provision of the applicable Service.

7.3. The Company shall notify the Customer thirty (30) days' in advance of any intended changes concerning the addition or replacement of any Sub-processor during which period the Customer may raise objections to the Sub-processor's appointment. Any objections must be raised promptly (and in any event no later than fourteen (14) days following Company's notification of the intended changes). Should the Company choose to retain the objected to Sub-processor, the Company will notify the customer at least fourteen (14) days before authorizing the Sub-processor to process Personal Data and then the Customer may immediately discontinue using the relevant portion of the Services and may terminate the relevant portion of the Services.

7.4. For the avoidance of doubt, where any Sub-processor fails to fulfill its obligations under any sub-processing agreement or under applicable law the Company will remain fully liable to the Customer for the fulfillment of its obligations under this DPA.

8. Audit

8.1. In order to confirm compliance with this DPA, the Customer 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 must occur during Company's normal business hours and will be permitted only to the extent required for the Customer to assess Company's compliance with this DPA. In connection with any such audit, the Customer will ensure that the auditor will: (a) review any information on Company's premises;

(b) observe reasonable on-site access and other restrictions reasonably imposed by the Company; (c) comply with Company's policies and procedures, and (d) not unreasonably interfere with Company's business activities. The Company reserves the right to restrict or suspend any audit in the event of any breach of the conditions specified in this Section 8.

8.2. In the event that the Customer, a regulator or data protection authority requires additional information or an audit related to the Services, then, the Company agrees to submit its data processing facilities, data files and documentation needed for processing Personal Data to audit by the Customer (or any third party such as inspection agents or auditors, selected by Customer) to ascertain compliance with this DPA, subject to being given notice and the auditor entering into a non-disclosure agreement directly with the Company. The Company agrees to provide reasonable cooperation to Customer in the course of such operations including providing all relevant information and access to all equipment, software, data, files, information systems, etc. used for the performance of Services, including processing of Personal Data. Such audits shall be carried out at the Customer's cost and expense.

8.3. The audit may only be undertaken when there are specific grounds for suspecting the misuse of Personal Data, and no earlier than two weeks after the Customer has provided written notice to the Company.

8.4. 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. The costs of the audit will be borne by the Customer.

9. Notification of A Data Breach

9.1. In the event of the Company aware of any breach of security that results in the accidental, unauthorized or unlawful destruction or unauthorized disclosure of or access to Personal Data the Company shall to the best of its ability, notify the Customer thereof with undue delay, after which the Customer 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 Company will endeavour that the furnished information is complete, correct and accurate.

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

9.3. The duty to report includes in any event the duty to report the fact that a leak has occurred, including details regarding:

the (suspected) cause of the leak;

the (currently known and/or anticipated) consequences thereof;
the (proposed) solution;
the measures that have already been taken.

10. Deletion and Return of Personal Data

10.1. The parties agree that on the termination of the provision of data-processing services, the Company and its subcontractors shall, at the choice of the Customer, return all the Personal Data transferred and the copies thereof to the Customer or shall destroy all the Personal Data and certify to the Customer that it has done so, unless legislation imposed upon the Company prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the Company warrants that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred

anymore. The Company and its subcontractors warrant that upon request of the Customer and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in Section 8.

11. Governing Law/Forum

11.1. This DPA shall be governed by and interpreted in accordance with the laws of United States of America.

11.2. Any and all claims, disputes or controversies arising under, out of, or in connection with this DPA, breach, termination or validity thereof, which have not been resolved by good faith negotiations between the Company and the Customer within period of thirty (30) calendar days after receipt of a notice from one party to the other requesting negotiations shall be resolved by final and binding arbitration in the Court of Commercial Arbitration . Disputes shall be settled by a single arbitrator. Arbitration proceedings shall be held in the, United States of America. The place of arbitration shall be United States of America. The language of arbitration shall be English. Relevant documents in other languages shall be translated into English if the arbitrators so direct. All expenses and costs of the arbitrators and the arbitration in connection therewith will be shared equally, except that the Company and the Customer will each bear the costs of its own prosecution and defense, including without limitation attorney's fees and the production of witnesses and other evidence. Any award rendered in such arbitration shall be final and may be enforced by either party.

11.3. The parties agree to keep all details of the arbitration proceedings and arbitral award strictly confidential and shall use all reasonable efforts to take such action as may be appropriate to prevent the unauthorized disclosure of the proceedings, any information disclosed in connection therewith and the award granted.

Appendix No. 1

Description of the technical and organizational measures implemented by the Company:

the Company shall implement the measures described in this appendix, provided that the measures directly or indirectly contribute or can contribute to the protection of Personal Data during the period of Company's Services rendering to the Customer. If the Company believes that a measure is not necessary for the respective Service or part thereof, the Company will justify this and come to an agreement with the Customer.

The technical and organizational measures are subject to technical progress and development. In this respect the Company is permitted to implement alternative adequate measures. The level of security must align with industry security best practice and not less than, the measures set forth herein. All major changes are to be agreed with the Customer and documented.

1. Risk management

1.1. Security risk management

1. The Company shall identify and evaluate security risks related to confidentiality, integrity and availability and based on such evaluation implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk.
2. The Company shall have documented processes and routines for handling risks within its operations.
3. The Company shall periodically assess the risks related to information systems and processing, storing and transmitting information.

1.2. Security risk management for personal data

1.2.1. The Company shall identify and evaluate security risks related to confidentiality, integrity and availability and based on such evaluation implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk of the specific Personal Data types and purposes being processed by the Company, including inter alia as appropriate:

- The pseudonymisation 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 the Customer's 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.

1.2.2. The Company shall have documented processes and routines for handling risks when processing Personal Data on behalf of the Customer.

1.2.3. The Company shall periodically assess the risks related to information systems and processing, storing and transmitting Personal Data.

1.3. Information security policies

1.3.1. The Company shall have a defined and documented information security management system including an information security policy and procedures in place, which shall be approved by Company's management. They shall be published within Company´s organization and communicated to relevant Company personnel.

1.3.2. The Company shall periodically review Company's security policies and procedures and update them if required to ensure their compliance with this Appendix.

2. Organization of information security

- The Company shall have defined and documented security roles and responsibilities within its organization.

- The Company shall appoint at least one data protection officer who has appropriate security competence and who has an overall responsibility for implementing the security measures under this Appendix and who will be the contact person for the Customer's security staff.

3. Human resource security

- The Company shall ensure that Company personnel handles information in accordance with the level of confidentiality required under the DPA.

- The Company shall ensure that relevant Company personnel is aware of the approved use (including use restrictions as the case may be) of information, facilities and systems under the DPA.

- The Company shall ensure that any Company personnel performing assignments under the Agreement is trustworthy, meets established security criteria and has been, and during the term of the assignment will continue to be, subject to appropriate screening and background verification.

- The Company shall ensure that Company personnel with security responsibilities is adequately trained to carry out security related duties.

- The Company shall provide or ensure periodical security awareness training to relevant Company personnel. Such Company training shall include, without limitation:

(a) How to handle customer information security (i.e. the protection of the confidentiality, integrity and availability of information);

(b) Why information security is needed to protect customers information and systems;

(c) The common types of security threats (such as identity theft, malware, hacking, information leakage and insider threat);

(d) The importance of complying with information security policies and applying associated standards/procedures;

(e) Personal responsibility for information security (such as protecting customer's privacy-related information and reporting actual and suspected data breaches).

4. Access control

The Company shall have a defined and documented access control policy for facilities, sites, network, system, application and information/data access (including physical, logical and remote access controls), an authorization process for user access and privileges, procedures for revoking access rights and an acceptable use of access privileges for Company personnel in place.

The Company shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.

The Company shall assign all access privileges based on the principle of need-to-know and principle of least privilege.

The Company shall use strong authentication (multi-factor) for remote access users and users connecting from an untrusted network.

The Company shall ensure that Company personnel has a personal and unique identifier (user ID), and use an appropriate authentication technique, which confirms and ensures the identity of users.

5. Physical and environmental security

The Company shall protect information processing facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities. This includes physical perimeter and access protection.

6. Operations security

The Company shall have an established change management system in place for making changes to business processes, information processing facilities and systems. The change management system shall include tests and reviews before changes are implemented, such as procedures to handle urgent changes, roll back procedures to recover from failed changes, logs that show, what has been changed, when and by whom.

The Company shall implement malware protection to ensure that any software used for Company's provision of the Services to the Customer is protected from malware.

The Company shall make backup copies of critical information and test back-up copies to ensure that the information can be restored as agreed with the Customer.

The Company shall log and monitor activities, such as create, reading, copying, amendment and deletion of processed data, as well as exceptions, faults and information security events and regularly review these. Furthermore, the Company shall protect and store (for at least 6 months or such period/s set by Data Protection Law) log information, and on request, deliver monitoring data to the Customer. Anomalies / incidents / indicators of compromise shall be reported according to the data breach management requirements as set out in clause 9, below.

The Company shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner.

The Company shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.

The Company shall ensure development is segregated from test and production environment.

7. Communications security

The Company shall implement network security controls such as service level, firewalling and segregation to protect information systems.

8. Company relationship with sub-suppliers

The Company shall reflect the content of this Appendix in its agreements with Sub-processors that perform tasks assigned under the DPA.

The Company shall regularly monitor, review and audit Sub-processor's compliance with this Appendix.

The Company shall, at the request of the Customer, provide the Customer with evidence regarding Sub-processor's compliance with this Appendix.

9. Data breach management

The Company shall have established procedures for data breach management.

The Company shall inform the Customer about any data breach (including but not limited to incidents in relation to the processing of Personal Data) as soon as possible but no later than within 36 hours after the data breach has been identified.

All reporting of security-related incidents shall be treated as confidential information and be encrypted, using industry standard encryption methods.

The data breach report shall contain at least the following information:

(a) The nature of the data breach,

(b) The nature of the Personal Data affected,

(c) The categories and number of data subjects concerned,

(d) The number of Personal Data records concerned,

(e) Measures taken to address the data breach,

(f) The possible consequences and adverse effect of the data breach, and

(g) Any other information the Customer is required to report to the relevant regulator or data subject.

To the extent legally possible, the Company may claim compensation for support services under this clause 9 which are not attributable to failures on the part of the Company.

10. Business continuity management

The Company shall identify business continuity risks and take necessary actions to control and mitigate such risks.

The Company shall have documented processes and routines for handling business continuity.

The Company shall ensure that information security is embedded into the business continuity plans

The Company shall periodically assess the efficiency of its business continuity management, and compliance with availability requirements (if any).