Data Processing Agreement (DPA)

1. Subject

The present data processing agreement (hereinafter the **« DPA »)** shall apply to any contract signed between Klaxoon and the Client (hereinafter the **"Contract** ") for the provision of Klaxoon' services (hereinafter **« Services »)**.

The purpose of this DPA is to set forth the conditions under whose Klaxoon and the Client (hereinafter the **"Parties"**) will collect Personal Data in accordance with the Regulation (EU) 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* (hereinafter **« GDPR »)** where they act as Data Controller and when Klaxoon collect Personal Data on behalf of the Client as a Data Processor.

2. Definitions

Capitalized terms used in the DPA shall have the same meaning as those defined in the Contract and the terms "**Data Controller**", "**Processor**", "**Personal Data Breach**" or " **Processing**" shall have the same meaning given to them in the GDPR.

« Applicable Laws » shall mean any laws, regulations, orders, codes in relation to personal data protection and notably the GDPR;

« Data Subjects » shall mean any physical person concerned by processing activity carries out respectively by Klaxoon and the Client ;

"Personal Data" shall mean any information related to a physical person who may be identified in a directly or indirectly manner;

« Standard Contractual Clauses » shall mean the current version of the standard contractual clauses provided by European Commission and every update thereof which apply to the Processor in case of Personal Data transfer;

« Subprocessor » shall mean a third party company selected by the Processor to subcontract a part of Services.

3. Obligations applicable to Klaxoon when acting as a Processor

3.1 General Processor's Commitments

This article set forth Klaxoon' commitments when the latter acts as a Processor and collects Personal Data on behalf of the Client acting itself as a Data Controller.

The Processor undertakes to collect Personal Data in accordance with the Contract, the present DPA and the article 28 of the GDPR.

Therefore, the Processor undertakes to use Personal Data under the Data Controller's documented instructions and in accordance with processing described in Appendix 1 of the DPA.

The Parties recognize the documented instructions shall mean the provisions of the Contract and those described in the DPA. The Data Controller may give further documented instructions during the term of the Contract provided those instructions are required by Applicable Laws and agreed between the Parties. Consequently, the Processor reserves the right to object to any non-documented or non-required by Applicable Laws instructions.

As a part of the Processing carried out under article 28 of the GDPR, Processor undertakes to:

- reasonably assist the Data Controller in satisfying its legal obligations ;
- promptly inform the Data Controller, unless prohibited by Applicable Laws, of any request and/or injunctions from legal authority relating to Personal Data collected for the purpose of the Contract. In this case, the Processor will attempt to redirect the legal authority to the Data Controller to allow the latter to object to the above-mentioned request in accordance with Applicable Laws. In case where the Processor shall respond directly to the legal authority, it undertakes to limit the disclosure of Personal Data to the strictly necessary to respond the legal request;
- not retain Personal Data for a duration exceeding those described in Appendix 1;
- implement all the necessary technical and organizational measures as described in Appendix 2 and required by article 32 of the GDPR in order to (i) ensure the confidentiality and the integrity of all Personal Data and (ii) to prevent Personal Data Breach;
- appoint a Data Protection Officer and communicate its contact details to the Data Controller on demand;
- take into account, as soon as the conception of the Services, the principles of *Privacy by design* and *Privacy by default* as required by Applicable Laws;
- reasonably assist the Data Controller in satisfying its legal obligations relating to the Data Subjects rights and inform the Data Controller without undue delay when a Data Subject send a request directly to the Processor;
- inform its personnel who access to Personal Data of all obligations described in the DPA. The Processor also undertakes to regularly train its personnel in order to arise awareness about the GDPR and Applicable Laws;
- reasonably assist the Data Controller to carry out an impact assessment, if applicable, and in accordance with article 35 of the GDPR.

3.2 Subprocessor

The Controller is advised the Processor may be entitled to subcontract a part of the Services to a Subprocessor and that the present DPA constitute a general authorization in accordance with article 28 of the GDPR.

During the Contract term, Processor may replace a Subprocessor and/or select a new Subprocessor provided prior written notification to the Controller.

The Controller may object to the new Subprocessor within eight (8) days after receiving the notification from the Processor. In such case, Controller may be entitled to terminate the Contract by sending written notice to the Processor and such termination will not involve any right of compensation of any kind to the benefit of the Controller. Failure to respond within such delay may be considered as acceptance of such Subprocessor in the meaning of article 28 of the GDPR.

The Processor shall ensure each Subprocessor is subject at a minimum to the same obligations as the Processor in terms of security and confidentiality and ensure the Subprocessor will comply with all Applicable Laws.

The Processor ensures each Subprocessor will comply with all obligations set forth in the DPA and Processor will be held liable for any breach of the DPA caused by Subprocessor in accordance with article « Liability » of the Contract.

3.3 Personal Data Transfer

For the purpose of the Contract, the Processor may transfer Personal Data and undertakes that such operation shall maintain Personal Data security and confidentiality levels as described in the DPA and as required by Applicable Laws.

In case where Processor was to transfer Personal Data outside the European Union or in the country for which the European Commission has not provided an adequacy decision (hereinafter the "**Third Country"**), the Processor undertakes to inform the Controller in advance and at the latest within thirty (30) days before such transfer.

The Controller may object to the transfer within eight (8) days from the notification of the Processor. In this case, the Controller may terminate the Contract by sending written notice to the Processor and such termination will not involve any right of compensation of any kind to the benefit of the Controller. Failure to respond to such notice within the delay may be considered as acceptance of such transfer of Personal Data.

For any transfer of Personal Data outside European Union or to a Third Party, the Processor undertakes to (i) implements all appropriate safeguards as required by article 46 of GDPR ; and (ii) sign the Standard Contractual Clauses with any Subprocessor concerned by the transfer.

3.4 Security of Personal Data

Personal Data collected by Processor collected as a part of use of Services are hosted on servers located in the European Union and authenticated by a certificate validated by a trusted third party.

The security of the Client Personal Data is a major concern for the Processor. Therefore, the Processor applies its technical infrastructure, hardware, and monitoring software such that it can safeguard the security and integrity of the Client Personal Data under conditions which comply with good professional working practices.

The Processor undertakes to implement all necessary technical and organizational measures as required by Applicable Laws and as described in the DPA to prevent any Personal Data Breach.

The Data Controller is advised the Processor may update, at its sole discretion or for complying with Applicable Laws, the technical and organizational measures providing such measures ensure at minimum the same level of security than those described in the DPA .

3.5 Personal Data Breach

In case of Personal Data Breach, the Processor undertakes to inform the Controller without undue delay and at the latest within 72 hours after becoming aware of such breach.

Said notification may provide at least the nature of the Personal Data Breach, the likely consequences and the corrective measures implemented by Processor to resolve such breach.

To the extent possible, the Processor may also provide the Data Controller with the categories and approximate number of concerned Data Subjects and the categories and approximate number of concerned Personal Data records.

Where, and in so far as, it is not possible to provide the above-mentioned information at the same time as the written notification of the breach, the information may be provided without undue further delay by Processor.

In any cases, the Data Controller shall inform the Data Subjects and the legal authority of the Personal Data Breach as soon as it receives the written notification from the Processor.

The Processor will implement all the necessary corrective measures to resolve the Personal Data Breach and will keep the Data Controller informed of the evolution of the situation. In the event where the corrective measures implemented by Processor would remain ineffective to resolve the breach, the Data Controller may be entitled to terminate the Contract for cause in accordance with the provisions of articles "Termination" and "Liability" of the Contract.

3.6 Audit

The Processor grants to the Data Controller an audit right for the sole purpose to verify the Processor's compliance with the DPA and Applicable Laws. The Data Controller will provide the Processor with fifteen (15) days prior written notice The Client may appoint external auditor provided that the latter: (i) is not identified as direct competitors of the Processor); (ii) be subjected at a minimum to the same confidentiality commitments as a Data Controller.

The audit will be carried out at the Data Controller request and at its own cost. The scope of the audit will be mutually defined between the Parties prior to the fulfillment of such audit.

The audit right granted to the Data Controller in the present DPA is a remote audit which will be carried out by the transmission of the documents (*the Contract, the DPA, audit and available certifications reports*). It is solely when the transmission of documents is not sufficient to demonstrate the compliance of Processor with the DPA, and after discussion between the Parties, that the client may be entitled to carry out the audit to Processor premises at the exception of all zones with status "Zone à Régime Restrictive" pursuant to the French Decree number 2011-1425 dated on 2 November 2011 relating to the protection of the scientific and technical potential of the French Nation, which the Client fully recognizes and accepts.

At the end of the audit term, the auditor shall return all copies of confidential information provided by the Processor. The audit conclusions will be communicated to the Data Controller who shall then state any observations or reservations within thirty (30) days. In the absence of any written report of such conclusions to the Processor, the latter shall be unconditionally deemed compliant.

In the event where the audit revels a breach of contractual and legal obligations of Processor, the latter shall implement all necessary corrective measures to resolve the breach. If the Processor does not succeed to resolve the breach, the Data Controller may be entitled to terminate the Contract in accordance with the article « Termination » of the Contract.

3.7 Obligations of the Data Controller

The Client is responsible for all Personal Data it collects as a part of the use of Services (*the user content*). Consequently, the Client undertakes to comply with all Applicable Laws.

The Client remain responsible of all data it creates, modifies, delete (*accidentally or not*) as part of the use of Services.

For Processing carried out by the Client, the latter undertakes to be designated as the contact point for the Data Subjects and manage directly their legal request.

4 Obligations applicable to Klaxoon when acting as a Data Controller

Klaxoon also collects Personal Data as a Data Controller for purposes described in Appendix 1. As part of its own processing activities, Klaxoon undertakes to comply with the Contract, the DPA, and the Data Privacy Policy available at the following link: https://static.klaxoon.com/website/pdf/privacy-policy.pdf

For sake of clarity, when the Parties both act as Data Controller, each of them determines individually and independently the means of the Personal Data collection and the purposes of the processing activities that each Party carries out as part of the performance of this Contract. Consequently, the Contract and the DPA shall not entail joint liability between the Parties regarding Personal Data processing activities.

When acting as a Data Controller, Klaxoon undertakes to:

- inform any competent legal authority of all Personal Data collected by Klaxoon for the purpose of the Contract;
- obtain the consent of all Data Subjects and inform them of their rights regarding the Applicable Laws;
- maintain a record up to date of all processing carry out by Klaxoon under its responsibility;
- implements all technical and organizational measures to ensure the confidentiality and integrity of Personal Data and prevent any Personal Data Breach;
- inform the Client without undue delay and at the latest within 72 hours after becoming aware of a Personal Data Breach and implement all the necessary corrective measures to resolve the breach;
- ensure that each Subprocessor, acting on its behalf and for the purpose of the Contract, provide appropriate safeguards and comply with all Applicable Laws;
- answer to Data Subjects request and especially of all requests of access, rectification, erasure, data portability. For this purpose, the Data Subjects may modify, delete or retrieve their Personal Data directly via the Services or by default may send their request by email to Klaxoon at the following address: legal@klaxoon.com.

KLAXOON Represented by Mathieu Hongrois Position:CFO On the……	…….. Represented by: Position: On the……..
Signature:	Signature:

Appendix 1 – Detail of processing activities

For the purpose of the Contract and for the performance of Services, Klaxoon carries out the following processing activities:.

I). Processing activity carried out by Klaxoon as a Processor

- Subject : hosting of Personal Data collected by the Client as a part of use of Services;
- Nature : collection, archival storage, erasure, hosting ;
- Purpose : secure storage of the Client's Personal Data ;
- Category of Personal Data : all Personal Data collected by the Client as a part of use of Services;
- Category of Data Subject: the users of Klaxoon solution;
- Retention period : until the user delete its Personal Data or as long as the user account is active.

II). Processing activities carried out by Klaxoon as a Data Controller.

Processing n°1

- Subject : creation and administration of users accounts ;
- Nature : collection, use, storage, erasure;
- Purpose : creation and administration of users accounts ;
- Category of personal data : name, surname, email address, photo (optional, at the client's discretion);
- Category of Data Subject : the users of Klaxoon solution;
- Retention period : as long as the account is active

Processing n°2

- Subject : management of the contractual relationship ;
- Nature : use, collection, storage, erasure ;
- Purpose : manage the contractual relationship between Klaxoon and the Client (sending of quote and invoice, contract renew, management of payment) ;
- Category of personal data : name, surname, email address, phone number ;
- Category of Data Subject : each person in charge of the contractual relationship for Klaxoon and the client;
- Retention period: the duration of the Contract and for complying with any legal obligation including accounting obligations (for the purpose of proof or communication to the competent authorities).

A) Processing n°3

- Subject : management of the client's relationship and support ;
- Nature : collection, use, storage, erasure ;
- Purpose : answer to users request, inform users about the use of the Service, answer to users request relating to technical support, management of request to access, modify, erasure, retrieve, or object personal ;
- Catégory of Personal Data : name, surname, email address, phone number, data of use ;
- Category of Data Subject : users of Klaxoon solution; ;
- Retention period : as long as the user account is active.

B) Processing n°4

- Subject : inform users for business and marketing purpose (Newsletters) ;

- Nature : Collection, use, storage, erasure ;
- Purpose : inform the users of Services evolutions as all new version of Services, new functionnality, new update, launching a new product and/or organization of event relating to the lauching of new product ;
- Category of personal data : Name, surname, email address ;
- Category of Data Subject: users of Klaxoon solution ;
- Retention period : As long as the user account is active. Personal Data collected for this purpose are retained by Klaxoon in accordance with Applicable Laws that is for a three (3) years period from the collection or the last contact of the user. Users have opportunity to unsubscribe from the sending list.

Appendix 2 –Technical and Security standards

Technical requirements for the use of the Service and Equipment

The Klaxoon Cloud Service is a collaborative SaaS application.

The application is available with an Internet connection, on all types of devices. There is nothing to download or install.

With the browser of your choice: Google Chrome; Mozilla Firefox; Windows Edge; Safari; Internet Explorer
Fully functional with the last 3 versions of these browsers (mobile and desktop mode).

Mandatory browser configuration: Javascript activation, cookie acceptance

With the device of your choice: Tablet, Smartphone, Desktop

Some synchronous activities use Klaxoon web-sockets requests on the client side, for this you must allow the following URL: wss://*.klaxoon.com/*

Equipment: In order to use the equipment in wifi mode, it is necessary to allow connection to a private wifi access point from the terminals (PC, smartphones, tablets).

Technical and organizational measures related to data security

Technical measures:

- Privacy by Default: Implementation of current best practices (top 10 OWASP, CWE, NIST) in software developments contributing to the Security by Design approach and the principle of Defense in Depth
- Physical access protection: KLAXOON offices and third-party offices (including datacenter) accesses are protected
- User authentication: Personal data can only be accessed by the User himself and the passwords are hashed. Alternatively, user authentication can be delegated to the Client (subject to a quotation)
- Identity access management: Different roles implemented with different accesses, least privileges and need-to-know principles implemented
- Segregation of networks for internal IT, R&D and Production
- Journaling of connections: All accesses are logged
- Data encryption in transit and at rest
- Access to the service by participants can be anonymized.

Organizational measures:

- An Information System Security Policy (ISSP) is implemented by KLAXOON
- KLAXOON staff and subcontractors are subject to the obligation of contractual confidentiality regarding the information to which they have access in the exercise of their mission
- A specific IT charter is enforced for KLAXOON staff
- A Data Protection Officer is nominated to manage data privacy at KLAXOON.

Further security information are available on the Site at the following address: https://klaxoon.com/solutions-trust-center