GROUP DATA PROTECTION POLICY

AUTHOR(S)	:	Andrew Jackson
DOCUMENT REFERENCE	:	0000035
VERSION	:	5.0
STATUS	:	Final
SOURCE	:	Atos
DOCUMENT DATE	:	5 May 2023
NUMBER OF PAGES	:	53

Role	Approval
Reviewers/Approvers	Paul Bayle (Head of Security, Group CISO) Cecilia Fernandez Arredondo (Deputy Group Data Governance Officer) Prasad Purayi (Regional Data Protection Officer)
Document Controller	Katarzyna Cieslak-Rylich
Document Owner	Andrew Jackson Group Chief Data Governance Officer
Senior Manager Atos	Roland Schreiner Group Legal AGGC Operations & Transformation

© Copyright 2023, Atos All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. For any questions or remarks on this document, please contact Atos, dpo-global@atos.net.

Contents

List of changes

version	Date	Description	Author(s)
1.0	18 June 2011	Introducing Data Protection Community's comments	Emmanuelle Bartoli
1.1	16 March 2015	Introducing comments from the German Works Councils	Lionel de Souza
1.2	7 July 2017	GDPR Impacts	Claude Bineau Lionel de Souza Agathe Mougel GDPR WG#1
2.0	17 May 2018	Content review Moved to new Atos word template. Quality check, final version.	Claude Bineau Agathe Mougel GDPR WG#1 Stéphane Larrière Katarzyna Cieslak-Rylich
2.01	1 July 2020	Periodic review	Michael Mingers
3.0	12 April 2021	Integration of Appendixes in the text of this Policy to simplify signature process New definitions in 1.6, add chapter 1.7 Abbreviations Periodic review Alignment with Atos SPRING DAY 3 updates in Atos organization	Claude Bineau Wissame En-Naoui
4.0	28 May 2021	Updates following Atos Spring and some DP workshop groups requests : WG CADP-P Legal (New vocabulary); WG DSR (Chapter 6); WG CADP-P Process (1.2.1 ; 3.1.1 ; 3.1.2; 4 ; 10; 13) Review Germany (1.6 ; 2.5 ; 3.1.1; 3.1.2 ; 5 ; 15 ;18 ; Appendix 2) Quality assurance	Michael Mingers Wissame En-Naoui Claude Bineau Marianna Bojarska
5.0	5 May 2023	Clarifications, updates to links. Appendices updated. Quality assurance	Andrew Jackson Kasia Cieslak-Rylich

1 Introduction

1.1 Purpose

For Atos, the protection of Personal Data is a topic of the utmost importance. The Processing of Data, including Personal Data, is part of its core activities, whether it does so as a Controller or as a Processor. Accordingly, compliance with Data Protection laws and regulations is one of Atos's main priorities.

In order to guarantee a strong level of protection to the Personal Data it processes, Atos has devised a comprehensive approach based on four main pillars supporting data protection (DP) compliance and good practice: DP policies, a DP community, practical DP tools and DP trainings (including mandatory DP training for all staff). As a fundamental element of the first pillar, Atos has adopted this Group Data Protection Policy ("Atos Group Data Protection Policy").

This Policy aims at applying strong Data Protection standards in order to protect the fundamental rights and freedoms of Data Subjects and, in particular, their rights to privacy and to the protection of their Personal Data. Atos considers that the implementation of such a policy raises awareness within the Group and helps Atos to comply with its legal obligations.

Subject to applicable law, every Atos entity and Atos Employee and manager is required to apply the Data protection principles set out in this Atos Group Data Protection Policy.

This Atos Group Data Protection Policy follows the same objectives and principles as those assigned and defined in the Group Binding Corporate Rules ("BCR") which are binding on all companies and on Employees of Atos Group companies, and which have been validated by the European Data Protection Authorities. For the sake of clarity, the Atos Group BCR are included to this Atos Group Data Protection Policy by reference.

1.2 Scope

1.2.1 Geographical Scope

Atos being an international group with its headquarters based in the European Union (EU), this Atos Group Data Protection Policy is influenced by the EU approach to the protection of Personal Data. Accordingly, this Atos Group Data Protection Policy takes into account the European General Data Protection Regulation ("GDPR").

This Policy applies to the Processing of Personal Data in the activities of any establishment of Atos Entities acting as a Controller or acting as a Processor regardless of their localization or jurisdiction.

1.2.2 Material Scope

This Atos Group Data Protection Policy covers all Processing of Personal Data irrespective of the nature of the Personal Data processed, the purpose of said Processing or the type of Processing (including automated and non-automated Processing).

As a result, this Atos Group Data Protection Policy notably covers processing of any personal data, such as Employee , Customer, Supplier, or Marketing and Communications Data, whether Atos acts as a Controller or as a Processor and regardless of the nature of the Data processed, whether "sensitive" or not.

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

1.3 Intended audience

1.3.1 Amongst entities

This Atos Group Data Protection Policy is legally binding amongst all entities of Atos.

Where one or several of the Atos Entities becomes aware or has reasonable reasons to believe that any applicable legislation prevents it from fulfilling either its obligations under this Atos Group Data Protection Policy or instructions it has received from a Controller, when acting as a Processor, , then the procedure set out in Appendix 9 shall apply.

1.3.2 Amongst Employees

This Atos Group Data Protection Policy is part of the Group Policies which all Employees are bound to respect according to their employment contract. Appropriate information and, where required, agreement with local Works Councils have been exchanged and obtained in order to ensure the full commitment and adherence to this Atos Group Data Protection Policy by all Employees.

This communication might be done via the employees' representatives and this document might be subject to labor process with the Works Councils.

1.4 Document maintenance and distribution

The document is made available to all Atos Employees and may be communicated to Customers upon request.

1.5 Related documents

This Atos Group Data Protection Policy is also composed of 10 Appendices; describing the procedures which enable Atos to ensure that this Group Data Protection Policy is effectively implemented.

This Atos Group Data Protection Policy is part of the overall system of policies and processes of Atos, which also comprise a Personal Data Breach Policy, Security Policies and other relevant functional policies.

In addition, as mentioned above, this Atos Group Data Protection Policy is directly connected and incorporates the principles of the Atos Group Binding Corporate Rules ("Atos Group BCR") by reference.

1.6 Keywords

The terms used in this Policy are defined as follows:

Atos means Atos S.E. together with all Atos legal entities irrespective of their jurisdiction.

Atos Entity means any of the entity owned and/or controlled by Atos. For the purposes of this Atos Group Data Protection Policy, Atos shall be deemed to have "control" over an entity where it holds more than 50% of the shares or voting rights in that entity.

Anonymization means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject. Contrary to "pseudonymization", the data are no longer related to a Data Subject after anonymization. Re-identification of the data subject must not be possible any more after anonymization.

Binding Corporate Rules ('Atos Group BCR') means the Atos Group Binding Corporate Rules adopted by Atos S.E. on behalf of the Atos Group, approved by the French Data Protection Authority (the *Commission Nationale de l'Informatique et des Libertés* – CNIL) as lead authority representing European data protection authorities through the "mutual recognition" principle on 4 November 2014, updated from time to time in compliance with the approved procedure in order to remain compliant with EU requirements for BCR, and attached as Appendix 6 to this Atos Group Data Protection Policy.

Biometric Data means Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioral characteristics of a Data Subject, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint Data.

Consent means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

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

Data concerning Health means Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data Protection Addendum is a contractual agreement that sets out the terms and conditions for the processing of personal data, including the obligations of the Data Controller and the Data Processor to protect the data and comply with relevant data protection laws and regulations.

Data Protection Authority means any local authority which is competent (by law, regulation or otherwise) to handle Data protection issues.

Data Protection Impact Assessment ('Atos DPIA') means a risk assessment of a processing activity (processing personal data) where the type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons. Note that in the EU, obligations regarding DPIA are set out in Art 35, 36 GDPR.

Data Subject means any identified or identifiable natural person whose Personal Data is processed.

Employee (or Atos Employee) means any natural person who is on the payroll of any Atos Entity, i.e. receives regular payments on the basis of a written or an oral labor agreement (including trainees), or anyone acting in the place of an employee, such as an individual contractor or staff provided via an employment agency.

European Economic Area (or EEA) is composed of all the Member States of the European Union, plus Iceland, Liechtenstein and Norway.

Genetic Data means Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Group Data Protection Policy ('Atos Group Data Protection Policy') means this Policy together with its Appendices.

Local Data Protection Office means, together, the local Data Protection Legal Experts ("DPLE") and the Local Data Protection Officer ("DPO") as defined in Section 14 of this Atos Group Data Protection Policy.

Group Data Protection Office (or GDPO) means the organization set out at Atos Group level to organize, coordinate and ensure a consistent and coherent approach to personal data protection within the Atos Group.

Personal Data means any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location Data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach means 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.

Personal Data Transfer means the disclosure of Personal Data to other Atos Entities or to any Third Party, the transmission of such Data to other Atos Entities or to Third Parties, or the process of making such Data available to other Atos entities or Third Parties in any form for inspection or retrieval.

Privacy Information Notice (or Privacy Notice) means information shared by Atos, as Controller to inform data subjects regarding the processing of their personal data, covering communication required by Data Protection legislations.

Processing (or Data Processing) means any operation or set of operations/activities which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor (or Data Processor) means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

Pseudonymization means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

Region means several countries for which competent legislators or authorities officially recognize that their legislations and regulations respectively provide an equivalent level of protection to the Personal Data processed.

Sensitive Personal Data means 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, genetic or biometric information, financial information such as bank account or credit card or debit card or other payment instrument details or Personal Data relating to criminal convictions and offences.

Subcontractor means a legal person (for example a company) or a natural person (an individual – but not in this case someone acting as an Atos Employee), contracted by Atos (where Atos is acting either as a Controller or as a Processor) for the provision of services entailing the Processing of Personal Data. Where Atos acts as a Controller, such a Subcontractor will normally be a Processor. Where Atos is acting as a Processor, the Subcontractor will be a sub-Processor.

Third Party means a natural or legal person, public authority, agency or body other than Atos as Controller or the Data Subject.

1.7 Abbreviations

The abbreviations used in this Policy are defined as follows:

BCR	Binding Corporate Rules
BIC	Book on Internal Control (Atos BIC)
CADP	Compliance Assessment of Data Processing ('Atos CADP')
CADP-C	Compliance Assessment of Data Processing where an Atos Entity acts as a Controller ('Atos CADP-C')
CADP-P	Compliance Assessment of Data Processing where an Atos Entity acts as a Processor ('Atos CADP-P')
CADP-S	Compliance Assessment of Data Processing for Supplier/Subcontractor ('Atos CADP-S')
CNIL	Commission Nationale de l'Informatique et des Libertés (lead Data Protection Authority for Atos as a Group)
DP	Data Protection
DPA	Data Protection Addendum ()
DPC	Data Protection Coordinator
DPE	Data Protection Expert
DPIA	Data Protection Impact Assessment
DPLE	Data Protection Legal Expert
DPO	Data Protection Officer
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation (Europe)
KPI	Key Performance Indicators
RACI	Responsible, Accountable, Consulted, and Informed (acronym for responsibility assignment matrix)
TOMs	Technical and Organizational Measures ('Atos TOMs')

2 Principles for Processing of Personal Data

The principles set out in this Atos Group Data Protection Policy shall be respected by Atos, except where local laws prevent the application of such principles or are providing for more stringent requirements than those set out in this policy.

2.1 Principles to be respected when Processing Personal Data as a Controller

When implementing a Processing of Personal Data, Atos, acting as a Controller, shall ensure that the Personal Data Processed is:

- processed lawfully, fairly and in a transparent manner in relation to the Data Subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed;
- processed in a manner that ensures appropriate security of the Personal Data.

Atos implements adequate processes and measures to do so, so that, at all times, it can demonstrate that the way in which it or its Third-Party Subcontractors process Personal Data in accordance with the requirements of the applicable Data protection legislation.

2.2 Principles to be respected when Processing Personal Data as a Processor

As a Processor, Atos commits to comply with the instructions it receives from the Controller, provided, however, that they appear to be lawful. In this respect, as a Processor, Atos commits to only process the Data it receives from the Controller for the purposes set out by the Controller and not for any other purpose without the prior written authorization of the Controller.

When Atos becomes aware of the fact that the Controller's instructions do not comply with any applicable law, including Data Protection Law, or this Policy, Atos, as a Processor, informs the Controller in order to request the Controller to modify its instructions in order to remediate the issue and to enable Controller to provide instructions that comply with applicable Law and this Policy.

When Atos Processes Personal Data on behalf of a Controller, it is the responsibility of the Controller to ensure that the Processing respects the principles which have to be complied with as per the applicable law of the Controller.

As per the terms of applicable law and / or the Agreement between Atos and the Controller, Atos shall assist the Controller in implementing the principles which have to be complied with by the Controller.

2.3 Legal grounds for Processing Personal Data as Controller

2.3.1 General legal grounds for Processing

Before starting any Processing of Personal Data, Atos, acting as Controller, shall make sure that the Processing relies on one of the following grounds:

- the Data Subject has given his or her Consent to the Processing of his or her Personal Data for one or more defined purposes;

  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 protect the vital interest of the Data Subject or of another natural subject;

  or

- 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 Atos.

2.3.2 Legal grounds for further Processing

Where Atos intends to implement a further Processing, which is not based on Data Subject Consent or applicable law, Atos shall ascertain whether such further Processing is compatible with the initial purpose. To conduct such evaluation, Atos will take into account, inter alia:

- any link between the purposes for which the Personal Data have been collected and the purposes of the intended further Processing;
- the context in which the Personal Data have been collected, in particular regarding the relationship between Data Subjects and Atos;
- the nature of the Personal Data, in particular whether Sensitive Personal Data are processed;
- the possible consequences of the intended further Processing for Data Subjects;
- the existence of appropriate safeguards (e.g. encryption or pseudonymization or any adequate measure).

2.4 Legal grounds for Processing Personal Data as Processor

When Atos processes Personal Data on behalf of a Controller, it is the responsibility of the Controller to ensure that the Processing is based on an appropriate legal ground as per the applicable law of the Controller.

In this respect, Atos shall process Personal Data on behalf of the Controller in accordance with the documented and agreed instructions received from the Controller and set out in a contract or any applicable legal act.

2.5 Processing of Sensitive Personal Data

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

(a) the Data Subject has given explicit Consent to the Processing of those Sensitive Personal Data for one or more specified purposes;

or

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Atos or of the Data Subject in the field of employment and social security and social protection law where authorized by applicable law;

or

(c) 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

(d) Processing relates to Personal Data which are manifestly made public by the Data Subject;

or

(e) Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

or

(f) Processing is necessary for reasons of substantial public interest;

or

(g) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of applicable law;

2.6 Security measures

2.6.1 Security measures when acting as a Controller

Atos shall process Personal Data in accordance with the provisions of the Atos Group Security Policies as implemented by Atos Entities 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, including, notably, as appropriate:

(a) the Pseudonymization and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

As a Controller, Atos shall take into consideration the nature and categories of the Personal Data it processes, the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, in defining and implementing relevant security measures

2.6.2 Security measures when acting as a Processor

When acting as a Processor (including the provision of services to customers), Atos shall, in accordance with the terms of its agreement with the entity hiring it as a Processor, implement appropriate technical and organizational measures to protect the Personal Data it processes on behalf of the Controller against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

To the extent required by applicable law or by the agreement with the entity hiring it as a Processor, Atos shall assist the Controller in defining and implementing adequate technical and organizational security measures to protect the Personal Data it processes on behalf of the Controller against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

3 Implementation of the principles of Section 2 for Atos Entities processing Personal Data as Controller and as Processor

3.1.1 Impact Assessment

In order to target an appropriate level of compliance with the principles defined in Section 2, Atos conducts, where appropriate, a Compliance Assessment of Data Processing ("Atos CADP" based on an Atos CADP template or comparable format) and, where required under Applicable Data Protection Law, a Data Protection Impact Assessment ("Atos DPIA") as detailed in Appendices 7 and 8.

Where an Atos Entity acts as a Controller an Atos CADP as Controller ('Atos CADP-C') must be completed for all processing. Where a Processing is already implemented, and the Atos CADP-C is not completed, it should be completed as soon as possible. Where a new Processing is considered, the Atos CADP-C is completed progressively as early as possible once the project is identified by the business owner of the Processing, assisted where necessary by relevant support functions (e.g. Security, Digital & Transformation, Atos IT, Procurement, etc.) and any Third-Party Subcontractor used. It shall be reviewed by the competent Data Protection Office.

Where Atos acts as a Processor, the Atos CADP as Processor ('Atos CADP-P') is completed progressively as part of the bidding and contracting process by the relevant members of the bidding, solution and sales team as well as, where relevant, Subcontractors, with the support of or on the basis of the information provided by the Atos's prospect or customer as Controller. The Atos CADP-P is reviewed by the competent Data Protection Office and may be attached to the agreement to be signed with the Controller.

3.1.2 Records of Processing activities

Atos maintains records of its Processing activities if and as required under Applicable Data Protection Law.

When acting as a Controller, such records shall be composed of the Atos CADP-Cs completed by the owner of the assessment and retained by the Group or Local Data Protection Office in an adequate fashion. Group or Local Data Protection Office shall support owners to comply to this policy.

When acting as a Processor, such records shall be composed of the Atos CADP-Ps completed and retained by the operational Business owner in an adequate fashion.

4 Selection and use of Subcontractors

As part of its Processing activities, Atos may use Subcontractors which will either process Personal Data on its behalf (i.e. when Atos is acting as a Controller) or on behalf of Atos's customer (i.e. when Atos is acting as a Processor). Where the Subcontractor is part of the Atos Group, it shall be designated as "Atos Internal Subcontractor". Where the Subcontractor is not an entity which is part of the Atos Group it shall be designated as "Third Party Subcontractor" or "External Subcontractor".

When selecting Subcontractors, Atos shall consider each Subcontractor's situation and the guarantees it provides with regards to compliance with Applicable Data Protection Law and implement adequate contractual measures to reflect the relevant obligations as per the requirements of Applicable Data Protection Law. When Subcontractors process personal data on Atos behalf or its Clients, an Atos Standard Data Protection Clause should be inserted in the main contract and an Atos Data Protection Addendum (DPA) and attachments should be annexed.

When acting as a Processor, Atos shall ensure that it has duly informed and obtained the Controller's prior consent (whether general or specific) to use a Subcontractor and shall ensure that the Subcontractor provides a level of protection to Personal Data similar to the level defined in its agreement with the Controller. In Bidding process and in Delivery process, the Atos CADP-P should be updated accordingly.

In such cases, Atos shall enter into adequate agreements governing the Processing of Personal data by such Subcontractors, including Atos Subcontractors.

5 International Transfers of Personal Data

Whether acting as a Controller or a Processor, Atos must ensure that an adequate level of protection is provided to Personal Data when it's transferred.

For this purpose, when transferring Personal Data outside of a defined jurisdiction or Region, Atos shall implement adequate safeguards as defined and required under Applicable Data Protection Law.

In the event that Personal Data is transferred from the European Economic Area (EEA) to an entity located in a jurisdiction which is not recognized by competent authorities as providing an adequate level of protection to Personal Data, the rules defined in Article 3 of the Atos Binding Corporate Rules (the Atos BCR, attached in Appendix 6 to this Atos Group Data Protection Policy) shall apply.

Before transferring Personal Data, Atos shall assess the laws and practices of the country of destination to determine if additional security measures are necessary to be implemented to ensure an adequate level of protection. Accordingly, Transfers of Personal Data shall be governed by adequate safeguards either through the application of the Atos BCR or the signature of adequate agreements, where necessary and relevant.

6 Data Subject's rights

Where Atos processes Personal Data as a Controller, Data Subjects shall be entitled to the following rights, subject to Applicable Data Protection Law:

- right to transparent information, i.e. being provided with clear and intelligible information regarding the Processing of the Data Subject's Personal Data (Atos Privacy Information Notice);
- right of access, i.e. being provided with the right to request from the Controller communication of a copy of the Personal Data it holds and processes about him/her;
- right to erasure (right to be forgotten), i.e. being provided, subject to the Data Subject having legitimate grounds to do so, with the right to request from the Controller the deletion of all or part of the Personal Data it holds about him/her and to be notified of such erasure;
- right to restriction of Processing, i.e. being provided with the right to request the interruption of the Processing of the Data Subject's Personal Data, subject to the Controller no longer being entitled to continue such Processing and to be notified of such restriction;
- right to Data portability, i.e. the right for the Data Subject to request from the Controller the provision of a copy of the Personal Data it holds about him/her in machine-readable format;
- right to object, i.e. being provided, subject to the Data Subject having legitimate grounds to do so, with the right to object to the Processing of his or her Personal Data by the Controller.
- right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

All such requests shall be made in accordance with the procedure set out in Appendix 2.

Where a Data Subject legitimately considers that, after exercising their Data Subjects rights, the request has not been treated correctly under applicable Data Protection Law, the Data Subject is granted the right to file a complaint in accordance with the terms of Appendixes 3, 4 or 5 to this Group Policy.

The procedure for the management of such complaints is set out in Section 7 below and in Appendix 3 to this Atos Group Data Protection Policy.

When acting as a Processor, the Controller shall remain responsible to provide Data Subjects with clear and effective mechanisms to exercise the rights set out above. Atos shall, where necessary, to the extent required by Applicable Data Protection Law and insofar as possible, assist the Controller, for the fulfilment of its obligation to respond to requests from Data Subjects to exercise their rights set out above.

7 Complaint Handling Procedure

7.1 Direct Complaint

If a Data Subject believes that the Processing of his or her Personal Data has caused him/her damage or that his or her Personal Data has not been processed in accordance with the provisions of this Atos Group Data Protection Policy or with applicable law, said Data Subject is entitled to file a complaint against the relevant Atos Entity.

Atos has established a time framed Complaint Handling Procedure which is defined in Appendix 3. Notwithstanding the above and Appendix 3, the Data Subject retains, at all times, the right to file a complaint directly with the competent Data Protection Authority. Data Subjects are however encouraged to favor the filing of a direct complaint as described in this section 7.1 and, if necessary, to escalate their complaints.

7.2 Indirect Complaint

Where a Controller reports a complaint from a Data Subject whose Personal Data is processed by Atos, Atos shall take all necessary steps to make sure that the Data Subject complaint is handled correctly. For this purpose, Atos shall comply with the procedure set out in Appendix 4 to this Atos Group Data Protection Policy.

Notwithstanding the above and Appendix 4, the Data Subject retains, at all times, the right to file a complaint directly with the competent Data Protection Authority. Data Subjects are however encouraged to favor the filing of an indirect complaint as described in this section 7.2 and, if necessary, to escalate their complaints.

7.3 Complaint of a Controller

Where Atos acts as a Processor, i.e. processes Personal Data on behalf of a Controller, the latter may raise issues regarding the Processing of its Personal Data.

Atos commits to handle such request from Controllers smoothly and efficiently, in accordance with the terms of Appendix 5.

8 Cooperation

Atos 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.

8.1 Cooperation with Controller

Where Atos processes Personal Data on behalf of a Controller, Atos shall, to a reasonable extent, provide the Controller with relevant information, in order to enable the Controller to comply with its own legal local requirements.

8.2 Cooperation with Data Protection Authorities

Atos shall also cooperate, in accordance with Applicable Data Protection Law and the Atos BCR, with competent Data Protection Authorities to handle requests or complaints from individuals or an investigation or inquiry by the competent Data Protection Authorities. Atos Entities shall, to a reasonable extent, abide by the advice of the Data Protection Authorities on any issues regarding Data protection.

9 Privacy by design, privacy by default

Data Protection should become an integral part of both technological development as well as any provision of a new product or service.

Privacy by design and privacy by default are important for any business to consider, especially in the case of a business providing digital services. While it is a positive change for customers, that is for Atos's clients, as well as for Data Subjects, the burden on any organization to comply with Data Protection legislation may become significant if not addressed at a foundation level. Accordingly, Atos will implement data protection by design and by default, to the extent possible, taking into consideration the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of Data Subjects posed by the Processing.

9.1 Privacy by design

Each team or person designing a new service or business process that makes use of Personal Data must take the protection of such Personal Data into consideration. Any organization Processing Personal Data needs to be able to show that it has adequate security measures in place and that compliance is monitored. In practice this means such organization must take data protection into account during the development or the whole life cycle of the system or process.

As a consequence, when designing products and offerings, Atos shall ensure that the protection of Personal Data is taken into consideration by factoring in all Data protection principles, including notably, the requirements of Data minimization, retention limitation, transparency and security and Data Subject rights.

For this purpose, Atos shall implement in its processes, the completion of Atos CADPs for new processes it implements as a Controller or as a Processor.

9.2 Privacy by default

Where Atos Processes Personal Data as a Controller, it shall implement processing settings designed to limit as much as possible the collection, use and disclosure of the data, taking into consideration the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

In this respect, Atos shall require its Processors to implement similar requirements regarding the Processing of Atos Personal Data.

As a Processor, Atos shall implement into its solutions, in accordance with Controller's instructions, default processing settings designed to limit as much as possible the collection, use and disclosure of the data, taking into consideration the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing. In addition, Atos will inform the Controller if their instructions appear to be in contradiction with this principle.

9.2.1 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 and involved at every stage of the project.

Where the Local Data Protection Office considers that 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.

It results from the above that Atos Employees who develop new projects shall make sure that either the Local or the Group Data Protection Office is involved in each project.

10 Register and National Formalities with Competent Data Protection Authorities

Where Local Data Protection Authorities request prior notification of the processing of personal data, Atos commits to respect local requirements in this regard.

Where Atos acts as a Controller, each Local Data Protection Office keeps a register of the processes which are implemented by Atos and gathers all prior notification forms that are submitted to local Data Protection Authorities.

Where Atos acts a Processor on behalf of a Controller, Atos commits to provide the Controller with all relevant information necessary to comply with local formalities requirements.

Where required by regulation or by local law, Atos will notify the details of the responsible Data Protection Officer (DPO) to the Local Data Protection Authority.

11 Personal Data Breach notification

Where Atos, acting as Controller, becomes aware of a Personal Data Breach, it shall immediately implement adequate remediation measures in accordance with the provisions of Applicable Data Protection Law and the Atos Personal Data Breach Policy, provided in Appendix 10.

Concurrently, Atos shall evaluate the elements of the Personal Data Breach – including, notably, any relevant remediation measures undertaken – to determine whether it is likely to result in a risk to the rights and freedoms of the Data Subjects affected. Based on such evaluation, to be conducted in accordance with Applicable Data Protection Law as well as the terms of the Atos Personal Data Breach Policy, Atos shall, where feasible and where required under Applicable Data Protection Law and without undue delay after having become aware of the Personal Data Breach, notify it to the competent Data Protection Authority and/or communicate the relevant elements of the Personal Data Breach to the Data Subjects affected in accordance with Applicable Data Protection Law and the Atos Personal Data Breach Policy.

Where Atos acts as a Controller, each Local Data Protection Office keeps a register of the Personal Data Breaches comprising the facts relating to each Personal Data Breach, its effects and the remedial actions taken as well as a copy of any notification made to the competent Data Protection Authority and of the communication made to the Data Subjects affected, if any.

When Atos, acting as a Processor, becomes aware of a Personal Data Breach affecting the Personal Data it processes for its clients, in coordination with the concerned client it shall implement the remediation measures which appear to be the most appropriate as soon as possible. Concurrently, Atos shall collect relevant information to provide it to the Controller in order to allow it to evaluate the nature and scope of the Personal Data Breach. Atos shall notify such Personal Data Breach to its client without undue delay.

12 Training and raising awareness

Atos believes that the rules and principles set out in its Personal Data protection policies (this Atos Group Data Protection Policy, the Atos Binding Corporate Rules, etc.) can be only enforceable and effective throughout the Atos Group 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 Atos Employees,
- Provide specific and appropriate training to those Atos Employees who 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 Atos Employees and specific training to Atos Employees who have permanent or regular access to Personal Data.

Specific modules taking into account organizational, functional or local specificities will also be developed.

Statistics relating to the attendance to the Data Protection Training will be monitored by the Data Protection Community together with the Human Resources Department.

Each manager is accountable to ensure that its direct reports have taken part to all relevant Data Protection trainings.

13 Audit

13.1 Internal Audit

Atos commits to audit Atos Group's compliance with regard to the implementation of this Atos Group Data Protection Policy.

Such audits shall be carried out on a regular basis. Such audits shall be carried out by Atos internal auditors and will include periodic audits of data protection controls included in the Atos Book of Internal Controls (BIC).

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

Upon request, Competent Data Protection Authorities may obtain results of any Data Protection Audits.

13.2 Subcontractors Audits

Where contracting with subcontractors acting as Processors of Atos's Personal Data or of Customers' Personal Data, Atos shall ensure that in its agreements, it is granted a right to audit.

13.3 Customer Audits

Where Atos acts as a Processor, Controllers can request an audit to be carried out on the Atos facilities used to process Controller's Personal Data.

Such audit request can be valid only provided that the Controller gives appropriate prior

notice to Atos.

14 Data Protection Community

Atos wants to ensure that the Atos Group Data Protection Policy is effectively implemented throughout the Group.

For this very reason, a Data Protection Community ("Atos DP Community") has been created.

The Data Protection Community is led by the Group Chief Data Governance Officer who coordinates the Group Data Protection Office (GDPO). The Group Chief Data Governance Officer reports to the Group General Counsel.

The Data Protection Community is composed of a network of Data Protection Legal Experts (DPLE), who could be part of the Legal, Compliance and Contract Management Department or any relevant organization, and of Data Protection Officers (DPO) who have local responsibilities and have reporting lines to local management and to the Group data protection organization.

At least one DPO shall be appointed for each country in which Atos operates. Where there is a legal requirement to do so or where it is considered expedient, Atos entities shall notify their DPO to the competent Data Protection Authority.

Together the DPO and DPLE form the Local Data Protection Office. The list of data protection contacts is maintained on the Atos Data Protection SharePoint Space.

The Atos data protection organization is described in Appendix 1.

15 Key Performance Indicators (KPI)

In order to ensure an effective implementation of this Atos Group Data Protection Policy, the Data Protection 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 (i.e. number of Personal Data Breaches as considered under Section 11 of this Atos Group Data Protection Policy) notified to a Data Protection Authority;
- Number of data breaches (i.e. number of Personal Data Breaches as considered under Section 11 of this Atos Group Data Protection Policy) 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 exercise their data protection rights;
- Number of requests from other data subjects to exercise their data protection rights.
- Percentage of Atos Employees taking part to a Data Protection Training, i.e. percentage of Atos Employees having successfully completed the Atos mandatory e-learning on Data Protection;

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

16 Investigation

Where an onsite investigation by a Data Protection Authority takes place 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 Data Protection Authority carrying out the investigation.

17 Update of the Atos Group Data Protection Policy

This Atos Group Data Protection Policy may be amended from time to time and where necessary, in particular where Applicable Data Protection Law evolves significantly and at least every two (2) years.

Any significant changes to this Atos Group Data Protection Policy shall be reported to all Atos Entities. Clear and easily available information regarding any such significant change shall be made for Atos Employees and Third Parties' information.

18 RACI

Activity	Group Data Protection Office	RBU & GDC DPLEs	RBU & GDC DPOs	Local DPLE	Local DPO
ADOPTION OF THE POLICY FOR THE ENTITIES					
Adopt an Intra-Group Agreement between Atos parent company and Atos entities regarding the bindingness of the Policy	A for the signature / R for the content of the IGA	I	I	R	R
For each policy, determine whether or not a Local Board Decision is necessary	I	I	I	A/R	C
if yes: Present to the Local Board to request validation by the Board	I	I	I	A/R	R
If not: Formal Statement by Local Function on behalf of the local entity that the policy is effective in the relevant entity	I	I	I	A/R	R

Activity	Group Data Protection Office	RBU & GDC DPLEs	RBU & GDC DPOs	Local DPLE	Local DPO
MAKING POLICY BINDING AMONGST EMPLOYEES					
Translate policy into local language when required by Local law	I	I	I	A/R	A/R
Determine the local requirements regarding Work Councils	I	I	I	A/R	A/R
Where necessary, prepare communication pack for Work Councils presentation	C	C	I	A/R	A/R
Where necessary, consultation or information needed: set up date and present to Works Councils	I	I	I	A/R	A/R
Where not necessary: communicate broadly to all Employees to comply with transparency and information requirement (via mailing or through appropriate local bulletin).	C (for drafting the communication) / I (for effective communication)	C (for drafting the communication) / I (for effective communication)	C (for drafting the communication) / I (for effective communication)	A/R	A/R
TRANSLATION OF ALL MATERIALS AND TOOLS INTO LOCAL LANGUAGE					
Ensure translation of all materials into local language	I	I	I	A/R	A/R

Activity	Group Data Protection Office	RBU & GDC DPLEs	RBU & GDC DPOs	Local DPLE	Local DPO
TRAINING					
Prepare the Global & General training	A/R (Design trainings (mandatory & dedicated)	C	C	C	C
Update DP training with local specificities, including translation (e.g. establish legal training content for local needs)	I	R	R	A/R	A/R
Monitor completion of mandatory DP training by Employees at Group and at local level and alert relevant management as necessary	A/R (mandatory training KPI)	C	A/R (support and report, specific training KPI)	C	A/R
If necessary, request Group and local action to promote compliance with mandatory training	A/R	C/I	A/R	C/I	A/C
Deliver classroom training when needed	A/R	A/R	A/R	A/R	A/R
Identify training needs	A/R	A/R	A/R	A/R	A/R
Make available training for DP Community	A/R	R	R		
Train local DPOs and DPLEs	C	A/R	A/R		

19 List of appendices

Appendix 1: Atos Data Protection Organization

Appendix 2: Form for Data Subject Rights

Appendix 3: Complaint Handling Procedure for Data Subjects against Atos acting as Controller

Appendix 4: Indirect Complaint Handling Procedure

Appendix 5: Complaint Handling Procedure for Controller which Personal Data are processed by Atos

Appendix 6: Atos Binding Corporate Rules

Appendix 7: Compliance Assessment of Data Processing when Atos acts as a Controller

Appendix 8: Compliance Assessment of Data Processing when Atos acts as a Processor

Appendix 9: Process where legislation prevents application of the Atos Group Data Protection Policy

Appendix 10: Personal Data Breach Policy

Appendix 1 – Atos Data Protection Organization

Data Protection Organization Principles

Reflect operating model	• Provide data protection support for Group and Local management • Maintain data protection expertise per Business Unit/Support Function
Adhere to jurisdictions	• Comply with legal obligations regarding appointment of data protection officers • Maintain necessary link to local legislation and Data Protection / Supervisory Authorities • Support regional / country cluster organization in the business
Allow evolutive approach	• Adapt role of Atos data protection specialists according to organizational and business development of the Group (iterative approach)

Data Protection Management Principles

Stay active	Data Protection is not a one-shot activity that required our attention, it is an ongoing endeavor. Atos needs a sound and stable data protection organization in order to be able to comply with its obligations and to be able to evidence that it does so (Accountability).
Adhere to the rules	Even if some units might feel remote from GDPR as they are not within the territorial scope of the law, Atos Binding Corporate Rules oblige all signing legal entities to adhere to the data protection principles and provisions set out in the Group Data Protection Policy and the Group Binding Corporate Rules. All units in Atos need to adhere to the Policy and to the BCR as well as to any locally applicable legislation.
Fill potential gaps	Entities need to assign colleagues to vacant DP roles/positions in order to ensure an effective data protection organization and a functioning data protection management system, as commonly required by data protection laws.
Allow for the means	Even in times of limited budgets, Data Protection obligations still remain, and possible fines as defined in GDPR threaten organizations who do not sufficiently care about protecting personal data. Hence data protection experts need sufficient means to fulfil their tasks. This includes realistic time allocation, tools that support the work, the necessary means for maintaining knowledge and expertise.

Group Data Protection Organization

- Cascaded organization covering the company matrix
- Two main role types: operational focus and legal focus
- Address local / national requirements as well as Group compliance requirements

Appendix 2 – Form for Data Subjects' Rights

This form below may be used by any Data Subject who wishes to exercise his or her rights according to Section 6 of the Atos Group Data Protection Policy. The information provided in this form will help Atos to handle a Data Subject request efficiently.

The form below should be addressed to the local Legal Expert on Data Protection or to the local Data Protection Officer. Find the list of your local Data Protection Office on the Data Protection Info Portal 2.0 on Atos SharePoint page Contacts.

The Atos Data Subjects Rights form can also be accessed via the "Privacy" section on the Atos Group website (https://atos.net/en/privacy)

Mail Form to Exercise your rights regarding your Personal Data	
First name	
Last name*	
Email address*	
Telephone number	
Preferred contact details*	Email: Phone: I prefer to be contacted by: ☐ EMAIL ☐ PHONE
Job title (Atos employee only)	
Data Subject's name and surname*	
Data Subject is:*	☐ An Atos Employee or Candidate ☐ A candidate for an Atos job ☐ An active employee ☐ A former employee. No longer employed by an Atos Group company. ☐ A Customer/Customer's employee ☐ Active ☐ Terminated ☐ Provider/Provider's employee ☐ Candidate ☐ Active ☐ Terminated ☐ A Guest at an Atos event ☐ An Atos website visitor ☐ Other: Please specify in box below:
Where Other, please specify relationship to Atos	

Employee DAS ID (only if active or former Atos employee)	
RBU / Practice / Legal employing entity (only if active or former Atos employee)	
Country of residence*	
Approximate date when data were initially collected*	
Which right do you want to exercise? *	☐ Right to information: I want to know which personal data is processed about me ☐ Right of access: I want to know which personal data is processed about me by Atos ☐ Right to rectification: I want to modify and rectify the personal data that is processed about me by Atos ☐ Right to erasure: I want my personal data not to be processed by Atos anymore and to be deleted ☐ Right to restriction of processing: I want my personal data not to be processed anymore but only stored by Atos ☐ Right to object: I don't want my personal data processed ☐ Right to data portability (if applicable): I wish to have a copy of my personal data in a portable format ☐ Right (where applicable) not to be subject to a decision based solely on automated processing ☐ Other. Please describe.
Category or categories of processing that this request relates to.	☐ Collection: My request concerns the collection of my personal data. ☐ Recording/Organization/ Structuring/ Storage: My request concerns the Recording/Organization/ Structuring or Storage of my personal data. ☐ Adaptation/Modification: My request concerns the adaptation or modification of my personal data ☐ Consultation/Making available or Disclosure: My concerns the way in which my personal data is available for others. ☐ Alignment/ Combination/Matching: My request concerns the combination of personal data that is carried out.
Justification. Please explain your request and the reason why you want to exercise your rights.	
Any relevant information that may help Atos provide Data Subject with the appropriate answer to their request. *	

Appendix 3 – Handling Data Subjects Complaints When Atos is acting as a Controller

Where a Data Subject believes that his or her rights under Atos Group Data Protection Policy (DP Policy) or under applicable Data Protection Law have been violated, and that his or her request to exercise his or her right(s) has been denied, Data Subject can enforce his or her rights against Atos by following the procedure set out in this Appendix and by fulfilling the attached form.

STEP 1: Raising the issue to the Data Protection Community

1.1 Addressing the complaint

Data Subjects shall first file their request regarding the exercise of their rights to the Local Data Protection Office at the relevant address that appears in Contact List (sharepoint.com)

1.2 Content of the claim

This request shall be made by using the attached form (Appendix 3 bis) and by submitting the following information:

- name of the data subject
- copy of documents which confirm the identity of the data subject
- contact details where the response shall be addressed to
- name of the Atos entity which has initially collected the personal data
- Approximate date of collection of the personal data
- type of personal data and processing purpose about which the data subject is complaining
- details regarding the claim, including the nature of any breach and the identity, if known, of any specific Atos Entity that the complaint concerns

Data subjects should make their claim as precise as possible in order to enable the Local Data Protection Office to handle the case within a reasonable period of time as defined in Step 2 of this Appendix 3.

STEP 2: Instruction of the complaint by the Local Data Protection Office

2.1 Acknowledgement of receipt

The Local Data Protection Office shall acknowledge receipt of the complaint no later than **one (1) week** after the complaint was received. The standard acknowledgement of receipt attached to this Appendix 3 (see Appendix 3 ter) can be used by the Local Data Protection Office.

2.2 Analysis of the complaint

2.2.1 Additional information requested

Where the information provided by Data Subjects is not sufficient for the Local Data Protection Office to handle the case, the latter shall address a request for additional information to the Data Subjects no later than **fifteen (15) days** after receipt of acknowledgement was sent.

2.2.2 Settlement of the complaint

Where the information provided by the Data Subject is sufficient for the Local Data Protection Office, or once the additional information requested in the previous paragraph is provided by the Data Subject, the Local Data Protection Office shall deal with the complaint without undue delay and in any event within one (1) month of receipt. Taking into account the complexity and number of the requests, that period may be extended by two further months at the utmost, in which case the data subject will be informed accordingly

The answer to the claim made by the data subject shall be as clear as possible and shall be drafted in a manner which is easily understandable by data subjects.

STEP 3: Escalation to Group Data Protection Office

3.1 Receipt of acknowledgment by Group Data Protection Office

Where Data Subject is not satisfied with the solution provided by the Local Data Protection Office as per STEP 2 of this procedure, he/she has the right to refer immediately its complaint to the Group Data Protection Office by addressing a mail to dpo-global@atos.net

The Group Data Protection Office shall acknowledge receipt of such complaint within two (2) weeks. For this purpose, the standard acknowledgement of receipt attached to this Appendix 3 (see Appendix 3 ter) can be used by the Group Data Protection Office.

3.2 Analysis of the complaint

The Group Data Protection Office shall take no longer than one (1) month to offer a solution to be agreed with Data Subject which would be satisfying for both parties.

STEP 4: Escalation to the competent Data Protection Authority

Where Steps 1 to 3 have not enabled Data Subjects to get a satisfying answer, Data Subjects retain the right to complain to the Local Data Protection Authority or to a similar Supervisory Authority in his/her Country, or to bring a claim before a Local relevant court in his/her country of location.

Appendix 3 bis

Complaint form for Data Subjects against Atos

The standard letter form below can be used by Data Subjects who intend to bring a complaint against Atos. Please note that this form should be filled in with relevant information.

This is only a template that may be used freely by Data Subjects – a complaint received in another format will also be studied according to the procedure described above.

****

Dear Local Data Protection Contact,

I, _____[indicate name and surname], hereby file a complaint regarding the processing of my personal data for which you are currently acting as a Controller.

Please find below, the information relating to my complaint, which I should be grateful if you could handle appropriately.

I acknowledge that the complaint procedure is time framed according to Appendix 3 of Atos Group Data Protection Policy and is deemed to have started as of _____ [indicate time where complaint is filed].

Please find also attached a copy of documents which should serve to prove my identity.

Data Subject's name and surname	
DAS ID	
Data Subject is:	☐ An Employee ☐ A candidate for an Atos job ☐ An active employee ☐ A former employee. No longer employed by an Atos Group company. ☐ A Customer/Customer's employee ☐ Active ☐ Terminated ☐ Provider/Provider's employee ☐ Candidate ☐ Active ☐ Terminated ☐ Guest ☐ Website visitor ☐ Other: Please specify:
Job Position (if employee, Customer or Provider)	

If Atos employee, employing entity and Industry / Practice / Functional Unit / RBU	
Date of this request	
Preferred contact details (email/ phone number)	
Approximate date when data were initially collected	
List of personal Data concerned by the complaint	
Description of the Complaint **Please give details regarding the right you wish to exercise, the category of processing activity at stake and, if relevant, the justification of why such processing seems illegitimate to you**	

Appendix 3 ter Standard Receipt of acknowledgment

Dear Data Subject,

We hereby acknowledge receipt of the complaint you have filed on _____ [indicate date complaint was sent by Data Subject] and that we received on _____ [indicate date complaint was received by Local/Global Data Protection Contact].

We will handle your compliant according to the Procedure and the time frame set up in Appendix 3 of the Atos Group Data Protection Policy.

In the meantime, we remain at your entire disposal to discuss this further.

Kind regards,

_____

The Local Data Protection Office / The Group Data Protection Office

Appendix 4 – Procedure for Handling Indirect Data Subject Complaints

For the purpose of this Appendix, Controller shall mean the Customer or any other third-party giving instructions to Atos for the processing of personal data at stake for the complaint.

Where one of Atos Controller's data subject is complaining about the processing carried out by the Controller, and where Atos acts as a Processor i.e., under the instructions of such Controller for the processing of personal data, Atos is willing to provide assistance to the Controller it is working with in order to make sure that the latter can handle its own Data Subjects' complaints.

STEP 1: Addressing the Controller's Data Subject request concern to the Data Protection Community

- Assistance of Atos where the complaint is addressed to the Controller

Controller shall make clear to Atos how Atos, as Processor can assist Controller regarding Data Subjects complaints and in particular, which information shall be provided by Atos. Atos will undertake all reasonable efforts to provide Controller with relevant requested information. As minimum, Controller shall be able to provide the level of information provided for in Appendix 4 bis.

For this purpose, Controller shall provide Atos a detailed request; otherwise, Atos will not be in a position to provide Controller with assistance.

This request shall first be filed to the Local Data Protection Office.

STEP 2: Instruction of the complaint by the Local Data Protection office

The Local Data Protection Office shall acknowledge receipt of the complaint no later than one (1) week after the complaint was received.

Where information provided by the Controller is not sufficient for the Local Data Protection Office, Local Data Protection Office shall address a request for additional information to the Controller no later than fifteen (15) days after receipt of acknowledgement was sent.

Where information provided by the Controller is sufficient for the Local Data Protection office, or once the additional information requested in the previous paragraph is provided by the Controller, Atos shall not take longer than one (1) month to provide Controller with relevant information.

STEP 3: Escalation to the Group Data Protection Office

Where the Controller considers that Atos has not provided Controller with relevant information to enable Controller to address Controller's Data Subject's complaint, the matter shall be escalated to the Group Data Protection Office.

The Group Data Protection Office shall acknowledge receipt of such indirect complaint and shall take no longer than one (1) month to propose a solution to be agreed with Controller on a solution which would be satisfying for both parties.

Controller always remains accountable and responsible for the communication to the data subject and the monitoring of his or her complaint.

Appendix 4 bis

Complaint form for Controller against Atos regarding the processing of Controller's Data subjects' personal data.

The standard letter form below shall be used by Customers who intend to bring a complaint against Atos. Please note that this form shall be filled in with relevant information.

This is only a template that may be used freely by Customer – a complaint received in another format will also be studied according to the procedure described above.

*****

Dear Local Data Protection Contact,

I, _____[name and surname of the contacting person] representing _____[indicate name of the name of the Company; Country of establishment] acting as a Controller, hereby require assistance of Atos and transmit the complaint of a Data Subject for whom I am acting as Controller for the processing of his or her Personal Data.

Please find below, the information relating to the complaint, which I should be grateful if you could handle appropriately.

I acknowledge that the complaint procedure is time framed according to Appendix 4 of Atos Group Data Protection Policy and is deemed to have started as of _____ [indicate time where complaint is filed].

Please find also attached a copy of Data Subject ID card which should serve to proof Data subject's identity.

Name, First Name of the Data Subject	
Approximate date where Personal Data was collected	
List of Personal Data concerned by the complaint	
Purpose of the processing at stake	
Description of Controller's Data Subject's complaint	
Controller's Contact details to provide information	

Kind regards,

_____

Appendix 5 – Procedure for Handling a Complaint from a Controller Regarding Processing of its Personal Data by Atos

Where a Controller complains about the processing of the Personal Data processed on its behalf by Atos, the following procedure shall be applied in order to guarantee a swift and efficient answer to Controller's concern.

Several types of incidents may occur, and the applicable procedure should differ according to the request sent by the Controller.

STEP 1: Controller's request

Controllers which identify a possible breach, or an existing breach of Data Protection Policy shall fulfill the form attached in Appendix 5 bis. This form is also made available on Atos website.

This request shall be sent to the Local Data Protection Office which will acknowledge receipt of the Controller's request within seven business days. This receipt of acknowledgement of receipt shall be made by using the standard letter set up in Appendix 5 ter.

STEP 2: Reception of the Controller's request and identification of the level of risk

The Local Data Protection Office shall then qualify the type of complaint according to the set of criteria set up below.

Amber level	- Potential risk identified by Controller - Question regarding the security measures - Data subject right of access or deletion not appropriately handled according to Controller - Suspected Atos Group Data Protection Policy violation
Red Level	- Risk realized and identified by Controller - Customer issuing lawsuits - Data Protection Authority contacting Atos

STEP 3: Handling the case

Where the issue is considered as being of Amber level, the Local Data Protection Office shall provide Controller with an answer to its concern within **one (1) month**.

Where the issue is considered as being of Red level, the Local Data Protection Office shall forward the case to the Group Data Protection Office. Both the Local and the Global Data Protection Office shall work closely together in order to solve the issue in the most expedient way.

Cooperation and discussions with the Controller as set up in Section 10 of the Atos Group Data Protection Policy.

Appendix 5 bis

Complaint form for Controller against Atos

The standard letter form below shall be used by Controller who intends to bring a complaint against Atos. Please note that this form shall be filled in with relevant information.

* *

*

Dear Local Data Protection Contact,

I, _____[name and surname of the contacting person] representing _____[indicate name of the name of the Company; Country of establishment] acting as a Controller, hereby file a complaint regarding the processing of the Personal data you are currently bound to process under the Service Agreement [Indicate reference of the contract] and according to the instructions I provided you through the form attached to the contract [if Atos CADP, give its name] .

Please find below, the information relating to our complaint, which I should be grateful if you could handle appropriately.

I acknowledge that the complaint procedure is time-framed according to Appendix 5 of Atos Group Data Protection Policy and is deemed to have started as of _____ [indicate time where complaint is filed].

Please find also attached a copy of my identity documents which should serve to prove my identity.

Name, First Name	
Contact details	
Approximate date Personal Data were collected	
Description of the Complaint	☐ Risk regarding the processing of personal data carried out on behalf of Customer. Please describe the risk with details and impact assessment. ☐ Question regarding the security measures. Please describe the question. ☐ Data subject right of access or deletion not appropriately handled according to Customer. Please give relevant information as per Appendix 4. ☐ Suspected Group Data Protection Policy violation. Please justify which provisions are at stake. ☐ Other. Please describe

Appendix 5 ter

Standard Receipt of acknowledgment

Dear Controller,

We hereby acknowledge receipt of the complaint you have filed on _____ [indicate date complaint was sent by Controller] and that we received on _____ [indicate date complaint was received by Local Data Protection Contact].

We will handle your complaint according to the Procedure and the time frame set up in Appendix 5 of the Atos Group Data Protection Policy.

In the meantime, we remain at your entire disposal to discuss this further.

Kind regards,

_____

The Local Data Protection Office / The Group Data Protection Office

Appendix 6 – Atos Binding Corporate Rules

The Atos Binding Corporate Rules are available via the "Privacy" page on the Atos website:

Privacy - Atos

Appendix 7 – Compliance Assessment of Data Processing when Atos acts as a Controller

A Compliance Assessment of Data Processing as a Controller ("CADP-C") must be completed for all processes where Atos acts as a Controller in order to target an appropriate level of compliance. The purpose of this assessment 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. 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 a Data Protection Impact Assessment should be conducted or not.

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

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

The CADP-C should first be completed by the respondent(s) using the online MyCADP platform and then submitted for review by the Local or Group Data Protection Office, as appropriate.

Appendix 8 – Compliance Assessment of Data Processing when Atos acts as a Processor

A Compliance Assessment of Data Processing as a Processor ("CADP-P") must be completed for all processes where Atos acts as a Processor in order to target an appropriate level of compliance. The purpose of this assessment is to allow Atos to meet several requirements under data protection law. The CADP-P 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. The CADP-P must be completed at the earliest stage of the project.

The CADP-P enables Atos to collect the instructions of the Controller in a documented manner and enables Atos to maintain its Processor register of Processing Activities. A CADP-P should be compiled using the online MyClientCADP tool by the Atos project / bid team responsible for the proposal and for each project where Atos acts as a Processor, with the assistance of the functional team and with guidance and (final) validation from the responsible Data Protection Legal Expert (DPLE) and / or Data Protection Officer (DPO).

Appendix 9 – Process where legislation prevents application of the Atos Group Data Protection Policy

PROCESS WHERE LEGISLATION PREVENTS APPLICATION OF THE ATOS GROUP DATA PROTECTION POLICY

Where one or several of the Atos Entities becomes aware or has reasonable reasons to believe that applicable legislation prevents it from fulfilling

- its obligations under this Atos Group Data Protection Policy and/or
- instructions it may have received, when acting as a Processor, from a Controller

and such legislation has substantial effect on the guarantees provided by the Atos Group Data Protection Policy, it will promptly inform the Group Data Protection Office per e-mail or in writing.

In the absence of such notification, it is expected that the principles set out in this Atos Group Data Protection Policy are fully respected by the Atos Entity or Atos Entities in question.

- (a) Where Processing Data as a Controller

In such a case, where possible, the Local Data Protection Office handles the above issue, by identifying adequate courses of action (e.g. implementation of adequate processes or measures, review of the policy to ensure its local applicability, etc.) as soon as possible but in any case, not later than one month after the complaint is received.

Where the Local Data Protection Office cannot handle the issue within a month after the complaint is received, it shall refer the case to the Group Data Protection Office which shall work with the Local Data Protection Office and/or any other relevant stakeholders to define relevant actions to solve the issue (e.g. review of the policy, implementation of new processes, etc.) 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.

- (b) Where Processing Data as a Processor

Where Atos acts as Processor it shall also notify Controller any concern that it may have to consider for the delivery of the service by Atos in compliance with this Atos Group Data Protection Policy and with the Controller's instructions.

Such notification to the Controller shall be made in such a timely manner that it enables Customer to acknowledge the notification and, where relevant, take necessary actions to review its instructions as provided for under the terms of the Agreement between Atos and the Controller.

Appendix 10 – Personal Data Breach Policy

The Atos Data Breach Policy is available via the data protection key documents page in the Atos SharePoint document store here:

[Data Protection Key Documents (sharepoint.com)]

PERSONAL DATA BREACH POLICY

AUTHOR(S) : Fritz Beichbuchner
Andrew Jackson
DOCUMENT NUMBER : 0000036
VERSION : 4.0
STATUS : Final
SOURCE : Atos
DOCUMENT DATE : 12 July 2022
NUMBER OF PAGES : 24

OWNER : Andrew Jackson

Role	Names
Reviewers	Paul Bayle, Head of Group Security Janine Skinner, RBU DPO Americas Prasad Purayil, RBU DPO APAC Joos van Rooy, RBU DPO NE Peter Landsteiner, RBU DPO CE
Approvers	Paul Bayle, Head of Group Security Janine Skinner, RBU DPO Americas Prasad Purayil, RBU DPO APAC Joos van Rooy, RBU DPO NE Peter Landsteiner, RBU DPO CE Flora Gonzalez – Suescun, RBU DPO SE
Document Controller	Katarzyna Cieslak-Rylich
Document Owner	Andrew Jackson, Group Chief Data Governance Officer
Senior Manager Atos	Damien Catoir, Group General Counsel

End of Atos Group Data Protection Policy