AIRBUS

SPECIFIC PERSONAL DATA PROTECTION TERMS AND CONDITIONS

DATA PROCESSING AGREEMENT

WHEREAS

The provisions of this DPA shall apply to any Order placed by the Purchaser upon the Supplier under the relevant back of order terms and conditions of the Purchaser, unless otherwise expressly agreed between the Supplier and the Purchaser under a written agreement.

For the purpose of this DPA, unless otherwise defined below, capitalised terms, singular or plural, used in this DPA shall have the meaning of the applicable back of order terms and conditions to which this DPA is attached.

"**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Processing**", "**Personal Data Breach**", "**Binding Corporate Rules**", "**Supervisory Authority**", shall have the meaning of 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 referred as "**EU General Data Protection Regulation**" or **"EU GDPR"**).

"DPA" means this Specific Personal Data Protection terms and conditions incorporated into and appearing on the front of the Order and which intends to complement the applicable back of order terms and conditions.

"**Personal Data Transfers**" means all and any communication, exchange, copy, sharing or transmission of Personal Data through a network, or from one medium to another, irrespective of the type of support to any person, entity or service, since these Personal Data are intended to be processed, accessed and/or stored in the Third Country by any such person, entity or service.

"Third Country" means all states that are not members of the European Economic Area (E.E.A) or a country which has not been recognized as providing an adequate level of protection for Personal Data according to the applicable Data Protection Laws and Regulations.

Pursuant to the provision of the services under the Order and, in connection with Personal Data, the Parties acknowledge that the Purchaser is *data Controller* and the Supplier is *data Processor*. Without prejudice to any other requirements under applicable Data Protection Laws and Regulations, if a Processor infringes the applicable Data Protection Laws and Regulations by determining the purposes and means of processing, the Processor shall be considered to be a Controller in respect of that Processing.

Each Party asserts to comply with applicable personal data protection Laws and Regulations in force during the performance of the Order, including the EU GDPR (collectively referred as "**Personal Data Protection Laws and Regulations**"), including without limitation regarding Processor obligations as described hereinafter.

1. Identification of the related Personal Data Processing

Pursuant to the provision of the services under the Order, Personal Data processed by the data Processor may concern the following:

A. Subject Matter and Duration of the Processing as described in the Order and for the duration of the Order.

B. Nature and Purpose of the Processing: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination

or otherwise making available, alignment or combination, restriction, erasure or destruction required for the performance of the Services as ordered by the Purchaser.

    C. Categories of Personal Data: identification data, family, lifestyle and social circumstances, professional and education data, IT data, economic and financial data, location data as further instructed by the Purchaser.

    D. Categories of Data Subjects: Purchaser and affiliates employees (including its spouse/dependents, temporary workers, students, applicants), customers, suppliers/subcontractors and business partners, officials, visitors, guests, external speakers and any third party as further detailed by the Purchaser.

2. Processor's obligations

2.1 The data Processor undertakes to :

    A. process the Personal Data only on documented instructions from the data Controller, including with regard to Personal Data Transfers to a Third Country or an international organisation, unless required to do so by any applicable local law to which the data Processor is subject; in such a case, the data Processor shall inform the data Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The data Processor shall immediately inform the data Controller if, in its opinion, an instruction infringes the applicable Personal Data Protection provisions;

    B. ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

    C. take all measures required pursuant to Article 3 of the DPA;

    D. respect the conditions referred to in Article 5 of this DPA for engaging a sub-processor;

    E. taking into account the nature of the Processing, assist the data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in the applicable Personal Data Protection Laws and Regulations;

    F. assist the data Controller in ensuring compliance with the obligations pursuant to Articles 3 and 4 of the DPA taking into account the nature of Processing and the information available to the Processor (including but not limited for privacy impact assessment);

    G. at the choice of the data Controller, delete or return all the Personal Data to the data Controller after the end of the provision of Services relating to Processing, and deletes existing copies unless any applicable local law requires storage of the Personal Data;

    H. make available to the data Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by the data Controller or another auditor mandated by the data Controller.

2.2 The data Processor shall communicate to the data Controller the name and contact details of its Data Protection Officer if any in accordance with applicable Personal Data Protection Laws and Regulations.

3. Technical and Organisational measures

3.1 The data Processor ensures to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the Personal Data Protection Laws and Regulations and ensure the protection of the rights of the Data Subject.

3.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate: the pseudonymisation and encryption of Personal Data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

3.3 In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

4 Notification of a Personal Data Breach to the Supervisory Authority
4.1 The data Processor shall notify the data Controller without undue delay after becoming aware of a Personal Data Breach.
4.2 Where and in so far as, it is not possible to provide the information at the same time, and subject to data Controller prior information by the data Processor, the information may be provided by the data Processor in phases without undue further delay.

5 Sub-processor
5.1 The data Processor shall not engage a sub-processor without prior written authorisation of the data Controller as stated in the applicable back of order Conditions.
5.2 In case the data Processor engages another sub-processor for carrying out specific Processing activities on behalf of the data Controller, the same data protection obligations as set out in this DPA between the data Controller and the data Processor shall be imposed on that other sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the applicable Data Protection Laws and Regulations. Where that other sub-processor fails to fulfil its data protection obligations, the data Processor shall remain fully liable to the data Controller for the performance of that other sub-processor's obligations.

6 Personal Data access
6.1 The data Processor and any person acting under the authority of the data Processor, including sub-processor, who has access to Personal Data, shall not process that Personal Data except on instructions from the data Controller, unless required to do so by any applicable local laws and regulations.
6.2 The data Processor shall take steps to ensure that any individual acting under the authority of the data Processor who has access to Personal Data does not process them except on instructions from the data Controller, unless he or she is required to do so applicable local laws and regulations.

7 Cooperation with Supervisory Authority: The data Processor and, where applicable, their representatives, shall cooperate, on request, with the Supervisory Authority in the performance of its tasks.

8 Record of categories of processing activities: The data Processor states that it maintains a written record of all categories of Processing activities carried out on behalf of the data Controller, containing the mandatory information in accordance with applicable Personal Data Protection Laws and Regulations.

9 Personal Data Transfers: If Personal Data is transferred or accessed by the data Processor and/or sub-processor to/from a Third Country, a data transfer agreement in the form as set out by theEuropean Commission [EU decision No. C (2021) 3972 of June 4th, 2021] or any subsequent document decided by the European Commission and/or as set out by any other competent authority with the same purpose when applicable must be set forth. The data Processor undertakes to adopt and implement any supplementary measures required depending on the data transfer impact assessment related to the Processing in the scope of the Services to the extent necessary. The data Processor warrants that it has no reason to believe that the laws and practices in the Third Country applicable to the Processing under this DPA, including any requirements to disclose Personal Data or measures authorizing access by public authorities, prevent the data Processor from its commitments under the applicable legal transfer mechanisms. The data Processor shall immediately inform the data Controller of any relevant changes in the legislation or practices that might impact the data Processor fulfilling its obligations under this DPA.

10 Audit
10.1 The data Controller may carry out any verification that it deems necessary to ensure compliance by the data Processor with its obligations under this DPA, in particular by performing a data protection audit.
10.2 To this end, the data Processor undertakes to cooperate, respond to data Controller's audit requests even if carried out by a third party appointed for this purpose and make available to the

data Controller (or any external auditor) any documents related to the security of the processed Personal Data.

10.3 Audits shall provide evidence of compliance with the provisions of this DPA and all applicable Personal Data Protection Laws and Regulations and, in particular, to ensure that the security and confidentiality measures provided in this DPA are in place.

11. Order of prevalence: In the event of conflict the provisions of these DPA and another data processing agreement agreed between the data Controller and the data Processor with respect to the purpose of the Order under a separate written agreement, the one agreed under the written agreement shall supersede and take precedence over this DPA. In case of conflict between these DPA and the applicable data transfer agreement, the data transfer agreement shall prevail.

12. Effective Date: The DPA shall become effective between the Parties for the Processing described above, on the start/delivery date of the Item under the Order.