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

Appendix 9 - Audit Plan

This appendix describes the outline audit plan that will be used for any internal audits of the UK BCR-P. Such audit will be carried out at the request of the UK Data Protection Office or the Group Data Protection Office.

Internal audits will be carried out by Atos internal auditors. They will cover all aspects of the UK BCR-P.

The results of such audits will be communicated to the Local and Group Data Protection Offices and to the Atos Group Executive Board, along with any corrective action plan.

Follow up to corrective action will be monitored by the UK Data Protection Office.

I. STREAMS TO BE COVERED

The audits shall cover all aspects of compliance with the UK BCR-P including the following:

STREAM #1 – Bindingness of the UK BCR-P

(i) Vis-à-vis Atos Entities

The objective of this stream is to verify that all entities are effectively bound by the UK BCR-P. This means that we will control that they have all entered into the Intra Group Agreement (IGA). It will be particularly important to track that new entities have effectively entered into the IGA.

(ii) Vis-à-vis Atos Employees

At local level it will be important to make sure that the UK BCR-P are made binding vis-à-vis Data Subjects according to requirements mandated by applicable local law. For instance: making sure appropriate information is made available to Works Councils and other employee bodies; inclusion of the policy in the data protection information made available to employees; including material on BCR in mandatory data protection training and in other awareness material.

STREAM #2 –Transparency vis-à-vis data subjects and customers

(i) Vis-à-vis Data Subjects

It is important to control that UK BCR-P are made easily accessible on all Atos websites and tools. Also, the process for communicating with the UK Data Protection Office shall be tested.

(ii) Vis-à-vis Customers

The audit should determine whether the Customers are duly informed about the UK BCR-P and that UK BCR-P are effectively integrated into Service Level Agreements.

STREAM #3 - Data Protection principles

Each of the principles governing processing of Personal Data shall be verified in order to check that they are effectively incorporated into Atos tools, both for Atos itself and the tools that are developed for Customers.

STREAM #4 – Training

The training of Atos Employees needs to be monitored in order to ensure that all Atos Employees receive appropriate training in particular according to their specific functions but also according to specific requests that Customers may have regarding the training of our Employees.

STREAM #5 – Complaint procedures

The respect of the complaint procedures in terms of timeframe needs to be verified in order to demonstrate that we respect our commitment to have an effective respect of the right to complaint of Data Subjects and of Customers.

STREAM #6 – Data Protection Community

It will be important to check that the Data Protection Community is effectively constituted and that its members are effectively involved and aware about their roles and functions.

STREAM #7 – Update of the UK BCR-P

The update of the UK BCR-P procedures set up in the UK BCR-P themselves shall be verified. In particular, it is important to ensure that the list of Atos Entities bound by UK BCR-P is up to date and that in case of major changes relevant Customers and data protection authorities are informed.

STREAM #8 – Accountability including records of processing

Review of records of processing kept by Atos Entities related to processing under the UK BCR-P.

STREAM #9 – Review of any decisions taken as regards mandatory requirements under national laws that conflicts with the UK BCR-P.

Review of any decisions under national law, such as requirements for data localization or access to data by national authorities, that may conflict with the UK BCR-P.

II. AUDIT TYPES

Two different types of audits will be carried out.

Type of audit	Owner of the audit	S	Frequency
Random unofficial audits	Local Data Protection Offices with the help of the Global Data Protection Office	Selecting 3 streams minimum	Once a year
Official audits	Group Internal Audits	All streams	Max every 3 years

Audit reports will be made available to the Commissioner upon request.

Atos Entities will also cooperate with and facilitate any audits undertaken by or on behalf of a Controller, or by the Commissioner.