AIRBUS GROUP

BINDING CORPORATE RULES

AIRBUS GROUP

Introduction

The Binding Corporate Rules (hereinafter "BCRs") of the Airbus Group finalize the Airbus Group's provisions on the protection of Personal Data. These BCRs are intended to ensure a suitable level of protection in compliance with European Directive 95/46 dated 24 October 1995 (hereinafter referred to as "the Directive") when the Personal Data specified in the present document are transferred within the Airbus Group for the purposes of the Airbus Group's worldwide business.

The Airbus Group is committed to the right to privacy and protection of Personal Data in its Standards of Business Conduct and specifies in its Data Protection Policy the principles to be complied with within the Airbus Group in application of the said Standards.

The Binding Corporate Rules define the minimum standard of protection of Personal Data and Information Security measures and the Affiliated Companies are entitled to implement more protective policies and regulations on this matter.

1. SCOPE

The purpose of the BCRs is to ensure an adequate level of Personal Data protection in the Airbus Group in countries which are not members of the European Economic Area (hereinafter "EEA") in order to allow the Transfer of all Personal Data from the Affiliated Companies located in one Member State of the EEA to the Affiliated Companies in a Third Country and vice versa.

The BCR applies for all of the companies in the Airbus Group, i.e. Airbus Group N.V. and all of its dependent Subsidiaries and their Employees.

The BCRs apply to all Personal Data of the Airbus Group subject to EEA data protection legislation, transferred and processed within the Airbus Group outside of the EEA, in a Third Country.

2. RULES APPLICABLE TO TRANSFER AND PROCESSING

For Transfers and Processing of Personal Data, the principles described in the BCRs and Airbus Data Protection Policy applies to all Affiliated Companies.

In order to provide the Data Subject with an equivalent and suitable level of protection, the Affiliated Companies agree to comply with the principles described below and in the Data Protection Policy, i.e.;

- To collect, transfer and process the Personal Data fairly, transparently and lawfully
- To collect, transfer and process the Personal Data for determined, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,
- To collect, transfer and process Personal Data that are accurate, suitable, relevant and not excessive for the purposes of the Transfer and Processing, consequently, inaccurate or incomplete Personal Data must be rectified, supplemented, erased or their further processing must be suspended
- Not to keep the Personal Data beyond the length of time needed for Processing and Transfer,

- To adopt suitable means of security to protect the Personal Data during Transfer and Processing, particularly in compliance with the relevant Information Systems Policies in which the common principles are described.
- To inform the Data Subject of how his/her Personal Data is being processed. As a matter of principle, Personal Data will be collected directly from the Data Subject concerned. When collecting the Personal Data, the Data Subject is either be clearly aware of or appropriately be informed
- To provide the Data Subject the necessary information of his/her Personal Data if it has not been obtained from the Data Subject at the time of undertaking, the recording of their Personal Data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed.

Furthermore, the Processing of Personal Data, which are transferred, should be based on legal basis such as

- The Data Subject has unambiguously given his Consent; or
- The Processing of Personal Data is necessary for the performance of 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; or
- The Processing of Personal Data is necessary for compliance with a legal obligation to which the group is subject; or
- The Processing of Personal Data is necessary to save the vital interest of the Data Subject; or
- The Processing of Personal Data is necessary for the performance of a task carried out in the public interest or in the interest of the third party to whom the data are disclosed; or
- The Processing of Personal Data is necessary for the purposes of legitimate interests pursued by the Data Controller except where such interests are overridden by the interest or fundamental rights and freedom of the Data Subjects.

In cases where Sensitive Data are transferred, the processing must be based on the following basis:

- The Data Subject has given his explicit Consent to the Processing of Sensitive Data, except where the applicable laws prohibit it; or
- The necessity for the purposes of carrying out the obligations and specific rights of the Data Controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
- The Processing of Personal Data is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his Consent; or
- the Processing of Sensitive Data which are manifestly made public by the Data Subject; or
- the Processing of Sensitive Data is necessary for the establishment, exercise or defense of legal claims; or
- the Processing of the Sensitive Data is required for reasons of substantial public interest laid down either by national law or decision of the Competent Authority; or

- The Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Sensitive Data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Affiliated Companies affected by Data Transfer will take all suitable steps, in particular by including suitable clauses in contracts such as EU Standard Contractual Clauses approved by EU Commission 2001/497/EC or 2004/915/EC or 2010/87/UE or by adequate contractual means according to articles 16, 17, 25 and 26 of the Directive, with subcontractors, processors or Third Party controllers regarding Data Transfer and security and confidentiality measures.

Affiliated Companies located within the EEA will ensure that the Data Subjects have been informed of the transfer and that Data Subjects have been provided with their rights to access, rectify, complete, update, delete, object and block the information concerning them.

The fact that the Affiliated Companies complies with all the rules does not release them from their obligation to fulfill all the prior formalities with the relevant National Authorities as required by the applicable legislation.

3. INFORMATION AND TRAINING

In order to ensure that all the Data Subjects are informed of the BCRs and of the Airbus Group's rules on Data Protection, the Airbus Group will take all suitable steps and means to make the BCRs, as well as the Standards of Business Conduct and the Data Protection Policy available to the Data Subjects, in particular by making them available on the Airbus Group's corporate website and Intranet. In addition, the Affiliated Companies may consider further relevant steps and means to ensure that all the Airbus Group's Employees, Customer, Supplier and Partners receive the necessary information.

The Affiliated Companies affected by Data Transfers are obliged to convey the information contained in BCRs by setting up programs intended to increase employees' awareness of the special nature of Personal Data and by organizing training courses on the protection of Personal Data intended for people working directly or indirectly for Airbus Group, EEA Affiliated Companies, Affiliated Companies in a third Country or a sub-processor who has 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 BCRs apply.

4. GUARANTEES OF BCRs IMPLEMENTATION

The Airbus Group has appointed a Data Protection Organization to oversee and ensure the implementation of the BCRs. The Airbus Group Data Protection Officer is independent, appointed by the Group Chief Human Resources Officer and the Group Chief Compliance Officer, to supervise the adherence to national and international Data Protection regulations and is responsible for the Policies on Data Protection and privacy.

Audits

The Airbus Group will conduct annual audits to ensure that Personal Data are protected and the principles of the Directive and the BCRs are applied as follows:

- The **Airbus Group Data Protection Council** must verify the correct application of the in-house rules by :
  - sending a questionnaire to the management of all Affiliated Companies to ensure that the principles of the Policy and of the BCRs are applied correctly in each Affiliated Company;
  - leading audits in Affiliated Companies in full independence;

The Airbus Group Data Protection Council will meet annually to establish an annual audit plan. Each year, 8 audits are organized:

- Four outside the European Union
- Four within European Union

Audits cover all Affiliates and all BCRs principles. Independence is ensured through the audit process. An audit of an Affiliate would be carried out by another Data Protection Officer than the one in charge of advising the Affiliate concerned by the Audit.

and

- The Airbus Corporate Audit control includes Personal Data Protection matters in their annual audit plan in order to check the correct application of the in-house rules. The protection of Personal Data and in particular the BCRs are in the scope of these evaluations.

  Each year, the Airbus Corporate Audit plans a number of audits and it is entitled unrestricted to conduct Data Protection audits without the approval of the Data Protection Council.

A report of these evaluations is communicated to the relevant management and Data Protection Officer/ Privacy function of the audited Affiliated Companies and to the ultimate parent's board which may make recommendations to overcome any failings or shortfalls.

The Airbus Group undertakes that the results of the audit in connection with the BCRs could be brought to the attention of the relevant Competent Authorities when requested. In case the Competent Authority carries out the Data Protection audit itself all concerned Affiliated Companies will support the Competent Authority conducting the audit.

Complaint Procedure

The Airbus Group has set up a **complaint procedure** enabling any complaints of the Airbus Group's failings relative to the protection of Personal Data, particularly failure to comply with the BCRs. The Airbus Group undertakes that the Data Protection Officer in charge of handling complaints is granted an appropriate level of independency in the exercise of his/her function.

Any Data Subject who is asserting that there has been a breach of the BCRs may contact the Data Protection Officer in charge. In addition employees may contact their line managers or HR Business Partners, or use the dedicated mail-helpline. Details of this procedure are given in the Code of Ethics and the Data Protection Policy.

When a Data Subject files a complaint, the Data Protection Officer in charge has to reply within 2 months if no national legal requirement defines a shorter timeframe.

In case of rejection of the complaint by the Data Protection Officer in charge, the Data Subject will be informed within the answer about the possibility to escalate the complaint to the Group Data Protection Officer. So the Data Subjects can refer the matter to the Group Data Protection Officer for contesting the refusal and the Group data Protection Officer has to reply within 2 months.

If the Data Subject is not satisfied by this latest reply from the Group Data Protection Officer, he has the right to lodge a claim before the court/DPA.

Independent whether or not the internal complaint process has been exhausted the Data Subject has the right to lodge a claim before the court/DPA at any moment.

In compliance with labor legislation, Company policies and procedures and employment contract, individuals found to be negligent may be subject to disciplinary action.

The Affiliated Company responsible for the processing affected by a Data Transfer will set up, in compliance with the legislation applicable to the processing, a complaints process dedicated to Data Subjects not employed by the Group. The Affiliated Company will ensure that such Data Subjects are duly informed that the process exists and of how to access it.

If the failing cannot be corrected at local, company or divisional level, the Airbus Group Data Protection Officer will investigate and carry out appropriate corrective action.

Responsibility

The Parent Company will take all appropriate measures to encourage and promote the adherence of the BCRs within Airbus Group in order to ensure that the Affiliated Companies comply with the BCRs. Once an Affiliated Company adheres via a intra-group-agreement to the BCRs then the Parent Company delegates the responsibility for the implementation of the BCRs to the management of the Affiliated Companies. In order to strengthen the bindingness of Airbus BCRs the letter of adherence will be accompanied by a mission letter of the Airbus Executive Committee confirming the commitment of the Airbus Top Management with the BCRs and mentioning the respective liabilities as follows.

Liability

- In case of a transfer between two Data Controllers:

A Data Subject who has suffered damage as a result of any violation of the BCRs is entitled to receive compensation from the EEA Affiliated Companies or Affiliated Companies in a Third Country as Data Controller for the damage suffered.

The EEA Affiliated Company and the Affiliated Company in a Third Country will be liable vis-a-vis the Data Subject for their respective breach of the BCRs (“liability by due diligence”). In the event of such violation, the Data Subject may bring an action against either the EEA Affiliated Company or the Affiliated Company in a Third Country or both

If one of EEA Affiliated Company or Affiliated Company in a Third Country is held liable for a violation of the BCRs by the other, the latter will, to the extent to which it is liable, indemnify the first for any cost, charge, damages, expenses or loss it has incurred.

If the Data Subject files a complaint because of a breach of BCRs, the EEA Affiliated Company that transferred the Personal Data in a Third Country must prove that all suitable

measures were implemented to ensure compliance with the BCRs and whether the Affiliated Company in this Third Country is responsible for such breach.

If the EEA Affiliated Company can prove that the Affiliated Company in Third Country is responsible for such a breach providing evidence that it had put in place all suitable measures to ensure compliance with the BCRs, in this case it may discharge itself from any responsibility.

- In case of a transfer between a Data Controller and a Data Processor:

Data Subject, who has suffered damage as a result of any breach of the obligations referred to the BCRs by any party (EEA Affiliated Companies, Affiliated Companies in a Third Country or their sub-processor), is entitled to receive compensation from the data exporter for the damage suffered.

If a Data Subject is not able to bring a claim for compensation in accordance with the previous paragraph against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

If a data subject is not able to bring a claim against the data exporter or the data importer referred to in previous paragraphs, arising out of a breach by the sub-processor of any of their obligations referred to the BCRs because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The liability of the sub-processor is limited to its own processing operations under the Clauses.

Addressing Liability within contracts for Sub-processing

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter without the prior written consent of the data exporter. Where the data importer subcontracts its obligations, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer. Where the sub-processor fails to fulfil its Data Protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause for cases where the Data Subject is not able to bring a claim for compensation against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor is limited to its own processing operations under the Clauses.

The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to the data importer obligations, which shall be updated at least once a year. The list shall be available to the data exporter's Data Protection Competent Authority.

The provisions relating to data protection aspects for sub-processing of the contract referred in the BCRs is governed by the law of the Member State in which the data exporter is established.

5. THIRD PARTY BENEFICIARY RIGHTS

A Data Subject whose Personal Data are processed under the BCRs can enforce the following BCRs principles as rights before the appropriate Data Protection Authority or court where the EEA Affiliated Company that originated the transfer is based, in order to seek remedy and obtain compensation if a member of the group has not met the obligations and does not respect those principles.

More specifically, the principles which are enforceable as third party beneficiary rights are as follows and for a detailed description see the respective clauses in the Data Protection Policy and this BCR document:

- Purpose limitation (Data Protection Policy, § 5.3)
- Data quality and proportionality (Data Protection Policy, § 5.2 and § 5.4)
- Criteria for making the processing legitimate (Data Protection Policy, § 5.1 and § 6.1 – § 6.6)
- Transparency and easy access to BCRs (Data Protection Policy, § 10.1)
- Rights of access, rectification, erasure, blocking of data and object to the processing (Data Protection Policy, § 10.2 -§ 10.4)
- Rights in case automated individual decisions are taken (Data Protection Policy, § 9.1)
- Security and confidentiality (Data Protection Policy, § 11 - § 11.3)
- Restrictions on onward transfers outside of the group of companies (Data Protection Policy, § 7.1)
- National legislation preventing respect of BCRs (Data Protection Policy, § 4)
- Right to complain through the internal complaint mechanism of the companies (Data Protection Policy, § 14)
- Cooperation duties with Data Protection Authority (BCR document, clause 7)
- Liability and jurisdiction provisions (BCR document, clause 4)

6. CONFLICT OF RULES

If the local legislation requires a higher level of protection for Personal data it will take precedence over the Binding Corporate Rules. In any event Personal data shall be processed in accordance to the applicable law as provided by the Article 4 of the Directive 95/46/EC and the relevant local legislation.

If Affiliated Companies in a Third Country cannot apply to the present BCRs due to a local legislation they must immediately contact the Airbus Group Data Protection Officer.

In case of a conflict the Airbus Group Data Protection Officer will take a responsible decision on what action to take and will consult the relevant Data Protection Competent Authorities in case of doubt.

7. COOPERATION WITH THE COMPETENT AUTHORITIES

The Airbus Group undertakes to cooperate with the Competent Authorities, particularly by applying any recommendations and advice the Competent Authorities may make and by responding within a reasonable timeframe to requests the Competent Authorities may make regarding the BCRs, including audit requests.

8. UPDATING THE BCRs

The Airbus Group Data Protection Officer together with the Group Data Protection Council will validate any modifications of the BCRs and communicate the changes to the management of the Affiliated Companies.

The Airbus Group Data Protection Officer undertakes to inform the Competent Authority of any substantial modifications once a year.

The Airbus Group Data Protection Officer is responsible under all circumstances for updating the Group's BCRs and the list of Affiliated Companies and must make them available to the Competent Authorities for all intents and purposes.

No transfer to a new Affiliated Company is covered by BCRs until this Affiliated Company is effectively bound by the BCRs in written form and can deliver compliance with BCRs' rules.

9. CONTACT

Data subjects can raise any concerns with the Data Protection Officer of the relevant Affiliated Company or with the Airbus Group Data Protection Officer.

Airbus Group SAS
Airbus Group Data Protection Officer
HAP
1 rond-point Maurice Bellonte
31700 Blagnac cedex. France
Email: dataprotection@airbus.com
Internet: http.//www.airbusgroup.com