Personal Data Processing

1) Definitions and Interpretation

Capitalised terms not defined herein shall have the meaning ascribed to them in the Terms and Conditions.

"**Adequate Country or Sector**" means: (i) a country within the European Economic Area ("**EEA**"); or (ii) a country, territory or sector within a country which has been subject to an adequacy finding from the European Commission confirming that it has an adequate level of protection of Personal Data;

"**Client Personal Data**" means all Personal Data processed by Invoke on behalf of the Client under or in connection with the Purchase Order;

"**Data Protection Legislation**" means the General Data Protection Regulation 2016/679 (the "GDPR");

"**Sub-Processor**" means any entity engaged by Invoke or by any other sub-processor of Invoke who receives Client Personal Data for processing activities to be carried out on behalf of the Client; and

For the purposes of this document, the terms "**Personal Data**", "**Data Controller**", "**Data Processor**", "**process**" or "**processing**", "**Personal Data Breach**" and "**Data Subject**" have the meanings ascribed to them in the Data Protection Legislation.

2) Scope

2.1 This document applies to the processing of Personal Data by the Parties under the Purchase Order. Invoke processes Client Personal Data for the purpose of providing the Services under the Purchase Order. Invoke will process the Client Personal Data for the duration of the Purchase Order (or for as long as is reasonably required and to the extent permitted by Applicable Laws).

2.2 Where applicable, the processing of the Client Personal Data by Invoke will be described in detail below.

2.3 According to the applicable Data Protection Legislation and in the context of the performance of the Purchase Order:

- the Client shall act as Data Controller or, where applicable, Data Processor of its customers;
- Invoke Nordics shall act as Data Processor only on behalf of and on the documented and lawful instructions of the Client. Invoke SA (France) shall act as Sub-Processor of Invoke Nordics.

3) Data Protection Legislation

Each Party shall comply with their obligations under Data Protection Legislation.

4) Data Processor's Obligations

4.1 Invoke agrees:

4.1.1 to only process the Client Personal Data in accordance with the Client's instructions. The Parties agree that the attainment of the purpose of the Purchase Order as well as the use of the Service and in particular the Software in accordance with the Documentation constitute the Client's documented instructions.
Any additional instruction from the Client in relation to those referred to above must be brought to Invoke's attention in writing, specifying the purpose concerned and the operation to be carried out. The implementation of any additional instruction may be subject to the Client's acceptance of a quotation from Invoke.
Invoke undertakes to inform the Client by any means within five (5) days of Invoke becoming aware of the Client's instruction if, in its opinion, this instruction constitutes a violation of the Data Protection Legislation.

4.1.2 to process Client Personal Data as required under Data Protection Legislation, provided that Invoke informs the Client of such a requirement before processing the data, unless the law prohibits this on grounds of public interest;

4.1.3 to ensure only staff who are contractually bound to respect the confidentiality of Personal Data shall have access to the same;

4.1.4 to implement and maintain appropriate technical and organisational measures to protect the Client Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm that might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of the Client Personal Data and having regard to the nature of the Client Personal Data which is to be protected;

Pursuant to article 32.1 of the GDPR, the Client and Invoke agree to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks.
The means implemented by Invoke are listed in the Security documents attached to appendix 2 of the Purchase Order.
Invoke shall be responsible for the security of the Service only for aspects under its control. The Client shall thus remain responsible for the security and confidentiality of its systems and its Service access policy. The Client shall also be responsible for ensuring that the uses and configuration choices of the Service made available to it meet the requirements of the Applicable Regulations.

Invoke shall have no obligation to protect personal data stored or transferred outside the Service by the Client or by Invoke at the Client's instruction.

Invoke shall ensure that its personnel authorised to process Client Personal Data undertake to respect their confidentiality.
Invoke further undertakes to ensure that all its employees are made aware of the protection of Client Personal Data and that a confidentiality clause is inserted into their employment contracts.

4.1.5 at the Client's request and cost, to provide reasonable assistance to the Client in the Client's assessment and implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the Personal Data;

4.1.6 to inform the Client, as soon as reasonably practicable, if it receives a request notice or other communication from a Data Subject seeking to exercise his or her rights under Data Protection Legislation in respect of Personal Data, and, at the Client's request, shall assist the Client with respect to that communication, request or notice (at Client's cost and expense);

4.1.7 to assist the Client by providing such information to the Client as the Client may reasonably require, and within the timescales reasonably specified by the Client to allow the Client to comply with the rights of the Data Subject, including Data Subject Requests, or with notices served by the relevant supervisory authority or any other law enforcement or regulatory authority. Invoke shall be entitled to charge the Client for its assistance under this paragraph at Invoke's standard rate card;

4.1.8 delete the Personal Data and any copies thereof pursuant article 14.5 of the Terms and Conditions unless the applicable law requires the retention of such Client Personal Data.

4.1.9 to notify the Client about a Personal Data Breach as soon as possible (not to exceed 48 hours) after becoming aware of such a breach.
Invoke shall provide the following information to the Client as soon as possible (not to exceed 24 hours) from the above notification of the Personal Data Breach:

- the categories and approximate number of data subjects affected by the breach;
- the categories and approximate number of personal data records affected;
- a description of the likely consequences of the Personal Data Breach;
- a description of the measures taken or that Invoke proposes taking to address the personal data breach, including, where appropriate, measures to mitigate its possible negative consequences.

4.1.10 Invoke shall be entitled to charge the Client for its assistance: (i) with a Data Subject Request; or (ii) during a Personal Data Breach (unless the Personal Data Breach is directly attributable to Invoke); or (iii) when the Client requests Invoke's assistance to comply with Data Protection Legislation at Invoke's standard rate card.

5) Transfer of Client Personal Data outside the EEA

The Client's Data (and therefore the Client Personal Data) are located at one or more sites in the European Union.

In the event that Invoke is required to transfer any Client Personal Data to a country outside the EEA in respect of which the EU Commission has not made a positive finding of adequacy: (i) the Client herein consents to such transfer provided that this transfer is in the context of, and necessary for, the provision of the Services under the Purchase Order; and (ii) Invoke ensures that there is a written contract in place with any international recipient that shall include equivalent obligations relating to security and confidentiality, and ensure adequate protection and appropriate safeguards in place for such transfer of Client Personal Data in accordance with applicable Data Protection Legislation. Such adequate protection and appropriate safeguards may include entering into Standard Contractual Clauses with the Client.

6) Contacts

Invoke Contact: all notifications, information, requests, and generally written exchanges within the framework of this document must be sent by email to Invoke's Digital Protection Officer (DPO) at dpo@invoke.fr.

Client Contact: the Client undertakes to inform Invoke as soon as possible of the person or team to be contacted for any information, communications, notifications, or requests pursuant to this document**.**

7) Sub-Processor

The Client authorises Invoke to choose Sub-Processors to carry out Personal Data processing activities on behalf of the Client provided that the involvement of the Sub-Processors is strictly necessary for the performance of the Service.

Invoke undertakes to choose Sub-Processors offering sufficient guarantees regarding the implementation of appropriate technical and organisational measures in order to meet the requirements of the Data Protection Legislation.

Invoke undertakes to contractually impose on its Sub-Processors a level of obligation at least equivalent in terms of Personal Data protection to that set out in this document and by the Data Protection Legislation.

In any event, Invoke shall remain liable to the Client for the said Sub-Processor's fulfilment of its obligations.

Invoke undertakes to inform the Client of any addition or replacement of Sub-Processors as soon as possible.

The Client may object in writing within ten (10) working days of receipt of the information. The Client accepts that if no objections are expressed within this period, this shall be equivalent to acceptance of the Sub-Processor.

In the event of an objection, Invoke shall have the option of responding to the Client to provide elements capable of lifting these objections. If the Client maintains its objections, the Parties undertake to meet for a discussion in good faith of the continuation of their relationship.

The Client consents to the processing of Client Personal Data by any Invoke Affiliates or by Invoke's mother company engaged in the provision of the Service which shall be deemed as Sub-Processors.

8) Audit

If, despite the provision by Invoke of information intended to demonstrate compliance with its obligations under the provisions of paragraph 4.1.5, the Client wishes to conduct an audit of the processes and measures implemented by Invoke concerning the protection of Client Personal Data in the context of the performance of the Service, the following provisions shall apply:

(i) the Client shall submit a written audit request to Invoke by registered letter with acknowledgement of receipt, justifying and documenting its request;

(ii) Invoke undertakes to provide a response to the Client specifying the audit scope and conditions. The Client is informed and accepts that since the security of Invoke's information system and the Infrastructure relies on their restricted access, the scope of an audit shall be limited to the processes and measures implemented by Invoke concerning the protection of Client Personal Data.

The purpose of an audit pursuant to this clause shall be limited to verifying that Invoke is processing Client Personel Data in accordance with the obligations under the Purchase Order and Data Protection Legislation.

The audit may only take place after a period of twenty (20) working days from the Client's request under (i).

(iii) This audit may be conducted by the Client's internal auditors or may be entrusted to any other auditor chosen by the Client provided such an auditor is not a competitor of Invoke;

Auditors must make a formal commitment not to disclose information collected at Invoke regardless of how it is acquired. The auditors must sign the confidentiality agreement prior to the audit and inform Invoke.

(iv) For the purposes of the audit, Invoke shall provide access to its premises and in general to the documents and individuals necessary for the auditors to conduct the audit under satisfactory conditions. It is understood that the auditors must act reasonably and in good faith and not disrupt the operation of the Service.

(v) The audit report shall be made available to Invoke by the auditors before being finalised so that Invoke may make all its comments. The final report shall take into account and mention such comments. The final audit report shall then be sent to Invoke and reviewed at a meeting between the Parties.

In the event that the final audit report reveals breaches of commitments made with respect to the performance of the Service, Invoke undertakes to propose a corrective action plan within a maximum of ten (10) working days from the meeting between the Parties.

The duration of an audit may not exceed one (1) working day. If this duration is exceeded, Invoke shall invoice the Client for the additional days according to the price of the services in force at the time of the audit.

Unless an event legitimises the implementation of an audit within a shorter period, audits may be conducted by the Client at Invoke's site only once during the Initial Subscription Term and then once per Renewal Period.

9) Description of the processing activities

The nature of the operations carried out on the Client Personal Data, the purpose(s) of the processing, the processed Client Personal Data, the categories of data subjects, and the duration of the processing shall be available upon request made to Invoke.