Global Data Protection Statement Atos Group

Trusted partner for your **Digital Journey**

Atos

Contents

Preamble

Atos is a leading worldwide provider of Digital Transformation services and IT solutions. Atos's compliance with applicable statutory regulations for data protection and information security is the basis for our customers' confidence in our services. Atos provides its customers with comprehensive protection in these areas.

This document presents a high level view of the technical and organizational measures governing data protection and data security implemented by Atos under the terms of Article 32 of the General Data Protection Regulation (GDPR) to ensure confidentiality, availability and integrity during the processing of personal data as defined in AP17: the Atos Group Data Protection Policy. It does not include a description of the contractual scope of services delivered to a particular customer, nor does it reference any specific legal obligations that may apply in a particular jurisdiction.

Data Protection Statement

For the provision of the services agreed with the customer, Atos agrees to comply without restriction with all stipulations of applicable data protection law, in line with agreed countries within which services to the customer will be delivered, as well as, where applicable, the EU General Data Protection Regulation (GDPR).

Atos Binding Corporate Rules

Binding corporate rules (BCR) are corporate-wide binding policies. The concept of BCR was conceived by the former Article 29 Data Protection Working Party, which developed the specifications for BCR to enable multinational organizations and groups of companies to transfer personal data across national borders, while respecting the existing European data protection law.

Atos was the first IT company to achieve recognition of its BCR as both a Controller and a Processor, offering a means of facilitating international transfers of personal data within the Atos Group, both for itself and on behalf of its customers, while ensuring a consistent, compliant level of protection for the rights of data subjects.

There is a formal process by which Supervisory Authorities cooperate in evaluating and recognizing BCR as valid and their use as a means of protecting data transfers is sanctioned by the GDPR. The certification process requires that all European data protection authorities are involved in the approval of BCR and the legal situation of each country is taken into account.

A written confirmation was issued by the leading French Data Protection Authority CNIL in November 2014, a copy of which is available upon request. The decision was also published in the Journal of the French Republic. The most recent version of the Atos BCR may always be obtained from the 'Privacy' pages of the Atos corporate website.

Information Security and Data Protection Organization

Atos has a group-wide information security organization that is responsible for the Atos information security management system. It is responsible for assessing and managing information security risk. Specifically, it develops and maintains the security policies, procedures and guidelines that protect data. It also raises employee awareness of these topics, assesses compliance and controls implementation

The Atos Group Data Protection organization is closely integrated with its security organization. It provides advice and guidance to Atos on data protection compliance, develops and maintains data protection policy and coordinates the work of the Atos data protection community, which is made up of Data Protection Officers (DPOs) and Data Protection Legal Experts (DPLEs). The Atos DPO fulfills his/her tasks in compliance with local data protection law and, where applicable, with Article 37-39 of GDPR.

Employee Confidentiality Obligation

All employees engaged to provide services have been obliged on a written basis to comply with data confidentiality, pursuant to local employment and data protection laws, and to the keeping of business and official secrets. Where applicable, new hired employees with access to personal data will be obliged in writing not to process such data except on instructions from the Controller, unless required to do so by Union or Member State law, Art. 29 GDPR.

Technical and Organizational Measures - Article 32 of the GDPR

Measures taken to ensure the confidentiality, integrity, availability and resilience of processing systems.

Confidentiality (Art. 32 Section 1 lit. b GDPR)

In order to ensure the confidentiality of the data and systems, physical, logical and application access to systems that store, process, transfer or transmit personal data is strictly regulated and controlled by the technical measures described below. In addition, appropriate procedures of separate processing and / or pseudonymization of the data are used to ensure the confidentiality of the data and systems to the appropriate extent.

Physical Access Control

The goal of physical access control is to ensure that only authorized persons have access to systems that process or use personal data and to the facilities where such processing takes place.

All Atos Data Center sites are secured against unauthorized access through automated access control systems. In addition, security relevant areas are equipped with permanent or motion-controlled video surveillance and access is monitored by security personnel and/or entry gates. The security service performs regular patrols at night.

A clearly defined concept for authorized access to Atos facilities is in place. People's rights to access to administrative areas are controlled by badges and card readers at office and/or floor entrances (electronic access control). The given access rights are monitored and reviewed periodically. Security and reception personnel are present, too. Visitors and third parties are recorded in visitor lists and are only permitted to access to Atos premises accompanied by Atos staff.

Access to Data Center rooms is additionally secured:

- Automated access control is supplemented by other established methods of access authorization, such as biometrics, Pin-Pads, DES dongle, permanent security personnel, etc.
- Data Center rooms are partitioned on a multi-layer basis;
- Access to internal security areas is only permitted for a small, selected number of employees and technicians;
- In certain areas the access and presence of people is recorded by video.

Logical Access Control

The goal of logical access control is to ensure that only authorized persons are able to access systems that process and use personal data, and that such access is based on legitimate and authorized need to access.

Data terminals (PC, servers, network components and devices) are accessed by means of authorization and authentication in all systems. Access control regulations include the following measures:

- Passwords (lower- and upper-case letters, special characters, numbers, minimum 8 characters, changed regularly, password history);
- Company ID with PKI encryption (two-factor authentication);
- Role-based rights are tied to access ID (classified according to administrator, user, etc.);
- Screen lock with password activation in user's absence;
- Encryption of data storage devices while in transit (including laptop / notebook hard drives);
- Use of firewalls and antivirus software including regular security updates and patches.

Application Access Control

Application access control measures prevent unauthorized processing and activities (e.g. unauthorized reading, copying, modification or removal) in data processing systems by persons without the required level of authorization.

Atos ensures the system-wide authentication of all users and data terminals including access regulations and user authorizations by technical measures.

Application access control incorporates the following measures:

- A role-based authorization concept is in place;
- Access authorization is always based on the principle of restrictive allocation of rights;
- A program-related authorization concept is implemented;
- Shared systems have client separation/ separate data pools;
- A clear desk policy is in place;
- Data storage devices in all mobile systems are encrypted while in transit;
- Use of firewalls and antivirus software including regular security updates and patches;
- A regular review of all existing privileged accounts is carried out.

Separation Control

The goal of separation control is to ensure that data collected for different purposes is processed separately.

The following measures are implemented:

- To the extent that there are no dedicated systems in use for exactly one customer, the employed systems are multi-tenant capable;
- Development and quality assurance systems are completely separate from production systems in order to protect production operations and production data - the only exchange that takes place is in the form of files that are needed for processing data (program files, parameter files, etc.);
- Customer systems are only accessed by authorized persons from a secured administration network. Direct administrative transitions between client servers are likewise excluded, as is the ability to reach another client from one client network computer.

Pseudonymization and Encryption (Art. 32 Section 1 lit. a GDPR)

Pseudonymization

The objective of pseudonymization is to allow the processing of personal data to be carried out in such a way that the data can no longer be attributed to a specific data subject without additional information, provided that this additional information is kept separately and falls under the corresponding technical and organizational measures.

Pseudonymization can take place in different ways and must be coordinated between the controller and processor. As a rule, a central system is provided that processes personal data and converts it into codes according to the customer's requirements. Further details on the technical implementation of the pseudonymization are to be specified and assigned in individual cases.

The following common pseudonymization methods are i.e. used in practice by Atos:

- Anonymized identifiers, which can only be resolved using a separate database;
- Use of server identifiers, which conceal conclusions on the function;
- System hardening requirements include a strict prohibition on login banners with information about the type and version of the software used on the systems operated by Atos.

Encryption Measures

The aim of encryption of personal data is to protect data from unauthorized access or alteration.

The controller is responsible for the classification of the information. Based on this classification, the volume or sensitivity of data, a specific risk analysis, or the security policy of the Controller, personal data may be encrypted in compliance with instructions from the controller. The following common encryption technologies, among others, are used in practice by Atos:

- Point-to-point or End-to-end SSL-encrypted data transfer between systems;
- Application-driven encryption of the data before transfer to databases;
- Encryption of DB backups (dependent on contract);
- Volume based encryption;
- Database encryption, e.g. Oracle Crypto plug-in (available as an Add-on) or SQL encryption;
- Encryption of local data on client devices, such as desktops, laptops, mobile phones and tablets.

Integrity (Art. 32 Section 1 lit. b GDPR)

Transmission Control

The goal of transmission control is to ensure that personal data cannot be read, copied, modified, altered or removed while being transmitted, transported or saved to a data storage medium. In addition, transmission control makes it is possible to verify and establish to which bodies personal data may be transmitted using data transmission equipment.

Data can be transmitted from the customer to Atos and from Atos to subcontractors in a number of ways and the chosen means must be agreed between the parties prior to the transmission. Atos supports standard secure transmission types such as network-based encryption (server to server or server to client and/or to suppliers) and encrypted connection tunneling.

Additional measures are:

- Policy for mobile devices;
- Disposal of data storage devices in a manner compatible with data protection regulations -the media shall be physically destroyed in compliance with the European Security Standard DIN EN 66399 minimum security class 3;
- Clear desk policy is in place;
- Encryption of data storage media while in transit (including notebook hard drives);
- Encrypted E-mails (using of electronic certificates (Mime)).

Input Control

The goal of input control is to ensure by means of appropriate measures that the circumstances surrounding data input can be subsequently verified and established.

Atos has implemented access regulations and user authorizations that enable the identification of all users and data terminals in the system. The activities of users are traceable through extensive logging functions and are stored via remote logging outside of the monitored system. Modifications are logged on servers or programs.

All monitoring and logging measures are adapted to the state of the art and the criticality of the data to be protected and carried out in the associated economic framework.

Input in database systems is controlled as part of the standard procedures supplied with the database systems, which, depending on the system, may include logging of inputs and amendments or retention of before and after images.

Availability and resilience (Art. 32 Section 1 lit. b and c GDPR)

Availability Control

The goal of availability control is to ensure that personal data is protected from accidental damage or loss.

The following measures are implemented depending on the respective protection requirements of the personal data:

- Personal data and data saved for later processing in compliance with the purpose of the aforementioned processing is stored at a minimum in storage systems that are self-protected against hardware-related data loss - if the need for protection increases, data is stored in secure and redundant systems up to a spatially separate area, in order to ensure a short recovery time and a high overall availability in catastrophic scenarios;
- The implemented storage systems, in combination with appropriate software components, are equipped with a technology that enables defined data from certain points of time to be recovered. This also prevents losses due to incorrect input and any resulting inconsistency;
- The data backups (i.e. online/ offline; on-site/ off-site) will be done on a regular basis according to existing service agreements;
- System power supplies are protected against interruption, for example by Uninterruptible Power Supply (UPS) and / or generator backup.

Resilience / Rapid Recovery

For the so-called catastrophe case an emergency planning / crisis planning in connection with emergency and restart plans for the data centers is available. This measure ensures that personal data can be quickly recovered in the event of a physical or technical incident through an emergency management plan and regular recovery testing (at minimum annually).

The emergency plans are subject to a regular and continuous audit and improvement process.

Testing & evaluating TOMs (Art. 32 Section 1 lit. d, Art. 25 Section 2 GDPR)

[Additional procedures for regularly testing, assessing and evaluating the effectiveness of Technical and Organizational Measures (TOMs) for ensuring the security of the processing (Art. 32 Section 1 lit. d GDPR; Art. 25 Section 2 GDPR)]

Data Protection Management

Data protection at Atos is organized in a global organization with data protection officers and legal experts for the individual Regional Business Units (RBU) and countries.

Each Regional Business Unit has a data protection office with appointed data protection officer and at least one legal data protection expert. The Data Protection Office is part of the data protection and information security organization, which regularly exchanges on its topics.

The Group Data Protection Policy and the BCRs are the basis for data protection at Atos, which describes the principles of data protection as well as the processes concerning the rights of the persons concerned, audits, training and awareness raising and refers to the global information security policy with its further regulations.

The Data Protection Office provides predefined documents in the Atos Integrated Management System (AIMS), such as forms, checklists, manuals, and work instructions used in HR and business processes. All employees are committed to data secrecy and the observance of company and business secrets and are dependent on GDPR, Articles 29 and 32 (4) to process personal data only on the instructions of the data controller. In addition, they are obliged to comply with applicable data protection and commercial laws and, if appropriate, to safeguard social secrecy and / or bank secrecy.

In annual mandatory training sessions, Atos employees must update their privacy awareness.

The technical and organizational measures for data protection pursuant to GDPR, Article 32, are regularly reviewed within the scope of the Atos ISO certification and, where applicable, other security accreditations and audits. In addition, internal process audits also take account of data protection-relevant issues.

Risk and Security Management

Atos conducts its services on the basis of an information security management system. This includes, among other things, documented guidelines and guidelines for IT / Data Center operation. They are based on statutory as well as internally established regulations. The security processes used are regularly checked. The guidelines are also binding for our subcontractors. Atos employees are required to complete obligatory training sessions on security awareness every year.

Atos has implemented a risk management process across all company levels and has appointed dedicated risk managers at various levels of the organization to ensure the implementation of risk management.

The risk management processes are divided into operational risk management, which is relevant for proposals, contracts (from the transfer of the service to Atos or the start of the project to the completion of the project or the end of the service) and the operational area, i.e. the relevant locations, services and processes.

Risks, their assessment and the follow-up of the defined measures are documented in risk registers and regularly reviewed and updated by the responsible persons, with the involvement of the responsible risk manager and relevant experts. Controls are defined and documented for all inherent risks in the business. For each of these controls responsible persons are defined to regularly monitor the effectiveness.

Certification

Atos is certificated according to:

- DIN EN ISO 9001: 2015 (Quality Management);
- ISO / IEC 27001: 2013 (Information Security Management);
- ISO / IEC 20000-1: 2011 (IT Service Management);
- ISO / IEC 14001:2015 (Environmental Management);

by Ernst & Young CertifyPoint B.V.

Incident Response Management

Security events are addressed by Atos to standard operating procedures and tool-based processes, which are based on "ITIL Best Practice", in order to restore fault-free operation as soon as possible. Security incidents are monitored and analyzed promptly by the Atos Security Management organization in accordance with our customers and/or vendors. Depending on the nature of the event, the appropriate and necessary service teams and specialists will participate in the process, including the Atos "Computer Security Incident Response Team" (CSIRT).

Privacy by Design and Privacy by Default (Art. 25 Section 2 GDPR)

Data protection at Atos is taken into account at the earliest possible date by data protection-friendly presets ("Privacy by Design and by Default") in order to prevent unlawful processing or the misuse of data. Appropriate technical presetting is intended to ensure that only the personal data that is actually required for the specific purpose (need to know principle) is collected and processed.

Defaults for Privacy by Design and Privacy by Default are defined in the Atos Secure Coding Guideline and the Atos Secure Coding Policy.

In order to achieve a low-risk processing of personal data, inter alia the following protective measures are in place:

- Minimize the amount of personal data;
- Pseudonymize or encrypt data as early as possible;
- Create transparency with regard to procedures and processing of data;
- Delete or anonymize data as early as possible;
- Minimize access to data;
- Preset existing configuration options to the most privacy-friendly values;
- Document the assessment of the risks to the persons concerned.

Order Control

The goal of order control is to ensure that personal data which is processed on behalf of the customer is processed only in accordance with the customer's instructions (Art. 28 GDPR).

Activity of any kind is based on a customer order. At a minimum, there is an existing contract in effect.

A procedure described in accordance with ITIL "Best Practice" is used for change requests. Accordingly, only a previously authorized customer representative is authorized to release a change request.

Change Requests relating to the processing of personal data are also accepted exclusively by authorized persons of the customer. This is ensured by the workflow at the order entry interface. The selection of external service providers and suppliers is carried out exclusively according to Atos regulations according to a binding checklist. A review of the service providers takes place before the start of the processing and afterwards regularly.

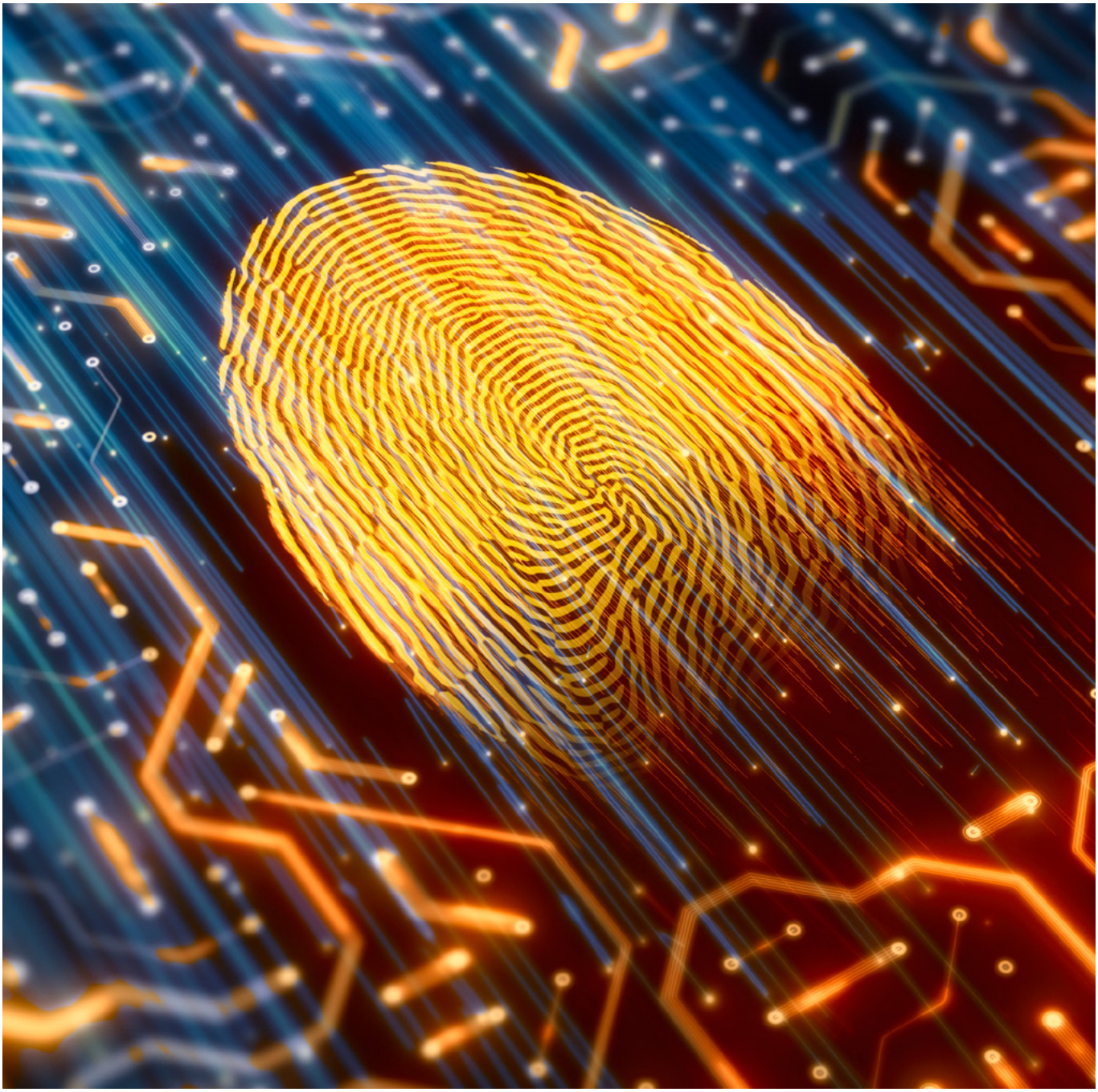
Additional Information Regarding Security Controls

Atos Statement of Applicability re ISO 27001 Annex A Controls

Customers may obtain more information regarding controls implemented within Atos via the Atos ISO Statement of Applicability, which documents the controls from ISO 27001 Annex A that have been implemented and provides internal documentary references for these.

Atos Compliance with Customer Security Policies and Contractual Requirements

Where applicable, Atos will comply with Customer security policies, standards and procedures. Atos will also comply with applicable contractual requirements regarding security.



Contact Data

Each Atos legal entity has their Data Protection Office. You can contact them directly or via the Group Data Protection Office.

Atos SE
Group Data Protection Office
95870 BEZONS
80 Quai Voltaire / PACIFIC NORTH 7
France

dpo-global@atos.net
To exercise your rights as a data subject please visit https://atos.net/en/privacy/exercise-rights-regarding-personal-data

White Paper

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos operates under the brands Atos and Atos|Syntel. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together