This policy forms an integral part of the standard terms of sale and service (ToS) of Libertify **(hereinafter the "Policy").** The purpose of this Policy is to set out the agreed terms and conditions on which Libertify shall Process Personal Data. This Policy comprises a first part (I/II), setting out the general terms and conditions of Processing and a second part (II/II), setting out the details of the Processing activities performed as part of the Service, by mutual agreement with Customer.

PART I/II: GENERAL TERMS AND CONDITIONS OF PERSONAL DATA PROCESSING

1) **Definitions:** the definitions in the ToS shall retain the same meaning in this document, unless expressly modified herein. In addition, the definitions below apply to the terms beginning with a capital letter, in the Policy:

Adequacy decision: refers to a decision adopted by the European Commission that a Third Country ensures an adequate level of protection for Personal Data, by virtue of its domestic legislation or international commitments it has entered into; **Controller:** refers to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing; **Data Protection Legislation:** refers to French Data Protection Act No. 78-17 of January 6, 1978 and to the GDPR; **Data Subject:** refers to an "identifiable natural person", e.g. a natural person 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 person; **EU:** refers to the European Union; **GDPR:** refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation); **Personal Data:** refers to Data of the Customer and Users corresponding to any information (any sequence of characters, signs, numbers or letters) relating to an identified or identifiable natural person; **Personal Data Breach:** refers to a security breach of the Data resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed; **Processing (of Personal Data):** means any operation or set of operations performed on Data or sets of 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; **Sub-Processor:** refers here to any third party in relation to the Parties having a contractual relationship with Libertify for the supply of equipment, software or Software-Powered Services in connection with the services covered hereunder; **Third Country:** refers to a country that does not belong to the European Union; **Transfer outside the EU:** refers to the transmission of Personal Data from an EU member country to a Third Country, or access to Personal Data, located within an EU member country, from a Third Country (e.g.: remote access to a database by entities located in a country outside the EU).

2) **Generalities and role of the Parties:** Customer is informed that the Data it sends to the Platform, or generates as part of the Service, can constitute Personal Data (identity and email address of Users; pseudonym; Login Credentials; Photograph; voices; activities on the Platform, etc.). Customer acknowledges and accepts that Customer is acting as a "Controller" of the Personal Data, within the meaning of Data Protection Legislation, and Libertify as the "Processor" and acting as such under the instructions given by Customer. Customer has instructed Libertify to process the Personal Data as follows.

3) **Reciprocal obligations:** as part of the Processing, (i) Libertify agrees (a) to comply with Applicable Legislation, and (b) not to process Customer's Personal Data for purposes other than the Service and/or contrary to Customer's instructions as documented by the ToS and the Policy, unless the Processing is required by law, in which case Libertify will give Customer advance notice to the extent permitted; (ii) Customer (a) hereby instructs Libertify (and authorizes Libertify to give instructions to each Sub-Processor) to proceed with the Processing of Customer's Personal Data and in particular, to transfer Customer's Personal Data to any country or territory subject to these provisions, in each case in a manner reasonably necessary for the provision of the Software-Powered Services and in accordance with the Agreement, and (b) warrants that Customer is and will at all times be duly authorized to give the aforementioned instructions and that it has communicated all information to the Data Subjects, and collected all necessary consents from the Data Subjects concerned by the Processing, in accordance with applicable law.

4) **Transfers of Personal Data outside the EU**: Customer authorizes Libertify to use the Personal Data in accordance herewith within the European Union, or outside the European Union only if such transfer complies with one of the following conditions: (i) the Processing is carried out in a Third Country benefiting from an Adequacy Decision of the European Commission; (ii) the Processing is governed by Standard Contractual Clauses issued by the European Commission. In such case, the Parties incorporate by reference into the Agreement said standard contractual clauses ("SCC"), which they agree to ratify for the implementation of the processing operation(s) concerned; (iii) the Processing is framed by appropriate safeguards such as "Binding Corporate Rules" or standard contractual clauses for Sub-Processors; (iv) the Processing falls within the "special derogations" provided for in Article 49 GDPR. If the condition(s) used to govern the Transfer become invalid, the Parties agree to meet as soon as possible to examine a new framework for governing the Transfer, without Libertify incurring any possible liability during this transitional period. The new framework will be deemed a "change" within the meaning of this Policy.

5) **Sub-Processor**: Customer gives Libertify a general authorization, for the entire term of this Agreement, to rely on Sub-Processors in the performance of the Services (e.g. hosting server operators) provided they are contractually bound by the same or similar Personal Data obligations as Libertify under the Agreement, with Libertify being liable for compliance therewith. Libertify records and updates a list of Sub-Processors, which Customer may have access to upon written request, and provided it uses as confidential information of Libertify. Liberty may also inform the Customer who asks for it, of any planned of effective changes concerning the addition or replacement of other sub-processors.

6) **Personal Data organizational and security measures**: the Parties agree to implement technical and organizational measures to ensure the physical and logical security of the Personal Data at whichever of the following three (3) levels is highest: (i) the measures taken by Libertify for its own data, (ii) measures aligning with best practices, including in particular recommendations published by data protection authorities or administrative authorities competent for cybersecurity matters, (iii) measures taken by Publishers for their own data. It is the respective responsibility of each Party to determine said security measures and to communicate them to the other Party upon request. For its part, Customer warrants that the Personal Data does not contain and is not a vector for any viruses, worms, Trojan horses or other harmful or destructive content likely to infringe either the rights of the Data Subjects or the Platform. For its part, Libertify has put in place and documented the following measures: (a) password policy, protection of sensitive IT environments with up-to-date antivirus software (programs and virus signature databases), use of IT tools for managing and protecting devices and applications (eg: MDM), monitoring of data center infrastructure by Libertify and its Sub-Processors; separation of Customer Data, with appropriate segmentation methods to protect and isolate Customer data from other customer organizations; transfers of encrypted data using industry-standard protocols such as Transport Layer Security (TLS); storage of encrypted data in compliance with best practices, such as the AES-256 encryption standard for data at rest (b) compliance processes with standards ISO 27001, 27017 and 27018, where applicable; (c) IT security management in accordance with ISO 27001 or a security framework based on industry standards. Libertify is under a duty of best efforts when it comes to security and organizational measures. Libertify is authorized to implement any equivalent measure that the Customer could be acknowledged of upon request, or by mean of an update, if necessary, of the Policy.

7) **Limits**: Customer acknowledges that Libertify has no control over the transit of Data, including Personal Data, via the public telecommunication networks used by Customer to access Software-Powered Services, particularly the Internet. The Customer acknowledges and accepts that Libertify is therefore unable to guarantee the confidentiality of Data when it is transferred to said public networks. Accordingly, Libertify disclaims any and all liability in case, inter alia, of the misappropriation, interception, corruption of Data, or any other event likely to affect it, occurring during its transit over public telecommunication networks, notwithstanding the use of secure transmission protocols and the implementation of organizational and security measures as per this Policy. As the Controller, Customer considers that given the nature of the Software-Powered Services and the risk Customer has been able to assess concerning the protection of Data Subjects' rights, the aforementioned measures and limits represent adequate safeguards and meet the requirements under Data Protection Legislation.

Any other additional measures or guarantees must be expressly requested from Libertify by giving it 45 (forty-five) days' notice. If Libertify accepts this request, it agrees to provide Customer, within the said period, with a quotation for the implementation of these new security measures if Libertify considers that they will have an impact on the price of the Software-Powered Services. If Libertify is unable to meet this request, the Parties shall meet to agree on a possible alternative solution to achieve the same result. If the Parties are unable to reach agreement on the requested measures, despite Customer justifying and documenting in writing that such measures are essential to comply with applicable

Legislation, the Agreement may be terminated, for the future only and subject to compliance with a minimum notice period of three (3) months, without any fault on this basis being attributable to Libertify.

8) **Notification of breaches**: each Party undertakes to inform the other Party of any Personal Data Breach within seventy-two (72) hours of the occurrence of such a breach of which it becomes aware. In accordance with Data Protection Legislation, Libertify will communicate to Customer the information in its possession, in the event that the Breach is caused in the course of the Software-Powered Services, to enable Customer to meet Customer's obligation to notify and remedy the Breach to the supervisory authority and to the data subjects. In fact, as the Controller, Customer has sole responsibility for reporting Breaches. In case of negligence on the part of Customer, Libertify may report the Breach to the competent authority, without Customer being able to assert against Libertify any noncompliance with time limits or any other obligations that would normally be incumbent on Customer.

9) **Judicial or administrative requisition**: subject to compliance with applicable legislation, Libertify agrees to inform Customer of any request for transmission or consultation of Personal Data issued by a judicial or administrative authority. Libertify will act on the instructions of Customer for the disclosure of said Data. In the event of non-disclosure instructions, Customer agrees to assume all the consequences of this "interference" as being exclusively attributable to Customer and to hold Libertify harmless from and against any such consequences, in particular pecuniary. Notwithstanding the foregoing, if compelled to comply, Libertify shall not incur any liability on this basis. In such case, or if instructed to disclose information, Libertify acts in discretion and would only disclose the Data strictly required.

10) **Compliance with the right of data subjects**: Customer is solely responsible for fulfilling all legal and regulatory obligations related to the protection of the rights of Data Subjects whose Personal Data are processed in connection with the Software-Powered Services. To comply with these obligations to Data Subjects, Customer has implemented organizational and technical measures enabling it to (i) clearly inform Data Subjects, (ii) obtain their consent where necessary, and (iii) respond to their requests to exercise their rights of access, rectification, erasure, objection, and portability of their Personal Data. In this respect, Customer is responsible for providing Data Subjects with clear, unambiguous information that is always accessible on the terms and conditions under which their Personal Data may be processed by third parties such as Libertify or its partners. Customer is solely liable for the consequences, in particular pecuniary, in the event of complaints from Data Subjects, if the Processing does not comply with Data Protection Legislation due to a lack of information or a lack of consent on the part of Data Subjects. At Customer's request, Libertify will be able to publish this information and operationally manage the collection of consent directly from the Platform, subject to a quotation for an additional fee. Libertify disclaims any and all liability on the basis of the implementation of this system in Customer's name and behalf.

11) **Fulfillment of requests by Data Subjects for the exercise of their rights:** Libertify shall fulfil, if it has the means to do so, any written instructions given by Customer, to proceed within a reasonable time with the deletion of Personal Data enabling Customer to meet its obligations vis-à-vis the Data Subjects. However, Customer acknowledges and accepts that Libertify does not have the technical ability to carry out partial or targeted deletions of one or more specific pieces of Personal Data. It is therefore possible that, in response to such as request by Customer, Libertify may be obliged to shut down the Software-Powered Services in whole or in part and to delete all Data, to the extent possible in accordance with the Agreement. In the exceptional event that Libertify receives, directly or through a Sub-Processor, a request from a Data Subject in connection with the aforementioned rights, Libertify agrees to inform Customer promptly so that Customer can meet its own obligations. In general, Libertify will make its best efforts, to the extent possible, to assist Customer in complying with its obligations as a Controller.

12) **Cooperation with supervisory authorities:** the Parties agree to cooperate with the supervisory authorities, and to keep each other informed as soon as they receive any formal notice, complaint or notification of inspection.

13) **Audit:** Customer may have an independent auditor conduct a compliance audit, once per year at most, and at its sole expense, provided that Libertify is given at least thirty (30) days' prior notice. The audit shall begin on the date mutually agreed upon by the Parties and shall be limited to a maximum of three (3) business days and conducted during Libertify's regular business hours. In no event shall the audit be conducted on Libertify's information system or that of its Sub-Processors. Libertify agrees, however, to provide all necessary documentation provided the auditor has signed appropriate confidentiality and non-disclosure agreements. The auditor must be always accompanied by a representative of Libertify and under all circumstances. The audit report will be shared with Libertify. If Customer considers that the report reveals a serious breach by Libertify, it must immediately inform Libertify by registered letter with delivery confirmation and can either (i) give notice of termination of the Agreement as per the applicable terms and

conditions; or (ii) request remedial measures from Libertify, which may be billable additionally. Customer's decision must be received within fifteen (15) days of the said notice, failing which the breach is deemed to have been accepted and/or remedied.

14) **Miscellaneous:** this Policy is subject in full to the application of the Agreement and to the provisions of the ToS, including as regards governing law and jurisdiction. Concerning the subject matter hereof, in case of conflict between the provisions of the Policy and those of the Agreement, the dispositions of the Policy shall be controlling. All claims in connection with the Policy and Processing are subject to the terms of the Agreement, including, but without restriction, the exclusions and limitations set out in the Agreement.

15) **Changes:** if, during the course of the Agreement, Customer wishes to make changes/improvements to these instructions, without these being imposed on Customer by a binding measure or a justified and proven risk of non-compliance with Data Protection Legislation under the conditions set out in the "Limits" section above, it shall make a change request to Libertify, and the latter shall treat it as an option to which additional fees apply. If Libertify is unable to handle the request, the latter shall inform Customer, without this giving Customer the right to terminate the Agreement early.

16) **Google API Services Disclosure**

Libertify's use and transfer to any other app of information received from Google APIs will adhere to the **Google API Services User Data Policy**, including the Limited Use requirements.

1. Data Accessed via Google Services

Libertify's application accesses specific Google user data to provide a seamless authentication and personalization experience:

- **Google Account Email (.../auth/userinfo.email):** Libertify accesses your primary Google email address to identify you and manage your account.
- **Personal Profile Information (.../auth/userinfo.profile):** Libertify accesses basic profile details, such as your name and profile picture (if publicly available), to personalize your dashboard and user interface.
- **OpenID (openid):** Libertify uses this to securely link your Google identity to your Libertify account for safe and easy sign-in.

2. Purpose and Usage of Data

Libertify uses the information collected from Google API services exclusively for the following user-facing features:

- **Authentication and Access:** To allow you to securely sign in to the Libertify platform without creating a separate password.
- **Account Management:** To communicate important service updates, billing notifications, and support information to your verified email address.
- **Personalization:** To display your name and profile picture within your private account area to enhance your user experience.

3. Data Storage and Retention

- **Secure Storage:** All data obtained via Google APIs is stored using industry-standard encryption, including **AES-256** for data at rest and **TLS** for data in transit.
- **Retention Policy:** Libertify retains your Google profile data only for as long as your account is active. Upon account termination, this data is deleted within six months, unless required by law for regulatory compliance.

PART II/II: DETAILS ON THE PROCESSING OF PERSONAL DATA

Type and category of Personal Data	Data to which Libertify may and/or must have access (clear-to-text) for the strict purposes of the Service: all Personal Data of the Customer that Libertify needs for providing the Services in accordance with the Agreement, including but not limited to: names and surnames of Users, their Identifiers, their professional email addresses, their phone numbers (if provided), billing address, logs, IP addresses, Chatbot conversations, Client payment information, image and voice recordings, documents uploaded to the Platform. Data to which Libertify's Subprocessors and partners have and/or must have access to provide part of the Service assigned to them : the Customer's banking data, to be completed for the payment of Services by the payment service provider used; identity and contact details of Users for managing appointments through the software used (Calendly or others); photo and voice of a User for creating an Avatar by the software used...
"Sensitive" Personal Data	The Customer is not authorized to have "sensitive" Personal Data (such as health data, criminal convictions, religious or political beliefs, social security number, for example) processed by the Service, unless prior notification is provided to Libertify and express consent is granted by the latter, subject to operational and financial terms to be defined.
Data Subjects	Primarily internal and external Users, as well as any individual whose Personal Data is processed.
Processing of Personal Data	Access to Personal Data, hosting of Personal Data, display, copying, temporary storage of Personal Data, transmission of Personal Data to partners without any sale or resale.
Purposes of Processing	Provision and improvement of Services
Sub-purpose 1 (on an indicative basis)	Management and monitoring of the Agreement, Orders and payments
Sub-purpose 2 (on an indicative basis)	Access and management of Back-Office and Customer account
Sub-purpose 3 (on an indicative basis)	Content generation
Sub-purpose 4 (on an indicative basis)	Maintenance of the Platform and security of Services and the Platform
Sub-purpose 5 (on an indicative basis)	Processing of User Data depending on the features used by Customer
Sub-purpose 6 (on an indicative basis)	Traceability of activities on the Platform for security purposes, or the purposes of statistics and license and credit count purposes
Sub-purpose 7 (on an indicative basis)	Exchanges of information with Sub processors to enable them to carry out a part of the service entrusted to them by Libertify.
Data location	Datacenters in the European Union and Third Countries, depending on the location of Customer or Customer's Users (automatic allocation based on the geolocation of the User by the Platform) and based on the data privacy provisions applied by Sub-processors.
Retention period	Customer authorizes Libertify to use the Personal Data during the entire term of the Agreement plus a period not to exceed 6 (six) months after the termination of the Agreement or following the last transmission thereof if they are not anonymized or aggregated, except to comply with a legal or regulatory obligation.
Specific limitation on Processing at Customer's request (exclusion of a Data category; exclusion of a Processing category, etc.)	N/A
Contacts dedicated to GDPR matters and Policy	Libertify contact : privacy@libertify.com;