DATA PROCESSING AGREEMENT

Last modified: November 3rd, 2022

This Data Processing Agreement (hereinafter, the "DPA") is entered into by and between Kit United, a French *société par actions simplifiée* having its registered office at 5 rue des italiens, 75009 Paris, France and registered under number 753 391 713 RC.S. Paris (hereinafter, "Hivebrite" or the "Company") and the party that electronically accepts or otherwise agrees or opts-in to this DPA, for instance by signing an order form (the "Customer"), it being specified that using the Hivebrite solution (hereafter the "Hivebrite Solution") constitutes acceptance of this DPA.

PREAMBLE

In the context of the EU Regulation 2016/679 (GDPR) and the Data Protection Act 2018 as amended by the Data Protection Privacy and Electronic Communications Regulations 2019 (UK GDPR), the present Data Processing Agreement aims to determine the rights and obligations of the Parties, as defined by the Data Protection Legislation, as defined herein.

In this regard, Hivebrite is particularly sensitive to the privacy of its Users and of the Customer with regard to the protection of their Personal Data, as well as to its obligations as Data Processor, as the case may be, as described in the present DPA.

It is expressly understood that the present DPA forms an integral part of the master subscription agreement applying to the Parties regarding the provision of the Hivebrite solution (hereafter, the "**Contract**").

ARTICLE 1 – DEFINITIONS

The terms used in the present DPA and having a capital first letter, whether singular or plural, shall have the following signification:

"**Administrator**" designates any person, employee, representative, or third party duly authorized by the Customer or one of its Administrators to access the administration panel of the Hivebrite Solution.

"**CCPA**" designates the full text of the California Consumer Privacy Act of 2018 as updated by the California Privacy Rights Act of 2020 (CRPA).

"**Customer Contact Email**" means the address email of the Customer that is communicated to Hivebrite for the purpose of notifying relevant information regarding the Processing carried out by the Company.

"**Data Controller**" means the natural or legal person, public authority or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"**Data Processor**" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

"**Data Protection Legislation**" means the GDPR, the UK GDPR and the CCPA as well as any legislation and/or regulation implementing or created pursuant to the GDPR, the UK GDPR, the CCPA and the e-Privacy Legislation, or which amends, replaces, re-enacts or consolidates any of them, and all other national applicable laws relating to processing of personal data and privacy that may exist under applicable law.

"**Data Subject**" means an individual who is the subject of Personal Data.

"**End-User**" means any User of the Hivebrite Solution, other than an Administrator and the Customer, that can access the Hivebrite Solution with the credentials provided to it by an Administrator and that interacts using the Hivebrite Solution.

"**GDPR**" (the General Data Protection Regulation) means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and its European and national implementing laws.

"**Personal Data**" means any information relating to an identified or identifiable natural person; 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.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**UK GDPR**" means Regulation (EU) 2016/679 as it forms part of the laws of the UK by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

“**User**” means any Administrator or End-User.

ARTICLE 2 – PROCESSING OF PERSONAL DATA

The Personal Data is collected and processed as follows.

1. The Personal Data of the Customer's staff

In accordance with its subscription to the Contract and the availability of the Hivebrite Solution, the Company collects information about the Customer's identification (corporate name, legal form, corporate address, intra-European VAT number) and its contacts Personal Data (emails, invoice contacts).

For the collection of Personal Data of the Customer's staff (including the Customer Contact Email), the Company will be qualified as a Data Controller.

2. The Personal Data of Users

The Users' Personal Data, which are processed through the use of the Hivebrite Solution, is the sole responsibility of the Customer who collects and processes the Personal Data for its own account, it being understood that the Customer determines the purposes and the general means of the processing of Personal Data in accordance with the applicable Data Protection Legislation.

3. The processing of Users' Personal Data by the Company

The Customer is informed that its User's Personal Data is collected for the sole purpose of executing the Contract and the Hivebrite Solution to which Customer has subscribed. If the Customer does not communicate the required Personal Data, the Customer will not be able to utilize the full functionality of the services.

The Customer is informed that the Company carries out statistical analysis, as well as measurements of audience, visits, and effective uses of the Hivebrite Solution, but only after de-identifying the Users' Personal Data. In addition, these statistical analysis, as well measurements of audience, visits, and effective uses of the Hivebrite Solution, are only destined to Hivebrite, and to the exclusion of all third parties, and for the sole purpose of optimizing and improving the functionalities of the Hivebrite Solution.

The Customer guarantees the accurate transmission of this information to the Users of the Hivebrite Solution.

4. The Obligations of the Customer as Data Controller

The Customer, while using the Hivebrite Solution, must be qualified as Data Controller of the Personal Data of Users.

As Data Controller, the Customer explicitly commits to:

(i) having a legal basis to collect and process its Personal Data prior to collecting, hosting. The Customer confirms that it is informed that it can obtain the User's consent through a feature provided by the Company in the Hivebrite Solution;

(ii) collect the Users' Personal Data only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(iii) keep a record of the processing of Personal Data carried out through the Hivebrite Solution;

(iv) put in place all necessary technical and organizational appropriate measures in order to ensure the safety of the processing that is carried out, guarantee the protection of the rights of the persons concerned by the processing and meet the requirements of the Data Protection Legislation;

(v) limit the access to Personal Data of the Users solely to the persons empowered to this effect, meaning the Users of the Hivebrite Solution;

(vi) increase awareness and train staff members regarding the processing of Personal Data, the provisions of the Data Protection Legislation as well as its consequences;

(vii) never transfer, in any way whatsoever, the Personal Data of the Users to a third party, unless this transfer complies with the Data Protection Legislation;

(viii) guarantee all rights regarding the access, portability, erasure, rectification, opposition, and limitation of the Personal Data of the Users collected during the use of the Hivebrite Solution; if the Customer requires the Company's assistance to do so, the Customer commits to notify any request to exercise any of the above mentioned rights without delay to the Company;

(ix) notify the appropriate supervisory authority of any security breach presenting a serious risk regarding the rights and liberties of the Users within 72 hours after becoming aware of the breach;

(x) following the termination of the Contract with the Company, and in the event retention is no longer necessary, proceed with the deletion of the Personal Data of the Users within a timeframe compatible with the Data Protection Legislation.

In the event that the information is directly collected from the Users, the Customer, as Data Controller, commits to provide the Users, as applicable, with the following information:

(i) the information regarding the identity of the Customer as well as the name of the Data Controller;

(ii) the purpose of the Personal Data processing;

(iii) the recipient of the Personal Data: the Customer and the Company, as well as its subcontractors;

(iv) the Personal Data conservation period;

(v) the existence of their rights regarding the access, rectification, erasure and portability of the Personal Data, or any limitation or opposition to the processing of such data;

(vi) where applicable, the right to withdraw their consent regarding the processing;

(vii) the right for the Users to lodge a complaint with the competent supervisory authority, if they consider that their rights have not been respected;

(viii) the Customer informs the Users that the refusal to communicate the above mentioned data shall result in the Hivebrite Solution not being available for use.

Pursuant to the present DPA, the Customer commits to carry out all declaratory formalities and/or authorization requests and/or impact assessments, if necessary, as well as to ensure the mandatory compliance with the competent supervisory authority in light of the processing it carries out in relation to the usage of the Hivebrite Solution.

In the event the Customer has not yet carried out the above-mentioned formalities, it explicitly commits to promptly do so.

The Customer remains responsible for the Personal Data Processing carried out under its own responsibility.

The Customer must communicate the Customer Contact Email to the Company.

5. Obligations of the Company as Data Processor

The use of the Personal Data of the Users within the context of the use of the Hivebrite Solution implies that Hivebrite must be qualified as a Data Processor.

The subject, the duration, the nature and the purpose of the Processing of the Personal Data, as well as the type of Personal Data which is processed and the categories of Data Subjects, are listed in Annex 1.

The Contract, its Appendices and the present DPA must be qualified as written instructions of the Customer, qualified as the Data Controller, to Hivebrite, qualified as the Data Processor, without prejudice to any additional instructions given in writing.

As Data Processor and pursuant to the privacy procedures provided by the Data Protection Legislation, Hivebrite can only use Personal Data pursuant to instructions of the Customer responsible for the processing of the same.

As Data Processor, Hivebrite commits to always present sufficient guarantees in order to ensure the implementation of the necessary security and privacy measures.

In addition, Hivebrite commits to:

(i) assist the Customer to fulfill the Customer's obligations to respond to request from Data Subjects to exercise their rights under the Data Protection Legislation where this assistance exceeds what is commercially reasonable, Hivebrite and the Customer shall agree on the financial terms applicable for the continuity of the assistance;

(ii) keep a record of the processing of Personal Data carried out through the Hivebrite Solution;

(iii) not to transfer the Personal Data of the Users to any third parties, to the exclusion of its subcontractors and as permitted under the Contract, its Appendices and the present DPA, and without having given prior notice to the Customer;

(iv) enable the Data Controller to carry out an audit of the processing carried out by Hivebrite, as well as any technical and organizational appropriate measures guaranteeing the security of the processing, the respect of the rights of the data subjects and the requirements of the Data Protection Legislation, it being specified that the Customer must inform the Company at least thirty (30) calendar days before by written notice. The audit will be carried out at the expense of the Customer and can only cover the technical and organizational appropriate measures guaranteeing the security of the processing, the respect of the rights of the data subjects and the requirements of the GDPR. The Customer commits to designate an independent auditor, which is not a competitor of the Company in the field of SaaS, which is prior approved by the Company and which must agree to a confidentiality agreement. The Company commits to collaborate with the auditor in the accomplishment of its mission by providing reasonable necessary information and answering its reasonable questions. A copy of the audit report prepared by the auditor shall be provided to each Party and shall be collectively discussed by the Parties during a meeting specifically organized for this purpose;

(v) the Company commits to assisting the Customer with the analysis of the question whether a data protection impact assessment is necessary for the Processing of Personal Data by the Customer. When the latter finds it necessary to conduct a data protection impact assessment, the Company commits to assisting the Customer in the performance of the data protection impact assessment and, where applicable, regarding prior consultation of the supervisory authority. This assistance is due under the same conditions as those set out in paragraph (i) of this Article 2.5;

(vi) restrict the access to Personal Data to authorized staff only. In this context, the Company informs the Customer that, pursuant to their labor contracts, its staff is bound by confidentiality clauses which explicitly refer to the Personal Data.

Furthermore, where Hivebrite is subject to the CCPA, Hivebrite undertakes to comply with this legislation, in particular with the prohibition to combine personal data received from the Customer with personal data received from another entity.

6. Data breach

The Company shall put in place all technical measures enabling the detection of personal data breaches (as defined by the Data Protection Legislation) and enabling the Data

Controller to be informed of the breaches within a reasonable timeframe.

In the event a Personal Data breach occurs or has occurred, the Company shall notify the Customer by email without undue delay, and in any event within 72 hours of becoming aware of the breach, using the Customer Contact Email.

Without prejudice to the legal obligations of the Company, the Customer shall be responsible for the notification of the breach to the competent authority(ies) and/or the affected individuals.

Without prejudice to the legal obligations of the Company, the Company shall assist the Customer in the best possible way with the notification of the breach to the competent authority(ies) and/or the affected individuals.

The Company shall in any event treat all questions/requests of the Customer concerning the breach as a priority.

In the event of breach, the Company shall take all measures necessary and appropriate to restore the Personal Data and/or to limit the negative impact of the breach as much as possible (including but not limited to the provision of forensic assistance to the Customer), it being understood that the Company shall, where reasonably possible, always consult the Customer on the measures to be taken.

7. Appropriate technical and organizational measures put into place by Hivebrite

At the outset of the Processing, the Company has put into place the appropriate technical and organizational measures in order to guarantee the security of the processing, as well as the respect of the rights of the persons involved and the requirements of the Data Protection Legislation.

The code of the Hivebrite Solution and the processed Personal Data are hosted on the Amazon servers and Google Cloud Platform, as these both present sufficient guarantees in terms of technical and organizational measures that are required pursuant to the Data Protection Legislation.

The Customer may consult the privacy policies of Amazon AWS and Google Cloud Platform at the following addresses:

- https://cloud.google.com/security/privacy/
- https://aws.amazon.com/compliance/gdpr-center/

The Company also makes a daily copy of the Personal Data hosted on the Amazon and/or Google Cloud Platform servers. The Personal Data is saved once every hour. The Company keeps the last save of each day for a period of thirty (30) days.

The Customer has the ability to extract the Personal Data of the End-Users in an Excel spreadsheet from its administration module.

For any additional questions, the Company invites its Customers to get in touch by email at privacy@hivebrite.com.

8. Sub-processors of the Data Processor

The Customer hereby consents to the Processing of Personal Data by the sub-processors listed at https://hivebrite.com/legal/subprocessors.

The Customer gives a general authorization to Hivebrite to make any modification, change, addition or replacement of these sub-processors, in which case Hivebrite will notify the Customer of this modification, change, addition or replacement, using the Customer Contact Email, by no less than 7 business days' notice. During this timeframe, Hivebrite shall, upon request, make available to the Customer all necessary information to demonstrate compliance of the engagement of the new sub-processor. The Customer has 7 days from the notification date to object this change, in which case Hivebrite will, at its choice:

- refrain from modifying, changing, adding or replacing the sub-processor;
- maintain the modification, change, addition or replacement, in which case the Customer may terminate the Contract within 30 days' notice, without further liability to either party. In such a case, this termination will not have the effects of a "Termination for Cause" as set forth in Section 12 of the MSA, and Hivebrite will not owe the Customer a refund of any fees the Customer has paid.

The COmpany warrants that each sub-processor is contractually subject to at least the same obligations as those the Company is subject to toward the Customer under this DPA. The Company guarantees that each sub-processor it relies on shall comply with these obligations.

In case of international transfers of Data by the Company to a sub-processor outside the European Economic Area (EEA), the adequate level of protection is guaranteed by the signature of model clauses, pursuant to Section 2.9. of this DPA.

In any event, the Company shall indemnify the Customer for any damage and claims that may arise from the non-compliance by the sub-processor with the model clauses signed by the sub-processor.

9. International Personal Data transfer

The Company may not transfer any Personal Data outside the EEA unless one of the following conditions is fulfilled:

- The country the Data is transferred is recognised by the European Commission as ensuring an adequate level of personal data protection; or
- The Customer or the Company has entered into model clauses as published by the European Commission with the organization the Data is transferred to. For this purpose, the Customer or the Company located in the EEA will be referred to as the "Data Exporter" and the sub-processor will be referred to as the "Data Importer". Where the Company transfers personal data to a sub-processor this way, it will select Module three ("Transfer processor to processor") of the SCC.

The Parties agree to replace the model clauses with the latest version of the model clauses as updated or replaced by the European Commission in accordance with Article 46, paragraphs 2(c) and 2(d) and Article 93 of the GDPR and with the provisions of the UK GDPR.

A transfer to a country outside the EEA is otherwise allowed only if this transfer is required on the basis of a regulation which is binding under European or French law. In such a case, the Company shall inform the Customer beforehand and in writing of the legal requirement on the basis of which the Company is obliged to proceed to the transfer of Data, unless the law concerned prohibits such notification on important grounds of public interest.

By adhering to this DPA, the Customer gives its authorization for transfers of Personal Data in the countries listed at https://hivebrite.com/legal/subprocessors and for transfers of Personal Data outside the EEA to sub-processors authorized under Article 2.8.

10. Personal Data Retention period

A. The Personal Data of the Customer's staff

Subject to the mandatory preservation period of all data related to customer files, which is three (3) years as of the end of the contractual relationship, the Customer's staff (including the Customer Contact Email) identification data shall be retained by Hivebrite for a period that shall not exceed the subscription period of same of the Hivebrite Solution, to the exclusion of the statutory period for archiving.

B. The Personal Data of Users

The Company hereby informs the Customer that it deletes the Personal Data of the Users within a period of thirty (30) to ninety (90) days following the termination of the Contract, notwithstanding any deletion request directly from Users.

At the end of the contractual relationship, the Company commits to return, free of charge and at the first request of the Customer formulated by registered letter with acknowledgement of receipt, all Personal Data belonging to the Customer that remains in possession of the Company in accordance with the terms of this DPA in a standard format (Microsoft Excel, SQL and CSV) within thirty (30) days following same request.

The Company commits to also respond to any questions formulated by the Customer with the thirty (30) calendar days following the receipt of the return request.

11. The Customer's responsibility

The Customer remains solely liable for the legality of the processing carried out during the use of the Hivebrite Solution.

In addition, the Customer remains solely liable for the Personal Data it collects and processes as Data Controller. The Customer commits to proceed with the collection and the processing of the Users' Personal Data in strict accordance with the Data Protection Legislation.

The Customer is informed that certain categories of Personal Data so called, "sensitive", pursuant to the Data Protection Legislation, cannot be collected nor processed without the prior explicit consent of the data subjects, or any other formality provided for by the applicable Data Protection Legislation (authorization request, impact assessment, etc.). The Customer commits to never proceed with the collection and processing of the sensitive Personal Data aside from what is provided for by the Data Protection Legislation for such processing. The Company declines any liability regarding the collection or processing of sensitive Personal Data. The Customer acknowledges and accepts that any potential sensitive personal data are subject to the same technical and organizational security measures as those the Company implemented for non-sensitive Personal Data.

The Company, as Data Processor, declines any liability regarding the quality, the relevance, and the legality of the Personal Data. Except as provided herein, the Company cannot be held liable in the event of a collection or Processing of Personal Data that would contravene with the provisions of the Data Protection Legislation.

The Customer guarantees the Company, at first demand, against any and all harm incurred

to it as a result of any action of a User or any third party due to the violation of the present clause, and/or any violation of any of its obligations as data controller pursuant to the Data Protection Legislation.

ANNEX 1. OVERVIEW OF THE PROCESSING

A. Duration of the Processing

For the duration of the contractual relationship between the Parties, including the period covering the Data Reversibility clause of the Contract.

B. Nature and purpose of the Processing

Personal Data will be processed for purposes of providing the services set out and otherwise agreed to in the Contract. In that regard, Hivebrite may carry out all kinds of processing operations.

C. Type of Personal Data Processed

Personal identification data (first name, last name, gender, ID/profile photograph, date of birth, language spoken, nationality, email, phone, address);

- Electronic identification data (IP addresses, cookies);
- Academic curriculum and results;
- Professional experience;
- Current job;
- Professional qualifications and certificates;
- Hobbies and areas of interest;
- Location data;
- More generally, any personal information submitted or posted by a User (payment data, etc.)

D. Categories of Data Subjects

Controller's Users including but not necessarily limited to Controller's community members, employees, contractors, collaborators, customers, prospects, suppliers and subcontractors.

E. Security measures

Data Processor shall implement appropriate technical and organizational measures and shall control compliance with these measures on a regular basis. This includes:

(a) Physical access control: Data Processor shall take reasonable measures to prevent unauthorized persons from gaining access to Personal Data, such as secured buildings, key management and logging of visitors.
(b) System access control: Data Processor shall take reasonable measures to prevent unauthorized access to IT systems such as strong authentication procedures (passwords, double authentication), documented access approvals.
(c) Data access control: Data Processor shall take reasonable measures to prevent unauthorized access to Personal Data such as granting access to personal data granted only on a need-to-know basis, confidentiality obligations and locking of workstations.
(d) Data transfer control: Data Processor shall take reasonable measures to ensure personal data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage and that it is possible to verify and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (data transfer control); such as data encryption at rest and in transit.
(e) Input control: Data Processor shall take reasonable measures to provide that it is possible retrospectively to check and establish whether and by whom Personal Data has been entered into data processing systems, modified or removed; such as logging systems.
(f) Job control: Data Processor shall take reasonable measures to ensure that personal data are processed in accordance with the directions of the Data Controller such as entering

into appropriate data processing agreements with sub-processors.

(g) Availability control: Data Processor shall take reasonable measures to prevent the accidental destruction or loss of Personal Data