PUBLIC

ATOS BINDING CORPORATE RULES
(ATOS BCR)

AUTHOR(S)	:	Stéphane Larrière
DOCUMENT NUMBER	:	ASM-BMS-P022
BIP NUMBER	:	AP22
VERSION	:	2.0
STATUS	:	Final
SOURCE	:	Atos S.E.
DOCUMENT DATE	:	July 2019
NUMBER OF PAGES	:	46

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

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, either as a Controller or as a Processor, Atos has adopted these Binding Corporate Rules ("BCR").

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

The implementation of such BCR 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 BCR apply to all Atos Entities regardless of their localization and competent jurisdiction.

1.2.2 Material Scope

These BCR cover all Personal Data Processing irrespective of the nature of the Personal Data processed. These BCR cover all type of processing carried out by Atos acting as Controller or as Processor. As a result, these BCR cover processing of HR, Customer, Supplier, or Marketing and Communications Data.

Atos commits to provide the same level of protection to its own Employees' Personal Data as to any Third Parties' Personal data.

1.2.3 Bindingness amongst entities

These BCR are part of the Intra Group Agreement which make all Group policies legally binding amongst all Atos entities which enter into the Intra Group Agreement and which are listed in Appendix 2. This appendix also lists the country in which each 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

BCR are part of the 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 BCR by all employees.

1.2.5 Bindingness vis-à-vis customers

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

1.3 Document maintenance and distribution

The BCR are made available to all Atos employees and may be communicated to Customers upon request as specified in Section 9.

1.4 Related documents

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

1.5 Keywords

The terms used in these BCR are defined as follows:

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

Atos Entity: any of entity owned and/or controlled by Atos and which is bound by these BCR.

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: this Policy together with its Appendices, all together referenced as Atos BCR (AP 44).

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.

Data Exporter: any entity (of the group or of a third party) acting as a Controller and which transfers Personal Data to a Data Importer located in a Third country.

Data Importer: any entity located in a Third Country (of the group or of a third party) receiving Personal Data from a Data Exporter.

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

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

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

Employee: any person who is hired permanently by Atos.

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 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: 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.

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 BCR.

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

Third Country: all countries where the level of protection is not adequate in comparison to the level of protection provided by the country where the Data Exporter is located.

Third Party: Third Party / Third Parties: natural and legal persons with whom Atos has existing or planned business relations.

Personal Data Transfer: the disclosure of Personal Data to Third Parties, the transmission of such data to Third Parties, or the process of making such data available to Third Parties in any form for inspection or retrieval.

2 Principles for processing of Personal Data

The principles set out in these BCR shall be respected by Atos irrespective of local laws, except where local laws provide more stringent requirements than those set out in these BCR.

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 Customer's instructions, Atos shall inform the Customer immediately.

Where one of the Atos Entity has reasons to believe that the legislation applicable prevents the company from fulfilling

- ✓ its obligations under these BCR

  and / or

- ✓ the instructions it may have received from a Controller

and that such legislation has substantial effect on the guarantees provided by the BCR, it will promptly inform the Local Data Protection Office per e-mail or in writing and where Atos acts as Processor it shall inform duly the Controller and in close cooperation with Customer, inform the competent Data Protection Authority.

Where possible, the Local Data Protection Office handles the above issue as soon as possible, but in any case not later than one month after the complaint is received.

Where the Local Data Protection Office cannot handle the issue within a month after the complaint is received, it shall refer the case to the Group Data Protection Office which shall take action to solve the issue within two months after the Group Data Protection Office receives the complaint from the Local Data Protection Office.

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.

Where Atos acts as a Processor it shall also notify a Controller of any concern that it may have to consider for the delivery of the service by Atos in compliance with these BCR and with the Customer's instructions. Such notification to Customer shall be made in such a timely manner that it enables the Customer 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 Atos to the Customer. The same shall apply where Atos acts as a Processor and it has reasons to believe that the existing and/or future applicable legislation may prevent it from fulfilling the instructions received from the Controller or its obligations under the BCR.

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 processing relies on one of the following grounds:

- ✓ the Data Subject has given his Consent;

  or

- ✓ the Data Processing is necessary for the purposes of Legitimate interests pursued by Atos Entity or by the third party or 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;

  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 Atos is subject;

  or

- ✓ the Data Processing is necessary to save the vital interest of the Data Subject;

  or

- ✓ the Data Processing is necessary for the performance of a task carried out in the public interest or in a third party to whom the Data are disclosed.

Where Atos acts as a Processor, it commits to help and assist the Controller to respect the above listed principles.

2.2 Principles to be respected when processing Personal Data

When implementing a new Processing of Personal Data, Atos entity, acting as a Controller, shall guarantee that:

- ✓ The Processing is fair and lawful

  and

- ✓ The purpose of the processing is determined, explicit and legitimate

  and

- ✓ The Personal Data processed are relevant and not excessive

  and

- ✓ The appropriate security measures are implemented according to Atos Security Policy.

Where Atos acts as a Processor, it commits to help and assist the Controller to respect the above listed principles and shall promptly inform the Controller where Atos is not in a position to enable the Controller to respect such principles.

While the processing is being carried out, Atos entity acting as Controller, shall guarantee that:

- ✓ The data are kept accurate and up to date, and where data are inaccurate or incomplete, data are rectified, supplemented or erased.

  and

- ✓ The data are not kept longer than necessary for the purpose for which they are processed.

When acting as a Processor, Atos shall implement, in accordance with Controller's instructions the appropriate measures to enable the Controller to comply with the above principles. In addition, at the termination of the contract that binds Atos as a Processor with a Controller, Atos 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 legislation imposed upon them prevents it from returning or destroying all or part of the personal data transferred.

2.3 Sensitive data

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

- ✓ The Data Subject has given his/her Consent

  or

- ✓ the Data Subject is not in a position to give his/her Consent (e.g. medical emergency) and the Processing is necessary to protect the vital interests of the Data Subject or of another person,

  or

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

  or

- ✓ the Data Subject itself has already manifestly placed the affected Sensitive Data in the public domain,

  or

- ✓ the 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

- ✓ Processing is explicitly permitted by national law (e.g. registration/protection of minorities).

2.4 Security

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

Atos commits to develop enhanced security measures for the processing of Sensitive Data.

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

2.5 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 to ensure the legitimate interests of the Data Subject.

The Data Subject has 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 authorized by law, (c) is based on the Data Subject's explicit consent.

2.6 Accountability

2.6.1 Impact Assessment

In order to target an appropriate level of compliance with the principles defined in this Section 2, Atos conducts, where appropriate, a Record of Processing Activities ("RPA"), a Compliance Assessment of Data Processing ("CADP") as detailed in Appendices 8 and 9 and, where required under Applicable Data Protection Law, a Data Protection Impact Assessment ("DPIA").

Where an Atos Entity acts as a Controller, a CADP must be completed for all Processes. It shall be reviewed by the competent Data Protection Office.

Where Atos acts as a Processor, the RPA or, as the case may be, CADP is completed. The RPA or CADP is reviewed by the competent Data Protection Office and attached to the agreement to be signed with the Controller.

2.6.2 Records of Processing activities

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

Depending on the nature and circumstances of the processing, the records of processing activities shall take the format of Atos Records of Processing Activities (RPAs) or Compliance Assessments of Data Processing for Atos as a Controller (CADP-C) or as a Processor (CADP-P).

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 Atos Group.

Under the provisions of these BCR, Personal Data Transfers are the responsibility of Data Controllers which shall endorse to provide an adequate level of protection to Personal Data which are transferred.

The expected and anticipated purposes of transfer of Personal data between Atos entities acting either as Controller or as Processor are described in Appendix 7.

The implementation of the following provisions is further documented and explained in Appendix 7.

3.1 Personal Data transfer by an Atos Entity acting as a Controller to an Atos entity or to a Third Party located in the EU.

Where an Atos Entity, acting as a Controller, transfers Personal Data to another Atos Entity, located within the EU, 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 Processing of the Personal Data.

3.2 Personal Data transfer by an Atos Entity acting as a Controller to an Atos entity located outside of the European Union.

Where an Atos Entity, acting as a Controller, transfers Personal Data to another Atos Entity, located outside the EU, the transfer is covered by these BCR.

3.3 Personal Data transfer by an Atos Entity acting as a Controller to a Third Party located outside the EU.

Where an Atos Entity, acting as a Controller, transfers Personal Data to a Third Party, located outside the EU, the Atos Entity transferring the Personal Data shall ensure compliance with Section 3.1 of these BCR and shall also ensure either that it signs the appropriate EU Model Clauses adopted by the European Commission, as specified below, or that the transfer is subject to other appropriate safeguards.

For transfers to Atos Entities acting as Controller out of the EU, the clauses resulting from the EU Commission Decision dated 24 December 2004 (2004/915/CE).

For transfers to Atos Entities acting as Processor out of the EU, the clauses resulting from the EU Commission Decision dated 5 February 2010 (2010/87/UE).

3.4 Personal Data transfer by an Atos Entity acting as a Processor to an Atos Entity located within the EU.

Where an Atos Entity acting as a Processor, transfers Personal Data on behalf of a Controller to another Atos Entity on behalf of a Controller, it shall ensure that the sub-processor commit to respect the same obligations as the one which are binding the Data Controller and the importing Atos Entity within the EU.

3.5 Personal Data transfer by an Atos Entity acting as a Processor to an Atos Entity located outside the EU.

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

3.6 Personal Data transfer by an Atos Entity acting as a Processor to a Third Party.

Personal Data Transfer by an Atos Entity acting as a Processor to a Third Party is possible only where the Controller has given its express consent and where there are guarantees to 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 Processing of the Personal Data. Where this Third Party is located outside the EU, Atos Entity acting as processor and transferring the Data shall also facilitate the signature of the appropriate EU Model Clauses adopted by the European Commission or other appropriate safeguards between the Controller and the Third Party importing the Personal Data.

4 Data Subject's rights

Where Atos processes Personal Data acting either as Controller or as Processor, Data Subjects shall have the right, upon request, to:

- ✓ have access to the data relating to him/her processed by Atos acting either as Controller or as Processor;
- ✓ request the rectification or deletion of (a) any inaccurate or incomplete Personal Data relating to him/her, and of (b) any Personal Data with respect to which the purpose of Processing is no longer legal or appropriate;
- ✓ request the restriction of processing of their Personal Data 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 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 processing pending verification whether the legitimate grounds of the controller override those of the data subject.
- ✓ request the portability of Personal Data, which the Data Subject has provided to Atos, where (a) the processing is based on consent given by Data Subject, (b) the processing is necessary for the performance of a contract to which the Data Subject is party, (c) the processing is carried out by automated means.
- ✓ object, to the Processing of their Personal Data at any time, on the basis of compelling legitimate grounds relating to his/her particular situation, unless such Processing is required by applicable law. Where the objection is justified, the Processing will not be pursued.

All such requests shall be made according to the procedure set up on atos.net/en/privacy/exercise-rights-regarding-personal-data or in Appendix 3.

Data Subjects are entitled to contact the Group Data Protection Office by sending an 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 BCR 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 have caused him/her damage or have not been processed according to these BCR, or according to applicable law, Data Subjects are granted a right to complain against Atos Group.

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.

5.2 Indirect complaint

Where a Controller reports a complaint from a Data Subject whose Personal Data are processed by Atos 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 5.

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

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, Atos should comply with the procedure set up in Appendix 5.

6 Controller's complaint

Where Atos 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 Third Parties smoothly and efficiently, according to Appendix 6.

7 Liability vis-à-vis Data Subjects

Where a data subject suffers from a damage as a result of a processing of Personal Data by Atos, acting either as a Controller or as a Processor, the provisions below shall apply. It is reminded that Data Subject should first try to file a complaint directly to Atos in order to find an amicable solution according to section 5 of the BCR.

7.1 Liability of Atos Entities acting as Controller

In case of damage suffered by a Data subject as a result of a processing made by an Atos entity, acting as Controller, located within the EU, the responsible Atos entity shall accept 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 the BCR by members of the BCR.

Where a Data Subject suffers damage as a result of a breach of Atos BCR by an Atos Entity located out of the EU, 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 the BCR by members of the BCR, and it reserves its rights to engage its Local Entity responsibility. In this case, having a right to receive compensation, data subject may exercise its rights before the courts or the data protection competent authority located where Atos S.E. is established.

7.2 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 EU, 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, Atos recognizes that Data Subjects have the right to bring a claim against Atos S.E., a EU based company. In this case, the Data Subject may exercise its rights before the courts or the data protection competent authority located where Atos S.E. is established.

Where violation of the BCR is effectively recognized by a competent court, and is the responsibility of an Atos entity acting as a Processor based in the EU, this EU Atos Entity accepts responsibility for and agrees to take the necessary action to remedy the acts of other members of the BCR established outside of the EU and to pay compensation for any damages resulting from the violation of the BCR.

Where violation of the BCR is effectively recognized by a competent court, and is the responsibility of an Atos entity acting as a Processor based out of the EU and/or of an external sub-processor located outside of the EU, Atos S.E., a EU based entity, accepts responsibility for and agrees to take the necessary actions to remedy the acts of other entities of the Group bound by the BCR and/or of external sub-processors established outside of the EU as well as to pay compensation for any damages resulting from the violation of the BCR.

7.3 Burden of proof

In any case, where section 7.1 or 7.2 apply, and where Data Subjects have demonstrated that they have effectively suffered damage and that they establish facts proving the likely link between the damage suffered and a breach of the BCR, Atos accepts to bear the burden of proof for demonstrating that it is not liable for any damage suffered by Data Subject.

8 Liability vis-à-vis Controller

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

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

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

9 Data Subject's information

9.1 Permanent information

Atos commits to make its Binding Corporate Rules (BCR) readily available to every Data Subject and Controllers. The BCR are published on atos.net website and is accessible from all IT applications made available to its own Employees.

Upon Controllers' request workshops can be organised by Atos to detail further Atos BCR.

9.2 Data Subject's information when Atos acts as a Controller

In addition, where it acts as a Controller, 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 purposes of the processing for which the data are intended;
- The recipients or categories of recipients of the data;
- The existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

9.3 Data Subject's information when Atos acts as a Processor

Where Atos acts as a Processor, the responsibility to inform Data Subject lies in the hand of the Controller, i.e. the Third Party which requests Atos to process Personal Data on its behalf. Given that Atos intends to provide its Customers 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 Group commits to cooperate actively with Third parties in order to make sure that applicable law and regulations regarding Data Protection are respected by all stakeholders.

10.1 Cooperation with Controllers

Where Atos process Data on behalf of Controllers, Atos shall, to a reasonable extent and in a reasonable timing, provide the Controllers with relevant information, in order to enable the Controllers to comply with local data protection law requirements.

10.2 Cooperation with Data Protection Authorities

Atos 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 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.

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

Atos Entities shall, to a reasonable extent, abide by the advice of the Data Protection Authorities on any issues regarding data protection.

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 Atos, acting as a Controller, becomes aware of a Personal Data Breach, Atos shall, where feasible, in accordance with Applicable law and without undue delay 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 Atos, acting as a Processor, becomes aware of a significant Personal Data Breach, Atos shall, where feasible and without undue delay after having become aware of the Personal Data Breach, notify it to the Controller.

12 Privacy by Design

12.1 Product and services development

Where one of the Atos entities or business team intends to develop new processing, it shall make sure that Data Protection is taken into account as of the beginning of the project.

For this very purpose, where a project is developed at local level, the business team in charge of the new processing shall produce a CADP as described in Appendix 8 or 9. The Local Data Protection Office shall receive a copy of the CADP, shall conduct random reviews of the CADP 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 or 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.

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 Atos 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 Atos intends to develop new business opportunities or to merge with or acquire a company, Atos 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 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.

13 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.

Where Atos 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.

Where Atos acts as a Processor on behalf of Third Parties, Atos commits to provide Third Parties with all relevant information necessary to comply with local registration requirements.

14 Training and raising awareness

Atos believes that its BCR can be enforceable and effective throughout the Group only to the extent that a Global Training Program is developed regarding data protection issues.

For this purpose, Atos commits to:

- ✓ Develop a comprehensive Global Data Protection Program,
- ✓ Provide basic training to all employees of Atos,
- ✓ Provide specific and appropriate training to those employees who have regular or permanent access to personal data, which are involved in the collection of personal data or are engaged in the development of tools used to process personal data.

For this very purpose, Atos has developed a Global Training Program which aims at providing general training to all Employees and specific training to Employees who have permanent or regular access to Personal Data.

Specific modules taking into account local specificities will also be developed.

The attendance to the Data Protection Training will be monitored by the Data Protection Community as part of the Compliance team together with the Human Resources Department.

15 Audit

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

Such audit shall be carried out randomly 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 Board. As a result the audit is initiated by the Atos Headquarters entity, i.e. Atos International.

The results of the audit shall be communicated to the Data Protection Community and corrective actions shall be proposed.

Upon request, Competent Data Protection Authorities and Third Parties may obtain results of the Data Protection Audit.

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 BCR is described in Appendix 11.

16 Data Protection Community

Atos wants to ensure that the BCR are effectively implemented throughout the Group.

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

The Legal branch is led by the Chief Legal Counsel in Data Protection and the Operational and Security branch, is led by the Group Data Protection Officer both together the Group Data Protection Office.

These two branches rely on a network of Local Legal Experts in Data Protection and on Data Protection Officers, both together forming the Local Data Protection Office. They are all listed in Appendix 1. The whole Data Protection Community, including its two branches, is coordinated and supervised by the Group Chief Compliance Officer.

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

17 Key Performance Indicators (KPI)

In order to ensure an effective implementation of the 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 requests for access to their personal data
- ✓ number of data breaches
- ✓ number of notifications to local Data Protection Authorities
- ✓ number of EU model clauses signed to frame international data transfers

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

18 Investigation

Where on site investigation take place the Local Data Protection Office shall be immediately contacted, 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 BCR

These BCR may be amended from time to time and where necessary, in particular where applicable data protection regulation applies.

Any significant changes to these BCR shall be reported to all Atos Entities as well as to Data Protection Authorities at least once a year. Clear and easily available information regarding any such significant change shall be made for Employees and Third Parties information.

Where Atos acts as Processor it also commits to inform its Customers acting as Data Controller of any update and amendment of the scope of the BCR. 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 BCR 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 paragraph 2 of this section.

20 Miscellaneous

Where, when acting as a Controller, Atos receives a legally binding request for disclosure of data by a law enforcement authority, unless prohibited by law, Atos 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 concerned as well as Atos' lead Data Protection Authority.

Where, when acting as a Processor, Atos receives a legally binding request for disclosure of data by a law enforcement authority, unless prohibited by law, Atos shall, subject to applicable legislation preventing or prohibiting it, communicate it to the Controller. Atos shall suspend execution of the request and the Data Protection Authority competent for the Controller and Atos' lead Data Protection Authority shall be informed about it.

If applicable laws prohibit the suspension of execution or communication of the request, Atos shall use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as possible and as soon as possible to the Controller and the relevant Data Protection Authorities, and be able to demonstrate that it did so.

If, despite having used its best efforts, Atos is not in a position to inform the relevant Data Protection Authorities, Atos will provide at least once a year, general information on the requests received to the relevant Data Protection Authorities (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

In any case, Atos shall use its best efforts to 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.

21 RACI

RACI: R: Responsible A: Accountable C: Consulted I: Informed

Activity	Group Data Governance Office	Local DPLE	Local DPO
ADOPTION OF THE BCR FOR THE ENTITIES			
Adoption of an Intra-Group Agreement between Atos parent company and Atos entities regarding the bindingness of the BCR	A/R	C (regarding the content of the IGA) / R (regarding the signature of the IGA)	I
For each BCR new member, determine whether or not a Local Board Decision is necessary	C	A/R	I
if yes: Presentation to the Local Board to request validation by the Board	C	A/R	I

Activity	Group Data Governance Office	Local DPLE	Local DPO
MAKING BCR BINDING AMONGST EMPLOYEES			
Translate BCR into local language when required by Local law	I	A/R	A/R
Determination of the local requirements regarding Work Councils	I	A/R	A
Where necessary, prepare communication pack for Work Councils presentation	C	A/R	A/R
Where necessary, consultation or information needed: set up date and present to Works Councils	C	A/R	A/R
Where not necessary: communicate broadly to all employees to comply with transparency and information requirement (via mailing or through appropriate local bulletin).	A (for effective Communication at global level) / R (for drafting the communication)	R (for effective communication at local level)	R (for effective Communication at local level)

Activity	Group Data Governance Office	GBU & GDC DPLE	GBU & GDC DPO	Local DPLE	Local DPO
TRANSLATION OF ALL MATERIALS AND TOOLS INTO LOCAL LANGUAGE					
Ensure translation of all materials into local language	I	I	I	A (as a DPO team) /R	A (as a DPO team) /R
TRAINING					
Prepare the Global & General training	A/R (Design trainings (mandatory & dedicated)	C	C	C	C
Update DP training with local specificities, including translation (e.g. establish legal training content for local needs)	I	R	R	A (as a DPO team) /R	A (as a DPO team) /R
Ensure DP training is effectively followed by Employees at local level (Roll-out mandatory and dedicated trainings)	R	R	R	A (as a DPO team) /R	A (as a DPO team) /R
Deliver class room training when needed	A/R (for the relevant scope)	A/R (for the relevant scope)	A/R (for the relevant scope)	A/R (for the relevant scope	A/R (for the relevant scope)
Identify training needs	A/R (for the relevant scope)	A/R (for the relevant scope)	A/R (for the relevant scope)	A/R (for the relevant scope)	A/R (for the relevant scope)
Make available training for DP Community	A/R	R	R		
Train local DPOs and DPLEs	C	A/R	A/R		

Activity	Group Data Governance Office	GBU & GDC DPLE	GBU & GDC DPO	Local DPLE	Local DPO	Operational
HANDLING CUSTOMERS' REQUESTS OR COMPLAINTS AT GLOBAL LEVEL						
Receive complaints of Customer	I	I	I			A/R
Send A/R of the complaint in due time	I	I	I			A/R
Analysis of the complaint	C	I	I			A/R
Resolution of the complaint	C	I	I	I	I	A/R
HANDLING CUSTOMERS' REQUESTS OR COMPLAINTS AT LOCAL LEVEL						
Receive complaints of Customer	I	I	I	I	I	A/R
Send A/R of the complaint in due time	I	I	I	I	I	A/R
Analysis of the complaint	I	C (where needed)	C (where needed)	R	R	A/R
Resolution of the complaint	I	I	I	C	C	A/R

HANDLING EMPLOYEES'/VISITORS REQUESTS OR COMPLAINTS (OR ANY OTHER DATA SUBJECTS WHEN ATOS ACTS AS CONTROLLER)						
Receive complaints of Customer	I	I	I	A (as a DPO team) /R	A (as a DPO team) /R	
Send A/R of the complaint in due time	I	I	I	A (as a DPO team) /R	A (as a DPO team) /R	
Analysis of the complaint	C (where needed)	C (where needed)	C (where needed)	A (as a DPO team) /R	A (as a DPO team) /R	
Resolution of the complaint	I	I	I	A (as a DPO team) /R	A (as a DPO team) /R	
HANDLING DATA SUBJECTS COMPLAINTS RECEIVED WHEN ACTING AS A PROCESSOR						
Receive complaints of Data Subjects	I (report of KPI by Local)	I (report of KPI by Local)	I (report of KPI by Local)	A (as a DPO team) /R	A (as a DPO team) /R	I (where concerned)
Send A/R of the complaint in due time				A (as a DPO team) /R	A (as a DPO team) /R	I (where concerned)
Provide the contract related to the Request/ Complaint	R			A (as a DPO team) /R	A (as a DPO team) /R	R
Reviewing the provisions of the Contracts regarding the agreed responsibilities with Clients regarding Data Subjects	C (where needed)	C (where needed)	C (where needed)	A (as a DPO team) /R	A (as a DPO team) /R	I (where concerned)

According to the terms of the Agreement, transfer the request/complaint to the Client	I (report of KPI by Local)	I (report of KPI by Local)	I (report of KPI by Local)	I	I	A/R
According to the terms of the Agreement, direct resolution of the request/complaint	C (where needed)	C (where needed)	C (where needed)	A (as a DPO team) /R	A (as a DPO team) /R	R
HANDLING OF THE LEAD DATA PROTECTION AUTHORITY'S REQUESTS						
Receive request (ensuring that there is an effective process in place)	A/R			C (if concerned)	C (if concerned)	I (if concerned)
Send A/R of the request in due time	A/R			C (if concerned)	C (if concerned)	I (if concerned)
Analysis of the request	A/R			C (if concerned)	C (if concerned)	C (if concerned)
Answer to the request	A/R					
Follow up of the request	A/R					
HANDLING OF LOCAL DATA PROTECTION AUTHORITY'S REQUESTS						
Receive request (ensuring that there is an effective process in place)	I			A/R	R	I (if concerned)

Send A/R of the request in due time	**I**			**A/R**	**R**	**I (if concerned)**
Analysis of the request	**C**	**I**	**I**	**A (as a DPO team) /R**	**A (as a DPO team) /R**	**C (if concerned)**
Answer to the request	**C**	**I**	**I**	**A (as a DPO team) /R**	**A (as a DPO team) /R**	**C (if concerned)**
Follow up of the request	**I**	**I**	**I**	**A (as a DPO team) /R**	**A (as a DPO team) /R**	**C (if concerned)**
GENERAL NOTIFICATION/AUTHORIZATION REQUEST TO DATA PROTECTION AUTHORITIES						
Complete necessary local formalities with DPAs	**C**	**C**	**C**	**A (as a DPO team) /R**	**A (as a DPO team) /R**	
Monitoring of such requests/formalities	**C**	**C**	**C**	**A (as a DPO team) /R**	**A (as a DPO team) /R**	
Where necessary, contact the Data Protection Authority for processes at Global Level	**R**			**A (as a DPO team) /R**	**A (as a DPO team) /R**	
First response to local DP related events: identify legal obligations (notifications, etc.)	**I**	**A (as a GBU DPO team) /R**	**A (as a GBU DPO team) /R**	**R**	**R**	
DATA BREACH NOTIFICATION TO DATA PROTECTION AUTHORITIES						
Complete Data Breach Templates	**C**	**C**	**C**			**A/R**

Receive Data Breach Templates	**A/R (when the breach has a global impact)**	**R**	**R**	**A/R (when the breach has a local impact)**	**A/R (when the breach has a local impact)**	
Transmit the Data Breach Notification to the relevant DPA	**A/R (when the breach has a global impact)**	**R**	**R**	**A/R (when the breach has a local impact)**	**A/R (when the breach has a local impact)**	
DATA BREACH NOTIFICATION TO DATA SUBJECTS						
Complete Data Breach Templates	**C**	**C**	**C**	**C**	**C**	**A/R**
Receive Data Breach Templates	**A/R (when the breach has a global impact)**			**A/R (when the breach has a local impact)**	**A/R (when the breach has a local impact)**	
Transmit the Data Breach Notification to the relevant Data Subjects	**A/R (when the breach has a global impact)**			**A/R (when the breach has a local impact)**	**A/R (when the breach has a local impact)**	

Activity	Group Data Governance Office	GBU & GDC DPLE	GBU & GDC DPO	Local DPLE	Local DPO	Operational	Contract Lawyer
DATA PROTECTION CLAUSES IN GLOBAL CONTRACTS							
Ensuring that the Data Protection Clauses is part of all Contract where personal data is processed						A/R	
Reviewing DP clauses in major contracts	C (if needed)	I		I		C	A/R
Implementing standard clauses	I	I		I		A/R	C
Preparing Data Transfer Agreements	C (if needed)	I		I		A/R	C
Getting Data Transfer Agreements signed	I	I		I		A/R	C
Reviewing and approving the security appendices	C (if needed)	I		I		A/R (jointly with Group Security Officer)	I

DATA PROTECTION CLAUSES IN LOCAL CONTRACTS							
Ensuring that the Data Protection Clauses is part of all Contracts where personal data is processed				R (pass the message when reviewing the CADP)	R (pass the message when reviewing the CADP)	A/R	
Reviewing DP clauses in major contracts (i.e. above 100m€)	I (KPI)	I/C (when problems)	I	A/R	C	I	I
Reviewing DP clauses in all contracts below 100 m€	I	I/C (when problems)	I	C (if necessary)		I	A/R
Preparing Data Transfer Agreements in major contracts (i.e. above 100m€)	C (in case of difficulties)	C (in case of difficulties)		A/R	I	C	
Preparing Data Transfer Agreements in all contracts below 100m€	C (in case of difficulties)	C (in case of difficulties)		C (in case of difficulties)	I	C	A/R
Getting Data Transfer Agreements signed				C	I	C	A/R
Reviewing and approving the security appendices			C (in case of difficulties)	I	C	A/R (jointly with Security Officer)	I

Activity	Group Data Governance Office	GBU & GDC DPLE	GBU & GDC DPO	Local DPLE	Local DPO	Operations (Business Owner + relevant support functions)
COMPLIANCE ASSESSMENT OF DATA PROCESSING (CADP) AT GLOBAL LEVEL						
Completing the CADP as Controller (CADP-C)	C	I (SP register)	I (SP register)	I (SP register)	I (SP register)	A/R for Business Owner C for Support Function
Submitting the CADP as Controller for GDPO review	I (SP register)	I (SP register)	I (SP register)	I (SP register)	I (SP register)	A/R for Business Owner C for Support Function
Reviewing the CADP as Controller (CADP-C)	A/R	R (SP register)	R (SP register)	I (SP register)	I (SP register)	R
Ensuring the CADP is embedded in the Contract	C (where needed)					A/R
Implementing corrective measures, after notification of the Client and Submit to Review if needed						A/R

Implementing corrective measures, after instructions to the Supplier/service Provider and Submit to Review if needed						**A/R**
Monitoring Supplier's / Service Provider's Data Protection practices	**C (where needed)**					**A/R**
COMPLIANCE ASSESSMENT OF DATA PROCESSING (CADP) AT LOCAL LEVEL						
Fulfilling the CADP	**I (SP register)**	**I (SP register)**	**I (SP register)**	**C**	**R (support)**	**A/R**
Submitting the CADP for Local Review	**I (SP register)**	**I (SP register)**	**I (SP register)**	**I (SP register)**	**I (SP register)**	**A/R**
Reviewing the CADP	**I (SP register)**	**I (SP register)**	**I (SP register)**	**A (as a DPO team)/R**	**A (as a DPO team)/R**	**R**
Completing the CADP-P	**I (figures in Dashboard)**	**I (figures in Dashboard)**	**I (figures in Dashboard)**	**I (figures in Dashboard)**	**I (figures in Dashboard)**	**A/R for Business Owner C for Support Function**
Reviewing the CADP-P	**I (figures in Dashboard)**	**I (figures in Dashboard)**	**I (figures in Dashboard)**	**I (figures in Dashboard)**	**I (figures in Dashboard)**	**R**
Giving corrective measures in case CADP raises alerts	**I (SP register)**	**C (for legal issues) / I (for technical issues)**	**C (for technical issues) / I (for legal issues)**	**A as a DPO team/R (give Go/No go)**	**A as a DPO team/R (give Go/No go)**	**C**

Ensuring the CADP is embedded in the Contract	**C (in case of arbitrage)**	**C (in case of difficulties)**	**C (in case of difficulties)**	**C**	**C**	**A/R**
Implementing corrective measures, after notification of the Client and Submit to Review if needed	**I**	**I**		**I**	**I**	**A/R**
Implementing corrective measures, after instructions to the Supplier/service Provider and Submit to Review if needed	**I**	**I**		**I**	**I**	**A/R**
Monitoring Supplier's / Service Provider's Data Protection practices				**C (where needed)**	**C (where needed)**	**A/R**
RECORD OF PROCESSING ACTIVITIES (RPA) AT GLOBAL LEVEL						
Creating RPA for processing begun before 25.05.18, that will continue after 25.05.18.	**I (SP register)**	**I (SP register)**	**I (SP register)**	**I (SP register)**	**I (SP register)**	**A/R**
Reviewing the RPA	**R**	**I (SP register)**	**I (SP register)**	**A (as a DPO team) /R**	**A (as a DPO team) /R**	**C**

RECORD OF PROCESSING ACTIVITIES (RPA) AT LOCAL LEVEL						
Completing the RPA for processing begun before 25.05.18, that will continue after 25.05.18.	**I (SP register)**	**I (SP register)**	**I (SP register)**	**I (SP register)**	**I (SP register)**	**A/R**
Reviewing the RPA	**I (SP register)**	**I (SP register)**	**I (SP register)**	**A (as a DPO team)/R**	**A (as a DPO team)/R**	**C**
REGISTER OF PROCESSING ACTIVITIES						
Creating the register	**I**	**I**	**I**	**C**	**C**	**A/R**
Reviewing the Register	**C**	**I**	**I**	**A as a DPO team/R (for local projects)**	**A as a DPO team/R (for local projects)**	**C**
Ensuring that the latest CADP is downloaded in the Register	**C (for global projects)**	**I**	**I**	**C (for local projects)**	**C (for local projects)**	**A/R**

22 APPENDICES – PROCEDURES

Appendix 1 – Organisation of the Data Protection Community and Roles

Appendix 2 – List of entities bound by the BCR

Appendix 3 – Form for Data Subject's rights exercise

Appendix 4 – Complaint Handling Procedure where Atos acts as a Controller

Appendix 5 – Complaint Handling Procedure where Atos acts as a Processor

Appendix 6 – Complaint Handling Procedure for Third Parties which Personal Data are processed by Atos

Appendix 7 – Transfer of Personal Data – Standard clauses and guidelines

Appendix 8 –Compliance Assessment of Data Processing where Atos acts as a Controller

Appendix 9 –Compliance Assessment of Data Processing where Atos acts as a Processor

Appendix 10 – Local Data Protection Points of Contact

Appendix 11 – Audit plan