**CONTRACTUAL ANNEX**   
**COVERING THE DEFINITION AND CONDITIONS FOR PROCESSING PERSONAL DATA ON BEHALF OF THE CONTRACTING AUTHORITY**

The purpose of this annex to the contract is to define the conditions under which the contractor undertakes to process the personal data defined below on behalf of the contracting authority.

1. **Description of the personal data processing**

The contractor is authorised, for the term of this contract, to process on behalf of the contracting authority certain personal data as required for provision of the following services, constituting the purpose of the processing within the meaning of GDPR:

* Stakeholder consultations
* Surveys and interviews
* Workshops

The data subjects concerned by the processing of their personal data are as follows:

Employees

Candidates for any procedure required to execute this contract

Suppliers and service providers

Visitors

Prospects

Partners

Other:

The data categories to be processed are:

Title, identity, identification data

Private life (lifestyle, family situation, etc.)

Professional life (CV, e-mail address, professional training, academic history, etc.)

Economic and financial information (income, financial situation, tax position, etc.)

Connection data (IP address, connection logs, etc.)

Location data (travel, GPS & GSM data, etc.)

Other:

If highly personal data is also collected and processed:

Banking data (account details, bank card data, financial transactions, etc.)

Data about social problems

If categories of sensitive data is also collected and processed:

Data on racial or ethnic origin

Data on political opinions

Data on religious or philosophical beliefs

Data on trade union membership

Genetic data

Biometric data

Health data

Data on lifestyle or sexual orientation

Data on criminal convictions and offences or related security measures

1. **Obligations of the contractor vis-à-vis the buyer (Article 28.3 GDPR)**

The contractor notably undertakes to:

* process personal data solely for the purposes of the contract;
* process data as set out in the contractual documents. If the contractor considers that instructions are issued in violation of personal data regulations or any other provision of EU law or that of a member state on personal data, it must immediately notify the contracting authority.

If the contractor is required to transfer data to a third country (outside the EU) or to an international organisation under EU law or that of any member state by which it is bound, it must notify the contracting authority of such a legal obligation prior to performing the relevant processing, unless prohibited from doing so under any applicable law;

* guarantee the confidentiality and security of the personal data processed under this contract;
* ensure that persons authorised to process personal data under this contract:
* undertake to maintain its confidentiality or are bound by an appropriate legal obligation of confidentiality;
* receive the necessary personal data protection training;
* gives due consideration, with regard to its systems, products, applications or services, to the data protection principles of privacy by design and privacy by default.

1. **Outsourcing of processing activities (Articles 28.2 and 28.4 GDPR)**

Where the contractor uses a data processor to carry out specific processing activities, it shall notify the contracting authority in advance and in writing of any planned change with regard to the addition or replacement of other processors. Such notification must clearly state the processing activities to be outsourced, the identity and contact details of the processor and the contract dates.

In order to obtain acceptance and authorisation from Expertise France, the contractor must present its processor by means of a special processing document, for which the formal requirements are set out in form DC4 or any other equivalent document (available for download at <http://www.economie.gouv.fr/daj/formulaires-declaration-candidat>).

1. **Data subjects’ right of information and exercise of said right (Articles 13 to 15 GDPR)**

The contractor shall provide the contracting authority with the means of notifying data subjects of all relevant processing activities at the time data is collected.

1. **Notification of personal data breaches (Article 33 GDPR)**

The contractor shall notify its contract contact person at Expertise France of any personal data breach, within 24 hours of becoming aware of any such breach.

It shall notify the contracting authority by any means able to unequivocally establish the date and time of receipt of the notification. Any such notification shall be accompanied by all relevant documentation in order to enable the contracting authority, as required, to notify the breach to the competent authorities (in this case, the French data protection agency, CNIL) within a reasonable period of time after becoming aware of the breach.

On receipt of written authorisation from Expertise France, the contractor shall notify the personal data breach to the competent authorities on behalf of Expertise France within 72 hours, unless said the breach is unlikely to pose any threat to the rights and liberties of natural persons.

The notification shall at least include:

* a description of the nature of the personal data breach, where possible including the categories and approximate number of data subjects affected by the breach, and the categories and approximate number of personal data records in question;
* the name and contact details of the data protection officer or of another contact person from whom additional information may be obtained;
* a description of the probable consequences of the personal data breach;
* a description of the measures taken, or which the contractor plans to take, in agreement with the contracting authority in order to rectify the personal data breach, including, as applicable, the measures to mitigate any negative consequences.

If it is not possible for the contractor to provide all such information at the same time, it may be forwarded in stages yet without undue delay.

1. **Support from the contractor to the contracting authority to enable its obligations to be complied with**

The contractor undertakes to collaborate with the contracting authority in the preliminary investigations of the supervisory authority.

1. **Security measures**

The contractor shall employ all resources, measures and procedures enabling it to:

* anonymise the personal data to be processed (pseudonyms, encryption, etc.);
* guarantee the confidentiality, integrity, availability and permanent reliability of processing systems and services;
* re-establish the availability of and access to personal data within an appropriate period of time in the event of any physical or technical incident;
* regularly test, analyse and assess the effectiveness of the technical and organisational measures implemented to ensure secure processing.

1. **Fate of personal data (Article 28.3.g GDPR)**

On expiry of the contract, and at the discretion of Expertise France, the contractor and any data processor it may use must:

* return to Expertise France, or to a third party designated by the latter, all personal data in their possession;
* destroy or permanently delete all personal data and copies thereof in their possession, regardless of the medium on which it may be held, and be able to certify destruction vis-à-vis Expertise France.

1. **Data protection officer (Articles 37 to 39 GDPR)**

On signature of the contract, the contractor shall notify Expertise France of the name and contact details of its data protection officer, if it has designated such a person under Article 37 GDPR, or, failing this, the identity and contact details of the contact person charged with data protection matters.

1. **Processing register (Article 30 GDPR)**

The contractor shall maintain a written register of all processing activities performed on behalf of Expertise France, containing:

1. the names and contact details of the personnel or other representatives of Expertise France on behalf of whom it is acting, of any processors it may employ and, as applicable, of the data protection officer;
2. the categories of processing performed on behalf of Expertise France;
3. as applicable, transfers of personal data to a third country or international organisation, including identification of such third countries or international organisations, and, in the case of transfers covered by the second subparagraph of Article 49(1) GDPR, the documents certifying the existence of appropriate guarantees;
4. to the extent possible, a general description of the technical and organisational security measures satisfying your personal data protection obligations.
5. **Documentation (Article 28.3.h GDPR)**

The contractor shall make available to the contracting authority all necessary documentation demonstrating compliance with all its obligations and, as applicable, to enable audits to be performed, including inspections by the contracting authority or by an auditor engaged by the latter, and fully collaborate in such audits.

1. **Obligations of the contracting authority vis-à-vis the contractor**

Expertise France undertakes to:

* Collaborate with the contractor in order to satisfy the obligations relating to the “Description of the personal data processing” as set out in Article 1 of this annex;