**Personal Data Processing Annex**

This Personal Data Processing Annex (here in after called “PDPA” or the “PDP Annex”) governs the processing of Personal Data exchanged by the Parties in the frame of the Contract and, as such, it forms an integral part of the Contract. In case of conflict between the terms and conditions of the Contract and the terms and conditions of this Annex, the terms and conditions of this Annex shall prevail.

1. Definitions

For the purpose of this Annex, the Parties agree to the following specific definitions as well as the ones set forth in the ESA Personal Data Protection Framework defined in (5) below:

1. **“Agreed Purpose”** (of Processing) means:
2. the performance of the Contract, including implementation, management, monitoring of the work;
3. management of the relationship of the Parties in relation to the Contract, notably for administrative, financial, audit or for communication purposes.
4. **“Agreed Retention Period”** (of Personal Data) means the duration necessary to fulfill the Agreed Purpose of Processing, but in any case no longer than 5 (five) years from the close-out of the Contract.
5. **“Agreed Territory”** (of Processing) means the following territories:
6. ESA Member States, as they are listed on the following website

<http://www.esa.int/About_Us/Welcome_to_ESA/New_Member_States>; and

1. European Union;
2. countries recognized by the European Commission as ensuring an Adequate Level of Protection of Personal Data under the European Union’s legal framework.
3. **“Contractor”** means the natural or legal person who has entered into the Contract with the Agency and which with regards to Personal Data, acts either as a Data Controller or as a Data Processor.
4. **“Contractor Personnel”** means Contractor’s employees and as well Subcontractors’ employees.
5. **“Contractor Personal Data”** means the Personal Data referred to in Section 3.3 herein.
6. **“Controller”** or **“Data Controller”** means any natural or legal person who makes the decision, alone or conjointly, to Process Personal Data, or commissions others to Process Personal Data on its behalf. The quality of Data Controller belongs to Party itself as an entity, not to the Party’s personnel who is materially involved in the related activities.
7. **“Data Privacy Regulations”** means collectively:
8. ESA PDP Framework, i.e. the Personal Data Protection Framework of ESA available on ESA website at the URL

<http://www.esa.int/About_Us/Law_at_ESA/Highlights_of_ESA_rules_and_regulations>

1. the Personal Data protection laws and regulations applicable to the Agreed Territory of Processing to the extent that these laws and regulations provide an Adequate Level of Protection under the ESA PDP Framework.
2. **“Data Protection Incident”** means intentional or unintentional activity which violates the provisions set forth in the Data Privacy Regulations.
3. **“Data Subject”** means an individual who is the subject of Personal Data.

1. **“Disclosure** (or **“transfer”**) **of Personal Data”** (or **“Disclose”**) means any movement of Personal Data, including by copy, by moving Personal Data through a network or from one (1) medium to another (e.g. from a computer hard disk to a server), and/or by rendering remotely accessible Personal Data.
2. **“ESA”** or the **“Agency”** means the European Space Agency, including any of its establishments, centres, sites, and any other Agency’s facilities, being identified as Party to the Contract.
3. **“ESA Personal Data”** means the Personal Data referred to in Section 3.2 herein.
4. **“ESA Personnel”** means ESA employees and as well seconded agents, consultants, experts or employees of Third Parties, as long as these individuals act under an engagement of confidentiality and for which the need to know has been authorised by ESA.
5. **“Personal Data”** means any information concerning an identified or identifiable Data Subject, provided that this information can be related to the said Data Subject without unreasonable efforts.
6. **“Data Processor”** (or **“Processor”**) means any natural or legal person which Processes Personal Data upon decision of the Data Controller for a specific purpose. The quality of Data Processor belongs to Party itself as an entity, not to the Party’s personnel who is materially involved in the related activities.
7. **“Processing”** **(or “Process”)** means any operation or set of operations performed in particular by electronic means, on Personal Data, such as collection, recording, organisation, storage, retrieval, use, Disclosure, transfer, deletion. It also includes sub-Processing, whenever it is authorized by the Data Controller under Contract.
8. Roles of the Parties

In the performance of the Contract:

1. each Party will act as Data Processor of Personal Data submitted to it by the other Party;
2. each Party will act as Data Controller of the Personal Data it submits to the other Party; and
3. when acting as Data Processor, each Party shall process such data solely for the Agreed Purpose.
4. Personal Data exchanged by the Parties
   1. Each Party shall communicate to the other Party only those Personal Data that is strictly necessary for the Agreed Purpose.
   2. As Data Controller, the Agency will communicate to the Contractor only the Personal Data concerning ESA representatives/contact persons including name, work address, email and telephone numbers.
   3. As Data Controller, the Contractor will communicate to the Agency only:
5. Personal Data concerning the Contractor’s representatives/contact persons including name, work address, email and telephone numbers;
6. Personal Data concerning the Contractor’s key personnel, including title, name, work address, email, telephone numbers, education, professional experience, description of the persons job and responsibilities and the precise assignment of the person to the activity under the Contract.
7. Data Controller’s obligations
   1. The Data Controller is responsible for the collection and update of the Personal Data, for the lawfulness and the quality of the Personal Data and of the means by which they were collected. Should the legal basis for the collection of the Personal Data cease to exist, the Data Controller will inform the Data Processor without undue delay.
   2. The Data Controller will handle and answer any Third Party(ies) request regarding the Personal Data communicated by the Data Controller, subject to prompt and written notification thereof by the Data Processor.
   3. The Data Controller undertakes to enforce the relevant provisions of the Data Privacy Regulation with respect to audits and to data breaches, involving the Personal Data processed under the Contract as per Section 12 below.
   4. The Data Controller shall ensure, in its area of responsibility, that the level of protection resulting from the Data Privacy Regulations is met.
8. Data Processor’s obligations
   1. The Data Processor shall process the Personal Data:
9. in compliance with this PDP Annex and, generally, and the level of protection resulting from the Data Privacy Regulations then in force;
10. solely for the Agreed Purpose of Processing;
11. solely in the Agreed Territory;
12. without exceeding the Agreed Retention period;
13. in such a way as to minimise, by means of suitable preventive security measures, the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, or Processing operations that are either unlawful or inconsistent with the Agreed Purpose.
    1. The Data Processor shall promptly investigate any reasonable suspicion of Personal Data Breach and act in accordance with Section 12 below.
    2. The Data Processor shall cooperate with the Data Controller to enable the latter to guarantee to every Data Subject or his/her delegates the possibility to exercise the rights granted to him/her by the Data Privacy Regulations. The Data Processor acknowledges that Data Subject rights shall be exercised only through the Data Controller. Therefore, the Data Processor undertakes to immediately notify the Data Controller of any request that Data Subjects, address directly to the Data Processor, and will not respond to any such request or take any other related action, until authorised by the Data Controller.
    3. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction from the Data Controller infringes any provision on the Processing of Personal Data under the present Agreement.
14. Deletion of Personal Data

Following expiration of the Agreed Retention Period, all Personal Data must be effectively destroyed/deleted, unless required otherwise by the Data Privacy Regulations in the frame of audits, inspections, incidents.

1. Confidentiality

The Parties shall ensure the confidentiality of the Personal Data processed in particular by:

(i) ensuring that the Personnel, recipients of the personal data of each Party:

* are properly authorised on a need-to-know basis;
* have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
* have received the appropriate personal data protection training.

(ii) take into consideration, in terms of IT tools, product, applications, the principles of personal data protection by design and by default.

1. Security

The Parties shall adopt appropriate technical and organisational security measures, giving due regard to the risks inherent in the processing and to the nature, scope, context and purpose of the processing, in order to ensure the following as appropriate:

* the on-going confidentiality, integrity, availability and resilience of processing systems and services;
* measures to protect Personal Data from accidental or unlawful destruction, loss, modification, unauthorised disclosure or access to personal data transmitted, stored or otherwise Processed.

1. Data Protection Officer

As far as required by the Data Privacy Regulation, the Parties shall appoint a Data Protection Officer and communicate the contact details to the other Party.

1. Transfer

Transfer of Personal Data outside the Agreed Territory requires prior written approval of the Data Controller.

1. Sub-contracting
   1. The Contractor is authorised to disclose the Personal Data received by the Agency for the Agreed Purpose and within the scope of the Contract to its Subcontractors indicated in Clause 10 of the Contract. Such Subcontractors will be considered as sub-Processors. All the obligations of the Contractor in its role as Data Processor shall be passed on to the sub-Processors by flowing down these provisions in the respective sub-contracts. The Processing of the Personal Data by the sub-Processors is only allowed for the Agreed Purpose and provided that the Personal Data are not transferred outside the Agreed Territory. Disclosure of the Agency’s Personal Data to other sub-Processors requires prior approval of the Agency.
   2. The Agency may engage sub-Processors to support its internal operations that process Personal Data. It is the responsibility of the Agency to ensure that such sub-Processors assume obligations consistent with the Data Privacy Regulations in order to guarantee an adequate level of protection of Personal Data.
2. Personal Data Breaches – Incident Management

In case of any actual or suspected Personal Data Protection Incident falling in the Data Processor’s area of responsibility, the Data Processor shall promptly:

1. report to Data Controller about it within 48 hours;
2. investigate and inform, in writing, the Data Controller of all stages of Data Processor’s investigation as well as on the results thereof:
   1. if such Incident actually occurred and about the date of occurrence;
   2. on the causes and the nature of the Incident;
   3. on the Personal Data which were affected by the Incident;
   4. on other consequences of the Incident;
   5. on the measures taken to mitigate the Incident;
   6. the actions taken to prevent similar Incidents from occurring in the future.
3. coordinate with the Data Controller in any aspect related to complaints (if any) lodged by the affected Data Subject to the Data Processor, in particular provide the Data Controller with reasonable assistance and accurate information about the Incident, in particular (but not only) in case a complaint is, or likely to be, lodged by a Data Subject in relation to the breach;
4. to put in place controls and audits.
5. Law and dispute resolution

The Parties agree that:

1. notwithstanding any other provisions on the governing law set forth elsewhere in the Contract, the provisions of the Data Privacy Regulations, as defined herein, will apply and prevail, in case of conflict;
2. notwithstanding any other dispute resolution provisions set forth elsewhere in the Contract:
3. any Personal Data-related Incidents or disputes shall be submitted to the independent Data Protection Supervisory Authority established by ESA Council Resolution; and
4. the Rules of Procedure for the Data Protection Supervisory Authority, as set forth ESA PDP Framework, shall apply.
5. Duration

This PDP Annex enters into force simultaneously with the Contract. Its terms and conditions will survive the expiration or termination of PDP Annex for as long as the Personal Data are protected by the Data Privacy Regulations.