Appendix 1 to the Special Conditions of Contract: General Data Protection Regulation Compliance Clause

I) General context

These clauses are intended to define the conditions under which the contractor undertakes to carry out the personal data processing operations defined below.

The following will be defined from the 1st meeting organised by the EdA concerning the respect for personal data:

- the nature of the operations carried out on the data;
- the processing purpose(s) as well as the processed personal data;
- a description of the envisaged processing operations;
- the categories of data subjects, the method of collecting the information necessary for the purpose of the services, as well as the information necessary for the proper execution of the provisions anticipated below;
- the processing methods for data defined as "sensitive";
- the retention period of the data collected by each of the parties;
- the recipients of the processed data;
- the processors involved in the processing(s), as well as their location;
- possible data transfers;
- security measures related to the processing.

In the context of their contractual relations, the contractor undertakes to comply with the Regulations in force applicable to the processing of personal data and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable from 25 May 2018 (hereinafter, the "European Data Protection Regulation" or "GDPR") and Law n°78-17 of 6 January 1978 on data processing, files and freedoms, as amended by Order n°2018-1125 of 12 December 2018 adopted pursuant to Article 32 of Law n°2018-493 of 20 June 2018 on the protection of personal data and amending Law n°78-17 of 6 January 1978 on data processing, files and freedoms and various provisions concerning the protection of personal data.

The EdA is the controller and the contractor is the data processor within the meaning of the aforementioned regulation.

II) Obligations of the processor vis-à-vis the EdA

1. Commitment of the contractor

The contractor undertakes, for the purchase orders, and the subsequent contracts notified, to:

- comply with the processing terms and conditions;
- process the data only for the sole purpose(s) that is/are the subject of the service under this framework agreement;
- process the data in accordance with the controller's instructions. If the Contractor considers that an instruction constitutes a breach of the European Data Protection Regulation or any other provision of Union or Member State law relating to data protection, it shall immediately so inform the Data Protection Officer. In addition, if the contractor is required to carry out a data transfer to a third country or an international organisation, under Union law or the law of the Member State to which it is subject, it must inform the controller of this legal obligation before processing, unless the relevant law prohibits such information on significant grounds of public interest;
- guarantee the confidentiality of personal data processed in the context of

this framework agreement;

- ensure that persons authorised to process personal data under this framework agreement:
  - undertake to respect confidentiality or are subject to an appropriate legal confidentiality obligation anticipated in the Special Conditions of Contract (SCC) of the framework agreement;
  - receive the necessary training in personal data protection;
  - take into account, with regard to any tools, products, applications or services, the principles of data protection by design and data protection by default;
- implement the necessary data protection tools (example: anti-virus software), notably for data defined as sensitive;
- promptly inform the EdA of any request for communication of information made to the contractor and/or one of its co-contractor(s)/processor(s).

The contractor shall provide the EdA with the name and contact details of its Data Protection Officer, if it has appointed one in accordance with Article 37 of the European Data Protection Regulation.

2. Individuals' right to information and the exercise of their rights

The contractor is required to provide the data subjects of the processing operations with information relating to the data processing that it undertakes at the time of data collection.

The wording and format of the information will be agreed with the Data Protection Officer prior to data collection.

In addition, the contractor is required to provide assistance to the EdA in order to fulfil its obligation to respond to requests for the exercise of the rights of data subjects. As part of its general obligation to advise as set out in this document, it notably informs the EdA of any request related to the exercise of these rights.

3. Notification of personal data breaches

By e-mail, the contractor notifies the EdA of any personal data breach immediately upon becoming aware of it, while undertaking to enable the latter to notify the CNIL within 72 hours. This notification shall be accompanied by all relevant documentation in order to enable the EdA to report this breach to the competent supervisory authority.

The notification shall therefore at least contain:

- a description of the nature of the personal data breach, including the categories and approximate number of data subjects involved in the breach and the categories and approximate number of personal data records involved;
- the name and contact details of the processor or other point of contact from which additional information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to be taken by the processor to remedy the personal data breach, including, where applicable, measures to mitigate any negative consequences. If, and to the extent that, it is not possible to provide all such information at the same time, the information may be provided in a staggered manner without undue delay.

If necessary, apart from the exclusions cases anticipated in Article 34.3 of the GDPR, the individuals concerned by the breach of their data must be informed by the Data Protection Officer.

4. Sub-processing of personal data

The processor shall provide the controller with prior written notification of the appointment of any new Sub-Processor, including full details of the processing to be carried out by the sub-processor. If within 30 days of receipt of such notification, the controller informs the processor in writing of any objections (on reasonable grounds) to the proposed designation:

i. The processor shall work in good faith with the controller in order to modify the provision of the services in a commercially reasonable manner that would avoid the use of the proposed sub-processor;

ii. When such a change cannot be made within 30 days of receipt by the processor of the controller's notification, notwithstanding any provision to the contrary in the contract, the controller may, by written notice to the processor effective immediately, terminate the contract in respect of the services requiring the use of the proposed sub-processor.

- The processor chooses this sub-processor with due care and pays particular attention to its reputation and experience in providing the subcontracted services and the adequacy of its technical and organisational measures. The processor shall enter into a written contract with any sub-processor. This sub-processing contract imposes on the sub-processor obligations as protective of personal data as those imposed on the processor. With regard to the subcontracted services, the subcontracted services are described, and the technical and organisational measures having to be implemented by the sub-processor, and that apply to the subcontracted services, are described. At the request of the controller and within a reasonable time, the processor shall provide a copy of the sub-processing contract.

- Throughout the duration of the contract, at no cost to the controller, the processor shall actively monitor, regularly audit and, where appropriate, take measures to ensure that each sub-processor complies with its obligations and shall report as soon as possible to the controller any breach of the provisions of this contract, detected or reported by the sub-processor and any measures taken to remedy it.

- In the event of a breach, the parties shall negotiate in good faith to determine whether and how the processor may continue to provide the services without the sub-processor in question. If the parties are unable to agree on a mutually acceptable solution, the controller may terminate the relevant services upon reasonable written notice.

- If a sub-processor is located outside of the EU / EEA, in a country not recognised as offering an adequate level of data protection, the processor must, upon request, provide the controller with the other information and relevant documentation on the international data transfer system in accordance with Art. 46 GDPR that is used to lawfully disclose the controller's personal data to the processor.

5. Audit

The data controller may at any time subject the processor to a security audit under Article 28 (h) of the GDPR for the purpose of verifying the compliance of the personal data processing with the provisions of this clause, and notably, but without being limited in any way, may inspect the offices, facilities, equipment, IT systems, technical elements, policies, controls and practices of the processor with regard to personal data protection in connection with this contract, subject to informing the processor in writing at least fifteen (15) days before the scheduled audit date.

In this context, the controller may notably test the working methods of the processor's staff, check the records, and the processor must provide the controller with any document or information related to the processing of subcontracted personal data. Except in the event of written justification from the Processor, the latter must allow all access required by the controller during the working days to the various places concerned by the execution of this contract.

The audit may be carried out by the data controller or any third party authorised by it, and lasts for the time necessary to carry out a complete audit.

Within thirty (30) days of the end date of the audit, the controller shall provide the processor with a report on the audit results showing any critical points and/or non-conformity.

If the findings of the audit reveal deficiencies, the processor shall define and implement corrective action plans at its own expense. The content of the corrective action plans is defined in consultation between the parties and the costs of implementing these corrective measures are the responsibility of the processor unless otherwise agreed in writing by the parties.

In any event, the controller seeks to limit the impact of the audit on the processor's day-to-day activity.

6. Security measures

The contractor undertakes to implement the security measures described in its tender and which meet the following obligations:

- means to ensure the ongoing confidentiality, integrity, availability and resiliency of processing systems and services;
- means to restore the availability of and access to personal data within an appropriate timeframe in the event of a physical or technical incident;
- a procedure for regularly testing, analysing and assessing the effectiveness of the technical and organisational measures serving to ensure the processing security.

7. Data processing at the end of the services

The contractor is required to certify that the documents and information in its possession, concerning the services performed under this contract as well as all personal data manipulated, are deleted from any computer medium and that no edition or copy is retained by the contractor at the end of the contract. These destruction and non-conservation actions are formalized in a certificate.

8. Register of categories of processing activity

The contractor declares maintaining a written register of all categories of processing activities carried out on behalf of the EdA, notably including:

- the name and contact details of the controller on whose behalf it is acting, any processors and, where applicable, the Data Protection Officer;
- the categories of processing actions carried out on behalf of the controller;
- where applicable, transfers of personal data to a third country or international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49 (1) of the European Data Protection Regulation, documents attesting to the existence of appropriate safeguards;
- where possible, a general description of the technical and organisational security measures, including but not limited to, as appropriate:
    - Pseudonymisation, anonymisation and encryption of personal data;
    - Means for ensuring the ongoing confidentiality, integrity, availability and resiliency of the processing systems and services;
- means to restore the availability of and access to personal data within an appropriate timeframe in the event of a physical or technical incident;
- a procedure for regularly testing, analysing and assessing the effectiveness of the technical and organisational measures serving to ensure the processing security.

9. Documentation

The contractor shall make available to the EdA the documentation necessary to demonstrate compliance with all of its obligations and to allow the performance of audits, including by a third party.