Atos Group Binding Corporate Rules as a Processor (Atos Group BCR-P)

Document last update: November 2024

Table of contents

List of changes

version	Date	Description	Author(s)
0.1	April 2023	Initial draft version	Andrew Jackson
0.8	March 2023	Draft version including changes made in October 2023 Atos Group BCR	Andrew Jackson
1.0	January 2024	Draft separate BCR-P version	Andrew Jackson Cecilia Fernandez
2.0	November 2024	Update of the draft separate BCR-P version	Thierry Peliks Sara Bonomi Bedirhan Kursun Yann Rim

Document Reviewed and Approved by Group DPO, Cecilia Fernandez Arredondo.

The French Data Protection Authority CNIL, approved the original document and reviewed newer versions in accordance with their official approval process.

1. Introduction

1.1. Purpose

Atos has always put data protection as one of its top priorities. As such, Atos has committed to applying best in class standards in terms of corporate responsibility (adhesion in the GRI, UN Global Compact). In order to guarantee the highest level of protection to the data it processes, as a Processor, Atos has adopted these Atos Group Binding Corporate Rules as a Processor ("Atos Group BCR-P").

These Atos Group BCR-P aim at setting up data protection principles and processes which every entity of Atos commits to apply.

The implementation of such Atos Group BCR-P will raise legal awareness within Atos and is intended to ensure a high level of protection for Personal Data within Atos.

1.2. Scope

1.2.1. Geographical Scope

These Atos Group BCR-P apply to all Atos Entities regardless of their localization and competent jurisdiction and benefits all Data Subjects – without any geographical restriction - whose personal data are transferred within the scope of the BCR-C from an entity under the scope of application of Chapter V GDPR.

1.2.2. Material Scope

These Atos Group BCR-P cover all Personal Data Processing irrespective of the nature of the Personal Data processed. These Atos Group BCR-P cover all types of processing carried out by Atos acting as a Processor.

1.2.3. Bindingness amongst entities

These Atos Group BCR-P are part of an Intra Group Agreement which makes them legally binding amongst all Atos Entities which enter into the Intra Group Agreement. These Atos Entities are listed in Appendix 2. This appendix also lists the country in which each Atos entity is incorporated and therefore identifies which entities are located within the EEA and which are located within third countries.

1.2.4. Bindingness amongst Employees

Atos Group BCR-P are part of the Atos Group Policies which Employees are bound to respect according to their employment contract. Appropriate information and, where required, agreement with local Works Councils have been obtained in order to ensure the full commitment and adherence to these Atos Group BCR-P by all Employees.

1.2.5. Bindingness vis-à-vis customers

Where an Atos Entity acts as a Processor, the Atos Entity commits in the Service Level Agreement that binds the Atos Entity and its Customer, to respect these Atos Group BCR-P.

1.3. Document maintenance and distribution

This Atos Group BCR-P document is publicly available via the privacy page of the Atos website (https://atos.net/en/privacy), and in addition are made accessible to all Employees via the Atos corporate intranet. The Atos BCR-P may be communicated to any Customer upon request as specified in Section 4 and are annexed, referred or linked to relevant Agreements.

1.4. Related documents

These Atos Group BCR-P are also composed of 10 Appendices which describe the procedures which enable Atos to guarantee that the Atos Group BCR-P are effectively implemented.

1.5. Keywords

The terms used in these Atos Group BCR-P are defined as follows:

Atos: Atos SE and all entities within the Atos group of companies whose ultimate parent is Atos SE ("Atos Group"), irrespective of the jurisdiction.

Atos Entity: any entity within the Atos Group which is directly or indirectly controlled by Atos SE and which is bound by these Atos Group BCR-P.

Atos S.E.: a company incorporated under French law, having its registered office at River Ouest – 80 quai Voltaire – 95870 Bezons, registered with the Trade and Companies Registrar under number 412 190 977 RCS Pontoise.

Applicable law: means all current laws and regulations applicable to Personal Data Processing under the BCR, including laws of the European Union or any Member State (which shall include, but not limited to GDPR) or any other applicable laws of any other country, province, state or jurisdiction to which the Personal Data Processing is subject.

Binding Corporate Rules as a Processor: this Policy together with its Appendices, all together referenced as Atos Group BCR-P

Consent: explicit manifestation of willingness to consent given by any appropriate method enabling a freely given specific and informed indication of the Data Subject's wishes, either by a statement or by a clear affirmative action by the Data Subject.

Controller: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data.

Customer: a party by whom an Atos Entity is contracted to process Personal Data as a Processor, for example the Controller or a Processor on whose behalf an Atos Entity is acting as a subcontractor.

Data Exporter: any entity (of Atos Group or of a third party) acting either as a Controller or a Processor which transfers Personal Data to a Data Importer located in a Third country.

Data Importer: any entity located in a Third Country receiving Personal Data from a Data Exporter.

Data Protection Authority(ies): any local authority which is competent to handle data protection issues.

Data Protection Impact Assessment: an assessment of the impact of the envisaged processing operations on the protection of Personal Data as required by Article 45 of GDPR.

Data Subject: any identified or identifiable natural person whose personal data is processed.

EEA: European Economic Area as defined by the European Union.

Employee: any person who is hired permanently or temporarily by an Atos Entity, or is supplied by an agency to undertake work for an Atos Entity.

GDPR: 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.

Group Data Protection Office: The Atos Group data protection compliance office headed by the Atos Group Data Protection Officer.

Local Data Protection Office: both the local Legal Experts on Data Protection and the Local Data Protection Officer as defined in Section 16 of these Atos Group BCR-P.

Personal Data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

Personal Data Processing: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Personal Data Transfer: the disclosure or transmission of Personal Data by one entity to another entity or the process of making such data available to that other entity in any form, including remote access to or display of such Personal Data on a screen.

Processing: has the meaning given to it in the GDPR.

Processor: a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of and under the strict instructions of the Controller.

Public Authority: (a) any individual, body or entity acting at national, regional or local level for the prevention and detection of criminal offences, the investigation and prosecution of criminal offences or the execution of criminal penalties including the safeguarding against and the prevention of threats to public security (e.g. judicial authorities, the police, any law enforcement authorities, etc.), or (b) any other individual, body or entity to which the law of any jurisdiction entrusts the exercise of authority or prerogatives of public power at national, regional or local level.

Region: several countries recognizing that they provide an equivalent level of protection to the Personal Data processed.

Service Level Agreement: any contract describing contractual relationships between two parties and the service to be provided.

Sensitive Data: Special Category Data or confidential financial information - such as bank account or credit card or debit card or other payment instrument details – provided that such financial information is not in the public domain.

Special Category Data: data that refer directly or indirectly to the racial or ethnic origin, political opinions, philosophical or religious opinions, trade union memberships, health or sexual life and orientations or biometric information of a natural person, provided that any information that is manifestly made public by the data subject or furnished under any other law for the time being in force shall not be regarded as Special Category personal data or information for the purposes of these Atos Group BCR-P.

Third Country: all countries where the level of protection of Personal Data is not adequate in comparison to the level of protection of Personal Data provided by the country where the Data Exporter is located, e.g. all country that is located outside EEA when the Data Exporter is located in EEA.

Third Party(ies): natural and legal persons with whom Atos has existing or planned business relations, such as suppliers and subcontractors that are not a member of the Atos Group.

GDPR: 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.

Group Data Protection Office: The Atos Group data protection compliance office headed by the Atos Group Data Protection Officer as described in Section 16 of these Atos Group BCR-P.

2. Requirements for processing of Personal Data

1. The requirements and principles set out in these Atos Group BCR-P shall be respected by Atos irrespective of local laws, except where local laws provide more stringent requirements than those set out in these Atos Group BCR-P.
2. Notwithstanding the elements contained in this Section 2, where Atos acts as a Processor, under the instructions of a Controller, it shall, in addition, respect the instructions provided by the Controller regarding the data processing, the security and the confidentiality measures that are agreed in a contract between the Controller and the Processor. Where Atos acting as a Processor is not able to comply with the Controller's instructions, Atos shall inform the Controller immediately.
3. Where an Atos Entity has reason to believe that the local laws or practices, or a change to the applicable laws or practices, prevents it from fulfilling
   - ✓ its obligations as a Processor under these Atos Group BCR-P

     and / or
   - ✓ the instructions it may have received from a Controller

     and / or if
   - ✓ that such legislation has substantial effect on the guarantees provided by the Atos Group BCR-P
4. the Atos Entity will promptly inform the Local Data Protection Office and the Atos legal entity acting as the main Processor in front of the Client. As a Processor Atos shall also inform the Controller and cooperate with the Customer, should the customer inform the competent Data Protection Authority
5. In particular, for the case of international transfer of personal data and in accordance with the EDPB Recommendations 1/2022 the Atos legal entity acting as Data Exporter shall commit to promptly identify supplementary measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted by the Atos legal entities acting as Data Exporter and/or Data Importer, in order to enable them to fulfil their obligations under these Atos Group BCR-P.
6. Furthermore, if the Data Exporter, along with Atos SE and the Group Data Protection Office, assesses that the Atos Group BCR-P – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed to that effect by a competent Data Protection Authority, it commits to suspend the transfer or set of transfers at stake, as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended.
7. If compliance is not restored within one month following such a suspension, the Atos Entity acting as Data Exporter has to end the transfer or set of transfers.

8. In such cases as the above, the Data Exporter and the Group Data Protection Office will inform other Atos Group BCR-P members so that any similar transfers may be identified, and similar consideration may be given to implementing supplementary measures or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.
9. Atos Entities acting as Data Exporters will, on an ongoing basis, also monitor developments in Third Countries that may affect the assessments of the level of protection and the decisions taken accordingly regarding transfers to such countries in collaboration with Atos Entities acting as Data Importers.
10. In case of doubt, with regard to the interpretation of local laws, the Local Data Protection Office and/or the Group Data Protection Office shall seek the Data Protection Authority's or external counsel's advice in order to ensure compliance with the most stringent provisions.
11. Where an Atos Entity acts as a Processor it shall also notify a Controller of any concern that it may have regarding the delivery of the service by the Atos Entity in compliance with these Atos Group BCR-P and with the Controller's instructions. Such notification to the Controller shall be made in such a timely manner that it enables the Controller to acknowledge the Processor's statement and to take necessary actions according to the applicable revision clause stated in the Service Level Agreement which binds the Atos Entity to the Controller. The same shall apply where an Atos Entity has reasons to believe that the existing and/or future local legislation may prevent it from fulfilling the instructions received from the Controller or its obligations under the Atos Group BCR-P.
12. With regards to requests for disclosure of personal data by a Public Authority that could affect compliance with the obligations under these Atos Group BCR-P or the instructions received from the Controller, the Atos Entity will apply the procedure described in Section 20.
13. The same Principles to be respected when processing Personal Data as stated in section 2.2 should apply to any copies of the Personal Data. When Personal Data is deleted by request or by obligation, the Data Importer should certify the deletion of the Personal Data to the Data Exporter. Therefore, until the Personal Data is deleted or returned, the Data Importer should continue to ensure compliance with these Atos Group BCR-P.
14. 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 these Atos Group BCR-P and will only process the Personal Data to the extent and for as long as required under that local law.

2.1. Legal grounds for processing Personal Data

Where an Atos Entity acts as a Processor, it commits to help and assist the Controller to ensure that the processing relies on one of the following grounds:

- ✓ the Data Subject has given Consent to the processing of his or her personal data for one or more specific purposes;

  or

- ✓ the Data Processing is necessary for the purposes of the legitimate interests pursued by the Atos Entity or by the Third Party or Third Parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the data subject is a child;

  or

- ✓ the Data Processing 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;

  or

- ✓ the Data Processing is necessary for compliance with a legal obligation to which the Atos Entity is subject;

  or

- ✓ the Data Processing is necessary to protect the vital interests of the Data Subject or of another natural person;

  or

- ✓ the Data Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.

2.2. Principles to be respected when processing Personal Data

When implementing a new Processing of Personal Data, an Atos Entity, acting as a Processor, shall provide support and assistance to the Controller to help ensure that:

- ✓ The Processing is lawful; processing activities are based on established legal grounds, restricted solely to legitimate interest, legal obligations, contractual obligations, vital interests, public tasks, or data subject's consent;

  and

- ✓ The Processing is fair; data subjects are allowed to make well-informed decisions about processing their personal data and are provided clear mechanisms to effectively exercise their rights. Additionally, the impact of data processing activities on the rights and safeguards of data subjects is rigorously assessed;

  and

- ✓ The Processing is transparent; data subjects are provided with comprehensive information, presented in clear and intelligible language, about the processing of their personal data, alongside an explanation of their rights and guidance on how to exercise them;

  and

- ✓ The Personal Data Processing adheres to purpose limitation; Personal Data is processed solely for specified, explicit and legitimate purposes and is not to be processed in a way that deviates from these purposes.

  and

- ✓ The Personal Data Processing adheres to data minimization; only Personal Data that is directly relevant and essential for specific purposes is collected and processed, to prevent the collection or retention of excessive information.

  and

- ✓ The Personal Data Processing adheres to accuracy; only accurate and up-to-date information is collected and maintained throughout its life cycle to prevent the use of outdated, incorrect or improperly altered data.

  and

- ✓ The Personal Data Processing upholds integrity and confidentiality; appropriate technical and organizational security measures are implemented to secure personal data against unauthorized or unlawful processing and to protect it from accidental loss, destruction or damage, in compliance with to Atos Security Policy and the requirements of applicable law;

  and

- ✓ Appropriate technical and organizational measures are implemented for the fulfilment of the Controller's obligations to respond to requests for exercising Data Subjects' rights

  and

- ✓ The Personal Data will be sub-processed by other Atos Entities or by Third Parties only with the prior informed specific or general written authorization of the Controller.

  and

- ✓ Onward transfers of Personal Data are strictly limited; Personal Data transferred under this framework may only be onward transferred outside the EEA to third parties when adequate safeguards are in place to ensure that the level of protection provided by GDPR is maintained.

  and

- ✓ These same commitments should apply to any copies of the data.

An Atos Entity acting as a Processor shall implement, in accordance with Controller's instructions, the appropriate measures to enable the Controller to comply with the above principles. This commitment also includes implementing technical and organizational measures to process sensitive personal data in line with the Controller's instructions. In addition, at the termination of the contract that binds an Atos Entity as a Processor with a Controller, the Atos Entity shall, according to the Controllers' instructions, return all the personal data transferred and the copies to the Controller or shall destroy all the Personal Data and certify to the Controller that it has done so, unless applicable law prevents it from returning or destroying all or part of the personal data transferred.

The Controller shall have the right to enforce these Atos Group BCR-P against any Atos Entity in relation to any data breach which that Entity has caused. The Controller shall also have the right to enforce these Atos Group BCR-P against Atos SE in case of: (i) a breach of these Atos Group BCR-P or of a relevant Service Level Agreement by a Atos Group BCR-P member established outside of EEA, or (ii) a breach of a written agreement with any subsequent external sub-processor established outside of the EEA.

2.3. Security

Atos Entities shall process Personal Data in accordance with the provisions of Atos Group Security Policies in order to ensure appropriate technical and organizational measures are in place to protect the data against: accidental or unlawful destruction; accidental loss, alteration or corruption; unauthorized disclosure or access; and unauthorized or unlawful processing.

Atos commits to implement enhanced security measures for the processing of Sensitive Data, such as encryption of data at rest, multi-factor authentication and role-based access controls.

In addition, when acting as a Processor, Atos Entities commit to cooperate with the Controller to ensure that Atos security measures and applicable policy meet the Controller's security requirements.

2.4. Accountability

2.4.1. Impact Assessment

In order to target an appropriate level of compliance with the principles defined in this Section 2, Atos conducts, where appropriate, a Compliance Assessment of Data Processing as Processor ("CADP-P") as detailed in Appendix 7. Where Atos acts as a Processor, the Atos CADP-P is completed. The CADP-P is reviewed by the Global or Local Data Protection Office. Atos will assist the Controller, where required under GDPR Article 35, with completion of a Data Protection Impact Assessment ("DPIA") and with any subsequent prior consultation with the competent Data Protection Authority where the Controller's assessment in the DPIA concludes that the proposed processing is likely to result in a high risk to the rights and freedoms of individuals, either without further mitigation measures or when the residual risk remains high after mitigation measures are applied. Atos DPIA shall be reviewed by the competent Data Protection Office.

2.4.2. Records of Processing activities

When acting as a Processor, all Atos entities falling within the scope of these Atos Group BCR-P shall maintain records of their respective Processing activities. Such records shall be retained in writing, including electronic form, and shall be made available upon request to the competent Data Protection Authority.

The Atos CADP-P record shall contain at least the following information:

1. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
2. the categories of processing carried out on behalf of each controller;
3. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organization and the details of safeguards and mechanisms for the transfer;
4. where possible, a general description of the technical and organizational security measures.

3. Transfer of Personal Data

Being an international information technology services company, established worldwide, Atos is acting internationally and transferring data all over the globe. As a result, we process Personal Data in several countries and from different origins.

It is therefore necessary to frame the transfer in order to guarantee that the level of protection provided to the data transferred is harmonized throughout the Atos Group.

Under the provisions of these Atos Group BCR-P, Personal Data Transfers are the responsibility of Data Exporters which shall undertake to provide appropriate safeguards to Personal Data which are transferred. Additional safeguards may be required depending on the nature of the Personal Data and the location to which Personal Data is to be transferred. In such a case, the Atos Entity and the Group and/or Local Data Protection Office will be informed and involved in such assessment.

Personal Data transferred under this framework may only be transferred further to the entities outside of the EAA which are not bound by this BCR-P provided that the general principles for transfers under the GDPR are respected. This requires the implementation of adequate safeguards to ensure that the level of protection for Data Subjects offered by the GDPR is maintained.

The expected and anticipated types of data and purposes of transfer of Personal data by Atos Entities acting as Processors, are described in Appendix 6.

No transfer of Personal Data to an Atos Entity will be made on the basis of these Atos Group BCR-P unless the Atos Entity concerned is effectively bound by them and can demonstrate compliance.

When an Atos Entity acting as Data Importer, relying on this BCR-P for transfers, has a reason to believe or becomes subject to laws and practices that prevent it from fulfilling its obligations under this framework, it must promptly notify the Atos Entity acting as Data Importer. This information must also be promptly communicated to the liable BCR member(s).

Upon verification of such notification, Atos Entity acting as Data Importer, in cooperation with the relevant Local Data Protection Office and liable BCR Member(s), shall promptly identify and implement supplementary measures to support the concerned Atos Entity to restore compliance under this framework. This requirement also applies if an Atos Entity acting as Data Importer has grounds to believe that Atos entity acting as Data Exporter is unable to demonstrate compliance under this framework.

3.1. Personal Data transfer by an Atos Entity, located anywhere, acting as a Data Exporter, to another Atos Entity, located within the EEA.

Where an Atos Entity, located anywhere, acting as a Data Exporter, transfers Personal Data on behalf of a Controller to another Atos Entity located within the EEA, it shall ensure by a way of a contract or other legal act under Union or Member State law that the sub-processor commits to provide sufficient guarantees to implement appropriate technical and organizational measures to respect the same obligations as the ones which are binding the Controller and the importing Atos Entity within the EEA.

3.2. Personal Data transfer by an Atos Entity located in the EEA acting as a Data Exporter to an Atos Entity located outside of the EEA bound by Atos Group Atos Group BCR-P.

Where an Atos Entity in the EEA, acting as a Data Exporter, transfers Personal Data on behalf of a Controller to another Atos Entity, located outside of the EEA, the transfer is covered by these Atos Group BCR-P. Atos commits to obtain the Controller's authorization prior to such transfer. Atos Entity will also ensure full transparency regarding the use of these Atos Group BCR-P for the framing of the above-mentioned transfer out of the EEA.

3.3. Personal Data transfer by an Atos Entity in the EEA acting as a Data Exporter to a Third Party acting as a sub-processor located outside the EEA.

Personal Data Transfer by an Atos Entity in the EEA, acting as a Data Exporter to a Third Party is possible only where the Controller has given its authorization and where there are guarantees by way of a contract or other applicable legal instrument to ensure that the entity receiving the Personal Data commits in writing to provide sufficient guarantees in respect of the technical and organizational measures governing the processing of the Personal Data.

Where this Third Party is located outside the EEA in a country that has not received an Adequacy Decision from the European Commission, Atos Entity acting as Data Exporter and transferring the Data shall sign the appropriate module of the EU Standard Contractual Clauses adopted by the European Commission or other appropriate safeguards between the Controller and the Third Party importing the Personal Data, and document the assessment of the risk of such a transfer in accordance with Section 3.3

4. Data Subject's rights

Where an Atos Entity processes Personal Data acting as a Processor, Data Subjects shall have the right, to enforce against such Atos Entity the following:

- ✓ The Atos Entity's duty to respect the instructions from the Controller regarding the data Processing including for data transfers to Third Countries;
- ✓ The Atos Entity's duty to implement appropriate technical and organizational security measures;
- ✓ The Atos Entity's duty to notify any personal data breach to the Controller;
- ✓ The Atos Entity's duty to respect the conditions when engaging a sub-processor either within or outside the Atos Group;
- ✓ The Atos Entity's duty to cooperate with and assist the Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights;
- ✓ The Atos Entity's duty to provide easy access to these Atos Group BCR-P;
- ✓ The right to complain through an internal complaint mechanism;
- ✓ The Atos Entity's duty to cooperate with Data Protection Authorities;
- ✓ The Atos Entity's duty to comply with the liability, compensation and jurisdiction provisions.

In addition, in a case where:

a. The Controller has factually disappeared or
b. The Controller has ceased to exist in law or
c. The Controller has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law,

Data Subjects shall have the right, upon request, to enforce against the Atos Entity acting as Processor the following elements of the Atos Group BCR-P:

- ✓ The Atos Entity's duty to respect these Atos Group BCR-P;
- ✓ The right to be provided with easy access to these Atos Group BCR-P and in particular easy access to the information about third-party beneficiary rights for the Data Subject that benefit from them (see section 7);
- ✓ The right to be informed regarding the complaint handling procedure and to have easy access to it, including the possibility to lodge a complaint before a Data Protection Authority and before the courts;
- ✓ The Atos Entity's duty to accept liability for paying compensation and to remedy breaches of these Atos Group BCR-P;
- ✓ The right to be informed of the fact that the burden of proof lies with the Atos Entity and not with the Data Subject according to the terms of these Atos Group BCR-P;
- ✓ The Atos Entity's duty to cooperate with the competent Data Protection Authority;
- ✓ The Atos Entity's duty to cooperate with the Controller;
- ✓ To be informed of the data protection principles including the rules on transfers or onward transfers of Personal Data;
- ✓ To be informed regarding Atos Entities bound by these Atos Group BCR-P;
- ✓ To be informed, where legally permitted, when national legislation prevents an Atos Entity from complying with its obligations under these Atos Group BCR-P.

5. Complaint handling procedure

5.1. Direct complaint

If a Data Subject believes that the Processing of his / her Personal Data which is subject to these Atos Group BCR-P have caused him / her damage, he / she may complain to the Atos Group. Similarly, if a Data Subject believes that the Processing of Personal Data which is subject to these Atos Group BCR-P has not been conducted according to these Atos Group BCR-P or applicable law, Data Subjects are granted a right to complain against Atos. Such complaints will be notified to the Controller without undue delay unless otherwise agreed with the Controller. Data subjects have two main channels to submit their complaint to Atos:

- By e-mail: dpo.global@atos.net.
- By Mail: complaints can be directed to our global headquarters address at River Ouest, 80 Quai Voltaire, 95877 Bezons Cedex – For other countries, please refer to our office addresses available in the following link: https://atos.net/en/worldwide-locations

Atos has established a time framed Complaint Handling Procedure which is defined in Appendix 4.

Data Subjects are encouraged to submit a direct complaint as described in this section 5.1 and to escalate the complaint according to Section 7 where Atos fails to comply with the commitments of this section.

The Atos Entities concerned accept responsibility for investigating such complaints and for ensuring that action is taken, and remedies provided, as appropriate.

In case a complaint is ultimately rejected by the Local Data Protection Office, the Data Subject must be informed of the rationale leading to this decision.

The use of this complaint procedure will not affect a Data Subject's right to bring a claim before a national court (a court in the country in which a processing Atos Entity is based) should they

5.2. Indirect complaint

Where a Controller reports a complaint in accordance with the means listed under Section 5.1, from a Data Subject whose Personal Data are processed by an Atos Entity as Processor, Atos shall take all necessary steps to make sure that the Data Subject's complaint is addressed. For this purpose, Atos should comply with the procedure set up in Appendix 4.

Where a Data Subject whose Personal Data are processed by an Atos Entity as a Processor files a complaint directly to the Atos Entity, Atos shall immediately inform the Controller about the claim and act according to Appendix 4 to escalate the claim, unless otherwise agreed with the Controller.

Where the Controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law, any complaint regarding processing of Personal Data under these Atos Group BCR-P becomes a complaint against the Processing by the Atos Entity and the Atos Entity should comply with the procedure set up in Appendix 5.

5.3. Right of Complaint to a Data Protection Authority or to bring a complaint before a Court.

If a Data Subject believes that the Processing of his / her Personal Data, which is subject to these Atos Group BCR-P, have caused him/her damage or have not been processed according to these BCR-P, or according to applicable law, Data Subjects are granted a right to complain to a competent Data Protection Authority and / or (where applicable) to bring a claim before the competent court in the EU member state where the competent Data Protection Authority is

located or where the Data Controller or Data Processor has an establishment, or where the Data Subject has their habitual residence.

The Data Subject may also lodge a complaint to the competent Data Protection Authority which can either be that of the EU Member State of their habitual residence, place of work or place of the alleged infringement.

6. Controller's complaint

Where an Atos Entity processes Personal Data on behalf of a Controller, the latter may raise issues regarding the processing of their Personal Data.

Atos commits to handle such request from a Controller smoothly and efficiently, according to Appendix 5.

7. Liability vis-à-vis Data Subjects

Where a Data Subject suffers material or non-material damage as a result of a processing of Personal Data by an Atos Entity, acting as a Processor, the provisions below shall apply. It is emphasized that a Data Subject is encouraged first to file a complaint directly to Atos in order to find an amicable solution, however Data Subjects have the right to complain to the relevant Data Protection Authority or courts, whether or not they have first complained directly to Atos. Complaints and the rights of Data Subjects are addressed in sections 3 and 4 of these Atos Group BCR-P.

7.1. Liability of Atos Entities acting as Processor

In case of damage suffered by a Data Subject as a result of a Processing made by an Atos Entity, acting as a Processor, located in or outside the EEA, and where one of the listed below hypothesis happen:

a. The Controller has factually disappeared or
b. The Controller has ceased to exist in law or
c. The Controller has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law,

then, the Atos Entity recognizes that Data Subjects have the right to seek compensation or a remedy directly from Atos S.E., an EEA based company. The Data Subject may also exercise his or her rights before the courts or the competent Data Protection Authority. In addition, Atos accepts that in certain cases remedies other than monetary compensation may be appropriate to address the damage suffered by a Data Subject as a result of a Processing made by Atos.

Whether or not a violation of the Atos Group BCR-P has been effectively recognized by a court, it is the responsibility of an Atos Entity acting as a Processor based in the EEA to deal with the claims in good faith; this Atos Entity accepts responsibility for and agrees to take the necessary action to remedy the acts of other members of the Atos Group bound by the Atos Group BCR-P established outside of the EEA and to pay compensation for any damages resulting from the violation of the Atos Group BCR-P.

Whether or not a violation of the Atos Group BCR-P has been effectively recognized by a court, in the case of an Atos Entity acting as a Processor based outside of the EEA and/or of an external sub-processor located outside of the EEA, Atos S.E., an EEA based entity, accepts responsibility for and agrees to take the necessary actions to remedy the acts of other entities of the Atos Group bound by the Atos Group BCR-P and/or of external sub-processors established outside of the EEA as well as to pay compensation for any damages resulting from the violation of the Atos Group BCR-P.

7.2. Burden of proof

In any case, where section 7.1 applies, and where a Data Subject has demonstrated that they have suffered damage that is likely to have been caused by a breach of the Atos Group BCR-P, the Atos Entity accepts to bear the burden of proof for demonstrating that any damage suffered by the Data Subject was not caused by a breach of the Atos Group BCR-P by the Atos Entity.

8. Liability vis-à-vis Controller

Where an Atos Entity acts as a Processor, and where it fails to satisfy a Controller's instructions, the Atos Entity shall inform the Controller that it has the right to enforce the Atos Group BCR-P against the exporting Atos legal entity according to the applicable liability regime set up in the Service Level Agreement signed between the Atos Entity and the Controller.

The Controller's rights shall cover the judicial remedies and the right to receive compensation.

In any case, the Atos Entity shall not exclude its liability vis-à-vis Controller where the violation is a result of a sub-processor.

The above does not limit the Atos Entity's primary responsibility and liabilities towards any Data Subjects under the Atos Group BCR-P and/or under local applicable law.

9. Data Subject's information

9.1. Permanent information

Atos commits to make its Binding Corporate Rules as a Processor (Atos Group BCR-P) readily available to every Data Subject and Controller. The Atos Group BCR-P and its appendices are published on the atos.net website at the following link: https://atos.net/en/atos-binding-corporate-rules.

Where Processing is performed that is subject to these Atos Group BCR-P, these Atos Group BCR-P will be included as an annex to a Service Level Agreement with the Controller.

9.2. Data Subject's information when Atos acts as a Processor

Where Atos acts as a Processor, the responsibility to inform Data Subjects lies in the hands of the Controller. Given that Atos intends to provide its Controller with a high level of service and to act in full transparency, Atos commits to provide relevant information to Controllers it works with, which will enable a Controller to fulfil its legal requirements to inform Data Subjects.

10. Cooperation

Atos Entities commit to cooperate actively with Third Parties in order to make sure that applicable law and regulations regarding Data Protection are respected by all stakeholders. For this purpose, all Atos Entities shall comply with any applicable data protection legislation in their contractual and business relations with customers, suppliers, partners and subcontractors. This commitment shall include enabling the exercise of data subject rights in accordance with the Section 4 and cooperation with supervisory authorities.

10.1. Cooperation with Controllers

Where an Atos Entity processes Personal Data on behalf of a Controller, Atos shall, to a reasonable extent and in a timely manner, provide the Controller with relevant information, in order to enable the Controller to comply with local data protection legal requirements while at the same time the Atos Entity will comply with all its contractual commitments.

10.2. Cooperation with Data Protection Authorities

Atos Entities shall also cooperate and assist each other to handle a request or complaint from an individual or an investigation or inquiry by a Data Protection Authority.

Atos Entities shall also cooperate actively with all requests from Data Protection Authorities, in particular to ensure adequate a nd timely response to any request received from Data Protection Authorities. This includes the obligation to provide, upon request, any information pertaining to processing activities.

Atos also accepts to be audited by Data Protection Authorities to verify compliance with applicable data protection legislation and with these Atos Group BCR-P.

Atos Entities shall, comply with the advice of the Data Protection Authority in relation to these Atos Group BCR-P and comply with any applicable decisions or notices issued by a Data Protection Authority.

11. Personal Data Breach reporting

For the purposes of this section, the expression "Personal Data Breach" shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

In the event that an Atos Entity, acting as a Processor, becomes aware of a Personal Data Breach, Atos shall, without undue delay, notify it to the Controller and, taking into account the nature of Processing and the information available to the Processor, shall assist the Controller with its response to the Personal Data Breach, in particular in respect of any notification to a Data Protection Authority or to Data Subjects affected by the breach.

In any event of a data breach, Atos Entities shall document the breach including records relating to the factual elements of the breach, its impact on data subjects, together with a risk assessment and the remedial actions implemented. Such documentation shall be provided to the competent Data Protection Authorities upon request, in accordance with the applicable legal requirements and the principle of accountability.

12. Privacy by Design

12.1. Product, service and process development

Where one of the Atos Entities or business team intends to develop new processing, for example by submitting a proposal to a new Customer or proposing a project to a Customer, it shall make sure that Data Protection is taken into account as of the beginning of the project, including any requirement to comply with other applicable local law.

For this very purpose, where a project is developed by an Atos Entity, the business team in charge of the new processing shall produce an Atos CADP-P as described in Appendix 7. The Local Data Protection Office shall receive a copy of the Atos CADP-P, shall conduct random reviews of the Atos CADP-P and shall make recommendations to have the project run in a compliant manner.

Where requested, an Atos Entity will assist a Controller in the performance of a DPIA.

Where the Local Data Protection Office considers that this is necessary it will consult the Global Data Protection Office, which will provide appropriate support.

It results from the above that Employees who develop new projects shall make sure that the Local or Global Data Protection Office are involved in each project.

12.2. New business opportunities and M&A

Where an Atos Entity intends to develop new business opportunities or to merge with or acquire a company, the Employees involved in the project shall make sure that Data Protection aspects are taken into account.

For this very purpose, where new business opportunities are possible at local level, the Local Data Protection Office shall be consulted as of the beginning of the project and involved at every stage of the project. The Local Data Protection Office shall produce a risk assessment regarding the project in order to make recommendations to make sure that all data protection aspects are taken into account, in particular regarding the implementation of the data centers or the structuring of the company.

Where the Local Data Protection Office considers that this is necessary it will consult the Group Data Protection Office, which will provide appropriate support.

Where a project is developed at global level, the Group Data Protection Office shall be consulted as of the beginning of any bid management or beginning of a project and it shall be involved at every stage of the project. The Group Data Protection Office shall produce a risk assessment regarding the project in order to make recommendations to make sure that all data protection aspects are taken into account, in particular regarding the implementation of data centers or the structuring of the company.

It follows from the above that Atos Employees who undertake such projects shall make sure that the Local or Global Data Protection Office are involved in each project.

13. National Notification to Competent Data Protection Authorities

Where local Data Protection Authorities request prior notification of particular Processing, Atos commits to respect this.

Atos keeps records of its Processing activities a Processor.

Atos entities will maintain such registrations as are required by local Data Protection Authorities.

Where an Atos Entity acts as a Processor on behalf of a Controller or a sub-processor on behalf of another Processor, the Atos Entity commits to provide such Third Parties with all relevant information necessary to comply with applicable law.

14. Training and raising awareness

Atos has a group-wide mandatory training program that includes training in Security / Cyber Security, Data Protection and Code of Ethics.

Atos commits to:

- ✓ Regularly update training;
- ✓ Undertake activities to raise staff awareness of data protection;
- ✓ Monitor and report on rates of completion of mandatory training;
- ✓ Provide specific and appropriate training on data protection and these Atos BCR-C to those Employees who have regular or permanent access to personal data, are involved in the collection of personal data or are engaged in the development of tools used to process personal data.

The mandatory training aims to equip all employees with the knowledge and skills required to handle personal data responsibly and in compliance with the applicable regulations, including GDPR. The training is conducted latest 3 months after onboarding, then on an annual basis, with additional refresher courses provided as needed to ensure all personnel stay up to date with the latest policies and procedures.

The training covers a range of data protection topics, including data protection principles and regulations, individual rights and consent management, data breach response procedures, data retention and deletion policies, data security measures, privacy by design and default, and procedures for managing requests for access to personal data by public authorities.

Atos Group mandatory training is part of an integrated learning platform provided to members of staff, which prompts them when training is due and maintains individual training records that are monitored by immediate line managers. Data Protection is one of the modules. Failure to complete mandatory training may affect performance assessments and can lead to disciplinary action. When the employee starts the Data Protection Training, the first step is to undergo an entry test that allows to evaluate his/her existing knowledge on the various Data Protection topics covered by the E-learning. Based on the replies provided, the training will focus on the weak areas evidenced by the test, thus delivering a training that is tailored to the employee's needs.

Completion of mandatory Data Protection Training is monitored by the Data Protection organization together with the Human Resources Department in order to provide assurance that new training is being taken up and to allow identification of any areas of the business where additional effort is required to ensure completion.

15. Audit

Atos commits to audit Atos Group's compliance with regard to these Atos Group BCR-P including the implementation of these Atos Group BCR-P and methods of ensuring corrective action is taken.

Such audit shall be carried out on a regular basis, with no more than 3 years between each audit. Such audit shall be carried out by our internal audit team whose reports are presented during Internal Audit Committee to the Atos S.E. Board. As a result, the audit is initiated by the Atos headquarters entity, i.e. Atos S.E.

The results of the audit shall also be communicated to the Atos Group Community and liable BCR Member and corrective actions shall be proposed by the Atos Group Data Protection Officer, who will report on their completion to the Atos SE Board.

Upon request, Competent Data Protection Authorities and Third Parties shall obtain results of the Data Protection Audit and details of any corrective actions.

All professionals in charge of carrying out said audits are guaranteed independence as to the performance of their duties.

Where Atos acts as a Processor, Controllers can request an audit to be carried out on the Atos and/or sub-processors' facilities used to process the Controller's personal Data. Such audit requests can be valid only provided that the Controller gives appropriate prior notification to Atos.

The audit plan dedicated to these Atos Group BCR-P is described in Appendix 9.

A Competent Data Protection Authority may, without restriction, conduct or upon request, access the results of an audit of any Atos Entity in respect of Processing undertaken under these Atos Group BCR-P. This is in addition to any audit rights as defined in applicable data protection legislation.

16. Data Protection Community

Atos will ensure that the group data protection policy and its binding corporate rules, including these Atos Group BCR-C are effectively implemented throughout the Group.

For this very reason, a Data Protection Community ("Atos DP Community") is created. This Atos DP Community is composed of two branches which shall cooperate and work together: the legal branch and the operational branch.

The Atos DP Community is coordinated by the Group Data Protection Office (GDPO) which is led by the Group Data Protection Officer. The GDPO includes legal data protection specialists and experienced practitioners. These individuals represent Atos at the group level.

The Group Data Protection Officer reports directly to a member of the Atos Group Board and enjoys the highest management support for the fulfilling of this task. Moreover, the Group Data Protection Officer can inform the highest management level if any question or matter arise during the performance of his/her duties.

In any case, the members of the Atos DP Community, when performing their duties as a Data Protection Officer, should not have any tasks that could result in conflict of interests.

At the local level, Local Data Protection Legal Experts and Local Data Protection Officers, both together form the Local Data Protection Office.

The complete organization is described in Appendix 1 together with the respective roles and responsibilities of each role within the organization.

17. Key Performance Indicators (KPI)

In order to ensure effective implementation of the group data protection policy and its binding corporate rules, including these Atos Group BCR-P, the Data Protection Community maintains KPI as designed by the Group Data Protection Office.

These KPI cover in particular, but not exclusively:

- ✓ Number of complaints from employees
- ✓ Number of data breaches;
- ✓ Number of data breaches notified to a Data Protection Authority;
- ✓ Number of data breaches notified to Data Subjects;
- ✓ Number of complaints from vendors or suppliers;
- ✓ Number of complaints from others (for example from other data subjects);
- ✓ Number of requests from Employees, vendor or supplier personnel to exercise their data protection rights;
- ✓ Number of requests from other data subjects to exercise their data protection rights.

Each Local Data Protection Office collects these KPIs, which are then centralized and analyzed by the Group Data Protection Office every six (6) months.

18. Investigation

Where an on-site investigation or audit takes place (for example by a Controller or a Data Protection Authority), the Local Data Protection Office shall be contacted immediately, and it shall immediately contact the Group Data Protection Office.

As described in Section 10, the Local Data Protection Office and the Group Data Protection Office shall actively cooperate with the authority carrying on the investigation.

19. Update of the Atos Group BCR-P and communication

These Atos Group BCR-P may be amended from time to time and where necessary, in particular where necessary to comply with applicable data protection law or to incorporate changes within the Atos Group.

Any significant changes to these Atos Group BCR-P, such as those that:

- potentially affect their data protection compliance;
- are potentially detrimental to Data Subject rights;
- potentially affect the level of protection offered by the Atos Group BCR-P;
- affect the binding nature of the Atos Group BCR-P,

shall be reported to all Atos Entities without undue delay and with an explanation for the change. Clear and easily available information regarding any such significant change shall be made for Employees and Third Parties information. Other changes, such as changes to the list of bound Atos Entities, will be reported to all members on a regular basis and will be reported to Atos's lead Data Protection Authority annually.

Where Atos acts as Processor it also commits to inform its Customers acting as Controller of any update and amendment of the scope of the Atos Group BCR-P. Such notification to Customer shall be made in such a timely manner that it enables Customer to acknowledge Customer statement and to take necessary actions according to the applicable revision clause stated in the Service Level Agreement which binds Atos to the Customer.

In any case, a list of Atos Entities bound by these Atos Group BCR-P as well as a list of amendments shall be kept up to date in Appendix 2. These two lists will be kept up to date by the Group Data Protection Office which shall ensure appropriate communication as described in the precedent paragraph.

Any administrative changes and more significant changes to these Atos Group BCR-P will be documented and communicated as above.

Where a modification to these Atos Group BCR-P would possibly be detrimental to the level of the protection offered by these BCR-P or significantly affect them, the change must be communicated in advance to Atos's lead Data Protection Authority, with a brief explanation of the reasons for the update. In this case, the Authority will be able to assess whether the changes made require a different BCR approval process.

Once a year, the Atos's lead Data Protection Authority should be notified of any changes to these Atos Group BCR-P or to the list of members, with a brief explanation of the reasons for the updates. The Atos's lead Data Protection Authority should also be notified once a year in instances where no changes have been made, including confirmation related to the fact BCR members have sufficient assets to effectively compensate a claim and that Atos SE is capable of paying for damages in case of breach of the BCR.

Disclosure of Personal Data to a Public AuthorityDisclosure of Personal Data to a Public Authority

1. Where an Atos Entity acting as Data Importer receives a legally binding request for disclosure of Personal Data by a Public Authority under the laws of the country of destination, or of another Third Country, the Atos Entity acting as a Data Importer, shall as soon as possible, subject to applicable legislation preventing or prohibiting it, communicate it to the Data Exporter. Such communication will include the information available about the personal data requested (e.g. the requesting authority, the legal basis for the request and the response provided, if any). The Data Importer shall suspend execution of the request, and the Data Protection Authority competent for the Controller and Atos's lead Data Protection Authority shall be informed about it. The Data Importer will also, where requested and legally permitted notify any affected data subjects.
2. The Atos Entity acting as Data Importer receiving the request will review the legality of the request for disclosure, in particular whether it resides within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable and enforceable obligations under international law or principles of international comity.
3. The Atos Entity acting as Data Importer will, under the same conditions, pursue possibilities of appeal.
4. When challenging a request, the Atos Entity acting as Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until required to do so under the applicable procedural rules.
5. The Atos Entity acting as Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible by the laws and/or regulations to which the requesting authority is subject, make the documentation available to the Data Exporter and/or Data Controller as agreed with the Data Exporter. It will also make it available to the Competent Data Protection Authority(ies) upon request.
6. The Atos Entity acting as Data Importer will not provide more than the minimum amount of information when responding to a request for disclosure, based on a reasonable interpretation of the request.
7. The Atos Entity acting as Data Importer will maintain records of such requests for as long as the relevant Data is subject to the Atos Group BCR. These records will include: number of applications for disclosure, type of data requested, requesting authority or authorities, whether requests have been challenged (if possible) and the potential or actual outcome of such challenges, etc. These records will be communicated to the Data Exporter at regular intervals and make them available to the Competent Data Protection Authority(ies) upon request.

8. If applicable laws prohibit the suspension of execution or communication of the request, the Data Importer shall use its best efforts to obtain the right to waive this prohibition, then communicate as much information as possible and as soon as possible to the relevant Data Exporter and relevant Data Protection Authorities, and shall document it.
9. If an Atos Entity acting as Data Importer is not in a position to inform the relevant Data Protection Authority(ies) despite its best efforts, it will provide to the Competent Data Protection Authority, at least once a year, general information on the requests – e.g. number of applications for disclosure, type of data requested and requesting authority or authorities.
10. In any case, the Data Importer shall ensure that any Transfers of Personal Data to any Public Authority will not be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society.
11. If an Atos Entity acting as Data Importer becomes aware of any direct access by Public Authorities to personal data transferred pursuant to these BCR-P, Atos shall as soon as possible, subject to applicable legislation preventing or prohibiting it, communicate it to the Controller and/or Data Exporter. Such communication will include all the information available about the Personal Data accessed.

20. Appendices – Procedures

Appendix 1 – Organization of the Data Protection Community and Roles

Appendix 2 – List of entities bound by the Atos Group BCR-P

Appendix 3 – Form for Data Subject to exercise their rights

Appendix 4 – Complaint Handling Procedure where Atos is acting as a Processor

Appendix 5 – Procedure for Handling Complaints from Controllers whose Personal Data are processed by Atos

Appendix 6 – Data Transfers – Categories of Data, Categories of Data Subject and Purposes of Data Transfer

Appendix 7 – Compliance Assessment of Data Processing where Atos acts as a Processor

Appendix 8 – Local Data Protection Points of Contact

Appendix 9 – Audit plan (Streams)

Appendix 10 - Responsibility assignment matrix: RACI

About Atos

Atos is a global leader in digital transformation with circa 78,000 employees and annual revenue of circa €10 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 68 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Learn more at: atos.net

Atos Group is deploying safe and responsible AI solutions (internal and/or 3rd party based) for the internal use by its employees, collaborators and advisors when developing and delivering products and/or services to its customers as well as when and offering AI based solutions. A specific policy has been deployed across all the Group employees to ensure the protection of the confidentiality and the security of own data and our customers' data through the use of solutions vetted by our legal, security and data protection teams.

Additionally, the Group offers professional services that can help companies to understand requirements, to anticipate legislations applicable to AI, and to be better prepared to achieve compliance with those AI regulations as they are adopted.

106237-RR