BEACON PLATFORM INCORPORATED
DATA PROTECTION & PRIVACY POLICY

Beacon Platform Incorporated ("**BPI**") extends this Data Protection & Privacy Policy ("**DPA**") to all BPI licensed clients (each a "**Client**", and, collectively, the "**Clients**").

Capitalized terms not defined in this DPA shall have the meaning defined in the respective licensing agreement between BPI and each of its Clients (each a "**License Agreement**").

BPI will notify Clients of any changes to this DPA after the Effective Date of any such Client's License Agreement.

1. **DEFINITIONS.**

In this DPA, the following terms shall have the meanings set out below:
"CCPA" means California Consumer Privacy Act; and the terms **"Business"**, **"Collecting"**, **"Consumer"**, **"Personal Information", "Processing"**, **"Selling"**, **"Service Provider"**, **"Sharing"**, **"Third Party"**, **"Unique Identifier"** shall have the same meaning as in the CCPA or equivalent term in any applicable Data Protection Laws
"Data Protection Laws" means all applicable laws and regulations, including but not limited to laws and regulations of the United States and the CCPA (**"US"**); the United Kingdom and the Data Protection Act 2018 (**"UK"**); the European Union and the GDPR (**"EU"**), the European Economic Area (**"EEA"**) and their Member States and Switzerland, applicable to the Collecting, Processing, Selling of Personal Information under the Agreement;
"GDPR" means EU General Data Protection Regulation 2016/679 and the terms: **"Commission"**, **"Controller"**, **"Data Subject"**, **"Member State"**, **"Personal Data"**, **"Processing"**, **"Processor"**, and **"Supervisory Authority"** shall have the same meaning as in the GDPR or equivalent term in any applicable Data Protection Laws;
"Independent Auditor" means an auditor from an internationally recognized auditing firm;
"Regulator" means a data protection authority or other regulatory, governmental or supervisory authority with authority over all or any part of the Processing of Client's Personal Information / Personal Data.
"Sub-processor" means any third party appointed to Process Personal Information in connection with a License Agreement

2. **USE OF PERSONAL INFORMATION / PERSONAL DATA.**

2.1. BPI does not Collect, retain, use, disclose or otherwise Process Personal Information / Personal Data other than for the purposes of performing the Services or other actions for the benefit of a Client that are specified in a License Agreement with such Client. BPI does not combine the Personal Information / Personal Data it Processes or Collects on behalf of each Client with any other Personal Information it Collects from any other another client or individual unless necessary for the provision of the Services. BPI certifies that it understands the obligations and restrictions placed on it under any applicable Data Protection Laws.

2.2. Affiliates shall have the same rights that a Client has under this DPA when such Affiliate is a Controller in respect of the Personal Data.

3. THE COLLECTING OR PROCESSING OF PERSONAL INFORMATION / PERSONAL DATA

1.1. The only Personal Data / Personal Information that BPI Collects or Processes are the names and email addresses of Authorized Users under License Agreements. BPI is not involved in the Selling of Personal Information / Personal Data.

1.2. **Compliance with applicable Data Protection Laws.** BPI will comply with its obligations under applicable Data Protection Laws in the event that it is Collecting or Processing Personal Information / Personal Data. BPI shall only Process or permit the Processing of Personal Information / Personal Data in line with a Client's express written instructions and in line with the agreed obligations under a License Agreement.

1.3. **Instructions for Collecting, Processing, or transferring Personal Information.** BPI, in performing its obligations under the Agreement, will Process Personal Information in accordance with the requirements of Data Protection Laws. If a Client provides Personal Information to BPI, the Client shall have sole responsibility for the accuracy and quality of Personal Information and for obtaining consent. By entering in a License Agreement with BPI, Client instructs (and BPI shall instruct each Sub-processor) to transfer Client's Personal Information or Personal Data to any country or territory, as reasonably necessary for the performance of BPI's obligations under and consistent with the relevant License Agreement.

4. RIGHTS OF CONSUMERS AND DATA SUBJECTS

1.1. **Consumer Request.** BPI shall, unless prohibited by applicable laws, promptly after receipt notify a Client (and provide reasonable assistance to the other party where required) if it receives a request from a Consumer or Data Subject to exercise any right of: access; rectification; restriction or prohibition of Collecting or Processing; erasure/deletion; data portability, object to the Collecting or Processing; or not to be subject to an automated individual decision making; regarding Consumer or Data Subject's Personal Information / Personal Data ("**DSAR**") or any other query received by BPI regarding the privacy practices of a Client.

1.2. **Assistance.** BPI shall assist a Client by appropriate technical and organizational measures, insofar as this is possible, sufficiently, and promptly enough for the fulfilment of a Client's obligation to respond to a DSAR under Data Protection Laws. If a Client, in performing its obligations under a License Agreement, does not have the ability to address a DSAR, BPI shall upon request provide commercially reasonable efforts to assist such Client in responding to such DSAR, unless legally prohibited by applicable laws and if the response to such DSAR is required under Data Protection Laws. To the extent legally permitted, BPI shall be responsible for its own costs arising from the provision of such assistance.

5. Requests by Regulators and Other Authorities

1.3. BPI shall promptly notify a Client of any complaints received or any notices of investigation or non-compliance from any Supervisory Authority or other data protection regulator relating to the Collection or Processing of Personal Information / Personal Data unless BPI is prohibited from doing so under Data Protection Laws.

1.4. BPI shall cooperate with a Client and the relevant Supervisory Authority or other data protection

regulator in the event of any investigation or litigation concerning Personal Information / Personal Data and shall abide by the advice of the relevant Supervisory Authority or other data protection regulator with regard to the Processing of such Personal Information / Personal Data, provided that such Client shall compensate BPI for the costs of any such cooperation and/or implementation of such advice in the event that such costs are anything other than negligible.

1.5. If any Personal Data provided to BPI by or on behalf of a Client or otherwise accessed in connection with the provision of Services is requested or subject to an order for compelled disclosure by any law enforcement or security authorities or other government agencies, or BPI has any reason to believe that such request may be made, in each case BPI shall:

1.5.(a) promptly redirect the third party to request the data directly from such Client and notify such Client, unless prohibited under applicable law or by the relevant authority, in which case BPI shall use all lawful efforts to waive the prohibition and shall communicate as much information to such Client as soon as possible;

1.5.(b) use all lawful efforts to challenge the request or order for disclosure on the basis of any legal deficiencies under the applicable laws or any relevant conflicts with Data Protection Laws;

1.5.(c) upon request by a Client, suspend or cease Processing any Personal Information / Personal Data provided to it by or on behalf of a Client with immediate effect and without penalty or termination fee or other liability to such Client; and

1.5.(d) not make transfers of Personal Information / Personal Data to any law enforcement or security authorities or other government agencies in breach of Data Protection Laws or a License Agreement, unless such transfer is required under applicable law.

6. SUB-PROCESSORS. By entering in a License Agreement with BPI, Client instructs BPI to utilize a cloud provider for the provision of the solution and Services as a Sub-processor. BPI has entered in written agreement(s) with cloud providers that containing data protection obligations substantially similar to those in this Agreement with respect to the protection of Personal Information / Personal Data to the extent applicable to the nature of the Services provided by such cloud provider.

7. **PERSONNEL**

7.1. **Confidentiality.** BPI personnel engaged in the Processing of Personal Information / Personal Data are informed of the confidential nature of Personal Data / Personal Information and have received appropriate training on their responsibilities and have executed written confidentiality agreements.

7.2. **Integrity.** BPI takes commercially reasonable steps to ensure the integrity of any personnel engaged in the Processing of Personal Information / Personal Data.

7.3. **Limitation of Use.** Access by BPI personnel to Personal Information / Personal Data is used only to the extent necessary to provide the Services and in accordance with a License Agreement.

7.4. **Data Protection Officer**. BPI has appointed a representative authorized to address matters arising under this DPA or Data Protection Laws. Inquiries should be sent to: Alla Liberman, Chief Operating Officer, Beacon Platform Incorporated, ***5 Hanover Square, 20th Floor, Suite 2001, New York,***

NY 10004. alla.liberman@beacon.io with cc: .

1. SECURITY.

1.6. **Controls for the Protection of Personal Information / Personal Data.** BPI has implemented and maintains appropriate technical and organizational measures designed to protect the confidentiality, integrity, and security of Personal Information / Personal Data. (Including protection against unauthorized or unlawful Collecting, Processing or Selling and against accidental or unlawful destruction, loss or alteration, unauthorized disclosure of, or access to, Personal Information / Personal Data). BPI regularly monitors compliance with these measures.

1.7. BPI ensures a level of security appropriate to the risk, taking into account 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; provided, however, that such measures shall at a minimum include:

1.7.(a) the technical, physical, administrative and organizational measures described in a License Agreement, any cybersecurity, business continuity and disaster recovery requirements in the Agreement and, if applicable those measures set out in Annex II to the Appendix to the Standard Contractual Clauses available upon request, which shall apply whenever BPI Processes Personal Data;

1.7.(b) encryption of Personal Data / Personal Information at rest;

1.7.(c) the ability to restore the availability and access to Personal Information / Personal Data in a timely manner in the event of a physical or technical incident; and

1.7.(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

1.8. **Audit.** BPI will reasonably cooperate with any Client audit requests to the extent necessary to ensure compliance with this DPA, and as required by Data Protection Laws. Any such audit will be subject to the confidentiality obligations set forth in the relevant License Agreement. Information and audit rights under this Section 8.3 arise ***only to the extent*** that the relevant License Agreement does not otherwise give information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR). A Client may appoint an Independent Auditor, with such access, on reasonable written notice (minimum thirty (30) calendar days) and within normal working hours, to those records pertaining to Personal Information / Personal Data as may be reasonably required by a Client to exercise its rights of audit as set out in this Section 8.3. Certain sensitive information in relation to BPI's IT and security will be redacted before being audited and may only be audited at BPI's premises. With BPI's agreement, this audit may cover documents only or may include an onsite audit, subject to such Client notifying BPI of the identity of any onsite Independent Auditors and that any Independent Auditors have entered into appropriate confidentiality agreements, approved by BPI (such approval not to be unreasonably withheld or delayed). Such Client shall use reasonable endeavors to minimize any disruption caused to BPI's business activities because of such audit. No audit will last more than five (5) working days each time unless a longer period is required to fulfill any request or comply with any requirement of any regulator. Audits will take place no more than once in any calendar year unless and to the extent that such Client (acting reasonably and in good faith) has reasonable grounds to suspect any breach of this DPA by BPI, in which case the parties will agree to a

timescale for an audit. Costs of the audit, including appointment of the Independent Auditor, will be borne by such Client. To the extent legally permissible, BPI will be entitled to reasonable time to review and retain any audit report and to consult the Independent Auditor on the content, prior to the report being submitted to such Client. All confidential information of BPI obtained by such Client or an Independent Auditor pursuant to any audit will be maintained in confidence by such Client and its Independent Auditor and may not be disclosed to any third party, including, without limitation, any other agents or representatives of such Client, except to the extent necessary to assert or enforce any of such Client's rights under this DPA or is required to be disclosed by Data Protection Laws, by any regulatory or Supervisory Authority or by a court or other authority of competent jurisdiction provided that, to the extent it is legally permitted to do so, it gives BPI as much notice of this disclosure as possible and, where notice of disclosure is not prohibited and is given in accordance with this section, it takes into account the reasonable requests of BPI in relation to the content of this disclosure. Neither the Independent Auditor nor such Client will be permitted to perform penetration tests, vulnerability scans, or otherwise interrogate the BPI's network or information technology systems. In no circumstances will such Client or the Independent Auditor have access to (a) individual payroll and personnel files; (b) individual expenditure or records.

2. DATA INCIDENT MANAGEMENT AND NOTIFICATION.

BPI maintains security incident management policies and procedures and will notify a Client without undue delay and in line with the timelines required by applicable Data Protection Laws after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to such Client's Personal Information, transmitted, stored or otherwise Processed by them which results in any actual loss or misuse of Personal Information (a "**Data Incident**"). BPI will make reasonable efforts to identify the cause of such Data Incident and take those steps as the affected Client deems necessary and reasonable to remediate the cause of such a Data Incident to the extent the remediation is within BPI's reasonable control. If there is a Data Incident, such affected Client will be responsible for notifying its Consumers and any relevant regulatory or Supervisory Authorities. If legally permissible and before any such notification is made, such affected Client must consult with and provide BPI an opportunity to comment on any notification made in connection with a Data Incident**.**

3. RETURN AND DELETION OF DATA.

BPI will, at any time on the request of a Client and upon expiration or termination of the relevant License Agreement, return all Personal information to such Client or at such Client's request delete the same from its systems, so far as is reasonably practicable and other than any back-up copies which BPI is required to retain for compliance with applicable laws or regulatory requirements provided that such copies are kept confidential and secure in accordance with the relevant License Agreement.

4. LIMITATION OF LIABILITY

BPI's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to a breach of its obligations under this DPA, whether in contract, tort or under any other theory of liability, are subject to the 'Limitation of Liability' section of the relevant License Agreements, and any reference in such section to the liability of a party means the aggregate liability of BPI and all of its Affiliates under the relevant License Agreement.

5. DATA PROTECTION IMPACT ASSESSMENT

Upon a Client's request, BPI will provide the Client with reasonable cooperation and assistance, needed to fulfil the Client's obligation under Data Protection Laws to carry out a data protection impact assessment related to Client's use or performance of BPI's services, to the extent such Client does not otherwise have access to the relevant information, and to the extent such information is available to BPI. BPI will provide reasonable assistance to such Client in the cooperation or prior consultation with the regulator or Supervisory Authority in the performance of its tasks relating to this Section 12, to the extent required under Data Protection Laws.

6. TRANSFER MECHANISMS FOR DATA TRANSFERS

1.9. If in the future, a Client asserts that Personal Data is being transferred pursuant to a License Agreement from the European Union, the European Economic Area and/or their Member States, Switzerland or the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws, then BPI and the Client will execute Annex 1 to the Standard Contractual Clauses (and other European equivalent clauses) available upon request. In such event, nothing in this DPA shall contradict, directly or indirectly, the Standard Contractual Clauses, or prejudice the fundamental rights or freedoms of Data Subjects. In the event of such a contradiction, the Standard Contractual Clauses shall prevail.