

PUBLIC

**ATOS UK BINDING CORPORATE RULES AS A
CONTROLLER**

(ATOS UK BCR-C)

Atos

AUTHOR(S)	: Atos UK DPO
VERSION	: 2.0
STATUS	: Final
SOURCE	: Atos UK
DOCUMENT DATE	: October 2023
NUMBER OF PAGES	: 29

version: 2.0

Contents

1	Introduction	5
1.1	Purpose	5
1.2	Scope	5
1.3	Document maintenance and distribution	5
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	Special Category data	9
2.4	Security	10
2.5	Automated individual decisions	10
2.6	Accountability	11
3	Transfer of Personal Data	12
3.1	Personal Data transfer by an Atos Entity located in the UK acting as a Controller to an Atos Entity located in the UK.	12
3.2	Personal Data transfer by an Atos Entity located in the UK acting as a Controller to an Atos Entity located outside of the UK.	12
3.3	Personal Data transfer by an Atos Entity in the UK acting as a Controller to a Third Party located outside the UK in a country that has no UK adequacy decision.	12
4	Data Subject’s rights	13
5	Data Subject Complaints	15
5.1	Direct complaint	15
5.2	Right of Complaint to the Commissioner and to bring a complaint before a UK Court	15
6	Liability with regard to Data Subjects	16
6.1	Liability of Atos Entities acting as Controller	16
6.2	Burden of proof	16
7	Data Subject’s information	17
7.1	Permanent information	17
7.2	Data Subject’s information when Atos acts as a Controller	17
8	Cooperation	18
8.1	Cooperation with the Commissioner	18
9	Personal Data Breach reporting	19
10	Privacy by Design	20
10.1	Product and services development	20
10.2	New business opportunities and M&A	20
11	Notification to the Commissioner	21

version: 2.0

12	Training and raising awareness	22
13	Audit	23
14	Data Protection Community	24
15	Key Performance Indicators (KPI)	25
16	Investigation.....	26
17	Update of the UK BCR-C	27
18	Legally Binding Requests for Disclosure of Data	28
19	APPENDICES – PROCEDURES	29

version: 2.0**List of changes**

Version	Date	Description	Author(s)
1.0a	December 2020	Initial version	UK DPO
1.0b	20 January 2021	RACI included	UK DPO
1.0c	04 June 2021	Response to ICO review	UK DPO
1.0d	23 June 2021	Amended following UK Legal review	UK Legal
1.0e	24 June 2021	Resubmission to ICO	UK DPO
1.0f	08 July 2021	Amended following ICO comments	UK DPO
1.0	05 August 2021	Version for publication	UK DPO
2.0	October 2023	Added use of IDTA for transfers	UK DPO

version: 2.0

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. In order to guarantee the highest level of protection to the data it processes, as a Controller, Atos has adopted these UK Binding Corporate Rules as a Controller ("UK BCR-C").

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

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

1.2 Scope

1.2.1 Geographical Scope

These UK BCR-C apply to all Atos Entities regardless of their localization and competent jurisdiction.

1.2.2 Material Scope

These UK BCR-C cover all Personal Data Processing irrespective of the nature of the Personal Data processed. These UK BCR-C cover all types of processing carried out by Atos acting as a Controller. As a result, these UK BCR-C cover processing of HR, Customer, Supplier, or Marketing and Communications Data. For further information please see Appendix 5 of these UK BCR-C.

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

1.2.4 Bindingness amongst Employees

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

1.3 Document maintenance and distribution

This UK BCR-C document is publicly available via the privacy page of the Atos website (<https://atos.net/en-gb/united-kingdom/privacy-uk>), and in addition is made accessible to all Employees via the Atos corporate intranet. It may be communicated to any Third Party upon request.

version: 2.0

1.4 Related documents

These UK BCR-C are also composed of 8 Appendices which describe the procedures which enable Atos to guarantee that the UK BCR-C are effectively implemented.

1.5 Keywords

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

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

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

Atos IT Services UK Limited: a company incorporated under UK law, having its registered office at MidCity Place, 71 High Holborn, London WC1V 6EA, registered in the UK at Companies House - registered number 1245534, a subsidiary of Atos SE.

Atos UK Data Protection Officer: the Data Protection Officer (DPO) of Atos IT Services UK Limited.

Commissioner: the UK Information Commissioner.

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

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

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

Data Exporter: any Atos Entity in the UK acting as a Controller and which transfers Personal Data to a Data Importer located in a Third country.

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

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

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

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

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

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

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

version: 2.0

Personal Data Transfer: the disclosure or transmission of Personal Data by one entity to another entity or the process of making such data available to that other entity.

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

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

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

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

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

Third Country: a country or territory outside the UK.

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

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

UK Data Protection Office: both the UK Legal Experts on Data Protection and the Atos UK Data Protection Officer as described in Section 14 of these UK BCR-C.

UK GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

version: 2.0

2 Principles for processing of Personal Data

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

Where one of the Atos Entities has reasons to believe that the local legislation prevents the company from fulfilling

- ✓ its obligations as a Controller under these UK BCR-C

and / or

- ✓ the instructions it may have received from an Atos Controller

and / or that such legislation has substantial effect on the guarantees provided by the UK BCR-C, it will promptly inform the Atos UK Data Protection Officer and the Controller, who will inform the Commissioner.

The Atos UK Data Protection Officer will handle the above issue as soon as possible, but, in any case, not later than one month after the notification is received.

In case of doubt, with regard to the interpretation of UK laws, the Atos UK Data Protection Officer shall seek the Commissioner's or external counsel's advice in order to ensure compliance with the most stringent provisions.

See also Section 18 - Legally Binding Requests for Disclosure of Data.

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 Consent to the processing of his or her personal data for one or more specific purposes;

or

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

or

- ✓ the Data Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

or

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

or

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

or

version: 2.0

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

2.2 Principles to be respected when processing Personal Data

When implementing a new Processing of Personal Data and while such Processing is being carried out, an Atos Entity, acting as a Controller, shall guarantee that:

- ✓ The Processing is transparent, 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 technical, organisational and security measures are implemented according to Atos Security Policy and at least meet the requirements of UK law
- and**
- ✓ Appropriate technical and organisational measures are implemented for the fulfilment of the Controller's obligations to respond to requests for exercising Data Subjects' rights
- and**
- ✓ The Personal Data will be sub-processed by other Atos Entities or by Third Parties only with the prior informed specific or general written authorisation of the Controller.

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

- ✓ The Personal Data are kept accurate and up to date, and where data are inaccurate or incomplete, data are rectified, supplemented or erased.
- and**
- ✓ The Personal Data are not kept longer than necessary for the purpose for which they are processed.

2.3 Special Category data

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

- ✓ The Data Subject has given his/her Consent to the processing of those Personal Data for one or more specified purposes, except where UK law provides that the prohibition on the Processing of such data may not be lifted by the Data Subject
- or**
- ✓ Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by UK law or a collective agreement pursuant to UK law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject,
- or**

version: 2.0

- ✓ Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent,
or
- ✓ the Processing is required in the context of preventive medicine or medical diagnosis by a health professional under UK law,
or
- ✓ the Data Subject has already manifestly placed the affected Special Category 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 necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of UK law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy
or
- ✓ Processing is otherwise explicitly permitted by UK law.

2.4 Security

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

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

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 and will implement measures, where applicable, to protect the right of the individual in such circumstances not to have such a decision taken based solely on automated processing.

The Data Subject has the right not to be subject to a decision based solely on automated processing, 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) required or authorised by UK law which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or (c) is based on the Data Subject's explicit consent.

version: 2.0

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 Compliance Assessment of Data Processing (“CADP”) as detailed in Appendix 6 and, where required under UK Law, a Data Protection Impact Assessment (“DPIA”). Where such a DPIA indicates that the Processing would result in a high risk to the rights and freedoms of individuals, the Controller will consult the Commissioner prior to undertaking the Processing.

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

2.6.2 Records of Processing activities

When acting as a Controller, all Atos entities falling within the scope of these UK BCR-C shall maintain records of their respective Processing activities. Such records shall be retained in writing, including electronic form, shall comply with UK GDPR requirements for Controller records and shall be made available upon request to the Commissioner.

The records of Processing activities shall take the form of Atos Compliance Assessments of Data Processing for Atos as a Controller (CADP-C).

version: 2.0

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 UK BCR-C, UK Personal Data Transfers are the responsibility of UK Data Controllers which shall undertake to provide appropriate safeguards to Personal Data which are transferred.

The expected and anticipated types of data and purposes of transfer of Personal data by Atos Entities acting as Controllers to other Atos Entities, acting either as Controllers, are described in Appendix 5.

3.1 Personal Data transfer by an Atos Entity located in the UK acting as a Controller to an Atos Entity located in the UK.

Where an Atos Entity located in the UK, acting as a Controller, transfers Personal Data to another Atos Entity located within the UK, 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 located in the UK acting as a Controller to an Atos Entity located outside of the UK.

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

3.3 Personal Data transfer by an Atos Entity in the UK acting as a Controller to a Third Party located outside the UK in a country that has no UK adequacy decision.

Where an Atos Entity in the UK, acting as a Controller, transfers Personal Data to a Third Party, located outside the UK in a country that has no UK adequacy decision, the Atos Entity transferring the Personal Data shall ensure compliance with Section 3.1 of these UK BCR-C and shall also ensure EITHER:

that it signs an agreement with the Third Party that incorporates one of the following safeguard mechanisms:

- (a) In the case that Personal Data is transferred from both the UK and EEA, appropriate Standard Contractual Clauses, as approved by the European Commission in accordance with Article 46 2(c) of EU Regulation 2016/679 (the EU GDPR), together with the UK International Data Transfer Addendum as adopted under Section 119a of the UK Data Protection Act 2018; or,
- (b) In the case that Personal Data is transferred from the UK only, the UK International Data Transfer Agreement (IDTA) as adopted under Section 119a of the UK Data Protection Act 2018;

OR that the transfer is subject to other appropriate safeguards as permitted under Article 46 of the UK GDPR.

version: 2.0

4 Data Subject's rights

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

- ✓ The general data protection principles, in particular: purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for Processing, Processing of special categories of Personal Data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by these UK BCR-C;
- ✓ The right to be provided with easy access to these UK BCR-C and in particular easy access to the information about third-party beneficiary rights for the Data Subject that benefit from them;
- ✓ The right to have access to the data relating to him/her processed by Atos acting as Controller;
- ✓ The right to 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;
- ✓ The right to 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 defence 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.
- ✓ The right to 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;
- ✓ The right not to be subject to decisions based solely on automated Processing, including profiling;
- ✓ The right to 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;
- ✓ The Atos Entity's duty to respect these UK BCR-C;
- ✓ The right to be informed regarding the complaint handling procedure and to have easy access to it, including the possibility to lodge a complaint before the Commissioner and before the courts;
- ✓ The Atos Entity's duty to accept liability for paying compensation and to remedy breaches of these UK BCR-C;
- ✓ The right to be informed of the fact that the burden of proof lies with the Atos Entity and not with the Data Subject according to the terms of these UK BCR-C;
- ✓ The Atos Entity's duty to cooperate with the Commissioner;

version: 2.0

- ✓ The obligation under these UK BCR-C to be informed, where legally permitted, when national legislation prevents an Atos Entity from complying with its obligations under these UK BCR-C;
- ✓ The Atos Entity's duty to cooperate with the Controller;
- ✓ The right to be informed regarding Atos Entities bound by these UK BCR-C

All such requests shall be handled 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 UK Data Protection Officer by sending an email to uki.dpo@atos.net.

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

version: 2.0

5 Data Subject Complaints

5.1 Direct complaint

If a Data Subject believes that the Processing of his/her Personal Data which is subject to these UK BCR-C have caused him/her damage, he/she may complain to the Atos UK Data Protection Officer at dpo.uki@atos.net. Similarly, if a Data Subject believes that the Processing of Personal Data which is subject to these UK BCR-C has not been processed according to these UK BCR-C, or the UK GDPR or according to local applicable law, Data Subjects are granted a right to complain against Atos IT Services UK Limited at dpo.uki@atos.net.

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

Data Subjects are encouraged to submit a direct complaint as described in this section 5.1 and to escalate the complaint according to Section 6 where Atos fails to comply with the commitments of this section.

Atos IT Services UK Limited accepts responsibility for investigating such complaints and for ensuring that action is taken, and remedies provided, as appropriate.

The use of this complaints procedure will not affect a Data Subject's right to complain to the Commissioner and/or bring a claim before a UK court (or a court in the country in which an Atos Entity is based) should they wish to do so.

5.2 Right of Complaint to the Commissioner and to bring a complaint before a UK Court

If a Data Subject believes that the Processing of his/her Personal Data, which is subject to these UK BCR-C, have caused him/her damage or have not been processed according to these UK BCR-C, or according to the UK GDPR or local applicable law, Data Subjects are granted a right to complain to the Commissioner and / or to bring a claim before a UK Court.

version: 2.0

6 Liability with regard to Data Subjects

Where a Data Subject suffers material or non-material damage as a result of a processing of Personal Data by an Atos Entity, acting as a Controller, the provisions below shall apply. It is emphasised that a Data Subject is encouraged first to file a complaint directly to the Atos Entity in order to find an amicable solution, however Data Subjects have the right to complain to the Commissioner and/or make a claim in a UK court, whether or not they have first complained directly to the Atos Entity. Complaints and the rights of Data Subjects are addressed in section 5 of these UK BCR-C.

6.1 Liability of Atos Entities acting as Controller

Where a Data Subject suffers damage as a result of a breach of UK BCR-C by an Atos Entity located outside of the UK, Atos IT Services UK Limited, a UK based company, accepts responsibility for, and agrees to take necessary actions to remedy and pay compensation to the Data Subject for, any damages resulting from the violation of these UK BCR-C by members of the UK BCR-C. In addition, Atos accepts that in certain cases remedies other than monetary compensation may be appropriate to address the damage suffered by a Data Subject as a result of an Atos Entity acting as Controller. A Data Subject may also exercise his or her rights before the UK courts or the Commissioner.

6.2 Burden of proof

In any case, where section 6.1 applies, and where a Data Subject has demonstrated that they have suffered damage that is likely to have been caused by a breach of the UK BCR-C, the Atos Entity accepts to bear the burden of proof for demonstrating that any damage suffered by the Data Subject was not caused by a breach of the UK BCR-C by the Atos Entity.

version: 2.0

7 Data Subject's information

7.1 Permanent information

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

7.2 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 and contact details of the Controller;
- The contact details of the data protection officer, where applicable;
- The purposes of the Processing for which the Personal Data are intended as well as the legal basis for their Processing;
- Where applicable, the legitimate interests pursued by the Controller or by a Third Party;
- The recipients or categories of recipients of the Personal Data, if any and the categories of Personal Data concerned;
- Where applicable, information regarding data transfers to a Third Country and any relevant safeguards for such transfers;
- The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability, where applicable;
- The right to withdraw consent for Processing, where applicable;
- The right to lodge a complaint with the Commissioner;
- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
- The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the UK GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- Information regarding the source from which the Personal Data originate, and if applicable, whether the data came from publicly accessible sources.

version: 2.0

8 Cooperation

Atos Entities commit to cooperate actively with Third Parties in order to make sure that applicable law and regulations regarding Data Protection are respected by all stakeholders. To this end, all Atos Entities will comply with any applicable data protection local law in their contractual and business relations with Customers, suppliers, and subcontractors.

8.1 Cooperation with the Commissioner

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

Atos Entities shall also cooperate actively with all requests from the Commissioner, in particular to ensure adequate and timely response to any request received from the Commissioner.

Atos also accepts to be audited by the Commissioner to verify compliance with applicable data protection legislation and with these UK BCR-C.

Subject to applicable law, Atos Entities shall, consider any communication or recommendation from the Commissioner in relation to these UK BCR-C and comply with any applicable decisions or notices issued by the Commissioner.

version: 2.0

9 Personal Data Breach reporting

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

In the event that an Atos Entity, acting as a Controller, becomes aware of a Personal Data Breach, Atos shall, without undue delay and, where feasible, not later than 72 hours after having become aware of the Personal Data Breach, notify the Commissioner, 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 Atos UK 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 Atos UK 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.

version: 2.0

10 Privacy by Design

10.1 Product and services development

Where one of the Atos Entities or business teams intends to develop new Processing, it shall make sure that Data Protection is taken into account as of the beginning of the project, including any requirement to comply with UK and other applicable local law.

For this very purpose, where a project is developed by an Atos Entity, the business team in charge of the new Processing shall produce a CADP-C as described in Appendix 6. The Atos UK Data Protection Officer shall receive a copy of the CADP-C, shall conduct random reviews of the CADP-C and shall make recommendations to have the project run in a compliant manner.

Where required under UK law, an Atos Entity will undertake a DPIA.

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

It results from the above that the Employees who develop new projects for the UK shall make sure that the UK Data Protection Officer is involved in each project.

10.2 New business opportunities and M&A

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

For this very purpose, where new business opportunities are possible at UK level, the UK Data Protection Office shall be consulted as of the beginning of the project and involved at every stage of the project. The UK 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 centres or the structuring of the company.

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

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

version: 2.0

11 Notification to the Commissioner

Should the Commissioner request prior notification of particular Processing, Atos commits to respect this.

Atos keeps records of its Processing activities as both a Controller and a Processor. Where Atos acts as a Controller, the UK Data Protection Office keeps a register of Processing implemented by Atos and will gather any prior notification forms that are submitted to the Commissioner.

Atos UK companies will maintain such registrations as are required with the Commissioner.

version: 2.0

12 Training and raising awareness

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

Atos commits to:

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

Atos Group mandatory training is part of an integrated platform provided to members of staff, which prompts them when training is due and maintains individual training records that are monitored by immediate line managers. Data Protection is one of the modules. Failure to complete mandatory training may affect performance assessments and can lead to disciplinary action. Completion of mandatory Data Protection training is monitored by the DP Community as part of the Compliance team together with the Human Resources Department in order to provide assurance that new training is being taken up and to allow identification of any areas of the business where additional effort is required to ensure completion.

version: 2.0

13 Audit

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

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

The results of the audit shall also be communicated to the Atos Group DP Community and corrective actions shall be proposed by the Atos UK Data Protection Officer, who will report on their completion to the Atos IT Services UK Limited Board.

Upon request, the Commissioner may obtain results of the Data Protection Audit and details of any corrective actions.

The audit plan dedicated to these UK BCR-C is described in Appendix 8.

The Commissioner may, without restrictions, carry out an audit of any Atos Entity in respect of Processing undertaken under these UK BCR-C. This is in addition to the Commissioner's audit rights as defined in data protection legislation.

version: 2.0

14 Data Protection Community

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

For this very reason, a Data Protection Community (“DP Community”) has been created. This DP Community is composed of two branches which 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 Chief Data Governance Officer both together the Group Data Protection Office. These represent Atos Group, i.e. Atos SE, and are part of the Group legal & compliance management team.

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 UK is represented by the UK Data Protection Office, which includes the UK Data Protection Officer and a representative of the Atos UK legal team as local legal expert.

The UK Data Protection Office, which forms part of the DP Community, will take the lead in respect of implementing and monitoring the operation of these UK BCR-C.

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

version: 2.0

15 Key Performance Indicators (KPI)

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

These KPI cover in particular, but not exclusively:

- ✓ Number of data breaches;
- ✓ Number of data breaches notified to a Supervisory Authority (in the case of the UK, the Commissioner);
- ✓ Number of data breaches notified to Data Subjects;
- ✓ Number of complaints from Employees, vendors or suppliers;
- ✓ Number of complaints from others (for example from other data subjects);
- ✓ Number of requests from Employees, vendor or supplier personnel to access their personal data;
- ✓ Number of requests from other data subjects to access their personal data.

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

version: 2.0

16 Investigation

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

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

version: 2.0

17 Update of the UK BCR-C

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

Any significant changes to these UK BCR-C, such as those that:

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

shall be reported to all Atos Entities as well as to the Commissioner without undue delay with an explanation for the change. Clear and easily available information regarding any such significant change shall be made for Employees and Third Parties information.

Other changes, such as changes to the list of bound Atos Entities, will be reported to all members on a regular basis and will be reported to the Commissioner annually.

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

The UK Data Protection Office will maintain the list of bound Atos Entities, control changes to these UK BCR-C and make the above reports.

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

No transfer of Personal Data to an Atos Entity will be made on the basis of these UK BCR-C unless the Atos Entity concerned is effectively bound by them.

version: 2.0

18 Legally Binding Requests for Disclosure of Data

Where, when acting as a Controller under these Binding Corporate Rules, an Atos Entity receives a legally binding request for disclosure of Personal Data by a law enforcement authority, unless prohibited by law, the Atos Entity shall, subject to applicable legislation preventing or prohibiting it, attempt to suspend the execution of the request and inform the Commissioner.

If applicable laws prohibit the suspension of execution or communication of the request, the Atos Entity 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 Commissioner, and to be able to demonstrate that it did so.

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

In any case, the Atos Entity 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.

version: 2.0

19 APPENDICES – PROCEDURES

Appendix 1 – Organisation of the Data Protection Community and Roles

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

Appendix 3 – Form for Data Subject to Exercise Their Rights

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

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

Appendix 6 – Compliance Assessment of Data Processing where Atos acts as a Controller

Appendix 7 – Local Data Protection Points of Contact

Appendix 8 – Audit plan

Appendix 9 – Responsibility Assignment Matrix (RACI)