CookiePro™ Data Processing Addendum

1.1. *Definitions:* In this Clause, the following terms shall have the following meanings:

(a) "**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**") and "**special categories of personal data**" shall have the meanings given in Applicable Data Protection Law; and

(b) "**Applicable Data Protection Law**" shall mean any and all applicable data protection and privacy laws including, where applicable, EU data protection law.

(c) "**EU Data Protection Law**" means: (i) the EU General Data Protection Regulation (Regulation 2016/679); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iii) any and all EU Member State laws made under or pursuant to any of the foregoing; in each case as amended or superseded from time to time.

1.2. *Relationship of the parties:* You (the controller) appoint CookiePro as a processor to process the personal data described in the Agreement (the "**Data**") for the purposes described in the Agreement (or as otherwise agreed in writing by the parties) (the "**Permitted Purpose**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law, and CookiePro shall promptly inform You if, in CookiePro's opinion, Your processing instructions infringe Applicable Data Protection Law.

1.3. *International transfers & data localization laws:* If any Data originates from the European Economic Area ("**EEA**") under this Agreement, CookiePro shall not transfer the Data outside of the EEA unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Data to a recipient (a) in a country that the European Commission has decided provides adequate protection for personal data, (b) that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law, (c) in the United States that has certified its compliance with the EU-US Privacy Shield, or (d) that has executed standard contractual clauses adopted or approved by the European Commission.

For this purpose, you acknowledge that we shall provide adequate protection for such data by virtue of our or our affiliate having self-certified compliance with the EU-U.S. and Swiss-US Privacy Shield Frameworks. If any Data originates from any country (other than an EEA country) with one or more laws imposing data transfer restrictions or prohibitions and You have informed CookiePro of such data transfer restrictions or prohibitions, You and CookiePro shall ensure appropriate transfer mechanism (satisfying the country's data transfer requirement(s)) is in place, as reasonably requested by You and mutually agreed upon by both parties, before transferring or accessing Data outside of such country. For the avoidance of doubt, this transfer restriction does not pertain to You or your authorized users who have access to the CookiePro Service and Data, and CookiePro shall not be held responsible for actions of Customer or your authorized users. Neither you nor your authorized users shall be entitled to use the CookiePro Service in any country with data localization laws that would require your environment to be hosted in said country.

Data is hosted in a data center with CookiePro's cloud vendor as further detailed at https://community.cookiepro.com/s/article/hosting.

1.4. *Confidentiality of processing:* CookiePro shall ensure that any person it authorises to process the Data (an "**Authorised Person**") shall protect the Data in accordance with CookiePro's confidentiality obligations under the Agreement.

1.5. *Security:* 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, CookiePro shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (as specified in Article 32 of the EU General Data Protection Regulation) to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Breach**"). All penetration or other testing shall be done in a designated testing environment and pursuant to mutual agreement of the parties. OneTrust LLC's Information Security Management System (ISMS) is ISO/IEC 27001:2013 certified as reflected in the certificate found here: http://www.coalfireiso.com/Certificates/OneTrust-ISO-27001-Certificate-Award_2-12-2019.pdf.

1.6. *Subprocessing:* You consent to CookiePro engaging subprocessors to process the Data for the Permitted Purpose provided that: (i) CookiePro maintains an up-to-date list of its subprocessors on the CookiePro Community at community.cookiepro.com (or any future support website used by CookiePro), which it shall update with details of any change in subprocessors at least 30 days' prior to any such change (except to the extent shorter notice is required due to an emergency) and notify you of such change via CookiePro's support e-mail notification process; (ii) CookiePro imposes data protection terms on any subprocessor it appoints that require it to protect the Data to the standard required by Applicable

Data Protection Law; and (iii) CookiePro remains liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor. You may object to CookiePro's appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, you may suspend or terminate the Agreement (without prejudice to any fees incurred by you prior to suspension or termination). For the purposes of providing the CookiePro Service, you agree to processing by CookiePro and its affiliates and the use by CookiePro of the subprocessors identified in the CookiePro Community as set forth at https://community.cookiepro.com/s/article/List-of-Subprocessors.

1.7. *Cooperation and data subjects' rights:* CookiePro shall provide reasonable and timely assistance to you (at your expense) to enable you to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to CookiePro, CookiePro shall promptly inform you providing full details of the same.

1.8. *Data Protection Impact Assessment:* CookiePro shall provide you with reasonable cooperation (at your expense) to enable you to conduct any data protection impact assessment that it is required to undertake under Applicable Data Protection Law.

1.9. *Security breaches:* If it becomes aware of a Security Breach, CookiePro shall inform you without undue delay and shall provide reasonable information and cooperation (at its expense) to you so that you can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. CookiePro shall further take such reasonably necessary measures and actions to mitigate the effects of the Security Breach and shall keep you informed of all material developments in connection with the Security Breach.

1.10. *Deletion or return of Data:* Following termination or expiry of the Agreement, CookiePro shall (at your election) destroy or return to you all Data in its possession or control. This requirement shall not apply to the extent that: (i) CookiePro is required by applicable law to retain some or all of the Data; or (ii) or to Data it has archived on back-up and support systems, provided that CookiePro shall securely protect such Data.

1.11. *Audit:* CookiePro shall, upon reasonable notice (no less than thirty (30) days) and not more than once a year (unless there is a material Security Breach), allow its procedures and documentation to be inspected or audited by you (or your designee, subject to CookiePro's approval which shall not be unreasonably withheld) during business hours in order to ascertain compliance with the obligations set forth in this Data Processing Addendum. For the avoidance of doubt, the scope of such audit shall be limited to documents and records allowing the verification of CookiePro's compliance with the obligations set forth in this Data Processing Addendum and shall not include financial documents or records of CookiePro or any documents or records concerning other customers of CookiePro.

1.12. *Liability:* Each party's liability for one or more breaches of this Data Processing Addendum shall be subject to the limitations and exclusions of liability set out in the Agreement. In no event shall either party's liability for a breach of this Data Processing Addendum exceed the liability cap set out in the Agreement. Neither party limits or excludes any liability that cannot be limited or excluded under applicable law (such as for fraud).

Appendix 1: CookiePro Information Security Controls

CookiePro technical and organizational measures for data protection have been organized and implemented according to ISO 27001 and include the following types of controls:

A.5: Information security policies
A.6: Organization of information security
A.7: Human resource security
A.8: Asset management
A.9: Access control
A.10: Cryptography
A.11: Physical and environmental security
A.12: Operations security
A.13: Communications security
A.14: System acquisition, development and maintenance
A.15: Supplier relationships
A.16: Information security incident management
A.17: Information security aspects of business continuity management
A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws

CookiePro maintains the following policies and procedures in support of its privacy and security program:

Information Security Policies
To provide management direction and support for information security in accordance with business requirements, and relevant laws and regulations.

Organization of Information Security
To establish a framework for initiating and controlling information security implementation and operations at CookiePro.

Human Resource Security
To ensure that all workforce members are well suited for, and understand, their roles and responsibilities. To ensure that all workforce members are aware of, and that they fulfill, their information security responsibilities and obligations. To ensure that the organization's interests are protected throughout the employment process, from pre-employment to termination.

Asset Management
To identify CookiePro's information assets, and to define and assign appropriate responsibilities for ensuring their protection. To ensure an appropriate level of protection for information assets in accordance with their sensitivity level and importance to the organization. To prevent the unauthorized disclosure, modification, removal or destruction of information stored on media.

Access Control
Provides the framework for user, system and application access control and management, and user responsibilities. To limit access to information and information processing facilities. To ensure authorized user access and to prevent unauthorized access to systems and services. To make users accountable for safeguarding their authentication information. To prevent unauthorized access to systems and applications.

Cryptography
To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

Physical and Environmental Security
To prevent unauthorized physical access, damage and interference with CookiePro's information and information processing facilities. To prevent loss, damage, theft or compromise of CookiePro's assets, and interruption of its operations.

Operations Security
To ensure that information and information processing facilities are operated securely, protected from malware and loss of data. To ensure that security events are recorded appropriately. To ensure that operational system integrity is maintained, and exploitation of technical vulnerabilities is avoided.

Communications Security

To establish controls for the protection of information in networks and their associated facilities. To ensure the security of information being transferred within CookiePro and with external parties.

System Acquisition, Development and Maintenance

To establish information security as a vital part of information systems throughout the entire information lifecycle, including designing information security into the development of such systems. To ensure that sufficient controls are established to protect data used in testing.

Supplier Relationships

To ensure protection of CookiePro assets that are accessible by suppliers. To maintain an agreed-upon level of information security and service delivery in accordance with supplier agreements.

Information Security Incident Management

To ensure a consistent and effective approach to managing information security events, including incidents and weaknesses.

Information Security Aspects of Business Continuity Management

To embed information security continuity in CookiePro's business continuity management systems. To ensure availability of information processing facilities.

Appendix 2: Details on the processing of Data

Categories of Data subjects:

Your employees, contractors, agents, consultants, vendors and customers whose personal information is shared with CookiePro for the purpose of providing and using the CookiePro Service.

Categories of personal data processed:

- The Personal Data processed is personal data provided by Customer and processed by CookiePro in the course of providing the CookiePro Service.
- The personal data processed may concern identification data

Special categories of data (if appropriate)
The personal data processed will not include sensitive personal data including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, government issued identification numbers, health or medical records and criminal records.

Purpose of Processing operations
The personal data processed may be subject to the following basic processing activities: collect, record, organize, store, adapt, alter, retrieve, redact, consult, use, align or combine, block, erase or destruct, disclose by transmission, disseminate or otherwise make available Data as described herein, as strictly necessary and required to provide the CookiePro Service and otherwise in accordance with your instructions.

Specifically, processing operations include:

- Processing of name and e-mail addresses to provide login credentials, processing of name and e-mail address to provide support and help desk, storage of login credentials of users for authentication purposes.
- Hosting your environment which contains Data.
- CookiePro shall not access the Data unless you expressly grant CookiePro access. For example, for support purposes, You may create an external user in your environment and set an expiration date, after which CookiePro's access will automatically expire.

Specifically, systems (hardware/software) used will include:

- CookiePro Service
- Microsoft Azure (hosting)
- Sendgrid (e-mail notifications)
- Salesforce (account administration)

Duration of Processing
The personal data may be processed during the Term of the Agreement and any additional period which it is retained pursuant to Section 1.10 of the Data Processing Addendum