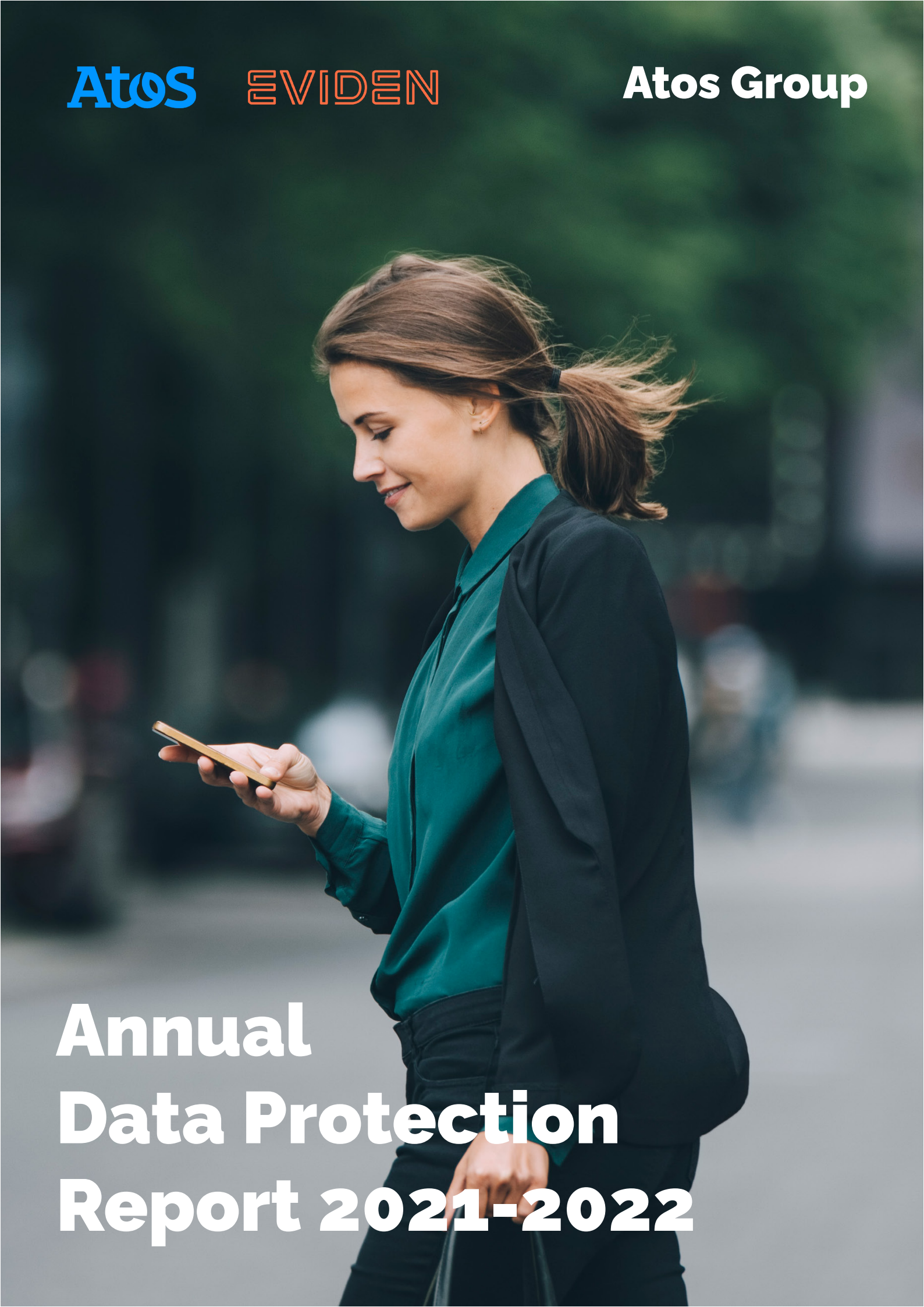
Atos EVIDEN Atos Group



Annual Data Protection Report 2021-2022

1. Introduction

1.1. Scope, objectives, and audience

This document is the Data Protection Report for 2021-22 of the Atos Group, hereinafter referred to as Atos or the company, and was prepared by the Atos Group Data Protection Office. The aim of the report is to provide an overview of the status of data protection in the company. In particular, it describes relevant events or actions and contains results achieved during the reporting period as well as suggestions for future steps.

This report covers the period from January 1, 2021, to December 31, 2022. Please note that achievements and improvements made during this period are tagged with a symbol.

The aim of this report is to inform interested parties, including Atos clients and partners, regarding the approach Atos has taken to data protection compliance across the Atos Group and how this evolved and changed during 2021-22.

2. Organization

2.1. Context

Being a Group with strong European roots, the Atos approach to data protection is founded on the concepts and requirements of European data protection law and practices, in particular the requirements of the EU General Data Protection Regulation (GDPR). Nevertheless, there are many other parts of the world where specific privacy laws have long been established, and the increasing adoption and development of general data protection laws outside the European Economic Area (where GDPR applies) means that Atos, as a global company, has to consider the requirements of multiple jurisdictions in its overall approach to data protection, as well as, plainly, ensuring that it remains compliant with specific local requirements.

Atos addresses this challenge by having defined general Data Protection policies and procedures based on GDPR, while at the same time being open to the possibility of additional controls that will enhance compliance in specific jurisdictions, without compromising compliance elsewhere, thus making it easier to implement national requirements. Should national legislation and Atos data protection policy or practice come into direct conflict this would, of course, have to be addressed. In 2021-22 no such case occurred.

2.2. Governance

The Atos Group Data Protection Office directs and coordinates the work of the larger Atos Data Protection Community and defines the Group policies on Data Protection.

Where organizational units either reflect a legal entity or represent a regional or national perimeter, a team consisting of a Data Protection Officer (DPO) and a Data Protection Legal Expert (DPLE) head the second line regarding Data Protection, giving consultancy and advice to the operational first line and performing specific validations and checks.

Where applicable, DPOs have been nominated to their respective Data Protection Authorities. While DPOs cover mainly tasks as set out in Art. 39 GDPR, DPLEs focus on contractual questions and legal frameworks. Both roles cover a basic understanding of the other one to ensure a smooth collaboration and easy access for colleagues searching for advice and support.

Where organizational units reflect a support function or any other organizational matrix across jurisdictions, a Data Protection Coordinator or Data Protection Expert supports his/her respective unit regarding Data Protection, giving consultancy and advice and supporting specific validations and checks. For specific legal questions; legal experts assigned to the respective function provide their support. Specialist legal advice is also provided by Legal Experts in the Group Data Protection Office.

2.3. Group Data Protection Office

The Atos Group Data Protection Office (GDPO) is embedded in the Atos Group Legal, Compliance and Contract Management Department. While enjoying the benefit of proximity to this strong community of lawyers and compliance experts in more than 70 countries, the Atos Data Protection Office also maintains a close relationship with the Atos Security organization. Regular synchronization points on different levels between Data Protection experts and Security experts ensure a complementary dovetailing of Security and Data Protection. Close collaboration with the Atos Compliance department as well as with HR, Quality, Corporate Social Responsibility, Risk Management and Group Internal Audit also enhances cooperation regarding Data Protection across the company.

- In 2021-22, the Atos Group Data Protection Office had 1 Group Chief Data Governance Officer, 1 Data Protection Officer, and 1-2 Data Protection Legal Experts. Where necessary the Group Data Protection Office has been supported by Legal Experts from other departments within Atos Legal, Compliance and Contract Management.

2.4. Group Chief Data Governance Officer

The Group Chief Data Governance Officer (CDGO) reports to the Group General Counsel. This role directs the work of the GDPO and coordinates the activities of the wider data protection community in supporting data protection across the company. This includes , defining Atos DP strategy, monitoring the implementation of data protection policies and processes, defining Atos DP strategy and organization, and coordinating communication and training.

2.5. Data Protection Officer

Data Protection Officers (DPO) are practitioners who report within their respective legal entity and organizational context. The responsibilities of the DPO reflects this context on different organizational levels:

- Regional Business Unit (RBU) - monitoring and condensing data protection at a regional level, supporting data protection topics in their perimeter, monitoring the implementation of the Atos data protection organization and supporting local DPOs. Working independently as well as in collaboration with their counterparts, these are experienced practitioners who drive local initiatives as well as taking an active role in defining Atos DP strategy, organization, communications and training. In addition, many of the Group-wide initiatives are led by one or more of the RBU DPOs.
- Global Delivery Center (GDC) or country cluster - managing and supporting data protection activities in their perimeter, supporting data protection topics in their perimeter, supporting and implementing data protection organization, guiding local DPOs, managing the GDC/ country-cluster Data Protection Office and supporting implementation of the DP strategy, as well as communication and training.
- Local - performing the tasks of a DPO within a specific jurisdiction, which may include advising and supporting on data protection topics in their perimeter; supporting and implementing data protection organization and strategy, acting (where required) as a point of contact for a DPA, responding to data subject requests and complaints and providing local awareness communications and training.

Where required DPOs have been nominated to the relevant Supervisory Authority / Data Protection Authority (DPA).

2.6. Data Protection Legal Expert

Data Protection Legal Experts report within the Legal, Compliance & Contract Management organization of their subunit. The responsibilities of the DPLE reflects this context on different organizational levels:

- Regional Business Unit (RBU) or country cluster or Global Delivery Center (GDC) - supporting the legal perspective of data protection topics in their perimeter, supporting and implementing the data protection organization, supporting contracts and negotiations regarding data protection in their perimeter, supporting RBU/country cluster/GDC Data Protection Office, supporting implementation of data protection strategy as well as communication and training.
- Local - supporting legal aspects of data protection topics in their perimeter, supporting and implementing data protection organization, supporting contracts and negotiations regarding data protection, supporting local Data Protection Office, supporting implementation of data protection-specific agreements such as intra group agreements, supporting implementation of data protection strategy as well as communication and

2.7. Data Protection Coordinator

Data Protection Coordinators (DPC) provide a point of contact where a need has been identified in a particular organizational context. Their responsibilities encompass acting as the DP expert within their Support Function, Practice or Operation and acting as the DP point of contact in their perimeter, as well as supporting data protection topics, assisting with implementation of the data protection organization, supporting implementation of the DP strategy, and facilitating communication and training.

DPCs have been nominated for the major organizational units, especially for Human Resources, IT, Finance, Procurement and Sales & Marketing.

As the Atos organization evolves, the location and responsibilities of DPCs will evolve in response.

2.8. Data Protection Community

The Atos Data Protection Community consist of:

- Group Data Protection Office
- all DPOs
- all DPLEs
- all DPCs

The Atos Data Protection Community collectively drives projects and synchronizes on all activities related to data protection as far as they are not limited to domestic regulations or specifics related to legal or organizational units. To ensure systematic and coordinated synchronization, the Atos Data Protection Community meets (virtually) once per week in the Global Data Protection Community Hub. To cover all relevant time zones, the Global Data Protection Community Hub is complemented by a Community Hub specific to India and Asia-Pacific. A representative of India and Asia-Pacific as well as the Group Chief Data Governance Officer attend both Community Hubs.

Regular topics addressed during these Community Hubs are:

- Internal data protection news
- Updates and changes in data protection legislation
- New rulings and decisions by Supervisory Authorities
- Info regarding security incidents
- Reports from task forces responsible for tooling
- Updates and deliverables from working groups & projects
- Proposals for new initiatives / working groups
- Data subjects' rights
- Assessments of proposals for new processing
- Data Protection Impact Assessments
- Data Protection Incidents
- Regular presentations (e.g. new guidelines, specific internal programs, etc.)
- Urgencies

Community Hubs foster a collaborative approach to data protection compliance. They are regularly recorded and documented via meeting minutes available to all Data Protection Community members.

- The Atos Data Protection Community numbered 140+ employees for the duration of the period 2021-2022.

2.9. Policies

At a Group level, a set of policies defines the framework for data protection within Atos. The key policies are:

- Atos Group Data Protection Policy
- Binding Corporate Rules (Atos Group and Atos UK)
- Atos Group Personal Data Breach Policy and Data Breach Assessment
- Atos Group Policy for Access to IT (Network) User Data

2.9.1. Group Data Protection Policy

Atos has adopted a Group Data Protection Policy which 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 Group DP Policy raises awareness within the Group and participates to the demonstration of Atos's compliance with its legal obligations.

As per applicable law, every Atos entity and Atos Employee and manager is required to apply the Data protection principles set out in the Group Data Protection Policy. It 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 employees of the Atos Group, and which have been validated by the European Data Protection Authorities.

The 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 and jurisdiction.

The Group DP Policy covers any and 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, the Group DP Policy notably covers Processing of Human Resources ('HR'), 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.

The Group Data Protection Policy covers:

- Principles for processing of personal data (as a Controller and as a Processor)
- Legal Grounds for processing of Personal Data (as a Controller and as a Processor)
- Processing of Sensitive Personal Data
- Security Measures (when acting as Controller and as a Processor)
- Impact Assessments / Compliance Assessments of Data Processing
- Records of Processing Activities
- Selection of Subcontractors
- International Transfers of Personal Data
- Data Subjects' rights
- Complaint Handling Procedure (direct, indirect and complaint of a Controller)
- Cooperation with Controllers and Data Protection Authorities
- Privacy by design & by default
- Register and National Formalities with Competent Data Protection Authorities
- Personal Data Breach notification
- Training and raising awarenes

- Audit (internal, subcontractor, customer)
- Data Protection Community

◆ **The Group Data Protection Policy was updated in May 2021 (current version as of publication of this report is from May 2023).**

2.9.2. Atos Group Binding Corporate Rules

To guarantee an adequate level of Data Protection within all Atos affiliates and especially for the transfer of EU Personal Data outside of the EU, Atos has adopted Binding Corporate Rules (BCR) which have been validated by the European Data Protection Authorities. These BCR follow the same objectives and principles as those defined in the Group Data Protection Policy.

The Atos Binding Corporate Rules cover:

- Principles for processing Personal Data
- Legal grounds for processing Personal Data
- Processing of Sensitive Personal Data
- Security Measures
- Automated individual decisions
- Accountability
- Transfer of Personal Data
- Data Subject's rights
- Complaint Handling Procedure (direct, indirect and complaint of a Controller)
- Liability vis-à-vis Data Subjects
- Liability vis-à-vis Controller
- Data Subject's information
- Cooperation with Controllers and Data Protection Authorities
- Personal Data Breach reporting
- Privacy by design & by default
- National notification to Competent Data Protection Authorities
- Training and raising awareness
- Audit (internal, subcontractor, customer)
- Data Protection Community
- Legally Binding Requests for Disclosure of Data [by a law enforcement authority]

◆ **The Atos Group Binding Corporate Rules were updated in April 2022. They are amended from time to time and where necessary. In particular, they are updated when applicable data protection regulation has been updated and in response to changes in regulatory guidance. Such amendments are communicated to Atos Group's lead Supervisory Authority (the CNIL) in line with its requirements and the approved process for making updates.**

◆ **The Atos BCR are published via the privacy page of the Atos website: https://atos.net/en/privacy.**

2.9.3. Atos UK Binding Corporate Rules as a Controller and as a Processor

Following the UK's exit from the EU and the EEA, the UK no longer formally recognized EU Binding Corporate Rules (BCR) as providing adequate protection for transfers of UK data to third countries. Atos therefore submitted UK-specific BCR to the Information Commissioner's Office (ICO) – in the form of separate UK BCR as a Controller and UK BCR as a Processor.

- The current versions were created in December 2020 and first submitted in draft form in February 2021. Formal approval was given by the Information Commissioner in November 2021.
- Atos has continued to apply its UK Binding Corporate Rules as a Controller and as a Processor in the subsequent period and these are published alongside the Group BCR via the privacy page of the Atos website: https://atos.net/en/privacy.

2.9.4. Personal Data Breach Policy

In its Personal Data Breach Policy Atos defines the principles of addressing Personal Data Breaches. It is intended to instruct Atos employees, and more especially the Atos team involved in security incident management, regarding the notion of Personal Data Breach and how to manage such an incident, especially regarding obligations to notify competent authorities and data subjects.

The Personal Data Breach Policy covers all internal and external systems and processes, whether Atos processes personal data as Controller or as Processor. It provides a baseline in terms of Data Protection and Security requirements, leaving room for more specific requirements to be added case-by-case.

As Personal Data Breaches are first and foremost security incidents the Atos security organization regarding security events and security incidents applies to any Personal Data Breach. This includes organizational units and immediate actions, severity-based response mechanisms, and comprehensive documentation. Any Personal Data Breach would therefore be reported as a security incident using the standard security incident management process, but with a requirement to engage the relevant data protection office.

The Personal Data Breach Policy covers:

- Identifying Personal Data Breaches
- Reacting to the Personal Data Breach
- Containing the Personal Data
- Assessing the Personal Data Breach
- Recording all information relevant to the Personal Data Breach
- Notification requirements (when acting as Controller and when acting as Processor)
- Communications Actions

For any Data Breach, it is a requirement that a Data Breach Assessment be completed, based on the information available. The assessment form is designed to help data protection specialists to determine the potential severity of a Personal Data Breach and to assess the resultant risks. This assessment is based on a standard questionnaire which results in a risk scoring and an overall risk level based on a red-amber-green scheme. This scoring is used as an indicator, but not as an automated decision, for actions related to the respective Personal Data Breach.

- **The Personal Data Breach Policy was updated in May 2020 and again in July 2022.**

2.9.5. Policy for Access to Atos IT (Network) User Data

The Policy for access to Atos IT (network) user data summarizes, in accordance with the Group Data Protection Policy, the basic rules and mode of conduct for Atos in case of the occurrence of an event which requires, on an exceptional basis, the monitoring, surveillance or review of the activities of any member of Atos staff using the Atos IT Network and/or using Atos provided IT equipment. Its purpose is to define the conditions under which the competent teams involved in the management or resolution of the event or issue are authorized to access, review and otherwise process the data of any Atos employee in order to respond to the specific request issued by a competent requester in specific cases. Such authorization will only be granted if no other means are available to effectively implement the necessary measures and protect the rights, interests and assets of Atos, Atos's customers or Atos's partners.

The Policy for access to Atos IT (network) user data covers:

- Principles
- Circumstances warranting access to User Data
- Process in case of Security Event or Incident
- Request from the Legal, Compliance and Contract Management department
- Request from the competent HR Organization
- Request from a client on the basis of contractual provisions
- Request from the Data Protection Officer
- Management of access requests (persons entitled, format, necessary approvals, information, additional steps)

◆ **The Policy for access to Atos IT (network) user data was updated in June 2022.**

2.10. Compliance Assessment of Data Processing

Like all organizations, Atos processes Personal Data for its own purposes, in other words in the role of Controller. In addition, as a provider of digital services, it processes personal data as acting as a Processor for its many clients.

Atos has developed its own assessments for both types of processing, which act as both records of processing activities as well allowing for the assessment of various aspects of data protection compliance, helping to manage privacy risks and promoting privacy by design.

In addition, applicable data protection laws and especially GDPR also require Controllers to perform a Data Protection Impact Assessment (DPIA) for any new processing activity where the proposed processing, taking into account its nature, scope, context and purposes, is likely to result in a high risk to the rights and freedoms of natural persons - in particular where it will be using new technologies. Such assessments must be performed prior to the processing and should cover the impact of the envisaged processing operations on the protection of personal data.

Atos will also provide assistance when requested to clients who are performing their own DPIA for any proposed processing.

By implementing mandatory assessments for all processing activities and linking such assessments also to sales processes Atos has reinforced awareness of data privacy among its workforces.

2.11. Atos acting as Controller

Before starting a new processing activity where Atos will be acting as a Controller, Atos employees are obliged to perform a Compliance Assessment of Data Processing as Controller (CADP-C).

Such CADP-C will document and reflect:

- Internal requestor / processing owner
- Processing purpose and description
- Type of processing activity and used application
- Lawfulness of processing
- Non-sensitive data elements to be processed
- Sensitive data elements to be processed
- Categories of Data Subjects
- Location of Data Subjects
- Main categories of processing activities
- Origin/source of personal data
- Retention periods and deletion mechanisms
- Risk factors (automated decision taking, use of new technologies, matching datasets, etc.)
- Implementation of Data Subjects' rights
- Suppliers acting as Processors (including mechanism for international data transfers and sub-processors)
- Data Transfers
- Technical and organizational measures
- Indicators suggesting a DPIA to be required

Each CADP-C is owned by a Business Owner and maintained by one or several Respondents acting on behalf of the Business Owner. Business Owners can also nominate additional Delegate Owners. CADP-C are reviewed and validated by one or more members of the Atos Data Protection Community, usually Data Protection Officers or Data Protection Legal Experts. Global processing activities are reviewed at a global level. These global assessments may be used as is by local Atos entities, or they may be cascaded to a local perimeter e.g. to cover local specifics and/or national legal requirements.

- **Since July 2020, all CADP-C have been created and maintained in "MyCADP", a specialized data base solution using the OneTrust Data Protection Management Solution. Records created using the predecessor to this system, which was a bespoke Excel template, have been migrated to the new platform.**

- **In 2021, the CADP-C template received a major update. In addition, a permanent task force made up of members of the DP community collects requests for change and drives continuous improvement in at least yearly releases.**

The records in MyCADP form the Atos register of processing activities as defined in Art. 30 (1) GDPR.

2.12. Atos acting as Processor

Before starting a new processing activity acting as Processor, Atos employees are required to perform a Compliance Assessment of Data Processing as Processor (CADP-P). The assessment is part of the Atos risk management process.

Such CADP-P will document and reflect

- Project owner / leading Atos entity
- Controller (customer)
- Processing purpose and description
- Location of Data Subjects
- Categories of non-sensitive personal data to be processed
- Categories of sensitive personal data to be processed
- Categories of Data Subjects
- Main categories of processing activities
- Origin/source of personal data
- Retention periods and deletion mechanisms
- Risk factors (automated decision taking, use of new technologies, matching datasets, etc.)
- Suppliers acting as Processors (including mechanism for international data transfers and sub-sub-processors)
- Data Transfers
- Technical and organizational measures

Each CADP-P is owned by the Client Account Owner who responsible for maintaining the assessment. CADP-Ps are reviewed and validated by Data Protection Officers.

CADP-Ps were previously created and maintained based on Microsoft Excel templates, covering the above-mentioned sections with detailed questions. As far as possible, answers were standardized, and the form was streamlined and made more user-friendly completed forms were stored in the central Account management space. However, it was recognized that moving to a managed platform would improve efficiency, accountability and compliance. Consequently, a working group was set up in the second part of 2021 to improve the CADP-P process and a project initiated to implement the CADP-P form on the OneTrust platform.

The result was a significantly improved process for managing the creation of processing records and the implementation of a platform similar to the existing one for Controller records, but with user administration handled differently due to the large volume of users that only required occasional access, referred to as MyClientCADP.

- **The improved CADP-P process was implemented in H1 2022.**
- **On 1 June 2022 MyClientCADP went live and has been used for all subsequent CADP-P records.**

CADP-P records form the Atos register of processing activities as defined in Art. 30 (2) GDPR.

2.13. Training & awareness

Atos recognizes that raising awareness of data protection across the entire organization is key to maximizing compliance and minimizing the risk of data breaches. It is apparent from reports of high-profile data breaches that one of the main sources of data breaches is human error. The likelihood of such errors can be significantly reduced b In this context, all Atos employees must complete the global mandatory e-Learning training on Data Protection including GDPR rules. In this training, Atos's employees learn about Atos's approach to Data Protection, the tools available to support compliance, their own obligation to protect data and the rights of Data Subjects.

In addition to the mandatory e-Learning training the Atos Group Data Protection Office in collaboration with the Data Protection Community members have created and performed further trainings and webinars during the year:

- **From 25 to 29 of January 2021, we celebrated the International Data Protection Day (January 28) with a week of activities. The theme taken was "The Great Acceleration" – which looked at the explosion in the exploitation of personal data. As well as drawing conclusions for how individuals might strive to protect their own privacy, it also drew conclusions regarding how Atos staff could help fulfill the company's raison d'être of helping to design the future of the information space by helping to "weave a safety net" to protect privacy.**

- **For Atos Quality Day in November 2021, two specific webinars were held on the subject of the evolution of privacy.**

- **January 2022, Data Protection Day event (in 5 different languages English, German, Spanish-Mexico, Spanish-Spain and French). On January 28, The Interview - David Restrepo Amariles (HEC Professor (ref. 4.9.3 to read more about Atos and HEC cooperation).**

- **The Data Protection learning month event started in May 2022 with «Data protection Processing Principles»: in May to act in a «lawful, fair and transparent» manner; in June, to understand more about «minimization» as a second principle; in July, the third topic was «Purpose limitation» which may be a less obvious topic to understand; in October, inserted in the Atos Cyber-Security month event for «Security & confidentiality» principle; in November, the «Storage limitation» principle; in December, the «Accuracy» principle.**

Members of the data protection community also provide local training and awareness to suit their needs.

3. External developments and their impact on Atos

3.1. GDPR enforcement

2021 again saw a significant increase in the number of fines being issued under GDPR by the various Supervisory Authorities, rising from around 340 to more than 500. The rise in numbers continued in 2022, with penalties issues in nearly 600 cases. Inevitably the greatest attention was drawn to the very substantial fines issued against key US providers, but looking beyond the headline cases it is clear that the focus of enforcement remains similar, with particular focuses being on (1) processing of data beyond what is legally justified (often in connection with marketing); (2) data breaches and the security shortcomings that are often revealed by these; (3) inadequate protection of data that is transferred outside the EEA; (4) failure to comply with subject rights.

By the middle of 2021, GDPR had been in force for three years and the vast majority of cases considered for regulatory action related to the GDPR period, rather than earlier. It is also clear that a more consistent and severe approach to enforcement was being taken – certainly with regard to the private sector.

In line with the above, Atos continued to focus its data protection compliance efforts on matters such as the legal bases that our processing operations are founded on, the implementation of sufficient technical and organizational measures (and the response to any breach should these prove insufficient), and the means for providing protection for international data transfers.

3.2. Processing Personal Data in pandemic context

On 30 January 2020, the World Health Organization (WHO) declared the coronavirus disease 2019 (COVID-19) outbreak a public-health emergency of international concern (PHEIC). Six weeks later, the outbreak was categorized as a pandemic. The COVID-19 pandemic impacted almost every aspect of our economy, society and mental health, and remained a constant factor through 2021 and much of 2022.

Like all organizations, Atos had to adapt it working practices to accommodate public health measures, restrictions on travel and the use of office space, as well as all the measures taken to support its employees in this difficult time and to maintain the delivery of services to its customers. It was also evident that Atos played a crucial role in enabling its customers to adapt their own services and working practices in response to the pandemic.

The way we conceive our privacy and the importance which we attach to the protection of our personal data has been heavily impacted by this first pandemic of the digital age. Personal Data of many kinds can be processed to prevent the virus from spreading, going from health data to localization data and facial recognition. However, concerns can all arise concerning the balance between the right to privacy, which is a fundamental right, and the duty at every level of society, from national governments to local businesses, to protect the health of those who depend on them.

The Atos DPO Community issued global guidance to help employees manage this delicate balance, and worked with colleagues to assess proposed measures that involved novel processing of data or potential privacy impacts.

It is to be hoped that, as 2022 saw the worst effects of the pandemic recede for many in the world, there will be lessons drawn about how best to protect people from harm while preserving their rights and freedoms.

3.3. Schrems II Ruling, EC Standard Contractual Clauses and TIAs

The "Schrems II" ruling on 16 July 2020, which invalidated the use of the US/EU Privacy shield as a means of providing adequacy of protection for transfers of personal data between the EU and the United States, inevitably meant that there would be an increase in the use of the European Commission (EC) Standard Contractual Clauses (SCC) as a means of providing protection for EU data that was transferred to Third Countries. Given that the judgement also had implications for the validity of the SCC themselves, in particular in addressing the risks that might be posed by specific transfers, as well the general view that the SCC (which predated GDPR) were anyway in need of modernization, the EC consulted on a new version. The new version was published on 4 June 2021.

The implementation timetable for the new SCC provided a short grace period in which contracts could be concluded using an old version of the SCC, but from 27 September 2021 only the new version of the SCC would be acceptable in any new or substantially revised agreement. Furthermore, existing contracts could only rely on previous versions of the SCC until 27 December 2022. Given the widespread use of SCC to protect transfers of data, it was essential for Atos, like all organizations operating in the EU, to identify any of their contractual agreements which included the SCC and to incorporate the new version where required.

Although the new version of the SCC is more flexible and comprehensive in the types of transfers it can be used to protect, it also comes with the additional requirement to conduct and document a Transfer Risk Assessment (TIA) for the proposed transfer. This requirement is a direct consequence of the Schrems II judgement.

The Atos Group Data Protection Office therefore set out to provide a templated means for assessing the laws and practices in third countries and for assessing any proposed processing that required SCC due to the proposed transfer of EEA personal data to such a country. Along with guided versions of the SCC variations, this enabled colleagues to address those contracts that required updates as well as providing the tools needed for new ones.

On 25 March 2022 the US President and the President of the EC jointly announced an agreement in principle on a new framework for transatlantic data flows. This was followed up by an Executive Order on 7 October 2022 which provided for enhanced US safeguards which were intended to address the concerns that had led to the Schrems II judgement. It therefore seemed likely that a new framework would indeed be put in place, although with the near certainty that there would be a legal challenge to its validity.

In its Q&A regarding the proposed new framework and the Executive Order that prepared the ground for it, the EC addressed the question of why the new arrangement, when in place, might survive legal challenge:

In 2022, The objective of the Commission has been to address the concerns raised by the Court of Justice of the EU in the Schrems II judgment and provide a durable and reliable legal basis for transatlantic data flows. This is reflected in the safeguards included in the Executive Order, regarding both the substantive limitation on US national security authorities' access to data (necessity and proportionality) and the establishment of the new redress mechanism.

Like many companies, Atos awaited to see how this re-imagining of the EU-US Privacy Shield arrangements would be received.

3.4. Brexit

Following the UK exit from the EU, there was some relief that serious disruption to the free flow of data between the EEA and the UK was avoided due to the "adequacy decision" of the European Commission, which was published on 28 June 2021. Given the complementary adequacy decision already adopted by the UK, this meant that there could be an element of business as usual for many organizations which relied on such data flows.

However, the need to directly comply with UK rather than EU law, meant that protections for data transfers from the UK to countries that were without a UK adequacy decision had to be reevaluated and updated. In particular, the implication for Atos was that it needed to supplement the protections provided by its existing Binding Corporate Rules (BCR). This resulted in the development of the Atos UK BCR as a Controller and Atos UK BCR as a Processor, which were both formally approved by the UK Authority, the ICO, on 30 November 2021.

3.5. Data Protection Legislation

The appearance of new legislation concerning privacy and data protection continued to be a regular occurrence in the period covered. There was often an element of data localization involved and, following the established European model, the new dispositions often included powers to issue large fines to organizations that transgressed.

There are many examples of this from around the world, but notable among these were the coming into effect of the LGPD in Brazil in August 2021, a law with significant similarities to GDPR, and the swift implementation of the PIPL in China in the second half of 2021, along with other measures to regulate digital security. There was also a great proliferation of privacy legislation the United States, where California was followed by Colorado, Connecticut, Utah and Virginia in enacting comprehensive data privacy laws.

In each case Atos has benefited greatly from the support of its network of data protection specialists located in different countries in assessing and adapting its practices and agreements to comply with these new requirements.

4. Projects and internal developments

4.1. Data Protection Community

Strengthening the Atos Data Protection Community and further expanding collaboration within the Atos Data Protection organization remained key objectives in 2021 and 2022. There were also significant initiatives to simplify processes, provide better tools and improve communication, so that colleagues who are non-specialists found it easier to navigate the requirements of data protection and thus improve compliance.

To reach this a set of measures has been prepared and implemented throughout the full year.

Working groups

The Atos Data Protection Community is notable for the willingness of many of its members to take an active role in developing all aspects of data protection in Atos, from policy and processes to the implementation of new tools, training courses and communications materials. It is worth noting that members of the DP community have also supported initiatives led by other parts of the company, such as Compliance, Procurement, Security, Group Legal, and Sales and Marketing.
The following gives a summary of the formal data protection working groups that have been active in the period covered by this report:

- Atos Data Protection cookbook (completed in 2020, with a further review commenced in 2022)
  Objective: review and update Atos Data Protection cookbook, an internal guideline for all Data Protection professionals
- Simplification exercise with Procurement (completed in 2020, reviewed in 2021 and 2022)
  Objective: review and update existing Data Protection Addendum templates, also review and update common process with Procurement to cover Data Protection requirements when involving external suppliers as (sub-)processors
- New DP Portal SharePoint (completed and moved to permanent task force)
  Objective: move existing content of the internal Atos Data Protection SharePoint to SharePoint online, at the same time re-design and re-work the existing content to be more user-friendly and use-case-centric
- Atos's global data protection principles for consent to marketing communications
  Objective: review and enhance global standards for consent to marketing communications, global catalogue has been provided, optional further steps have been suspended
- DP related Data Sovereignty (completed in 2022)
  Objective: reflect on data sovereignty principles and their implementation via legal texts, making these more accessible for the Data Protection Community, at the same time link these principles to Atos solutions and services. A document delivered in 2021 highlights the extraterritoriality of some specific laws
- DP related incident management process (completed in 2021)
  Objective: enhance the existing Personal Data Breach Policy by a process description which supports employees in case of a Personal Data Breach
- DPMS for Atos (completed in 2022)
  Objective: assess ISO 27701 compliance of the Atos DPMS – its structure, existing policies, guidelines, and organization and provide gap analysis of the existing Atos organization compared to the standard

- eSO working group (reported in 2022, completed in 2023)
  Objective: evaluate if the electronic Service Order tool can be used for internal assignments / internal data processing, if yes: prepare the use of eSO for internal data processing
- Data Protection compliant use of MS Forms and other survey methods (reported in 2021, completed in 2022)
  Objective: to ensure that the correct survey tools were identified, and guideline created to support safe and compliant use.
- Revision of Personal Data Breach Policy BIP-AP21 (completed in 2022)
  Objective: clarify and streamline Personal Data Breach Policy and improve assessment
- WG CADP Review Guidelines (completed in 2021)
  Objective: Produce guidelines for DPOs reviewing Atos records of processing to encourage consistency and thoroughness of reviews.

All working groups have been established either via the Data Protection Community Hub or by request of Group Data Protection Office. Each working group had at least one Data Protection Community member chairing it and several other members
or experts external to the community taking part in the collaboration. They have been reviewed during Data Protection Community Hub, with regular reports made
to that meeting at regular intervals. Results have been shared and agreed with the Data Protection community members. Working materials and results are available via a shared "expert space" that is open to all Hub members.

4.2. The New Standard Contractual Clauses

The European Commission issued a comprehensively revised set of "Standard Contractual Clauses" (SCC) on 4 June 2021, which included a new requirement for Transfer Impact Assessments which took into account the laws and practices of third countries to which personal data was to be transferred.

To address this new requirement, the Atos group data protection team, supported by members of the DP community, took the following approach:

- Conduct a global awareness campaign to alert Atos senior managers regarding the consequences of Schrems II and how to act.
- Provide detailed briefings to interested parties, such as those in the Legal and Procurement teams;
- Create easy to use, formatted versions of the SCC for specific scenarios;
- Use legal specialists to create candidate assessments of the laws and practices in particular jurisdictions;
- Create a tool and process for performing TIAs;
- Support colleagues who were identifying contracts that would require the new SCC;
- Train colleagues in Legal and Procurement regarding the background to the new SCC, the requirements and the toolbox that was provided.

Together the formatted SCC, the TIA tool and the assessments of laws and practices created by the Group Data Protection Office and Data Protection Community created a toolkit for implementing the new version of the SCC. Creations of these was followed up by a program of training for those in Atos Legal and in Procurement who would be implementing contracts using the new SCC.

These TIA rely on two sets of recommendations from the European Data Protection Board (EDPB) "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures" and "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2" – the former in the assessments of laws and practices, the latter when considering potential mitigating measures.

4.2.1. Communication and trainings

Information, transparency, and trainings are of the utmost importance when the targeted goal is compliance with a new law or situation. That is why, the first reaction to Schrems II, from Atos's data protection teams, was to make sure that employees were informed, that such information was clear and complete and that trainings were available for them to know how to handle Schrems II compliance situations.

One of the main general strategies Atos data protection teams have applied is to create communication networks within the group and at all levels to keep colleagues informed of all legislative, regulatory, and jurisprudential developments.

4.2.2. Assessment and compliance tools review and improvement

Where possible, Atos data protection teams aim at going further than legally required to when it comes to data protection compliance. That has led Atos to create and implement for several years now an assessment tool called CADP (Compliance Assessment of Data Processing, referred to at 2.11) that is used to assess all Atos processing activities. CADPs have allowed Atos employees to develop a reflex and habit to assess every processing operation to be implemented and to make sure risks are identified and safeguarded efficiently. The Schrems II jurisprudence has hence found Atos teams and collaborators already familiar with making assessments in all circumstances and for all processing activities.

4.2.2.1. Processing activities review and update as Controller or Processor

Making assessment and compliance tools Schrems II and EDPB recommendations compliant has allowed us, at all levels of the company, to identify processing activities that needed reviewing and updating. To that end, Atos data protection teams together with the business owners have on the one hand checked processing activities where Atos acted as Controller in the light of the ruling and recommendations from the EDPB, and on the other hand, amended and updated processing activities if required. Atos ensured that pre-Schrems II processing activities were compliant with the new positive law, at the same time making sure that the updated compliance and assessment tools would at all levels of the company guarantee such compliance where needed and relevant, following the step-by-step model outlined by the EDPB.

Where Atos acted as Processor, we made sure that our clients were supported and provided the assistance needed to ensure their compliance with the ruling. To achieve that goal, Atos has developed a two-tier strategy comprising a general part covering data protection in its entirety, and a specific part covering the Schrems II jurisprudence coupled with the EDPB recommendations.

4.2.3. General data protection strategy for customers

In addition to developing assessment and compliance tools, Atos ensures that they are implemented to safeguard data exchanges with all partners, regardless of the location where they are being processed and in compliance with the instructions Atos receives. One of the main achievements is to make sure that on a group level Atos shares the same tools and practices while having the same standard of protection that is, as stated above, at least equivalent to the level of protection required by European Union law.

Implementing and using such assessment and compliance tools may translate to:

- **Checking and documenting all our relationships and processes with our internal and external suppliers.**
- **Checking and documenting that our suppliers are fulfilling their legal and contractual obligations as stated in our agreements mirroring the obligations we have towards the law and our clients.**
- **Checking and implementing adequate and efficient legal instruments in the context of international data transfers (BCRs or Standard contractual clauses (hereinafter: SCCs) depending on the situation).**
- **Ensuring that the instructions Atos receive from clients are duly cascaded to suppliers and that they have implemented all safeguard mechanisms lawfully defined by clients in their role as Controller and that, regardless of our suppliers' location.**

While these are general rules Atos rigorously applied even before Schrems II, the new CJEU decision has given us the opportunity to enrich our general strategy and to add new rules and measures to offer our clients the assurance that personal data is safe in our hands.

4.2.3.1. Specific Schrems II strategy for customers

Complying with the Schrems II decision and the EDPB recommendations is a safe strategy for companies. In addition to updating processing and compliance tools such as the legal, technical, and organizational measures to reflect the jurisprudence and recommendations from authorities (especially the EDPB step-by-step model), Atos supports partners in:

- **Ensuring that valid and safe tools such as SCCs and BCRs are always used in the context of international transfers;**
- **Checking and foreseeing additional measures defined by the EDPB to be implemented when needed;**
- **Complying rigorously with clients' instructions with regards to international data transfers and access requests.**

Atos has furthermore, by means of a strategy statement, reiterated the commitment to customers to process their personal data not only within the defined legal limits but also to safeguard them with the same level of security that is provided when it comes to securing Atos data, taking into consideration the legal, technical, and organizational measures defined.

Although Atos is not the natural target of third country surveillance or mass surveillance laws, we have adopted the strategy to manage every international transfer of EU personal data with the same degree of seriousness and security.
Atos combines all resources to offer partners an exemplary level of protection that satisfies the European standard which remains one of the highest levels of personal data protection in the world today.

4.3. Compliance Assessment of Data Processing as Controller (CADP-C)

Following the migration of the Atos CADP-C records, effectively the records of processing as a Controller, to the managed MyCADP platform in 2020, there followed a process of consolidation as the template for the records and the processes around their creation were improved.

A particular focus of such exercises was to avoid adding unnecessary details, but rather to clarify and sharpen the questions, options and explanations so that users could more easily provide the necessary input.

The MyCADP project board organizes and schedules regular reviews meetings with DPOs to ensure that this valuable tool remains well managed. The BRM focuses on any significant changes and the corresponding business requirements for these. Incidents and minor clarifications are managed via the normal IT Service Management Processes.

Number of assessments / statistics:

2021

765 records were created (initialization of a compliance assessment questionnaire)

446 records were completed (submitted by respondent and validated by a DPO)

2022

1198 records were created (initialization of a compliance assessment questionnaire)

716 records were completed (submitted by respondent and validated by a DPO)

4.4. Compliance Assessment of Data Processing as Processor (CADP-P)

The CADP-P is the equivalent record for processing that Atos performs on behalf of its customers, as a Processor.

In 2021 the creation of this record remained a manual, if well-established process. The form itself has been refined following its original introduction to meet GDPR requirements but it was felt that a major review was required to improve its usability and quality. This update to functionality, but particularly the improved content was also intended to pave the way to the move to the same managed platform as the Controller records.

In 2022 In addition, a project for improving the fundamental CADP-P process was started.

This began with a comprehensive analysis of the global processes and how the creation of processing records as a Processor was integrated with these. A detailed analysis of weaknesses was carried out to determine areas requiring attention. Weaknesses in the current process were identified to determine areas for improvement. «Best in class» processes within the organization were identified by creating and using a questionnaire. Based on the results of the weakness analysis, an improvement plan for the CADP-P process was developed.

The sales platform now captures whether personal data is to be processed for a customer within the scope of particular data processing agreements (DPAs) for a particular customer project / Opportunity). It also records the existence of a CADP-P (processing record) for each project. Based on this information, a monthly report is generated to ensure necessary transparency and provide an overview of personal data processing and the availability of CADP-Ps.

These measures, which were all in place by the start of the second quarter of 2022, contributed to improving the CADP-P process, increasing transparency, and enhancing efficiency in managing privacy matters.

The project to improve the process was accompanied by a project to create a parallel platform to the existing MyCADP platform which would hold new client processing records, and to develop the new records and processes that would support this. A number of factors had to be addressed correctly to gain the maximum benefit from this, in particular:

- **The need to coordinate the creation of a record with the bid process, so that information was collected when it was likely to be available and would add value;**
- **A streamlined process for creating user accounts on the platform and other measures to ease the higher throughput of processing records;**
- **Measures to make it easier for those validating records to identify to manage their workload and identify the records they were responsible for.**

With the revised process now in place, testing and training for the new "MyClientCADP" platform were conducted in April and May 2022, followed by a full launch in June 2022. From that point on all new records were to be created using the new platform.

4.5. Book of internal controls

The BIC update was also one of the major improvements within Atos data protection teams in 2020.

- **Some improvements were also made in 2021 and also in 2022**

Pursuant the global action plan, a working group had been established to make the Book of internal Controls (BIC) more practical and more comprehensible.

The BIC Working Group was established to consolidate and streamline the number of controls while ensuring that none of the risks to be covered would be disregarded or overlooked . At the same time, the wording of the existing BIC did not in all cases allow audit participants to easily understand what controls had been established, why we are concerned with reviewing the items, who had responsibly over the item and the timing around conducting the audit and implementing the necessary remediation if any.

Comparable to the CADP-P update, the new version of the BIC focused on practicality, understandability, and quality of results. To that end, data protection teams conducted a deep reassessment of what is necessary to help understand the risks and help employees to focus on obtaining positive audit results. By these means Atos aimed at industrializing the BIC as well as the CADP-P as both tools are put closer to the production reality within the Atos organization.

Another important aspect about the BIC improvement as well as the CADP-P's is the focus on the most important and necessary aspects of such tools. This helps employees clearly understand the main requirements, raising therefore awareness and understanding of what is expected and how to efficiently deliver on that.

4.6. Human Resources

4.6.1. Mandatory e-Learning

Atos requires its employees to attend an e-Learning on Data Protection – one of four mandatory training courses. In 2021 the mandatory training courses moved to a new platform. This was followed in 2022 with the development of a revised data protection course. To successfully complete the e-Learning, employees must pass a test at the end of the training with at least 80% correct answers. Since 2020 the Data Protection training must be taken on an annual basis.

By the end of 2020, 94,3% of the total population of Atos employees had successfully completed the mandatory e-Learning on Data Protection. Following the move to the new platform and the introduction of the annual reset, the training figures were as follows:

- **2021 - 88%**
- **2022, - 90%**

4.6.2. Cooperation with HEC Paris

In 2021 and 2022 Atos continued its collaboration with the prestigious HEC university business school in Paris. Indeed, for Data Protection Day 2022, one of its distinguished academics, David Restrepo Amariles kindly agreed to be interviewed and provided a wide-ranging and illuminating view of the interplay between technology, privacy and regulation.

Following collaboration on the potential uses of AI in 2020, the Group Data Protection Office collaborated with academic staff at the institute to create workshop sessions for its Tech Law students around the concept of disruptive technologies. The students selected a wide variety of applications of technology to consider and some lively presentation sessions followed, as syndicate members returned with their proposals.

5. Conclusion and outlook

In 2021 and 2022 Atos continued to build on the strong foundations established by the Group data protection office and data protection community. Improved communication, processes and tools were central to this, but this was only possible through the collaboration and initiative of the community and the cooperation of so many colleagues in the wider business. All those working in data protection must continue to strive to make the subject clearer, to communicate the value and the importance of compliance with data protection regulation, and to face the challenge of protecting privacy as technology accelerates.

Alongside the requirements of legal compliance, the particular data protection challenges in the world of technology are how to keep personal data safe, and, of course, how to address the impact new technologies on the rights and freedoms of individuals – mitigating risks and enhancing benefits.

For 2023 the target will be to support organizational changes in the company and to build on the foundations that have already been laid: in skills, tools, policies, processes and communications, but especially in collaborating with all interested parties to improve data protection compliance. To this end Atos will continue to grow its Data Protection Community, to promote and maintain awareness of data protection, and pursue the continuous improvement of its systems that support the compliant processing of personal data.

About Atos

Atos is a global leader in digital transformation with 105,000 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 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.

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

Eviden business is operated through the following brands: Alia Consulting, AppCentrica, ATHEA, Atos Syntel, Bull, Cloudamize, Cloudreach, Cryptovision, DataSentics, digital.security, Eagle Creek, EcoAct, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Miner & Kasch, Motiv, Nimbix, Processia, Profit4SF, science+computing, SEC Consult, Visual BI, Worldgrid, X-Perion, zData. Eviden is a registered trademark. © Eviden SAS, 2023.

About Tech Foundations

Tech Foundations is the Atos Group business line leading in managed services, focusing on hybrid cloud infrastructure, employee experience and technology services, through decarbonized, automated and AI-enabled solutions. Its 52,000 employees advance what matters to the world's businesses, institutions and communities. It is present in 69 countries, with an annual revenue of € 6 billion.

Find out more about us

atos.net
atos.net/career

Let's start a discussion together