Atos global data protection statement

List of changes

Version	Date	Comment	Author
0.1	28.09.2018	Adapted for Global purposes. Basis for this document is the German version.	Josef Beck, Bernd Barban
0.2	01.11.2018	BDSG changed to local reference	Bernd Barban
0.3	21.02.2019	Review by Stephane Larrière and several corrections from reviews with other DPO.	Stephane Larrière, Bernd Barban
0.4	24.06.2020	Review by Group DP Office Global Data Protection Statement Working group	Andrew Jackson, Janine Skinner, Fatima El Oufi, Fritz Beichbuchner, Michael Mingers, Antoinette Schuster
0.5	07.10.2020	Version for review by GDPO working group	Andrew Jackson
1.0	06.11.2020	Final version following review by GDPO working group Quality assurance	Andrew Jackson, Marianna Bojarska
2.0	31.10.2023	Periodic review and update Quality assurance	Fritz Beichbuchner, Prasad Purayil, Andrew Jackson Marianna Bojarska
2.1	19.08.2024	Review & update Data Protection: Added: Global data protection methods relevant for clients	Michael Mingers, Bedirhan Kursun, Sara Bonomi, Peter Landsteiner, Joost van Rooy

Declaration of confidentiality

The information contained in this document and related attachments are Atos's property. In delivering this document, Atos assumes an agreement by the recipient to the confidential handling of the documents, in particular, not to make them available to third parties, copy or use them either in part or in their entirety for any purpose other than to assess the qualifications of Atos, without approval from Atos. To the extent necessary, this also applies to phases following contract termination.

Table of contents

1. Preamble

Atos is a leading worldwide provider of Digital Transformation services and IT solutions. Atos' 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 data protection methods Atos uses to protect the personal data of its stakeholders. It includes the technical and organizational measures 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 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.

2. Data Protection Statement and Methods

2.1 Data Protection Statement

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

2.2 Data Protection Vision and Policy

The right to informational self-determination is a fundamental human right and one of the cornerstones of every liberal basic order – it, therefore, deserves specific protection. As one of the largest IT service providers, we are aware of our responsibility in this context. In many jurisdictions, personal data is consequently subject to explicit laws and regulations, which we, as a company, are committed to complying with. We understand Data Privacy as one of Atos' key assets – we see it as an ongoing endeavor and everybody's responsibility within our company. Atos has installed a privacy organization, introduced data protection policies, guidelines and processes, established continuous employee training and awareness, implemented Binding Corporate Rules and adapted the internal control system to the requirements of data protection. Our aim is to think ahead and make data protection visible and tangible in our everyday business lives. Atos privacy policies are committed to the entire operations, all employees, partners and suppliers.

2.3 Binding Corporate Rules

Binding Corporate Rules (BCRs) are internal, legally binding data protection rules that enable the free flow of personal data within a corporate structure inside and outside of the EU. By streamlining cross border data transfers, they ensure that multinational companies comply with data protection regulations while transferring personal data among their entities.

Only a select number of companies can claim to have BCRs, as obtaining them requires a rigorous approval process by Supervisory Authorities. This stringent process highlights their robustness, meaning that organizations with BCR in place deliver a GDPR-compliant data protection level and thus adhere to the highest standards of data protection.

Atos was the first company to have BCR Frameworks as a controller and processor, approved by the competent supervisory authority. Today, Atos has two sets of valid BCR frameworks, which have been approved by CNIL in 2014 and by the ICO in 2021. While ensuring that our BCR frameworks align with the latest regulatory advice, Atos also have a thorough process to assess the eligibility of their legal entities, onboard them, and continuously monitor their compliance with BCRs.

2.4 Data Protection Organization

Atos has developed an extensive privacy organization with over 150 data protection professionals: data protection officers and data protection legal experts working as one global team, meeting at least every week while managing and monitoring all data protection related activities related to customer contracts, employee processes and supplier relations. This team ensures that all Atos activities remain compliant with all relevant local and global privacy regulations and their development over time. Atos Data Protection organization is closely integrated with its security organization. For Risk Management reasons, all data protection related processes have been considered in the internal control framework and book of internal controls (BIC)

2.5 Handling Security Incidents and Personal Data Breaches

Atos treats all privacy incidents, or any event with the potential to escalate into a personal data breach, as security incidents and ensures they are handled according to applicable contractual and legal provisions and subject to a strict incident response plan. For this purpose, Atos has implemented internal policies and procedures to define the framework for the management of privacy incidents. Structural prevention of recurrence and close cooperation with Atos Security teams are part of the standard process.

2.6 Data Subject Requests

Atos ensure that individuals can easily exercise their rights via a user-friendly online form available on our website. We handle Data Subject Access Requests (DSARs) through a globally standardized process. Atos.net "exercise-your rights-portal (Exercise your rights regarding your Personal Data - Atos)" allows all potential data subjects, including employees, clients, suppliers, and partners, to easily submit requests. Our six-step process involves receiving the DSAR, validating the request, assigning the DPO by our Global DSAR Coordinator, executing the request, informing the data subject, and closing the request.

2.7 Complaints

Atos has established a time framed Complaint Handling Procedure defined in appendix 4 of our BCRs. Atos Entities concerned accept responsibility for investigating such complaints and ensuring that action is taken and remedies provided as appropriate. The use of this complaint's procedure will not affect a Data Subject's right to raise a complaint with the competent Data Protection Authority or bring a claim before a national court (a court in the country in which a processing Atos Entity is based), should they wish to do so.

2.8 Data Protection Awareness and Employee Training

All Atos employees must update their data protection awareness in mandatory annual training sessions. In this way, we ensure a high and always up-to-date level of data protection awareness regarding our data and that of our customers. This is monitored locally and globally.

2.9 Relation to sub-processors

Atos is committed to maintaining high data protection standards both within our organization and with our sub-processors. Where we engage with a sub-processor, we ensure that they comply with the requirements of our privacy program, upholding the service standards set by our clients. This involves conducting thorough due diligence before engaging with potential sub-processors. In this context, we assess the supplier relationship in a separate assessment (CADP-S), describe technical and organizational measures (TOM), and, if needed, carry out additional assessments like transfer impact assessments (TIA). Additionally, we have established processes to enter into comprehensive data protection agreements (DPAs) with all sub-processors, clearly allocating responsibilities and obligations regarding handling personal data and establishing assurance processes that take into account our relationship with our clients.

2.10 International Personal Data Transfers

Atos ensures that all transfers for personal data outside of the UK, EU, or EEA are subject to a valid transfer mechanism compliant with the GDPR.

In the absence of an Adequacy Decision by the European Commission, we utilize adequate safeguards, including Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). When relying on such grounds, we follow and document a Transfer Impact Assessment (TIA) before conducting the transfer. When neither an adequacy decision nor adequate safeguards can be applied, we either refrain from transferring the personal data or rely on derogations as a last resort and ensure detailed documentation of such cases.

2.11 How do we protect customer's data?

Atos had defined an internal framework to ensure personal data protection through a multi-layered cybersecurity approach. This includes advanced encryption protocols, secure access controls, regular security audits, and robust incident response plans. We adhere to international standards, maintaining compliance with ISO certifications such as DIN EN ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, ISO/IEC 14001, demonstrating our commitment to the highest levels of information security and privacy management.

2.12 Law enforcement requests

If we are asked by law enforcement authorities or required by law to carry out certain data processing activities (such as disclosing information to public authorities) in a country outside the EEA that does not offer the same level of data protection, and this involves mass surveillance or monitoring, we will react as follows:
(i) inform the relevant stakeholders as soon as possible, unless legally prohibited, to get their written consent;
(ii) oppose the request, if possible, by explaining that we do not own or control the data; or
(iii) assist the stakeholder, at their expense, if they choose to take action against the request.

2.13 How do we stay up to date? (new laws, privacy developments, market needs...)

At Atos, we prioritize staying current with the latest developments in the privacy sphere. Atos Data Protection Community entails over 150 privacy experts from our offices all over the globe.

To ensure we remain at the forefront of data protection, we hold recurring meetings with a dedicated segment for our experts to share updates on regulatory changes, developments, or court and supervisory authority decisions globally and in their respective regions.

Additionally, we equip members of the Atos Data Protection Community with specialized tools, including tool-based assessments for any kind of processing activity and regulatory research platforms, to leverage their expertise and navigate the evolving realm of data protection more effectively.

2.14 Cookie and tracking technologies

Atos is committed to complying with the EU Directive on privacy in electronic communications. For this purpose, we have developed notices on our websites which intend to give everyone the means to manage the cookies and tracking technologies we use while you're visiting our website.

2.15 Privacy by design

Privacy by design is included in all solutions developed by Atos. Once a client solution is contracted, an extensive questionnaire (Compliance Assessment Data Protection for Processors) must be answered per contract processing personal data. This is a validated risk assessment and needs to be approved by a data protection expert before the processing of personal data may be implemented. The creation/maintenance of these registrations/assessments is monitored regularly. The same approach is used to implement solutions for the Atos internal processes. In this case, a more extensive questionnaire is used (Compliance Assessment Data Protection for Controllers)

2.16 Our commitments in relation to Generative AI

Atos is deploying safe and responsible AI solutions (internal and/or 3 rd party based) for internal use by its employees, collaborators and advisors. That is also the case when we develop and deliver products and/or services to our customers as well as when we offer AI based solutions. A specific policy has been deployed across the entire Atos Group to ensure the responsible use of AI and the protection of the confidentiality and security of our own data and our customers' data through the use of solutions vetted by our legal, security and data protection teams.

We commit to developing and/or deploying AI solutions compliant with the applicable legislation.

We do not use your data to train our AI models, nor do we make them accessible to AI solutions such as ChatGPT.

2.17 Data Protection and Corporate Social Responsibility / Environmental Social Governance

Atos has been pursuing ambitious goals in Environmental Social Governance (ESG) for more than 10 years now and receives regular certification from the most important institutions in this field. Data protection is a fundamental component of ESG and is therefore monitored at Atos not only by the competent data protection supervisory authorities but also by independent auditors as part of ESG audits.

2.18 Independent review

Atos uses a multi layered approach to continuously improve its Privacy Information Management System:

- Continuously: Key objectives and Key Performance Indicators coordinated at the global data protection level; to find weak spots
- Half yearly: internal self assessments worldwide driven by global audit
- Yearly: ISO-27001, 9001, 14000, 20000, both internally driven by global audit and by independent auditing companies checking certificate compliance
- Yearly: independent annual financial audits including explicitly data protection policies, processes and practices
- Ad hoc: Customer organized independent audits focusing on their delivery and including data protection practices

3. Employee Confidentiality Obligation

All employees engaged in providing services have been obliged on a written basis to comply with data confidentiality according to local employment and data protection laws and to the keeping of business and official secrets. Where applicable, newly 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 by Union or Member State law, Art. 29 GDPR.

4. Technical and Organizational Measures

To ensure the confidentiality of data and systems, Atos ensures that 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.

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

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

4.1.1. Physical Access Control

Physical access control ensures that only authorized persons have access to systems that process or use personal data and to the facilities where such processing occurs.

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 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 Atos premises accompanied by Atos staff.

Access to Data Center rooms is additionally secured as follows:

- Automated access control is supplemented by other established methods of access authorization, such as biometrics, Pin-Pads, DES dongles, 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 peoples access and presence are recorded by video

4.1.2. Logical Access Control

The goal of logical access control is to ensure that only authorized persons can access systems that process and use personal data and that such access is based on the 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:

- Two-factor authentication (company ID with PKI encryption)
- Strong passwords (lower- and upper-case letters, special characters, numbers, minimum 10 characters, changed regularly, password history);
- Role-based controls tied to access ID (classified according to administrator, user, etc.);
- Additional controls for admin users;
- Controls on the use of local admin rights;
- Screen lock with password activation in the user's absence;
- Encryption of mobile and local data storage devices (including laptop/notebook drives);
- Use firewalls and antivirus software, including regular security updates and patches.

4.1.3. 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
- Single Sign On (SSO)
- 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

4.1.4. Separation Control

Separation control aims 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 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

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

4.2.1. 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 occur 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 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

4.2.2. Encryption Measures

Encryption of personal data aims 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 Controller's security policy, 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

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

4.3.1. 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 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 several ways and the chosen means must be agreed upon between the parties before the transmission. Atos supports standard secure transmission types such as network-based encryption (server to server or server to client and/or suppliers) and encrypted connection tunneling.

Additional measures are:

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

4.3.2. Input Control

The goal of input control is to ensure using 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. Users' activities are traceable through effective 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.

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.

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

4.4.1. 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 including use of separate physical locations, 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 in time to be recovered (Recovery Point). This also prevents losses due to incorrect input and any resulting inconsistency
- Data backups (i.e. online/ offline; on-site/ off-site) will be done regularly according to existing service agreements
- System power supplies are protected against interruption, for example, by Uninterruptible Power Supply (UPS) and / or generator backup

4.4.2. Resilience / Rapid Recovery

Crisis planning and crisis management exercises test the company's ability to respond to catastrophic events. Business Continuity Plans provide resilience against disruptions to normal working arrangements, such as site disruptions or pandemics. Disaster/emergency planning and recovery testing assure that data can be recovered/ made available in a timely fashion in the event of a physical or technical incident.

Such plans are subject to a continuous audit and improvement process. They all help to protect the integrity and availability of data and systems.

4.5. 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)]

4.5.1. Data Protection Management

Atos has a global data protection organization that supports regional / cluster data protection officers (DPOs) and DPOs and legal experts for individual countries.

Each cluster has a data protection office with appointed data protection officer and at least one legal data protection expert. The Data Protection Office collaborates with data protection and information security organizations, which regularly exchange on common topics.

The Group Data Protection Policy and the BCRs are the basis for data protection at Atos. These describe the principles of data protection and the processes and protections concerning the rights of individuals whose data is processed, the persons concerned, audits, training and awareness raising. They also refer to the group information security policy with further provisions and controls to protect data.

The Data Protection Office provides predefined documents in the Atos Integrated Management System (AIMS), such as forms, checklists, manuals, and work instructions in HR and business processes. All employees are committed to respecting data confidentiality andprotecting company and business secrets, and, in line with GDPR, Articles 29 and 32 (4), must process personal data only on the instructions of the Controller. In addition, they are obliged to comply with applicable data protection laws and, if appropriate, safeguard social 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 27001 certification and, where applicable, other security accreditations and audits. In addition, internal process audits also take account of data protection-relevant issues.

4.5.2. Risk and Security Management

Atos conducts its services based on an information security management system. This includes, among other things, documented guidelines and guidelines for IT / Data Center operation. They are based on statutory and internally established regulations. The security processes used are regularly checked. The guidelines are also binding for our subcontractors. Atos employees must 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, that 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. Responsible persons are defined for each of these controls to monitor the effectiveness regularly.

4.5.3. Certification

Atos is certificated according to:

- DIN EN ISO 9001: 2015 (Quality Management);
- ISO / IEC 27001: 2022 (Information Security Management);
- ISO / IEC 20000-1: 2018 (IT Service Management);
- ISO / IEC 14001:2015 (Environmental Management);

by an independent certification body

4.5.4. Incident Response Management

Security events are addressed by Atos to standard operating procedures and tool-based processes, which are based on “ITIL Best Practice”, to restore fault-free operation as soon as possible. Security incidents are monitored and analyzed promptly by 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 Atos “Computer Security Incident Response Team” (CSIRT).

4.5.5. 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”) to prevent unlawful processing or the misuse of data. Appropriate technical presetting is intended to ensure that only the personal data that is 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 Group Secure Coding Guideline and the Atos Group Secure Coding Policy.

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 about 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

4.5.6. Order Control

The goal of order control is to ensure that personal data that is processed on behalf of the customer is processed only per 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 per ITIL “Best Practice” is used for change requests. Accordingly, only a previously authorized customer representative can 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.

4.6. Additional Information Regarding Security Controls

4.6.1. The 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.

4.6.2. 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.

5. Contact Data of the Data Protection Officer

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

About Atos

Atos is a global leader in digital transformation with c. 94,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its exper- tise 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 discussion together

105238 - JS + HC