
Appendix 6 to Atos Group Binding Corporate Rules as a Controller - Compliance and impact assessment of data processing when Atos acts a Controller

Author:	Group Data Protection Office
Version:	1.0
Document date:	November 2024
Doc. No:	

Contents

**Compliance and impact assessments of data processing when Atos
acts as a Controller 3**

Compliance and impact assessments of data processing when Atos acts as a Controller

An Atos Compliance Assessment of Data Processing when Atos acts as a Controller ("CADP-C") must be completed for all processes in order to target an appropriate level of compliance. The purpose of this document is to allow Atos to meet several requirements under data protection law. The CADP-C is used by Atos as its primary tool for creating a record of processing or "identity card" in which to gather all relevant information regarding a particular processing activity for which it is a Controller. The CADP-C must be completed at the earliest stage of the project.

Therefore, it enables Atos to identify potential risks associated with a processing of personal data in order to define relevant technical, organizational and security measures which should be implemented and determine whether an Atos Data Protection Impact Assessment (Atos DPIA) should be conducted or not. Atos DPIA must follow the requirements as set forth in Article 35 of the GDPR.

A CADP-C should be conducted by the business owner for the project, tool or solution as stated in the Atos Group BCR-C with the assistance of the functional team, and with guidance and (final) approval from the relevant Data Protection Office.

Atos CADP-C should be completed for each process where Atos acts as a Controller i.e. when it processes personal data for its own purposes and where Atos is able to decide the means of the processing.

An Atos DPIA is required in the case of:

- a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- b) processing on a large scale of sensitive data or of personal data relating to criminal convictions and offences
- c) a systematic monitoring of a publicly accessible area on a large scale.
- d) when a supervisory authority establishes that a DPIA is required for a particular type of processing operation

Atos DPIA shall contain at least:

- a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- c) an assessment of the risks to the rights and freedoms of data subjects and
- d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with regulations taking into account the rights and legitimate interests of data subjects and other persons concerned.

Where appropriate, the Atos Entity acting as Controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Where necessary, the Atos Entity acting as Controller shall carry out a review to assess if processing is performed in accordance with the Atos DPIA at least when there is a change of the risk represented by processing operations.