Atos Group Binding Corporate Rules as a Controller (Atos Group)

Document last update: November 2024

Table of contents

List of changes

Version	Date	Description	Author(s)
1.4	29/09/2014	Initial version	Lionel de Souza
2.0	July 2019	Update	Stéphane Larrière
2.1	February 2022	General updates, including: • Additional definitions; • Additional information on subject rights; • Expanded section on data subject information.	Andrew Jackson Wissame En-Naoui Cecilia Fernandez Claude Bineau
2.2	October 2023	General update in accordance with the Recommendations 1/2022 of the EDPB, including addition of assessment of necessity of additional measures when transferring EEA data to a Third Country.	Andrew Jackson Cecilia Fernandez
2.3	January 2024	Draft separate BCR-C version	Andrew Jackson Cecilia Fernandez
3.0	November 2024	Update of the draft separate BCR-C 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 Controller, Atos has adopted these Atos Group Binding Corporate Rules as a Controller ("Atos Group BCR-C").

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

The implementation of such Atos Group BCR-C 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-C 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 of the GDPR.

1.2.2. Material Scope

These Atos Group BCR-C cover all type of processing carried out by Atos acting as a Controller, irrespective of the nature of the Personal Data processed. In particular, these Atos Group BCR-C cover processing of Recruitment, HR, Customer, Supplier, or Marketing and Communications Data, although this is not an exhaustive list.

Atos is committed to ensuring that all Personal Data, whether relating to Employees or external Data Subjects, is subject to the same level of protection.

1.2.3. Bindingness amongst entities

These Atos Group BCR-C are part of the Intra Group Agreement which makes all Group policies legally binding amongst all Atos Entities that are part of the Intra Group Agreement and which 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-C 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-C by all Employees.

1.3. Document maintenance and distribution

The Atos Group BCR-C are made available publicly via the privacy page of the Atos website (https://atos.net/en/privacy), and in addition are made accessible to all Atos employees via the Atos corporate intranet. The Atos Group BCR-C may be communicated to any Customer upon request as specified in Section 7 and are annexed, referred or linked to relevant agreements.

1.4. Related documents

These Atos Group BCR-C are also composed of 9 Appendices which describe the procedures which enable Atos to guarantee that the Atos Group BCR-C are effectively implemented.

1.5. Keywords

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

Applicable Law: any law, including regulations, directives, or other legal instruments governing the processing of personal data, such as the General Data Protection Regulation (GDPR), national data protection laws, and the relevant laws of third countries, as well as authoritative guidance issued by courts or competent authorities.

Atos: Atos Headquarters together with their entities owned by Atos Group irrespective of the jurisdiction.

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

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.

Binding Corporate Rules as a Controller: this Policy together with its Appendices, all together referenced as Atos Group BCR-C.

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 Atos Entity acting as a Controller and which transfers Personal Data to a Data Importer located in a Third Country.

Data Importer: any Atos 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 35 of the EU GDPR.

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

EDPB Recommendations 1/2022: The European Data Protection Board Recommendations 1/2022 on the Application for Approval and on the elements and principles established for Binding Corporate Rules by the GDPR, adopted on 14 November 2022.

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 14 of these Atos Group BCR.

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 physical, physiological, mental, economic, cultural or social identity.

Personal Data Processing/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.

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.

Sensitive 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, biometric information, financial information such as bank account or credit card or debit card or other payment instrument details, provided that any information that is freely available or accessible in public domain or furnish under any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these Atos Group BCR-C.

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.

2. Requirements for processing of Personal Data

1. The requirements and principles set out in these Atos Group BCR-C 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-C.
2. Where an Atos Entity, acting as a Data Importer, has reason to believe that the applicable laws or practices, or a change to the applicable laws or practices, prevent it from fulfilling:
   - ✓ Its obligations as a Controller under these Atos Group BCR-C;

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

the Atos Entity will promptly inform the Local Data Protection Office, the Controller and any Atos legal entity concerned by the processing.

3. 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-C or the Atos Group BCR-P.
4. Furthermore, if the Data Exporter, along with Atos SE and the Group Data Protection Office, assesses that the Atos Group BCR-C – 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.
5. If compliance is not restored within one month following such a suspension and if the BCR-C cannot be complied with, the Atos Entity acting as Data Exporter has to end the transfer or set of transfers.
6. In such cases as the above, the Data Exporter and the Group Data Protection Office will inform other Atos Group BCR-C 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.
7. 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.

8. 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 Data Protection Authority or external counsel's advice in order to ensure compliance with the most stringent provisions.
9. Where acting as a Controller, Atos shall regulate its engagements with an internal or external processor through either a contract or another legal act in accordance with European Union or a Member State law. This legal framework must incorporate the precise elements of data processing and the processor's obligation to only follow documented instructions of Atos. Moreover, it must require processors to cooperate with Atos in safeguarding data subject rights, providing necessary information to demonstrate compliance, and implementing adequate technical and organizational safeguards.
10. In all cases, where an Atos Entity acting as a Data Importer ceases to be able to comply with these Atos Group BCR-C or ceases to be bound by them, or where otherwise requested to by the Data Exporter, it will promptly inform the Data Exporter, cease to process the Personal Data and return or delete such Personal Data, unless requested otherwise by the Data Exporter. The same applies if an Atos Entity acting as Data Exporter has reasons to believe that an Atos Entity acting as its Data Importer can no longer fulfil its obligations under this BCR-C.
11. 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-C or the instructions received from the Controller, the Atos Entity will apply the procedure described in Section 18.
12. 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-C.
13. 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-C 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

Before starting any Processing of Personal Data, the Atos Entity acting as Controller shall make sure that the Data Processing relies on one of the following grounds:

✓ the Data Subject has given his/her Consent to the processing of his/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/Parties to whom the data are disclosed, except where such interests are overridden by the interests for 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 Personal Data Processing and while such Processing is being carried out, an Atos Entity, acting as a Controller, shall guarantee that:

- ✓ The Personal Data 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 Personal Data 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 Personal Data 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.

2.3. Sensitive Data

When Atos acts as a Controller, Sensitive Data shall be processed only provided that:

- ✓ The Data Subject has given his/her Consent to the Personal Data Processing for one or more specified purposes, except where applicable law provides that the prohibition on the Processing of such data may not be lifted by the Data Subject;

  or

- ✓ Data Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by locally applicable law or a collective agreement pursuant to locally applicable law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;

or

- ✓ Data Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

or

- ✓ the Data Processing is required in the context of preventive medicine or medical diagnosis by a health professional under applicable national law;

or

- ✓ the Data Subject himself/herself has already manifestly placed the affected Sensitive Data in the public domain;

or

- ✓ the Data Processing is essential for the purpose of establishing, exercising or defending legal claims, provided that there are no grounds for assuming that the Data Subject has an overriding legitimate interest in ensuring that such data is not processed;

or

- ✓ the Data 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 law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy.

2.4. Criminal conviction data

When Atos acts as a Controller, criminal conviction data shall only be processed provided that:

- ✓ In addition to one of the conditions specified in 2.1 above, the Data Processing is carried out under the control of official authority or is authorized by applicable law which provides for appropriate safeguards for the rights and freedoms of Data Subjects.

2.5. 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 Personal 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.

2.6. Automated individual decisions

When automated Personal Data Processing may have a negative effect or a legal consequence on the Data Subject, Atos shall notify the Data Subject about the occurrence of such automated decisions and will implement measures, where applicable, to protect the right of the individual in such circumstances not to have such a decision taken based solely on automated processing.

The Data Subject has the right not to be subject to a decision based solely on automated processing subject to legal exemptions as outlined in Section 4.

2.7. Accountability

2.7.1. Impact Assessment

In order to target an appropriate level of compliance with the principles defined in this Section 2, Atos conducts a Compliance Assessment of Data Processing as Controller ("Atos CADP-C"). Atos CADP-C must be completed for all processes involving Personal Data, and it shall be reviewed by the competent Data Protection Office.

In addition, where a processing operation on Personal Data transferred under these Atos BCR-C is likely to result in a high risk to the rights and freedoms of natural persons, a Data Protection Impact Assessment ("Atos DPIA") should be carried out following the requirements in Article 35 of the GDPR. Atos DPIA shall be reviewed by the competent Data Protection Office.

Where such an Atos DPIA results in a high risk to the rights and freedoms of individuals, in the absence of measures taken by Atos to mitigate the risk, or where residual risk remains high after the risk mitigation, Atos will consult the competent Data Protection Authority prior to undertaking the Data Processing.

Atos CADP-C and Atos DPIA must be carried out as detailed in Appendix 6.

2.7.2. Records of Data Processing activities

When acting as a Controller, all Atos Entities falling within the scope of these Atos Group BCR-C shall maintain records of their respective Data 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 records of the Data Processing activities take the format of the Atos CADP-C.

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

1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
2. the purposes of the Data Processing;
3. a description of the categories of Data Subjects and of the categories of Personal Data;
4. the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations.
5. where applicable, the details of the transfers of Personal Data to a Third Country or an international organization and the details of safeguards and mechanisms for the transfer;
6. where possible, the envisaged time limits for erasure of the different categories of Personal Data;
7. where possible, a general description of the technical and organizational security measures.

3. Personal Data Transfer

Being an international information technology services company, established worldwide, Atos is acting internationally and transferring data all over the globe. As a result, Atos processes 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 Personal Data transferred is harmonized throughout the Atos Group.

Under the provisions of these Atos Group BCR-C, 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 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 Data Exporter to other Atos Entities, acting as Data Importer, are described in Appendix 7.

No transfer of Personal Data to an Atos Entity will be made on the basis of these Atos Group BCR-C 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-C 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 enable Atos Entity concerned to demonstrate 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 an Atos Entity or to a Third Party located in the EEA or in a Third Country that has received an adequacy decision from the European Commission.

Where an Atos Entity located anywhere, acting as a Data Exporter, transfers Personal Data to another Atos Entity located within the EEA or in a Third Country that has been recognized by the European Commission as providing adequate level of data protection standards through an adequacy decision, the Atos Entity transferring the Personal Data shall ensure that the entity receiving the Personal Data commits in writing to provide sufficient guarantees in respect of the technical security measures and organizational measures governing the Personal Data Processing.

3.2. Personal Data Transfer by an Atos Entity in the EEA, acting as a Data Exporter, to an Atos Entity bound by these Atos Group BCR-C which is located in a Third Country which has not received an adequacy decision from the European Commission.

Where an Atos Entity in the EEA, acting as a Data Exporter, transfers Personal Data to another Atos Entity, located in a Third Country which has not received an adequacy decision by the European Commission, the transfer is covered by these Atos Group BCR-C.

In such circumstances, in concordance with the EDPB Recommendations 1/2022, the Atos Entity acting as the Data Exporter shall assess, for each transfer or set of transfers, on a case-by-case basis (and considering the laws and practices in the Third Country of destination), whether there is a need to implement supplementary measures in order to provide for a level of protection essentially equivalent to the one provided by the GDPR. Such assessments shall be documented and made available to the Data Protection Authority upon request. In cases where it is determined that supplementary measures are required, the Local Data Protection Office of the Data Importer will be consulted.

Such assessments will be based on the understanding that laws and practices that respect the fundamental rights and freedoms of individuals, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in the GDPR, are not in contradiction with these Atos Group BCR-C.

When assessing the above in respect of a particular transfer or set of transfers, the Data Exporter and Data Importer will take the following into account:

1. The specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same Third Country or to another Third Country, including:
   - ✓ purposes for which the Personal Data are transferred and processed (e.g. HR, storage, IT support)
   - ✓ types of entities involved in the Data Processing (the Data Importer and any further recipient of any onward transfer);
   - ✓ economic sector in which the transfer or set of transfers occur;
   - ✓ categories and format of the Personal Data transferred;
   - ✓ location of the Data Processing, including storage; and
   - ✓ transmission channels used.
2. The laws and practices of the Third Country of destination relevant in light of the circumstances of the Personal Data Transfer, including those requiring entities to disclose Personal Data to public authorities or authorizing access by such authorities and those providing for access to these Personal Data during the transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards.
3. Any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under the Atos Group BCR-C, including measures applied during the transmission and to the Data Processing in the country of destination.

3.3. Personal Data Transfer by an Atos Entity in the EEA, acting as a Data Exporter, to a Third Party located outside the EEA in a country that has not received an adequacy decision by the European Commission

Where an Atos Entity in the EEA, acting as a Data Exporter, transfers Personal Data to a Third Party, located outside the EEA in a country that has not received an adequacy decision by the European Commission, the Data Exporter shall ensure compliance with Section 3.1 of these Atos Group BCR-C and, where applicable, shall also ensure either that the Personal Data Transfer is protected by a valid agreement that incorporates EU Standard Contractual Clauses as approved by the European Commission, including a documented assessment of the risk of such a transfer, taking into account the contractual clauses between the Data Exporter and the Third Party, together with an assessment of that the Third Country's legal system, in particular to access by public authorities, to ensure that the transfer is subject to other appropriate safeguards.

4. Data Subject's rights

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

- ✓ The general data protection principles, in particular: purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, legal basis for Processing, Processing of Sensitive Data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by these Atos Group BCR-C;
- ✓ The right to be provided with easy access to these Atos Group BCR-C and in particular easy access to the information about their third-party beneficiary rights under these BCR, as specified in section 6;
- ✓ The right to receive confirmation on whether Personal Data concerning him/her are being processed, and if so, to be granted access to such Personal Data, together with information concerning the purposes of the Data Processing, categories of Personal Data, recipients of such Personal Data from Atos acting either as Controller or as Processor;
- ✓ The right to request the rectification of any inaccurate or incomplete Personal Data relating to him/her without undue delay, and to be notified upon the completion of such rectification as stated in section 7;
- ✓ The right to request erasure of any Personal Data relating to him/her where (a) the Processing is no longer necessary in relation to the purposes for which they were collected, (b) the legal basis is Consent and where Data Subject withdraws Consent, (c) the purpose of Processing is no longer lawful or (d) if there are no legitimate grounds for processing are identified following the exercise of the right to object, and to be notified upon the completion of such deletion, as stated in section 7.
- ✓ The right to request the restriction of Processing of their Personal Data, as stated in section 7, where (a) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling verification of the accuracy of the Personal Data, (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the Controller no longer needs the Personal Data for the purposes of the Data Processing, but they are required by the Data Subject for the establishment, exercise or defense of legal claims; (d) the Data Subject has objected to the Data Processing pending verification whether the legitimate grounds of the Controller override those of the Data Subject, and to be notified upon the completion of such restriction.
- ✓ The right to request the portability of Personal Data as stated in section 7, which the Data Subject has provided to Atos, where (a) the Data Processing is based on Consent given by Data Subject, (b) the Data Processing is necessary for the performance of a contract to which the Data Subject is party, (c) the Data Processing is carried out by automated means.

- ✓ The right to object to the Processing of their Personal Data, as stated in section 7, where such Data Processing is justified by legitimate interest or public interest, on the basis of compelling grounds relating to his/her particular situation, unless such Data Processing is required by applicable law. Where the objection is justified, the Data Processing will not be pursued.
- ✓ The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her, except where this decision (a) is necessary for entering into, or performance of a contract to which the Data Subject is party, (b) is required or authorized by applicable law which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests or, (c) is based on the Data Subject's explicit Consent, as stated in section 2.6.
- ✓ The Atos Entity's duty to respect these Atos Group BCR-C, as stated in section 1.2;
- ✓ 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 with the possibility to be represented a not-for-profit body, organization or association, as stated in section 5.2;
- ✓ The Atos Entity's duty to accept liability for paying compensation and to remedy breaches in accordance with section 6 of these Atos Group BCR-C;
- ✓ 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-C, as stated in section 6.2;
- ✓ The Atos Entity's duty to cooperate with Data Protection Authorities as stated in section 8.2;
- ✓ The obligation under these Atos Group BCR-C to be informed, where legally permitted, when national legislation prevents an Atos Entity from complying with its obligations under these Atos Group BCR-C;
- ✓ Other Atos Entities' duty to cooperate with the Controller as stated in section 10;
- ✓ To be informed regarding any update to these Atos Group BCR-C and to the list of Entities bound by these Atos Group BCR, as stated in section 17.

Any Data Subject can exercise their Data Protection Rights by completing and submitting the Online Form to contact the Data Protection Office at: https://atos.net/en/privacy/exercise-rights-regarding-personal-data or by sending or by completing Appendix 3 of this Atos Group BCR-C and send the form by email to dpo-global@atos.net.

Where a Data Subject's request is denied, the Data Subject is granted the right set up in Article 5 of the Atos Group BCR-C relating to the Complaint Handling Procedure and may exercise this right according to the procedure set up in Appendix 4.

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-C have caused him / her damage, he / she may complain to the Atos Group. Similarly, if a Data Subject believes that the Data Processing which is subject to these Atos Group BCR has not been conducted according to these Atos Group BCR-C, 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-locationshttps://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 6 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 finally rejected by the Local Data Protection Office, the Data Subject must be informed of the rationale leading to this decision and their right to lodge a complaint with a supervisory authority.

The use of these complaints 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 wish to do so.

5.2. 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-C, have caused him/her damage or have not been processed according to these Atos Group BCR-C, 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. 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 Controller, 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, according to section 5 of the Atos Group BCR-C. 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 the Atos Entity. Complaints and the rights of Data Subjects are addressed in sections 4 and 5 of these Atos Group BCR-C.

6.1. Liability of Atos Entities acting as Controller

Where a Data Subject suffers damage as a result of a breach of these Atos Group BCR-C by an Atos entity, acting as Controller, located within the EEA, the responsible Atos entity accepts responsibility for and agree to take necessary actions to remedy and pay compensation to the Data Subjects for any damages resulting from the violation of these Atos Group BCR-C by members of the Atos Group BCR-C.

Where a Data Subject suffers damage as a result of a breach of these Atos Group BCR-C by an Atos Entity located out of the EEA, Atos S.E., a EU based company, accepts responsibility for and agrees to take necessary actions to remedy and pay compensation to the Data subject for any damages resulting from the violation of these Atos Group BCR-C by members of the Atos Group BCR-C. 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 an Atos Entity acting as a Controller. Data Subject may exercise its rights before the courts or the competent data protection authority located where Atos S.E. is established.

6.2. Burden of proof

In any case, where section 6.1 applies, and where Data Subject has demonstrated that they have suffered damage that is likely to have been caused by a breach of the Atos Group BCR-C, 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-C by the Atos Entity.

7. Data Subject's information

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

In addition, Atos commits to provide Data Subjects with the following information with regard to any Processing of Personal Data that it implements (where reasonably possible):

- The identity of the Controller;
- The contact details of the data protection officer, where applicable;
- The purposes of the Processing for which the Personal Data are intended as well as the legal basis for their Processing;
- Where applicable, the legitimate interests pursued by the Controller or by a Third Party;
- The recipients or categories of recipients of the Personal Data, if any, and the categories of Personal Data concerned;
- Where applicable, information regarding data transfers to a Third Country and any relevant safeguards for such transfers;
- The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from the 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 applicable;
- The right to withdraw consent for Processing, where applicable;
- The right to lodge a complaint to the competent Data Protection Authority and / or to Atos;
- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- Information regarding the source from which the Personal Data originate, and if applicable, whether the data came from publicly accessible sources.

8. Cooperation

8.1. Cooperation with Third Parties

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 such as defined below.

8.2. 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 Data Protection Authorities.

Atos Entities shall also cooperate actively with all Data Protection Authorities requests in particular to ensure adequate and 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-C.

Atos Entities shall comply with the advice of the Data Protection Authorities on any issues regarding data protection.

9. 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 Controller, becomes aware of a Personal Data Breach, Atos shall, without undue delay and no later than 72 hours after having become aware of the Personal Data Breach, notify the competent Data Protection Authority, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of the Data Subjects affected. Such notification shall at least:

a. describe the nature of the Personal Data Breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
b. communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
c. describe the likely consequences of the Personal Data Breach;
d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In addition, where the Personal Data Breach incurred by Atos as a Controller is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall communicate to the Data Subject information relating to the Personal Data Breach which shall include in plain and clear text:

a. the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
b. a description of the likely consequences of the Personal Data Breach;
c. a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

In the event that any Atos Entity detects a data breach it will notify the liable Atos Entity without undue delay, including informing the relevant Local Data Protection Office for the liable Entity.

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.

10. Privacy by Design

10.1. Product and services development

Where one of the Atos Entities or business teams intends to develop new Processing, 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 a CADP-C as described in Appendix 6. The Local Data Protection Officer shall receive a copy of the CADP-C, shall conduct an assessment of the CADP-C and shall make recommendations to have the project run in a compliant manner.

Where required under applicable law, an Atos Entity will undertake 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.

Where a project is developed at global level, the Global Data Protection Office shall be consulted and shall produce a risk assessment regarding the project in order to make recommendations to have the project run in a compliant manner.

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.

10.2. New business opportunities and M&A

Where an Atos Entity intends to develop new business opportunities or to merge with or acquire a company, 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 structuration of the company.

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

Where a project is developed at global level, the Global Data Protection Office shall be consulted as of the beginning of any bid management or beginning of the project and it shall be involved at every stage of the project. The Global 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.

It results 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.

11. National Notification to Competent Data Protection Authorities

Where local Data Protection Authorities request prior notification of the process implemented, Atos commits to respect local requirements in this regard.

Atos keeps records of its Processing activities as both a Controller and a Processor. Where an Atos Entity acts as a Controller, each Local Data Protection Office keeps a register of processing implemented by Atos and gather all prior notification forms that are submitted to local Data Protection Authorities.

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

12. 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.

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.

13. Audit

Atos commits to audit Atos Group's compliance with regard to these Atos Group BCR-C including the implementation of these Atos Group BCR-C 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.

Specific audits may be requested in addition to the regular audit by the Group or Local Data Protection Office.

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 audits are guaranteed independence as to the performance of their duties.

The audit plan dedicated to these Atos Group BCR-C is described in Appendix 11.

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-C. This is in addition to any audit rights as defined in applicable data protection legislation.

14. 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.

15. 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, the Data Protection Community maintains KPI as designed by the Global 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 KPI, which are then centralized and analyzed by the Group Data Protection Office every six (6) months.

16. Investigation

Where on site investigation or audit takes place the Local Data Protection Office shall be immediately contacted, and it shall immediately contact the Group Data Protection Office.

As described in Section 8, the Local Data Protection Office and the Group Data Protection Office shall actively cooperate with the authority carrying on the investigation.

17. Update of the Atos Group BCR-C and communication

These Atos Group BCR-C may be amended from time to time and 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-C, 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-C;
- affect the binding nature of the Atos Group BCR-C,

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.

In any case, a list of Atos Entities bound by these Atos Group BCR-C 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 Officer which shall ensure appropriate communication as described in the precedent paragraph.

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

Where a modification to these Atos Group BCR-C would possibly be detrimental to the level of the protection offered by these Atos Group BCR-C or significantly affect them, the change must be communicated in advance to the 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-C 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 claimant and Atos SE is capable of paying for damages in case of breach of the BCR.

17.1. Legally Binding Request for Disclosure of Personal Data to a Public Authority

Where an Atos Entity acting as a Data Importer under these Binding Corporate Rules receives a legally binding request for disclosure of Personal Data by a Public Authority, the Atos Entity shall, subject to applicable legislation preventing or prohibiting it: attempt to suspend the execution of the request and inform the Data Protection Authority competent for the Atos entity as well as Atos's lead Data Protection Authority. The Data Importer shall also notify, where possible, any affected data subjects.

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 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 will also, where requested and legally permitted, notify any affected data subjects.

The 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.

The Data Importer will, under the same conditions, pursue possibilities of appeal.

When challenging a request, the 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.

The 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. It will also make it available to the Competent Data Protection Authority(ies) upon request.

The 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.

The Data Importer will maintain records of such requests for as long as the relevant Data is subject to the Atos Group BCR-C. 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 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 Authorit(ies) upon request.

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 Data Exporter and the relevant Data Protection Authorities and shall document it.

If a 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.

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.

17.2. Direct access by Public Authorities to Personal Data subject to these BCR

If aData Importer becomes aware of any direct access by Public Authorities to personal data transferred pursuant to these BCR, 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 all the information available about the Personal Data accessed.

Where acting as a Controller, the Data Importer will also, where possible, promptly notify the affected Data Subjects (if necessary, with the help of the Data Exporter). Where acting as a Processor, the Atos Entity acting as Data Importer will, where requested, help the Controller to notify any affected data subjects.

18. Appendices – Procedures

Appendix 1 – Organization of the Data Protection Community and Roles

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

Appendix 3 – Form for Data Subject to exercise their rights

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

Appendix 5 – Data Transfers – Categories of Data, Categories of Data Subject and Purposes of Data Transfer

Appendix 6 – Compliance and impact assessment of data processing when Atos acts a Controller

Appendix 7 – Local Data Protection Points of Contact

Appendix 8 – Audit plan (Steams)

Appendix 9 – 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