

**AIRBUS**  
**BINDING CORPORATE RULES**

## TABLE OF CONTENTS

INTRODUCTION	3
LIST OF APPENDICES	5
1. SCOPE OF THE BINDING CORPORATE RULES (BCR)	6
1.1 Material scope	6
1.2 Geographical scope	6
2. RULES APPLICABLE TO PERSONAL DATA TRANSFER AND PROCESSING	6
2.1 Data Protection Principles	7
2.1.1 Lawfulness, fairness and transparency	7
2.1.2 Purpose limitation	9
2.1.3 Data minimization and accuracy	9
2.1.4 Limited storage periods	9
2.2 Processing of Special Categories of Personal Data	9
2.3 Processing of Personal Data relating to criminal convictions and offences	10
2.4 Security	10
2.4.1 Processing in compliance with the Airbus' Security Requirements	10
2.4.2 Obligations relating to Personal Data Breaches	11
2.5 Processing and Sub-processing	11
2.6 Personal Data Transfers to Third Parties whether as Data Controllers or Processors	11
2.7 Data Subject rights	12
2.8 Prior formalities	13
3. ACCOUNTABILITY MECHANISMS	13
3.1 Records of Processing activities	14
3.2 Privacy Impact Assessment (PIA)	14
3.3 Privacy by design and by default	14

# AIRBUS

Binding Corporate Rules

Airbus Amber

3.3.1. Privacy by design	14
3.3.2. Privacy by default	14
3.4 Other accountability mechanisms implemented by Airbus	14
4. INFORMATION AND TRAINING	15
5. GUARANTEES FOR BCR IMPLEMENTATION	16
5.1 Airbus Privacy Governance	16
5.2 Audits	16
5.3 Internal Complaint Procedures	16
5.4 Responsibility for BCR implementation	17
5.5 Liability	17
6. THIRD PARTY BENEFICIARY RIGHTS	18
7. CONFLICT OF RULES	18
7.1 General rules	19
7.2 Disclosure access request by Third Country public authority	19
8. COOPERATION WITH THE COMPETENT AUTHORITIES	20
9. UPDATING THE BCR	20
10. BINDING NATURE OF THE BCR	20
11. TERMINATION	21
12. NON-COMPLIANCE	21

## INTRODUCTION

The Binding Corporate Rules, with their appendices, (hereinafter the “**BCR**”) of Airbus reflect Airbus’ commitment on the protection of Personal Data. These BCR are intended to ensure a suitable level of protection in compliance with the EU General Data Protection Regulation (as defined in Appendix 1) when the Personal Data specified in the present document are transferred within the group of Airbus Companies (hereinafter “**Airbus**”) for the purposes of Airbus’ worldwide business activities.

The purpose of these BCR is to frame Personal Data Transfers (i) from BCR Affiliated Companies acting as Data Controllers to other BCR Affiliated Companies acting as Data Controllers and (ii) from BCR Affiliated Companies acting as Data Controllers to other BCR Affiliated Companies acting as internal Processors.

Airbus is committed to ensure the right to privacy and protection of Personal Data and as such, specifies in its Directive related to Requirements for Personal Data Protection (“**Directive**”) (Appendix

# AIRBUS

Binding Corporate Rules

Airbus Amber

3(a)) and the Method for Personal Data Protection (“**Method**”) (Appendix 3(b)), the principles to be complied with within Airbus.

The BCR define the minimum standard of protection of Personal Data and information security measures within Airbus. For UK Data Subjects, safeguards under these BCR are provided under a separate data transfer mechanism. The BCR Affiliated Companies are entitled to implement more protective policies and regulations to comply with any local personal data protection laws and regulations.

## LIST OF APPENDICES

**Appendix 1:** Definitions

**Appendix 2:** Airbus Code of Conduct

**Appendix 3:** Airbus Personal Data Protection policies - ***Confidential***

**Appendix 3(a):** Directive relative to Requirements for Personal Data Protection

**Appendix 3(b):** Method for Personal Data Protection

**Appendix 4:** Scope of the Personal Data Processing covered by the BCR

**Appendix 5:** List of BCR Affiliated Companies subject to the BCR - ***Confidential***

**Appendix 6:** Letter of Adherence to the BCR and Appendices - ***Confidential***

**Appendix 7:** Airbus Security Requirements - ***Confidential***

**Appendix 8:** Airbus Privacy Training and Communication Plan - ***Confidential***

**Appendix 9:** Airbus Intra-Group Data Processing Agreement - ***Confidential***

**Appendix 10:** Airbus Privacy Organisation - ***Confidential***

**Appendix 11:** Airbus Privacy Audit Programme - ***Confidential***

## 1. SCOPE OF THE BINDING CORPORATE RULES (BCR)

### 1.1 Material scope

The BCR apply to all Processing of Personal Data carried out by BCR Affiliated Companies acting as Data Controllers and/or internal Processors for the purpose of Airbus' business activities and covers:

- (i) all Employees Personal Data collected in the EU/EEA, transferred and processed within Airbus to manage its Human Resources at international level as part of its business,
- (ii) all Customers, Suppliers and Business Partners Personal Data collected in the EU/EEA, transferred and processed within Airbus to manage the relationship with these stakeholders,
- (iii) all visitors, sympathisers, guests and external speakers' Personal Data collected in the EU/EEA, transferred and processed within Airbus to manage the relationship with these stakeholders in the context of Airbus activities.

The categories and nature of Personal Data related to the EU/EEA Data Subjects listed above and processed for the purposes mentioned above are described in Appendix 4.

For sake of clarity, the BCR do not apply to (i) Airbus as a Processor for services provided to its customers nor to (ii) any transfers of Personal Data which are subject to the UK GDPR subject to separate legal transfer mechanism.

### 1.2 Geographical scope

The BCR apply to all EU/EEA Personal Data as follows:

- a. all Personal Data transferred by BCR Affiliated Companies established in the EU/EEA to any BCR Affiliated Company established in a Third Country within Airbus;
- b. all Personal Data related to EU/EEA Data Subjects processed by BCR Affiliated Companies established in a Third Country, where the Processing activities are related to the offering of goods or services to such Data Subject(s) in the EU/EEA or the monitoring of their behaviours as far as their behaviours take place in the EU/EEA;

subject to the following principles:

- (i) Personal Data Transfer from an Airbus Company established in the EEA to another Airbus Company in a Third Country is made only to BCR Affiliated Companies, being understood that a Personal Data Transfer to Third Parties would need other appropriate safeguard.
- (ii) In some countries, other local Laws and Regulations applicable to Personal Data Processing may be more stringent or require additional conditions. In such a case, the local BCR Affiliated Company will implement specific policies, considering the applicable local Laws and Regulations in addition to the BCR and to the extent the BCR do not conflict with local applicable Laws and Regulations. Otherwise, section 7 of the BCR applies.

## 2. RULES APPLICABLE TO PERSONAL DATA TRANSFER AND PROCESSING

For Personal Data Transfers and Processing as described in section 1.1 above and in order to provide the Data Subject with an equivalent and suitable level of protection, the principles described in

the BCR, the Directive and associated Method as attached in Appendix 3 apply to all BCR Affiliated Companies who adhered to those BCR through the Letter of Adherence attached in Appendix 6.

Personal Data will not be transferred to another Airbus Company as long as this company is not effectively bound and committed to comply with the BCR terms pursuant to the Letter of Adherence, unless another appropriate Personal Data Transfer mechanism (as further detailed in section 2.6 below) is effective to cover such Personal Data Transfer.

## 2.1 Data Protection Principles

### 2.1.1 Lawfulness, fairness and transparency

(i) According to lawfulness principle, all Personal Data Processing must be based on one or more of the following lawful basis:

- The Data Subject has unambiguously given its Consent to the Processing;
- The Processing of Personal Data is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- The Processing of Personal Data is necessary for compliance with a legal obligation to which a BCR Affiliated Company is subject;
- The Processing of Personal Data is necessary to protect the vital interests of the Data Subject or of another individual;
- The Processing of Personal Data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
- The Processing of Personal Data is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party, except where such interests are overridden by the interest or fundamental rights and freedoms of the Data Subjects which require protection of Personal Data.

(ii) According to fairness and transparency, the BCR Affiliated Companies will provide all required information via a privacy notice to the Data Subjects on the conditions of Processing and how to exercise their rights, in a concise, transparent, intelligible and easily accessible manner, using clear and plain language.

(iii) As a matter of principle, Personal Data will be collected directly from the Data Subject concerned. In that case, the BCR Affiliated Company acting as Data Controller must, at the time when Personal Data are obtained, provide the Data Subject with all the following information:

- the identity and the contact details of the BCR Affiliated Company acting as Data Controller and, where applicable, of its representative,
- the contact details of the Privacy Team or Privacy Focal Point appointed by the relevant BCR Affiliated Company,
- the purposes of the Processing for which the Personal Data are intended as well as the lawful basis for the Processing, and if under the legitimate interest, basis, the one pursued by BCR Affiliated Company, as Data Controller or by a Third Party,
- statutory or contractual necessity of the provision of Personal Data, or as a requirement necessary to enter into a contract, as well as whether providing Personal Data is compulsory or optional for the Data Subject and the possible consequences of failing to provide such Personal Data,
- the Recipients or categories of Recipients of the Personal Data,

# AIRBUS

## Binding Corporate Rules

Airbus Amber

- the applicable retention period under which the Personal Data will be stored, or if not possible, the criteria used to determine that period,
- where applicable, the fact that the Data Controller intends to transfer Personal Data to a Third Country and the existence or absence of an adequacy decision by the EU Commission, or reference to the appropriate or suitable safeguards such as EU SCC or BCR and any relevant technical, contractual and organisational measures if required and the means by which to obtain a copy of them or where they have been made available,
- the existence of the right to request from the Data Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability,
- where relevant, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal,
- the right to lodge a complaint with a Supervisory Authority; and
- the existence of Automated decision-making, including Profiling, and at least when such Processing produces legal effects concerning the Data Subject or similarly significantly affects them, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

(iv) Where Personal Data has not been obtained from the Data Subject, the BCR Affiliated Companies acting as Data Controller must provide the Data Subject with the information listed in the above paragraph (i), as well as the following additional information:

- the categories of Personal Data concerned, and
- from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources,

(v) Where Personal Data has not been obtained from the Data Subject, a BCR Affiliated Company acting as Data Controller must provide the above mentioned information to the Data Subjects, either:

- within a reasonable period after obtaining the Personal Data, but at the latest within one (1) month, having regard to the specific circumstances in which the Personal Data is processed;
- if the Personal Data is to be used for communication with the Data Subject, at the latest at the time of first communication to that Data Subject; or
- if a disclosure to another Recipient is envisaged, at the latest when the Personal Data is first disclosed.

(vi) This information requirement does not apply:

- where and insofar the Data Subject already has the information for direct or indirect collection of Personal Data;
- the provision of such information proves impossible or would involve disproportionate effort for indirect collection only. In such case, the BCR Affiliated Company shall take appropriate measures to protect Data Subject's privacy rights and legitimate interests, including making the information publicly available;
- where such indirect collection is expressly laid down by applicable law to which the BCR Affiliated Company is subject and which provides appropriate measures to protect Data Subject's legitimate interests; or
- where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by applicable law, including statutory obligation of secrecy.



## **2.1.2 Purpose limitation**

Personal Data are collected and processed for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

## **2.1.3 Data minimization and accuracy**

The BCR Affiliated Companies will ensure that Personal Data processed is:

- adequate, relevant and limited to what is strictly necessary for the purposes for which they are originally collected and processed, and
- accurate and, where necessary, kept up to date. Consequently, inaccurate or incomplete Personal Data must be rectified, supplemented or erased without delay. In order to ensure that the Personal Data processed by BCR Affiliated Company remains accurate and up-to-date, BCR Affiliated Company actively encourages Data Subjects to inform it of any changes and intends to develop user-friendly interfaces and tools allowing Data Subjects to directly update their Personal Data.

## **2.1.4 Limited storage periods**

The BCR Affiliated Companies will not keep the Personal Data in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Personal Data are processed.

However, Personal Data may be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or as required by applicable Laws and Regulations, and in line with the Airbus' Data Retention policy and/or any other applicable local data retention policies. The BCR Affiliated Companies will store Personal Data only in a secure manner in accordance with the Airbus Security Requirements (Appendix 7).

## **2.2 Processing of Special Categories of Personal Data**

BCR Affiliated Company will prohibit the Processing of Special Categories of Personal Data, unless where one or more of the following legal basis apply:

- The Data Subject has given his or her explicit Consent to the Processing of those Personal Data for one or more specified purposes, except where applicable Laws and Regulations provide that the prohibition referred to above may not be lifted by the Data Subject;
- Processing is necessary for the purposes of carrying out the obligations and specific rights of a BCR Affiliated Company or of the Data Subject in relation to employment and social security and social protection law in so far as it is authorized by applicable Laws and Regulations or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
- Processing is necessary to protect the vital interests of the Data Subject(s) or of another person where the Data Subject is physically or legally incapable of giving their Consent;

- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members or to the former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body to a Third Party without the Consent of the Data Subject(s);
- Processing relates to Personal Data which are manifestly made public by the Data Subject(s);
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest, on the basis of applicable Laws and Regulations which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject(s);
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of applicable Laws and Regulations or pursuant to contract with a health professional and under the responsibility of a professional subject to the obligation of professional secrecy under applicable national law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under applicable Laws and Regulations established by national competent bodies;
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of applicable Laws and Regulations which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject(s), in particular professional secrecy;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with EU GDPR and/or applicable Laws and Regulations, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject(s).

## **2.3 Processing of Personal Data relating to criminal convictions and offences**

BCR Affiliated Companies must ensure that the Processing of Personal Data relating to offences and criminal convictions or security measures are carried out only under the control of official authority, or as authorized by applicable Laws and Regulations subject to appropriate safeguards for the rights and freedoms of Data Subjects.

## **2.4 Security**

### ***2.4.1 Processing in compliance with the Airbus' Security Requirements***

The BCR Affiliated Companies will adopt appropriate technical and organisational measures to ensure security of Personal Data transferred (see Appendix 7). Where necessary, and following performance of a Transfer Impact Assessment, the BCR Affiliated Companies will implement additional technical, contractual and organisational measures as relevant (see section 3.5 below) to protect the Personal Data transferred.

## **2.4.2 Obligations relating to Personal Data Breaches**

In the event of an actual and/or suspected Personal Data Breach, the relevant BCR Affiliated Company is responsible to inform promptly the Privacy Focal Point within the relevant BCR Affiliated Company and the Privacy Team.

The Privacy Team and/or relevant BCR Affiliated Company through its Privacy Focal Point and in coordination with Privacy Team will assess whether or not the Personal Data Breach needs to be notified to the relevant Supervisory Authority(ies) and/or to the concerned Data Subjects. If so the Personal Data Breach will be promptly notified to the competent Supervisory Authority(ies) by the Privacy Team and/or relevant Affiliate Privacy Focal Point and if possible within seventy-two (72) hours from the time the relevant BCR Affiliated Company being aware of the Personal Data Breach; if the Personal Data Breach needs to be notified to the concerned Data Subject(s), this will be undertaken without undue delay.

The Privacy Team will maintain a Record and keep evidence(s) of any and all Personal Data Breaches, including but not limited to the facts relating to the Personal Data Breach, its effects and the remedial action taken, regardless of whether the Personal Data Breach has been notified or not to the Supervisory Authority and/or to the concerned Data Subject(s). Such documentation will be made available to the Supervisory Authority upon request.

## **2.5 Processing and Sub-processing**

The BCR Affiliated Companies must ensure that processors and/or sub-processor(s) if any (appointed either within Airbus Companies or Third Party acting on their behalf) will provide sufficient guarantees to meet and comply with EU GDPR requirements by adopting amongst other, appropriate technical and organisational security measures.

The BCR Affiliated Companies may use as processor(s) and/or sub-processor(s) other BCR Affiliated Companies based or located in a Third Country. In such a case, such BCR Affiliated Companies will implement an Intra-Group Data Processing Agreement or "**IGDPA**" (See template in Appendix 9).

If a BCR Affiliated Company uses Third Parties as processor(s) or sub-processor(s), such BCR Affiliated Company will only appoint sub-processors that commit to comply with all the requirements as set out in Article 28.3 of the EU GDPR in the form of a written binding data processing agreement and EU Standard Contractual Clauses (or any other appropriate Personal Data Transfer mechanism as required by applicable Laws and Regulations set out below) where applicable.

## **2.6 Personal Data Transfers to Third Parties whether as Data Controllers or Processors**

BCR Affiliated Companies transferring Personal Data to Third Parties shall implement appropriate Personal Data Transfer mechanisms with Third Parties (acting as Processors or Controllers) to protect the Personal Data Transfers including security and confidentiality measures.

Such Personal Data Transfer mechanisms include, in particular :

- EU Standard Contractual Clauses approved by European Commission decision No. (2021) 3972 of June 4th, 2021 or any other subsequent or similar document issued by any other competent Supervisory Authority,
- adequate protection provided according to the EU GDPR : articles 45 (transfers on the basis of an adequacy decision by the European Commission), 46 (transfers subject to appropriate safeguards, including binding corporate rules, approved codes of conduct, approved certification, etc.), 47 (rules applicable to binding corporate rules) and 48 (transfers based on an international agreement or other lawful basis),

- a derogation according to Article 49 (derogations for specific situations, including the Data Subject's Consent, performance of a contract, etc.) applies.

Such Personal Data Transfer mechanisms shall be completed by any supplementary technical, contractual or organisational measures if required further to the performance of the Transfer Impact Assessment as described in section 3.5.

## 2.7 Data Subject rights

The BCR Affiliated Companies acting as Data Controller shall guarantee each and every Data Subject the following rights:

- **Right of access:** Data Subjects have the right to access the Personal Data concerning them processed by BCR Affiliated Company.
- **Right to rectification:** Data subjects have the right to obtain from BCR Affiliated Company without undue delay the rectification of inaccurate Personal Data concerning them or the right to have incomplete Personal Data completed.
- **Right to erasure** ("right to be forgotten"): Data Subjects have the right to obtain from BCR Affiliated Company, the erasure of Personal Data concerning them without undue delay notably when (i) the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, (ii) the Data Subject withdraws Consent on which the Processing is based and where there is no other lawful basis for the Processing, (iii) the Data Subject objects to the Processing and there are no overriding legitimate grounds for the Processing, (iv) the Personal Data has been unlawfully processed, (v) the Personal Data has to be erased for compliance with a legal obligation in applicable law to which the Data Controller is subject, (vi) the Personal Data have been collected in relation to the offer of information society services.

BCR Affiliated Company shall not respond to such right of erasure / right to be forgotten, if the Personal Data is necessary for (i) exercising the right of freedom of expression and information, (ii) compliance with a legal obligation, (iii) reasons of public interest in the area of public health (iv) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, (v) the establishment, exercise or defence of legal claims.

- **Right to restriction:** Data Subjects have the right to obtain from BCR Affiliated Company, restriction of Processing where (i) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling BCR Affiliated Company to verify the accuracy of the Personal Data, (ii) the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests instead, restriction of their use, (iii) BCR Affiliated Company no longer needs the Personal Data for the purposes of the Processing, but the Data Subject requires them for the establishment, exercise or defence of legal claims, (iv) Data Subject has objected to Processing, restriction applies pending the verification whether the legitimate grounds of BCR Affiliated Company override those of the Data Subject.

Data Subject who has obtained restriction of Processing shall be informed by the BCR Affiliated Company acting as Data Controller or Processor before the restriction of Processing is lifted.

- **Right to data portability:** Data Subjects have the right to receive the Personal Data concerning them, which they have provided to BCR Affiliated Company, in a structured, commonly used and machine-readable format and have the right to transmit those Personal Data to another service provider or Third Party. Such right to portability will apply, subject to the rights and freedoms of others, in the following cases: (i) the

Processing is based on Consent or a contract, and (ii) the Processing is carried out by automated means.

- **Right to object:** Data Subjects have the right to object, at any time to Processing of Personal Data concerning them which is used for marketing purposes or leads BCR Affiliated Company to take decision based solely on Automated decision-making, including Profiling, which produces legal effects concerning a Data Subject or similarly significantly affects him or her, and based on the following lawful basis for Processing: (i) the performance of a task carried out in the public interest or in the exercise of official authority vested in BCR Affiliated Company, or (ii) the purposes of the legitimate interests pursued by BCR Affiliated Company or by a Third Party.

If the Data Subject exercises such right to object, the BCR Affiliated Company acting as Data Controller shall no longer process the Personal Data unless such BCR Affiliated Company demonstrates compelling legitimate grounds for the Processing or for the establishment, exercise or defence of legal claims.

However, if the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.

Applicable local Laws and Regulations may provide for additional Data Subject rights.

Data Subjects can exercise their rights or file a claim by contacting:

- preferably the specific personal data protection mailbox made available in the applicable Privacy Notice;
- Alternatively, the dedicated personal data protection mailbox set up by the Privacy Team at [dataprotection@airbus.com](mailto:dataprotection@airbus.com); or by mail: Airbus SAS, Legal & Compliance, Personal Data Protection Officer, 2 rond-point Emile Dewoitine 31700 Blagnac cedex France;
- or, for Airbus Employees, their line manager(s), HR Business Partners and/or the Airbus Ethics and Compliance organisation through notably the Airbus Ethics and Compliance Openline.

With the support of the relevant BCR Affiliated Company, the Privacy Team and/or relevant BCR Affiliated Company Privacy Focal Point shall coordinate and respond to the request of Data Subjects without undue delay and in any event within one (1) month from receipt of the Data Subject request, unless restrictive period applies under local law. This period may be extended by two (2) further months where necessary.

If the Data Subject is not satisfied by the response, the Data Subject has the right to lodge a complaint with the competent Supervisory Authority.

## 2.8 Prior formalities

The fact that the BCR Affiliated Companies comply with all the rules set forth in this Chapter 2 does not release them from their obligation to fulfil prior formalities, if any, with the relevant Supervisory Authorities as required by the applicable local Laws and Regulations.

## 3. ACCOUNTABILITY MECHANISMS

The BCR Affiliated Companies are responsible for and must be able to demonstrate compliance with the BCR notably by implementing the following documents and principles:

## 3.1 Records of Processing activities

Each BCR Affiliated Company acting as Data Controller and/or Processor is responsible to maintain a Record of the Processing activities under its responsibility as set out in Article 30 of the EU GDPR.

The Record must be in writing, including electronic form. The BCR Affiliated Company will use the Tool of the Privacy Team and seek the guidance of the Privacy Team where necessary.

The BCR Affiliated Company will make the Record available at any time to the Privacy Team which will be entitled to disclose it to the Supervisory Authority upon request by the latter.

## 3.2 Privacy Impact Assessment (PIA)

When a Processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the privacy rights for Data Subject(s), the BCR Affiliated Company acting as Data Controller is responsible to, prior to the Processing, carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data (PIA) unless otherwise agreed by Privacy Team.

Where a PIA indicates that the Processing would result in a high risk in the absence of measures taken by the BCR Affiliated Company acting as Data Controller to mitigate the risk, the competent Supervisory Authority, prior to Processing, shall be consulted.

## 3.3 Privacy by design and by default

### 3.3.1. Privacy by design

The BCR Affiliated Companies acting as Data Controller shall, both **at the time of the determination of the means for Processing and at the time of the Processing itself**, implement appropriate technical and organisational measures designed to implement data protection principles, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the requirements of the EU GDPR and protect the rights of Data Subject(s). This principle shall apply to every project, product or service provided by BCR Affiliated Companies.

### 3.3.2. Privacy by default

The BCR Affiliated Companies acting as Data Controller shall implement appropriate technical and organisational measures for ensuring that, **by default**, only Personal Data which are necessary for each specific purpose of the Processing are processed. This obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default Personal Data Protection principles as expressed in section 2.1 above are complied with.

## 3.4 Other accountability mechanisms implemented by Airbus

Without limitation, the BCR Affiliated Companies must also :

- Provide training / awareness campaigns on data privacy and BCR to the Personnel that have permanent or regular access to Personal Data or who are involved in the development of tools used to process Personal Data (as described in Chapter 4 below);
- Carry out regular internal audits to ensure verification of compliance with BCR (as described in section 5.2 below);
- Roll out Internal policies relating to Personal Data implementing the Directive, the Method and BCR.

## 3.5 Transfer Impact Assessment (TIA)

BCR Affiliated Companies shall, when necessary, perform Transfer Impact Assessment taking the following into account:

- the specific circumstances of the transfer (length of the processing chain, number of actors involved, transmission channels used, intended onward transfers, type of recipient, purpose of processing, categories and format of the transferred personal data, economic sector in which the transfer occurs, the storage location of the data transferred);
- the laws and practices of the third country of destination (including those requiring the disclosure of data of public authorities or authorising access by such authorities in light with the specific circumstances of the transfer and the applicable limitations and safeguards);
- any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under this BCR, including measures applied during transmission and to the processing of the Personal Data in the country of destination.

Any Transfer Impact Assessment shall be documented in writing and retained by the Data Exporter and Data Importer at least for the duration of the transfer. The Transfer Impact Assessment shall be made available to the competent Supervisory Authority on request.

## 4. INFORMATION AND TRAINING

In order to ensure that all the Data Subjects are informed of the BCR and of Airbus' rules on personal data protection, Airbus will take all suitable steps and means, to make the BCR as well as the Directive and Method, the Airbus Internal Privacy Notice ("**Privacy Documentation**") and the Airbus Code of Conduct available to the Data Subjects, in particular by publishing them on the Airbus corporate website, Intranet and/or will also make available e-learning modules on data privacy. In addition, the BCR Affiliated Companies may consider further relevant steps and means to ensure that all the Airbus Employees, Customers, Suppliers and Business Partners receive the necessary information.

The BCR Affiliated Companies are obliged to convey the information contained in the BCR by setting up programs intended to increase Employees' awareness of the Personal Data protection legal framework and by organising training courses on the BCR intended to Employees that have permanent or regular access to Personal Data or are involved in the collection of Personal Data or in the development of tools used to process Personal Data to which the BCR apply as described in Airbus "Training and Communication Plan" detailed in Appendix 8.

## 5. GUARANTEES FOR BCR IMPLEMENTATION

### 5.1 Airbus Privacy Governance

The Airbus Privacy Team as described in Appendix 10 and led by Airbus Personal Data Protection Officer is responsible for promoting, supporting and supervising BCR, EU GDPR and any other applicable privacy legal obligations compliance by the BCR Affiliated Companies.

The Privacy Team is independent and is supported by Airbus top management to fulfil its tasks as further detailed in the Method (Appendix 3(b)).

Each BCR Affiliated Company shall appoint in relevant area(s) of its organisation and as necessary, one or several Privacy Focal Point(s) to represent the BCR Affiliated Company and associated businesses, in relation to BCR implementation.

Each BCR Affiliated Company shall involve the relevant Privacy Focal Point(s) in a timely manner, in all issues and/or projects using and/or impacting Personal Data, including changes on existing processes or tools and the creation of new processes and tools when such processes or tools involve the Processing of Personal Data.

The BCR Affiliated Company Privacy Focal Point(s) shall notably be responsible for recording Personal Data Processing in the Tool made available by the Privacy Team, undertaking Data Protection Impact Assessment and/or Transfer Impact Assessment where needed, seeking guidance from and reporting issues to the Privacy Team as necessary, and facilitating the Privacy Team's action with the relevant BCR Affiliated Companies.

More information on the Airbus Privacy Governance may be found in Appendix 10 and in the Method (Appendix 3(b)).

### 5.2 Audits

To ensure proper compliance with the BCR, Airbus will define a yearly Privacy Audit Program.

Such audits will be performed by the Privacy Team. The audit will be based on various means: questionnaire, documentation, system review, floor inspection, interview, (...) as detailed in Appendix 11.

The Privacy Audit Program is described in Appendix 11 and covers all the significant aspects of the BCR, and its applicable Appendices (including Directive and Method), including methods of ensuring that corrective actions will take place.

The results of the audit in connection with the BCR will be communicated to the relevant BCR Affiliated Company management and BCR Affiliated Company Privacy Focal Point(s).

They will also be made accessible to the relevant Supervisory Authorities when requested. Supervisory Authorities can carry out a privacy audit of any BCR Affiliated Companies if required.

If the competent Supervisory Authority carries out the privacy audit itself, all concerned BCR Affiliated Companies will cooperate with the competent Supervisory Authority conducting the audit.

### 5.3 Internal Complaint Procedures

Airbus has set up an internal complaint handling procedure enabling any Data Subject to file complaints about any BCR Affiliated Company's failure to comply with the BCR. The procedure by which a Data Subject may file a complaint is set out as follows:



- preferably the specific data protection mailbox made available in the applicable privacy notice;
- alternatively, the dedicated data protection mailbox set up by the Privacy Team at [dataprotection@airbus.com](mailto:dataprotection@airbus.com); or by mail: Airbus SAS, Legal & Compliance, Personal Data Protection Officer, 2 rond-point Emile Dewoitine 31700 Blagnac cedex France; or
- For Airbus Employees, their line manager(s), its HR Business Partners and/or the Airbus Ethics and Compliance organisation through notably the Airbus Ethics and compliance Openline.

The Privacy Team, which is in charge of supervising the handling of complaints by Data Subject(s), is granted an appropriate level of independence to advise the relevant BCR Affiliated Company and deal with such complaints.

Regardless of whether the internal complaint process has been exhausted or not and if the Data Subject remains unsatisfied after having exercised its rights as described in section 2.7 above, the Data Subject has the right to lodge a claim before the competent court and/or before the competent Supervisory Authority.

If the complaint is justified, the relevant BCR Affiliated Company will implement the relevant measures it deems adequate to remedy the failure. The BCR Affiliated Company acting as Data Controller may seek the guidance of the relevant BCR Affiliated Company Privacy Focal Point and/or Privacy Team.

In compliance with labour legislation, Airbus and BCR Affiliated Companies policies and procedures and employment contract, Employees found to be negligent may be subject to disciplinary action.

Data Subjects are duly informed of the complaint handling procedure and how to file a complaint through the Method, these BCR and other Privacy Information notices published by Airbus on the corporate website, intranet and other media as described in Article 4 above.

## 5.4 Responsibility for BCR implementation

Once a BCR Affiliated Company adheres via a Letter of Adherence (as attached in Appendix 6), such BCR Affiliated Company and its management are bound to apply the BCR in the course of their Personal Data Processing activities.

## 5.5 Liability

As a matter of principle, where a Data Subject suffers from a damage as a result of a breach of the BCR by a BCR Affiliated Company and subject to such breach and damage being evidenced by the Data Subject, the BCR Affiliated Company which caused the damage :

- shall be liable towards the Data Subject, and
- shall immediately take the necessary action to remedy the damage and indemnify the Data Subject for any damages arising out the violation of the BCR by such BCR Affiliated Company.

To ensure the proper enforcement of Data Subject's rights under the BCR in case of Personal Data Transfer from an EU/EEA, BCR Affiliated Company (Data Exporter) to a Third Country BCR Affiliated Company (Data Importer), the Data Exporter shall be deemed to be jointly and severally liable with the Data Importer for damages arising out of the violation of the BCR provisions by the Data Importer.

The Data Subject is entitled to take action against and be indemnified by the Data Exporter, the Data Importer or by both.

The Data Subject can choose to lodge their claims, at their choice, either with the Supervisory Authority in the EU country of its usual residence, place of work or place of the alleged infringement or

the competent courts of the EU country where the BCR Affiliated Company (Controller or Processor) has an establishment or where the Data Subject has its usual residence.

The BCR Affiliated Companies accept for this purpose the competence of the courts or other relevant authorities in the EEA where the Data Exporter is established.

In case the Data Exporter has indemnified the Data Subject as a result of the joint and several liability above, then the Data Importer shall indemnify the Data Exporter for the amount paid to the Data Subject in proportion of its liability in the damage.

For the avoidance of doubt, in no event may a Data Subject be entitled to recover damages more than once in respect of the same losses suffered as a result of any violation of this BCR or a breach of any applicable personal data protection Laws and Regulations.

## 6. THIRD PARTY BENEFICIARY RIGHTS

A Data Subject whose Personal Data are processed under the BCR can enforce the following elements of the BCR before the competent Supervisory Authority or court in order to seek judicial remedies and right to obtain redress and, where appropriate, compensation in case of a breach of the enforceable principles of the BCR as enumerated below by a BCR Affiliated Company.

For a detailed description, please refer to the respective clauses in the BCR as listed below:

- Data Protection principles (as described in Chapter 2 of the BCR; the following sections of the Method: (i) section 5 (lawfulness and fairness, data minimisation, purpose limitation, data accuracy/quality, storage limitation, security, integrity, confidentiality, transparency, need to know, privacy by design, privacy by default, accountability), (ii) section 6 (lawfulness of Personal Data Processing), (iii) section 7 (Processing of Special Categories of Personal Data), (iv) section 8 (Privacy Impact Assessment), (v) section 10 (security and confidentiality measures), (vi) section 14 (Personal Data Transfers))
- Transparency and easy access to BCR (BCR, Chapter 4; A copy of these BCR is also available on Airbus website and intranet)
- Rights of access, rectification, erasure, restriction, objection to the processing, right not to be subject to decisions based solely on automated processing, including Profiling (BCR, section 2.7; Method, section 9.3)
- National Laws and Regulations preventing respect of BCR (BCR, Chapter 7)
- Right to complain through the internal complaint mechanism of the BCR Affiliated Companies (BCR, section 5.3; Method, section 9.4)
- Cooperation duties with Supervisory Authorities (BCR, Chapter 8)
- Liability and jurisdiction provisions (BCR, sections 5.4 and 5.5).

However, the Data Subjects may not extend their rights to those elements of the BCR implemented through internal mechanisms within BCR Affiliated Companies such as detail of training, audit programmes, Airbus Privacy Organisation, and mechanism for updating of the BCR.

## 7. CONFLICT OF RULES

## 7.1 General rules

BCR Affiliated Companies will comply with any applicable local Laws and Regulations relating to personal data protection and will ensure that any Personal Data collected and processed, is done in accordance with the provisions of the BCR.

If the local Laws and Regulations require a higher level of protection for Personal Data it will take precedence over the BCR. In any event, Personal Data shall be processed in accordance with the applicable Laws and Regulations as provided by Article 3 of EU GDPR and the relevant local legislation.

In case of a conflict the Privacy Team will provide guidance on what action to take and may consult the relevant Supervisory Authority if needed.

## 7.2 Disclosure access request by Third Country public authority

If a BCR Affiliated Company in a Third Country (the Data Importer) cannot apply the BCR due to local Laws and Regulations, or has reasons to believe that the Laws and Regulations applicable to such BCR Affiliated Company prevents it from fulfilling its obligations under the BCR or has substantial adverse effect on the guarantees provided by the BCR, it must immediately contact the Privacy Team, the BCR Affiliated Company (Data Exporter) and relevant BCR Affiliated Company Privacy Focal Point.

This includes any legally binding request for disclosure of the Personal Data by a local law enforcement authority or state security body or when becoming aware of any direct access by public authorities to personal data transferred pursuant to this BCR. In such a case, the Privacy Team will ensure that the requirements of the Article 48 of the EU GDPR are satisfied as a first resolution step prior to informing the competent Supervisory Authority about the request and, where necessary, the Data Subject. Such notification will include information about the data requested, the requesting authority or body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

Following the notification from the Data Importer to the Privacy Team pursuant to the above paragraph, or if the Data Exporter otherwise has reason to believe that the Data Importer can no longer fulfil its obligations under the BCR, the Data Exporter and Data Importer shall promptly identify appropriate technical and organisational measures that can be implemented by one or both BCR Affiliated Companies to ensure security and confidentiality of the Personal Data transferred in such Third Country.

If no appropriate safeguards for such transfer can be ensured or if instructed by the competent Supervisory Authority or the Data Exporter as Data Controller, the transfer of Personal Data shall be suspended.

In case of disclosure access request from local public authority to the Data Importer, the Data Importer, under the guidance of Privacy Team shall apply the following main steps:

- the legality of any request for disclosure from a public authority shall be reviewed by relevant Airbus and BCR Affiliated Company legal department;
- any disproportionate or unlawful request must be challenged and pursue possibilities of appeal

During this period, the Data Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. Personal Data shall not be disclosed to the public authority by the Data Importer until required to do so under the applicable procedural rules.

To the extent permitted by law and when appropriate, the BCR Affiliated Company that is importing the data must redirect such disclosure access requests to the BCR Affiliated Company that is exporting the data (Data Exporter).

If in specific cases the suspension and/or notification to the competent Supervisory Authority is prohibited, the requested BCR Affiliated Company in the Third Country (Data Importer) will use its reasonable efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If, in the above cases, despite such efforts, the requested BCR Affiliated Company is not in a position to notify the competent Supervisory Authorities, it must commit to annually provide general information on the requests it received to the competent Supervisory Authorities (e.g., number of applications for disclosure, type of data requested, requester if possible, etc.). Any disclosure access request must be documented by the Data Importer (including any legal assessment and any challenge to the request for disclosure) preserved at least for the duration of the transfer and made available to the competent Supervisory Authority on request and/or to the Data Exporter.

If legally compelled to disclose such Personal Data, the Data Importer shall provide the minimum of information (including Personal Data) necessary to the request, based on a reasonable interpretation of the request.

## 8. COOPERATION WITH THE COMPETENT AUTHORITIES

The BCR Affiliated Companies undertake to cooperate with the Supervisory Authorities, particularly by applying any recommendations and advice the Supervisory Authorities may make and by responding within a reasonable timeframe to requests the Supervisory Authorities may make regarding the BCR, including audit request.

## 9. UPDATING THE BCR

The Privacy Team is responsible for (i) updating the BCR and the list of BCR Affiliated Companies and must make them available to the Data Subjects or competent Supervisory Authorities upon request for all intents and purposes, (ii) approving any amendment of the BCR and (iii) communicating the changes to the management of the BCR Affiliated Companies and BCR Affiliated Company Privacy Focal Point without undue delay.

The Airbus Privacy Team undertakes to inform the competent Supervisory Authority of any substantial modifications to the BCR (that may affect the level of the protection offered by the BCR) with a brief explanation of the reasons justifying the update and to, annually, provide the list of BCR Affiliated Companies to the competent Supervisory Authority.

## 10. BINDING NATURE OF THE BCR

These BCR are binding upon BCR Affiliated Companies and their respective Employees.

To ensure that all the BCR Affiliated Companies are bound by the BCR including all the Privacy Documentation which implements the BCR principles, Airbus requests the management of each BCR Affiliated Company to sign the Letter of Adherence (attached in Appendix 6) as indicated in Article 2 of the BCR.

To make the BCR enforceable to Employees:

# AIRBUS

Binding Corporate Rules

Airbus Amber

- BCRs are referred to in the Airbus Directive and Method (attached in Appendix 3), are published on Airbus's internal portal and website and applicable to all employees of BCR Affiliated Companies.
- Where applicable, the content of the BCRs is incorporated in the BCR Affiliated Company's internal policies that are sometimes subject to the local work council information / consultation to ensure that Employees are aware of their rights and obligations with respect to personal data protection.

## 11. TERMINATION

The BCR Affiliated Company (acting as Data Importer), which ceases to be bound by the BCRs may keep, return or delete the Personal Data received under the BCRs.

If the BCR Affiliated Companies acting respectively as Data Exporter and Data Importer in relation to a personal data transfer agree that Personal Data may be kept by the Data Importer, appropriate personal data transfer protection must be maintained in accordance with EU GDPR.

## 12. NON-COMPLIANCE

The BCR Affiliated Company (acting as Data Importer) undertakes:

- (i) to promptly inform the BCR Affiliated Company (acting as Data Exporter) if it is unable to comply with the BCRs, for whatever reason, including the situations further described in section 7.2 above;
- (ii) where in breach of the BCRs or unable to comply with them, to suspend the transfer with the BCR Affiliated Company (acting as Data Exporter);
- (iii) at the choice of the BCR Affiliated Company (acting as Data Exporter), immediately return or delete the Personal Data (including any copies) that has been transferred under the BCRs in its entirety where :
  - the BCR Affiliated Companies have suspended the transfer, and compliance with the BCRs is not restored within a reasonable time, and in any event within one (1) month of suspension; or
  - the Data Importer is in substantial or persistent breach of the BCRs; or
  - the Data Importer fails to comply with a binding decision of a competent court or competent Supervisory Authority regarding its obligations under the BCRs.

Until the Personal Data is deleted or returned, the Data Importer should continue to ensure compliance with the BCRs.

In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer should warrant that it will continue to ensure compliance with the BCR, and will only process the Personal Data to the extent and for as long as required under that local law.

For cases where applicable law and/or practices affect compliance with the BCR, section 7 applies.

\* \* \*  
\*