ATOS BINDING CORPORATE RULES (ATOS BCR)

AUTHOR(S) : Lionel de Souza
DOCUMENT NUMBER : ASM-BMS-P022
BIP NUMBER : AP22
VERSION : 1.4
STATUS : Final
SOURCE : Atos S.E.
DOCUMENT DATE : 29 septembre 2014
NUMBER OF PAGES : 40
Contents

1 Introduction ........................................................................................................... 5
1.1 Purpose ............................................................................................................ 5
1.2 Scope ............................................................................................................... 5
1.3 Document maintenance and distribution .................................................. 6
1.4 Related documents ....................................................................................... 6
1.5 Keywords ........................................................................................................ 6
2 Principles for processing of Personal Data ................................................... 8
2.1 Legal grounds for processing Personal Data ............................................ 8
2.2 Principles to be respected when processing Personal Data .................. 9
2.3 Sensitive data ............................................................................................... 9
2.4 Security .......................................................................................................... 10
2.5 Automated individual decisions ............................................................... 10
2.6 Implementation of the principles of Section 2 ......................................... 10
3 Transfer of Personal Data ........................................................................... 11
3.1 Personal Data transfer by an Atos Entity acting as a Data Controller to an Atos entity or to a Third Party located in the EU .......... 11
3.2 Personal Data transfer by an Atos Entity acting as a Data Controller to an Atos entity located outside of the European Union ...... 11
3.3 Personal Data transfer by an Atos Entity acting as a Data Controller to a Third Party located outside the EU .................. 11
3.4 Personal Data transfer by an Atos Entity acting as a Data Processor to an Atos Entity located within the EU ........................ 12
3.5 Personal Data transfer by an Atos Entity acting as a Data Processor to an Atos Entity located outside the EU .................. 12
3.6 Personal Data transfer by an Atos Entity acting as a Data Processor to a Third Party ................................................. 12
4 Data Subject’s rights ................................................................................. 13
5 Complaint handling procedure ..................................................................... 14
5.1 Direct complaint ......................................................................................... 14
5.2 Indirect complaint ..................................................................................... 14
6 Data Controller’s complaint ....................................................................... 15
7 Liability vis-à-vis Data Subjects ................................................................ 16
7.1 Liability of Atos Entities acting as Data Controller ............................... 16
7.2 Liability of Atos Entities acting as Data Processor ................................. 16
7.3 Burden of proof ......................................................................................... 17
8 Liability vis-à-vis Data Controller .............................................................. 18
9 Data Subject’s information ....................................................................... 19
9.1 Permanent information ........................................................................... 19
9.2 Data Subject’s information when Atos acts as a Data Controller ........... 19
9.3 Data Subject’s information when Atos acts as a Data Processor ........... 19
10 Cooperation ............................................................................................. 20
10.1 Cooperation with Data Controllers ....................................................... 20
10.2 Cooperation with Data Protection Authorities ........................................... 20
11 Privacy by Design ............................................................................................ 21
11.1 Product and services development ................................................................. 21
11.2 New business opportunities and M&A ............................................................ 21
12 National Notification to Competent Data Protection Authorities ................. 22
13 Training and raising awareness ..................................................................... 23
14 Audit ................................................................................................................ 24
15 Data Protection Community ............................................................................ 25
16 Key Performance Indicators (KPI) ................................................................. 26
17 Investigation .................................................................................................... 27
18 Update of the BCR ........................................................................................ 28
19 Miscellaneous ................................................................................................ 29
20 RACI ............................................................................................................... 30
21 APPENDICES – PROCEDURES ..................................................................... 40
### List of changes

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


1 Introduction

1.1 Purpose

Atos has always put data protection as one of its top priority. As such, Atos has committed to applying best in class standards in terms of corporate responsibility (adhesion in the GRI, UN Global Compact). Following SIS integration and in order to guarantee the highest level of protection to the data it processes, either as a Data Controller or as a Data 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 intends 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 the Atos Entities regardless 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 being acting as Data Controller or as Data 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 than 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.

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 Data 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 précised in Section 9.

1.4 Related documents

These BCR are also composed of 9 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 Appendix, 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.

Data 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 Data 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.

Data 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 Data 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 15 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 are providing more stringent requirements than those set up in these BCR.

Notwithstanding the elements contained in this Section 2, where Atos acts as a Data Processor, under the instructions of a Data Controller, it shall in addition, respect the instructions provided by the Data Controller regarding the data processing, the security and the confidentiality measures that are agreed in a contract between the Data Controller and the Data Processor. Where Atos acting as a Data Processor is not able to comply with Customer’s instructions, Atos shall inform immediately Customer.

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 Data 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 Data Processor it shall inform duly the Data 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 handled 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 counsels advice in order to ensure compliance with the most stringent provisions.

Where Atos acts as Data Processor it shall also notify Data Controller any concern that it may have to consider for the delivery of the service by Atos in compliance with these BCR and with Customer’s instructions. 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. The same shall apply where Atos acts as Data Processor and that it has reasons to believe that the existing and/or future applicable legislation may prevent 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, Atos Entity acting as Data 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 Data Processor, it commits to help and assist Data 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 Data 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 Data Processor, it commits to help and assist Data Controller to respect the above listed principles and shall promptly inform the Data Controller where Atos is not in a position to enable Data Controller to respect such principles.

While the processing is being carried out, Atos entity acting as Data 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 of which they are processed.

When acting as Data Processor, Atos shall implement, in accordance with Data Controller’s instructions the appropriate measures to enable Data Controller to comply with the above principles. In addition, at the termination of the contract that binds Atos as Data Processor with a Data Controller, Atos shall, according to Data Controllers’ instruction’s return all the personal data transferred and the copies to the Data Controller or shall destroy all the personal data and certify to the data 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 Data 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 Data Processor, cooperate with Data Controller, to ensure that Atos security measures and applicable policy meet Data 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.

2.6 Implementation of the principles of Section 2

The implementation of the principles set up in this Section 2 shall be monitored by conducting Privacy Impact Assessment as detailed in Appendices 8 and 9 which enable the Data Privacy Community to ensure that the data processed by Atos either as a Data Controller or as a Data Processor are provided with a high and appropriate level of protection.
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 Data controller or as Data Processor are described in Appendix 7.

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

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

Where an Atos Entity, acting as a Data 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 Data Controller to an Atos entity located outside of the European Union.

Where an Atos Entity, acting as a Data 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 Data Controller to a Third Party located outside the EU.

Where an Atos Entity, acting as a Data 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 that it signs the appropriate EU Model Clauses adopted by the European Commission.

For transfers to Atos Entities acting as Data 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 Data 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 Data Processor to an Atos Entity located within the EU.**

Where an Atos Entity acting as a Data Processor, transfers Personal Data on behalf of a Data Controller to another Atos Entity on behalf of a Data 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 Data Processor to an Atos Entity located outside the EU.**

Where an Atos Entity, acting as a Data Processor, transfers Personal Data on behalf of a Data Controller to another Atos Entity, located outside the EU, the transfer is covered by these BCR. Atos commits to obtain Data Controller’s consent prior to such consent. Atos 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 Data Processor to a Third Party.**

Personal Data Transfer by an Atos Entity acting as a Data Processor to a Third Party is possible only where Data 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 between Data Controller and the Third Party importing the Personal Data.
4 Data Subject’s rights

Where Atos processes Personal Data acting either as Data Controller or as Data 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 Data Controller or as Data Processor;
- ✔ request the rectification, deletion or suspension 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;
- ✔ 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 in Appendix 3.

Where Data Subjects requests is denied, Data Subjects are granted the right set up in Article 5 of the BCR relating to Complaint Handling Procedure, and 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 its Personal Data have cause him/her a 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 privilege 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 Data Controller reports a complaint from a Data Subject whose Personal Data are processed by Atos as Data Processor, Atos shall take all necessary steps to make sure that Data Subject complaint is handled. For this purpose, Atos should comply with the procedure set up in Appendix 5.

Where a Data Subjects whom Personal Data are processed by Atos as a Data processor file directly complaint to Atos, Atos shall immediately inform the Data Controller about the claim and act according to Appendix 4 to escalate the claim.

Where the Data 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 Data Controller by contract or by operation of law, Atos should comply with the procedure set up in Appendix 5.
6 Data Controller’s complaint

Where Atos processes Personal Data on behalf of Data 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 Data Controller or as a Data 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 Data Controller

In case of damage suffered by a Data subject as a result of a processing made by an Atos entity, acting as Data 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 a 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 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, 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 Data Processor

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

a. The Data Controller has factually disappeared or
b. The Data Controller ceased to exist in law or
c. The Data Controller has become insolvent, unless any successor entity has assumed the entire legal obligations of the Data 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 subjects 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 recognised by a competent court, and is of the responsibility of an Atos entity acting as a Data Processor based in the EU, this EU Atos Entity accepts responsibility for and agree 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 recognised by a competent court, and is of the responsibility of an Atos entity acting as a Data 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 agree 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 of any damage suffered by Data Subject.
8 Liability vis-à-vis Data Controller

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

The Data 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 Data 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 Data Controllers. The BCR are published on atos.net website and is accessible from all IT applications made available to its own Employees.

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

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

In addition, where it acts as a Data 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 Data Processor

Where Atos acts as a Data Processor, the responsibility to inform Data Subject lies in the hand of the Data Controller, e.g. 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 Data Controllers it work with, with relevant information which will enable Data Controller to fulfill 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 Data Controllers

Where Atos process Data on behalf of Data Controllers, Atos shall, to a reasonable extent and in a reasonable timing, provide Data Controllers with relevant information, in order to enable Data 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 issues.
11 Privacy by Design

11.1 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 Privacy Risk Assessment as described in Appendix 8 or 9. The Local Data Protection Office shall receive a copy of the Privacy Impact Assessment and shall conduct random review of the Privacy Impact Assessment and shall make recommendations to have the project run in a compliant manner.

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 Office shall produce a risk assessment regarding the project in order to make recommendation 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.

11.2 New business opportunities and M&A

Where Atos intends to develop new businesses 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 recommendation 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.

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 **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 Data Controller, each Local Data Protection Office keep a register of processing which are implemented by Atos and are gathering all prior notification form that are submitted to local Data Protection Authorities.

Where Atos acts a Data Processor on behalf of Third Parties, Atos commits to provide Third Parties with all relevant information necessary to comply with local registration requirements.
13 Training and raising awareness

Atos believes that its BCR can be only 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 whom have regular or permanent access to personal data, which are involved in the collection of personal data or 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.
14 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 which 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 Data Processor, Data Controllers can request an audit to be carried out on the Atos and/or sub-processors’ facilities used to process Data Controller’s personal Data. Such audit request can be valid only provided that Data Controller gives appropriate prior notification to Atos.

The audit plan dedicated to these BCR is described in Appendix 10.
15 **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 are relying 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.
16 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 request for access to their personal data
- number of data loss
- number of notification to local Data Protection Authorities
- number of EU model clauses signed to framed 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.
17 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.
18 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. A clear and easily available information regarding any such significant change shall be made for Employees and Third Parties information.

Where Atos acts as Data 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.
19 **Miscellaneous**

Where Atos receives legally binding request for disclosure of data by a law enforcement authority, unless prohibited by law, Atos shall communicate it to the Data Controller, and shall be put on hold and the DPA competent for the controller and the lead DPA shall be informed about it.
## RACI

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Chief Legal Counsel DP and Security</th>
<th>Group DPO</th>
<th>Local Legal Expert</th>
<th>Local DPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADOPTION OF THE BCR FOR THE ENTITIES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adoption of an Intra-Group Agreement between Atos parent company and Atos entities regarding the bindingness of the BCR</td>
<td>A/R</td>
<td>I</td>
<td>C (regarding the content of the IGA) / R (regarding the signature of the IGA)</td>
<td>I</td>
</tr>
<tr>
<td>For each BCR, determine whether or not a Local Board Decision is necessary</td>
<td>A</td>
<td>I</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>If yes: Presentation to the Local Board to request validation by the Board</td>
<td>A</td>
<td>I</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>If not: Formal Statement by Local Function on behalf of the local entity that the BCR are effective in the relevant entity</td>
<td>A/R</td>
<td>A/R</td>
<td>R</td>
<td>C</td>
</tr>
</tbody>
</table>
### Activity

<table>
<thead>
<tr>
<th>Activity</th>
<th>Chief Legal Counsel DP and Security</th>
<th>Group DPO</th>
<th>Local Legal Expert</th>
<th>Local DPO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAKING BCR BINDING AMONGST EMPLOYEES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Translate BCR into local language when required by Local law</td>
<td>A</td>
<td>A</td>
<td>C</td>
<td>R</td>
</tr>
<tr>
<td>Determination of the local requirements regarding Work Councils</td>
<td>I</td>
<td>I</td>
<td>A/R</td>
<td>I</td>
</tr>
<tr>
<td>Where necessary, prepare communication pack for Work Councils presentation</td>
<td>A/R</td>
<td>A/R</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Where necessary, consultation or information needed: set up date and present to Works Councils</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Where not necessary: communicate broadly to all employees to comply with transparency and information requirement (via mailing or through appropriate local bulletin).</td>
<td>A (for effective communication) / R (for drafting the communication)</td>
<td>A (for effective communication) / R (for drafting the communication)</td>
<td>R (for effective communication)</td>
<td>R (for effective communication)</td>
</tr>
</tbody>
</table>
# PRIVACY IMPACT ASSESSMENT ON GLOBAL LEVEL

<table>
<thead>
<tr>
<th>Activity</th>
<th>Chief Legal Counsel DP and Security</th>
<th>Group DPO</th>
<th>Local Legal Expert</th>
<th>Local DPO</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fulfilling the PIA</td>
<td>A</td>
<td>A</td>
<td></td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Reviewing the PIA</td>
<td>A/R</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Giving corrective measures in case PIA raises alerts</td>
<td>A/R</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td>C</td>
</tr>
</tbody>
</table>

# PRIVACY IMPACT ASSESSMENT AT LOCAL LEVEL

<table>
<thead>
<tr>
<th>Activity</th>
<th>Chief Legal Counsel DP and Security</th>
<th>Group DPO</th>
<th>Local Legal Expert</th>
<th>Local DPO</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fulfilling the PIA</td>
<td></td>
<td>A/R</td>
<td>A/R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Reviewing the PIA</td>
<td>I</td>
<td>I</td>
<td>A/R</td>
<td>A/R</td>
<td></td>
</tr>
<tr>
<td>Giving corrective measures in case PIA raises alerts</td>
<td>C (for legal issues) / I (for technical issues)</td>
<td>C (for technical issues) / I (for legal issues)</td>
<td>A/R</td>
<td>A/R</td>
<td>C</td>
</tr>
</tbody>
</table>
### Handling Customers' Complaints at Global Level

<table>
<thead>
<tr>
<th>Activity</th>
<th>Chief Legal Counsel DP and Security</th>
<th>Group DPO</th>
<th>Local Legal Expert</th>
<th>Local DPO</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive complaints of Customer</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td>A/R</td>
</tr>
<tr>
<td>Send A/R of the complaint in due time</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td>A/R</td>
</tr>
<tr>
<td>Analysis of the complaint</td>
<td>C</td>
<td>C</td>
<td></td>
<td></td>
<td>A/R</td>
</tr>
<tr>
<td>Resolution of the complaint</td>
<td>C</td>
<td>C</td>
<td></td>
<td></td>
<td>A/R</td>
</tr>
</tbody>
</table>

### Handling Customers' Complaints at Local Level

<table>
<thead>
<tr>
<th>Activity</th>
<th>Chief Legal Counsel DP and Security</th>
<th>Group DPO</th>
<th>Local Legal Expert</th>
<th>Local DPO</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive complaints of Customer</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>A/R</td>
</tr>
<tr>
<td>Send A/R of the complaint in due time</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>A</td>
<td>R</td>
</tr>
<tr>
<td>Analysis of the complaint</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>R</td>
<td>A/R</td>
</tr>
<tr>
<td>Activity</td>
<td>Chief Legal Counsel DP and Security</td>
<td>Group DPO</td>
<td>Local Legal Expert</td>
<td>Local DPO</td>
<td>Operational</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------------------------------</td>
<td>-----------</td>
<td>--------------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Resolution of the complaint</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>R</td>
<td>A/R</td>
</tr>
<tr>
<td>Receive request (ensuring that there is an effective process in place)</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Send A/R of the request in due time</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Analysis of the request</td>
<td>C</td>
<td>I</td>
<td>A/R</td>
<td>A/R</td>
<td>C</td>
</tr>
<tr>
<td>Answer to the request</td>
<td>C</td>
<td>I</td>
<td>A/R</td>
<td>A/R</td>
<td>C</td>
</tr>
<tr>
<td>Follow up on the request</td>
<td>I</td>
<td>I</td>
<td>A/R</td>
<td>A/R</td>
<td>C</td>
</tr>
<tr>
<td>Activity</td>
<td>Chief Legal Counsel DP and Security</td>
<td>Group DPO</td>
<td>Local Legal Expert</td>
<td>Local DPO</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>-----------</td>
<td>--------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td><strong>REVIEWING DATA PROTECTION CLAUSES IN GLOBAL CONTRACTS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewing DP clauses in major contracts</td>
<td>A/R</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementing standard clauses</td>
<td>A/R</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preparing Data Transfer Agreements</td>
<td>A/R</td>
<td>C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Getting Data Transfer Agreements signed</td>
<td>A/R</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewing and approving the security appendices</td>
<td>C</td>
<td>A/R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>REVIEWING DATA PROTECTION CLAUSES IN LOCAL CONTRACTS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewing DP clauses in major contracts (i.e. above 100m€)</td>
<td>I/C (when problems)</td>
<td>A/R</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementing standard clauses</td>
<td>A</td>
<td>R</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td>Chief Legal Counsel DP and Security</td>
<td>Group DPO</td>
<td>Local Legal Expert</td>
<td>Local DPO</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td>-----------</td>
<td>--------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>TRAINING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preparing Data Transfer Agreements</td>
<td>I</td>
<td></td>
<td>A</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Getting Data Transfer Agreements signed</td>
<td>I</td>
<td>I</td>
<td>A/R</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Reviewing the security appendices</td>
<td>I</td>
<td>C</td>
<td>I</td>
<td>A/R</td>
<td></td>
</tr>
<tr>
<td>Prepare the training</td>
<td>A/R</td>
<td>A/R</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Update DP training with local specificities</td>
<td>C</td>
<td>C</td>
<td>A/R</td>
<td>A/R</td>
<td></td>
</tr>
<tr>
<td>Ensure DP training is effectively followed by employees at local level</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Deliver classroom training when needed</td>
<td>A/R</td>
<td>A/R</td>
<td>A/R</td>
<td>A/R</td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td>Chief Legal Counsel DP and Security</td>
<td>Group DPO</td>
<td>Local Legal Expert</td>
<td>Local DPO</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------------------------------------</td>
<td>-----------</td>
<td>--------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td><strong>HANDLING DATA SUBJECTS' COMPLAINTS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive complaints of Data Subjects</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Send A/R of the complaint in due time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis of the complaint</td>
<td>C (where needed)</td>
<td>C (where needed)</td>
<td>A/R</td>
<td>A/R</td>
<td></td>
</tr>
<tr>
<td>Resolution of the complaint</td>
<td>C</td>
<td>C</td>
<td>A/R</td>
<td>A/R</td>
<td></td>
</tr>
<tr>
<td><strong>NOTIFICATION TO DATA PROTECTION AUTHORITIES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit the existing processing at Global level</td>
<td>A/R</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Checking notification status</td>
<td>A/R</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Audit the existing processing at Local level</td>
<td>C</td>
<td>C</td>
<td>A/R</td>
<td>A/R</td>
<td></td>
</tr>
<tr>
<td>Checking notification status</td>
<td>C</td>
<td>C</td>
<td>A/R</td>
<td>A/R</td>
<td></td>
</tr>
</tbody>
</table>
### Handling Data Subjects' Complaints

<table>
<thead>
<tr>
<th>Activity</th>
<th>Chief Legal Counsel DP and Security</th>
<th>Group DPO</th>
<th>Local Legal Expert</th>
<th>Local DPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive complaints of Data Subjects</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>R</td>
</tr>
<tr>
<td>Send A/R of the complaint in due time</td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
</tr>
<tr>
<td>Analysis of the complaint</td>
<td>C (where needed)</td>
<td>C (where needed)</td>
<td>A/R</td>
<td>A/R</td>
</tr>
<tr>
<td>Resolution of the complaint</td>
<td>C</td>
<td>C</td>
<td>A/R</td>
<td>A/R</td>
</tr>
</tbody>
</table>

### Notification to Data Protection Authorities

<table>
<thead>
<tr>
<th>Activity</th>
<th>Chief Legal Counsel DP and Security</th>
<th>Group DPO</th>
<th>Local Legal Expert</th>
<th>Local DPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit the existing processing at Global level</td>
<td>A/R</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Checking notification status</td>
<td>A/R</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Audit the existing processing at Local level</td>
<td>C</td>
<td>C</td>
<td>A/R</td>
<td>A/R</td>
</tr>
<tr>
<td>Checking notification status</td>
<td>C</td>
<td>C</td>
<td>A/R</td>
<td>A/R</td>
</tr>
<tr>
<td>Activity</td>
<td>Chief Legal Counsel DP and Security</td>
<td>Group DPO</td>
<td>Local Legal Expert</td>
<td>Local DPO</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>-----------</td>
<td>--------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Ongoing monitoring of Global process notification</td>
<td>A/R</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Ongoing monitoring of Local process notification</td>
<td>C</td>
<td>C</td>
<td>A/R</td>
<td>A/R</td>
</tr>
</tbody>
</table>
21 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 Data Controller

Appendix 5 – Complaint Handling Procedure where Atos acts as a Data 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 – Privacy Impact Assessment Form where Atos acts as a Data Controller

Appendix 9 – Privacy Impact Assessment Form where Atos acts as a Data Processor

Appendix 10 – Audit plan