Annual Data Protection Report 2020

Trusted partner for your **Digital Journey**

Atos

Contents

Introduction

Scope, objectives, and audience

This document is the Annual Data Protection Report of the Atos Group, hereinafter referred to as Atos or the company, and was prepared by the Atos Group Data Protection Office. This report provides 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, 2020 to December 31, 2020.

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 has evolved and changed during 2020.

1 Organization

Organization

Being a Group with strong European roots, Atos has decided to organize Data Protection alongside GDPR. Nevertheless, as Data Protection legislation outside the European Economic Area is usually a national solo-effort, a multitude of additional Data Protection laws must be respected and adhered to. Atos masters this challenge by having defined general Data Protection rules based on GDPR, while at the same time implementing national requirements and establishing a process to cope with cases where national legislation and Atos Data Protection policies and procedures would cause a conflict. In 2020 no such cases has occurred.

A Group Data Protection Office heads the overall 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 Point-of-Contact 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. In the absence of a specific legal expert the Group Data Protection Legal Experts cover this.

Group Data Protection Office

The Atos Group Data Protection Office is embedded in its Legal, Compliance and Contract Management Department. While taking benefit from the proximity to legal experts and the strong community of lawyers in more than 70 countries, the Atos Data Protection Office keeps 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 Atos Compliance department as well as with Quality, Corporate Social Responsibility, Risk Management and Group Internal Audit completes cooperation regarding Data Protection across the company.

In 2020, 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.

Organization

Group Chief Data Governance Officer

The Group Chief Data Governance Officer reports to the Group Deputy General Counsel. This role globally manages Data Protection Compliance, supporting data protection for all Atos, monitoring the implementation of data protection policies and processes, guiding the Atos DP Community, defining Atos DP strategy and organization as well as communication and training.

Data Protection Officer

Data Protection Officers (DPO) 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 on RBU level, supporting data protection topics in their perimeter, monitoring the implementation of data protection organization, guiding local, GDC/country-cluster DPOs, acting as counterpart at least for one Industry, taking active role in defining Atos DP strategy and organization as well as communication and training.
- 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 GDC/country-cluster Data Protection Office, supporting implementation of DP strategy as well as communication and training.
- Local - performing 2nd line tasks of a (designated) DPO, supporting data protection topics in their perimeter/ country, supporting and implementing data protection organization, managing local Data Protection Office, supporting implementation of DP strategy as well as communication and training.

Where required DPOs have been nominated towards the relevant Supervisory Authorities.

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 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 strategy as well as communication and training.

Data Protection Coordinator

Data Protection Coordinators (DPC) report within their respective legal entity and organizational context. Their responsibilities encompass acting as the DP expert within their Division, Practice, Operation or Support Function, acting as the DP point of contact in their perimeter, supporting data protection topics, supporting implementation of data protection organization, supporting implementation of DP strategy as well as communication and training.

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

With the further development of the Atos organization, Division DPCs will move to Products or Practices.

Data Protection Experts

Several organizational units have started to introduce the role of Division Data Protection Experts (DPE). Their responsibilities encompass maintaining the repository of processing activities for existing projects and services (Compliance Assessment when Atos acting as data processor), by validation of assessments, by supporting bid teams in risk management and assessment processes (where xDPE are assigned they take over this mission on behalf of the DPO in their perimeter).

With the further development of the Atos organization, Division DPEs will move to Products, Practices, or Industries (xDPE).

Data Protection Community

The Atos Data Protection Community consist of

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

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 Data Protection Community Hub. To cover all relevant time zones, the Global Data Protection Community Hub is completed 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 to both Community Hubs.

Regular topics addressed during these Community Hubs are:

- GDPO News
- Developments to be shared
  - Topics to be discussed in the community
  - Updates and changes in data protection legislation
  - New rulings and decisions by Supervisory Authorities
  - News regarding organizational changes / new joiners in the DP community
  - Other internal news
  - Other external news
  - Info regarding security incidents
- Permanent data protection tooling task forces
- Working groups & projects
- Data subjects' rights
- Assessments (Atos acting as data controller)
- Data Protection Impact Assessments
- Data Protection cartography
- Regular presentations (e.g. new guidelines, specific internal programs, etc.)
- Urgencies

Community Hubs do not aim at creating solutions during the meeting but at synchronizing, validating or correcting deliverables from working streams, and sharing information and best practices. They are regularly recorded and documented via meeting minutes available to all Data Protection Community members. They have been established in 2020 to replace a series of weekly and bi-weekly meetings on specific topics.

The Atos Data Protection Community counted 96 members by end of 2020.

Policies

On Atos Group level a set of policies defines the framework for data protection. These are

- Group Data Protection Policy (ASM-BMS-P017)
- Personal Data Breach Policy (ASM-BMS-P021)
- Atos Binding Corporate Rules (ASM-BMS-P022)
- Policy for access to Atos IT (network) user data (ASP-SEC-0082)

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' 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 Atos Employees and managers of the Atos Group and which have been validated by the European Data Protection Authorities.

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

Organization

The Group Data Protection Policy covers:

- Principles for processing of personal data (as a Data Controller and as a Data Processor)
- Legal Grounds for processing of Personal Data (as a Data Controller and as a Data Processor)
- Processing of Sensitive Personal Data
- Security Measures (when acting as Data Controller and as a Data Processor)
- Impact Assessments / Compliance Assessments of Data Processing
- Record of Processing Activities
- Selection of Subcontractors
- International Transfers of Personal Data
- Data Subjects' rights
- Complaint Handling Procedure (direct, indirect and complaint of a Data Controller)
- Cooperation with Data 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 awareness
- Audit (internal, subcontractor, customer)
- Data Protection Community

The Group Data Protection Policy has been reviewed in 2020 and is due to be reviewed again by June 2021.

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 handle such a breach, especially regarding obligations to notify competent authorities and data subjects.

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

A specific assessment form supports employees in charge of dealing with Personal Data Breaches to determine the potential risks of such Data Breach.

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 Data Controller and when acting as Data Processor)
- Communications Actions

As Personal Data Breaches are first and foremost security incidents the Atos security organization regarding security events and security incidents apply. This includes organizational units and immediate actions, severity-based response mechanisms, and comprehensive documentation.

An assessment to determine the risk level associated to each such incident has to be done as a mandatory action for each Personal Data Breach. This assessment is based on a standard assessment 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 has been reviewed in 2020 and is due to be reviewed again by June 2021.

Atos 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 Data Controller)
- Liability vis-à-vis Data Subjects
- Liability vis-à-vis Controller
- Data Subject's information
- Cooperation with Data 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

The Atos Binding Corporate Rules have been reviewed in 2019. They are amended from time to time and where necessary, in particular where applicable data protection regulation applies.

Compliance Assessment of Data Processing

Atos is processing Personal Data in the role of the Data Controller as well as acting as Data Processor for clients. Applicable data protection laws and especially GDPR require Data Controllers to perform a Data Protection Impact Assessment (DPIA) for each processing activity where the type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons. Such assessment must be performed prior to the processing and should cover the impact of the envisaged processing operations on the protection of personal data.

Atos decided already several years ago to assess most processing activities to be performed, no matter

- If acting as Data Controller or as Data Processor
- If the processing is likely to result to a high risk for data subjects based on the indicators as listed in GDPR or if it is a processing activity not covering any of the indicators as specified in GDPR

Consequently, Atos has been assessing its processing activities when acting as Data Controller as well as when acting as Data Processor. Wherever such assessment shows a potential high risk to the rights and freedoms of natural persons and Atos acts as Data Controller, Atos additionally performs a DPIA.

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

Atos acting as Data Controller

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

Such CADP-C will usually 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 Data Processors (including mechanism for international data transfers and sub-processors)
- Data Transfers
- Technical and organizational measures
- Indicators suggesting a DPIA to be required

Organization

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 on global level. These assessments may be used also by local Atos entities or they may be cascaded to local perimeter e.g. to cover local specifics and/or national legal requirements.

Until June 2020 CADP-C have been created and maintained based on Microsoft Excel templates, covering the above-mentioned sections with detail questions. As far as possible answers have been standardized. For its affiliates in Germany Atos has been using an individual data base solution to maintain assessments (so-called *Verfahrensbeschreibung*) comparable to CADP-C.

Since July 2020 all CADP-C are created and maintained in "MyCADP", a specialized data base solution using the OneTrust Data Protection Management Solution. CADP-C templates have been enriched and implemented upfront in MyCADP to reflect all relevant assessment details. The migration of existing assessments has been / will be done in two steps: until end of 2020 all existing CADP-C have been migrated from Excel-format to MyCADP. This covers all assessments except the assessments *Verfahrensbeschreibung* for Atos affiliates in Germany. These assessments will be migrated to MyCADP during 2021.

As MyCADP is part of the Atos IT tooling landscape it benefits from standard processes such as regular Business Review Meetings (monthly, collecting input from Data Protection Community, discussing open points and requests for change) and regular Customer Advisory Boards (quarterly, defining general priorities and next major steps). Necessary urgent changes are implemented on demand / immediately. As far as possible major changes regarding the assessment template are limited to one per semester.

The CADP-Cs form the Atos register of processing activities as defined in Art. 30 (1) GDPR.

Atos acting as Data Processor

Before starting a new processing activity acting as Data Processor, Atos employees are usually obliged 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 usually document and reflect

- Project owner / leading Atos entity
- Data 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 Data Processors (including mechanism for international data transfers and sub-sub-processors)
- Data Transfers
- Technical and organizational measures

Each CADP-P is owned by one or more Business Owners who also create and maintain the assessment. CADP-P are reviewed and validated by Data Protection Experts, Data Protection Officers, Data Protection Legal Experts or Deal Lawyers.

CADP-P have been created and maintained based on Microsoft Excel templates, covering the above-mentioned sections with detail questions. As far as possible answers have been standardized. The template has been updated twice in 2020. A permanent task force is collecting requests for change and drives the continuous improvement in at least yearly releases.

The CADP-Ps form the Atos register of processing activities as defined in Art. 30 (2) GDPR. Atos is also collaborating with HEC Paris in a research project to incorporate Natural Language Processing in the assessment of processing activities when acting as Data Processor.

2 General conditions and external developments

General conditions and external developments

GDPR enforcement

Two years after what could be deemed as a cautious period for GDPR enforcement, although France issued in 2019 the highest GDPR enforcement fine to date, 2020 was the year with the most issued fines in European Data Protection history. Out of 664 GDPR enforcement penalties published so far, 336 were issued by European Supervisory Authorities in 2020 alone. This abundance of enforcement actions has led to the gathering of valuable data that have helped us outline and understand the concrete trends that begin to emerge; and adjust our focus when it comes to privacy actions and policies.

A quick analysis of enforcement trends shows that data processing operations with insufficient legal bases (a sum of penalties of € 166,516,848 for a total of 237 fines) and/or insufficient technical and organizational measures (a sum of € 66,004,419 for a total of 139 fines) are most likely to result in significant fines. Furthermore, as of today, the highest average fines have been provided in the media, telecoms, and broadcasting sector (a sum of penalties of € 132,462,915 for a total of 123 fines).

In that sense, Vodafone Italia was fined over € 12,000,000 for infringing among others the main principles of the GDPR, while on the same ground TIM (telecommunications operator) was fined a total of € 27,800,000.

Although fines in the telecommunications sector are large and numerous, they are not the only ones. Indeed, the German authority has fined H&M for example for non-compliance with the GDPR up to € 35,000,000 and Marriott international up to € 20,000,000.

This situation has led us to give more focus not only to the legal bases that our processing operations are justified with, but also to the implementation of sufficient technical and organizational measures; the latter's evolution being also heavily influenced by the impact of the Schrems II ruling.

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 has impacted almost every aspect of our economy, society and mental health.

The way we conceive our privacy and the importance which we attach to the protection of our personal data has also been heavily impacted by this ground-breaking event. Personal Data 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 national security. In the data-intensive world of today, ubiquitous data points and digital surveillance tools can easily exacerbate those concerns.

For example, China has been reportedly using ubiquitous sensor data and health-check apps to curb the disease spread. According to a New York Times report, there is little transparency in how these data are cross-checked and reused for surveillance purposes. The report said that Alipay Health Code, an Alibaba-backed government-run app that supports decisions about who should be quarantined for COVID-19, also seems to share information with the police. In Italy, the local data-protection authority was urged, on 2 March 2020, to issue a statement to clarify the conditions of lawful data use for mitigation and containment purposes. In its statement, the authority warned against the privacy-infringing collection and processing of data by non-institutional actors (e.g., private employers).

Two weeks later, the European Data Protection Board issued a statement on the importance of protecting personal data when used in the fight against COVID-19 and flagged specific articles of the General Data Protection Regulation that provide the legal grounds for processing personal data in the context of epidemics. For example, Article 9 allows the processing of personal data "for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health," provided such processing is proportionate to the aim pursued, respects the essence of the right to data protection and safeguards the rights and freedoms of the data subject.

General conditions and external developments

Schrems II ruling

On July 16, 2020, the CJEU rendered the Schrems II decision invalidating the Privacy Shield which has been a safeguard mechanism that many companies relied upon to perform international Personal Data transfers for commercial purposes between the European Union and the United States.

In the context of the ruling, the European Court was asked to clarify from a EU law standpoint, if the European Standard Contractual Clauses (SCCs) and/or the Privacy Shield provide(s) a sufficient level of protection against the Law in the United States relating to access to Personal Data for Intelligence and State Security purposes (Section 702 of the FISA and E.O. 12333). A legal question to which the court answered in two parts:

First, the court held that the SCCs were valid with an additional burden for both companies that export Data and companies that import Data. Second, the court ruled that on the same issue, the privacy shield was invalid considering that U.S. law does not effectively set out limits on the activities of the intelligence services and does not provide effective remedies for individuals whose data has been transferred.

The CJEU ruling did not obviously mean that Data transfers could no longer occur between EU and U.S. companies for commercial purposes. Data transfers between the U.S. and the EU are a major part of the global economy. Thus, the Privacy Shield being invalid meant that one of the mechanisms to safeguard those transfers could not be used anymore. At Atos, we already had been committed to taking a proactive approach to secure our customers' and collaborators' Personal Data without geographical limitations before the ruling. Therefore, though the Schrems II ruling had shaken the data protection world and made major headlines, it had a a lower practical impact on how we, in Atos, safeguard international transfers of Personal Data as we have implemented and been using, long before the ruling, other valid data transfer mechanisms as per our internal policies and applicable laws.

Indeed, the two remaining alternative mechanisms pursuant the European Court's decision were already well implemented and used within Atos for most of our personal data exportations to the US. Regarding the transfers that were concerned by the decision as well as other compliance needs from the ruling, we have taken a set of actions to ensure compliance.

Brexit

With Brexit (or "British exit") the United Kingdom (UK) withdrew from the European Union (EU) and the European Atomic Energy Community (EAEC or Euratom) at 23:00 31 January 2020 GMT (00:00 CET). The UK is the sole member state which ever formally left the EU. The UK has been a member state of the EU and its predecessor, the European Communities (EC), since 1 January 1973, hence for 47 years. The UK continued to participate in the European Union Customs Union and European Single Market during a transition period that ended on 31 December 2020 at 23:00 GMT (00:00 CET).

Leaving the EU has wide reaching consequences, including in the field of data protection. Even though UK data protection law now includes a UK GDPR, a UK regulation formed from the GDPR, the United Kingdom could have become a 3rd country with no adequacy decision by 1st Jan 2021 (seen from EU perspective). This could have massively affected data flows between the EU and the UK, even though the UK government already had adopted an adequacy decision for the EU before end of 2020 and hence data flows from UK to EU were not at risk anymore.

Based on agreements between the UK and the EU, the UK will not be treated as a third country for the first 4 months of 2021. This period could be extended by additional 2 months. Meanwhile the EU is considering an adequacy decision for the UK.

Data Protection Legislation

Mainly driven by the aim to strengthen online privacy rights and boost the digital economy, Data Protection Legislations evolved in the recent years at a very high pace. After the implementation of the EU GDPR, and the earthquake effect it had, many countries followed the path to implement or improve its Data Protection Legislation. The year 2020 was not spared by those evolutions.

In fact, after several discussions and postponements the Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018 entered into force. The LGPD is Brazil's first comprehensive data protection regulation and it is largely aligned to the EU General Data Protection Act (GDPR).

Although the law is now in force, the penalties issued by the LGPD will only be enforceable starting August 2021. However, public authorities (such as consumer protection bodies and public prosecutors) as well as the data subjects can currently enforce their rights under the LGPD.

Prior to the LGPD, data privacy regulations in Brazil consisted of various provisions spread across Brazilian legislation. Hence, the LGPD attempts to unify the over 40 different statutes that currently govern personal data, both online and offline, by replacing certain regulations and supplementing others.

The LGPD applies to any processing operation carried out by a natural person or a legal entity, of public or private law, irrespective of the means used for the processing, the country in which its headquarter is located or the country where the data are located, provided that:

- The processing operation is carried out in Brazil
- The purpose of the processing activity is to offer or provide goods or services, or the processing of data of individuals located in Brazil, or
- The personal data was collected in Brazil

What are the punishments provided by the law? Companies that violate the new law will be subject to the application of warnings, fines, embargoes, suspensions and partial or total bans to performing their activities. Article 52 states that the maximum fine for a violation is "2% of a private legal entity's, group's, or conglomerate's revenue in Brazil, for the prior fiscal year, excluding taxes, up to a total maximum of 50 million reals" (roughly €11 million).

3 Projects and internal developments

Projects and internal developments

Projects and internal developments

During the reporting period 23 working groups have been launched of which 9 delivered their final result already in 2020, 3 have been transformed into permanent task forces, 1 has been moved to a research project in GDPO, 1 has been put on hold, and 9 have still been ongoing by December 31, 2020. These working groups are:

- ACM project (completed in 2020)
  Objective: using the existing Atos Contract Management system in data protection context, especially regarding Compliance Assessments of Data Processing when acting as Data Processor
- ASD-SEC-0082 Policy for Access to Atos IT (Network) User Data (completed in 2020)
  Objective: review and update Policy for Access to Atos IT (Network) User Data
- ASM-BMS-P021 Personal Data Breach Policy BIP-AP21 (completed in 2020)
  Objective: review and update Personal Data Breach Policy
- Atos DP awareness session 2020 (completed in 2020)
  Objective: create an additional awareness campaign on top of European Data Protection Day / International Data Privacy Day in January; led to and prepared Atos Data Protection Week in Q4/2020
- Atos Data Protection cookbook (completed in 2020)
  Objective: review and update Atos Data Protection cookbook, an internal guideline for all Data Protection professionals
- Atos Global Data Protection Statement (completed in 2020)
  Objective: create the Atos Data Protection Statement, a general document describing how Atos is processing personal data and giving focus to technical and organizational measures implemented as a standard to protect personal data
- KPI improvement (completed in 2020)
  Objective: review existing KPI in Data Protection and create a global minimum set of KPI to be monitored and reported
- Privacy Notices / Data Protection Information Notices for Processing (completed in 2020)
  Objective: review and update existing Data Protection Information Notices templates
- Simplification exercise with Procurement (completed in 2020)
  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
- CADP-P update (moved to permanent task force)
  Objective: review and update existing CADP-P template, 2 iterations done in 2020
- MyCADP project (moved to permanent task force)
  Objective: create a tool for company-wide use when assessing processing activities with Atos acting as Data Controller, migrate existing CADP-C to new environment
- New DP SharePoint (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
- CADP-P automation / HEC (moved to research project in Group Data Protection Office)
  Objective: evaluate how a system based on Natural Language Programming supports creating and maintaining different contractual and assessment artifacts with Atos acting as Data Processor when processing personal data, at the same time evaluate if such solution could replace the existing CADP-P solution
- Atos' global data protection principles for consent to marketing communications (on hold)
  Objective: review and enhance global standards for consent to marketing communications, global catalogue has been provided, optional further steps have been suspended
- AP17 Group Data Protection Policy updates with SPRING
  Objective: revie and update Atos Group Data Protection Policy, especially with regard to changes invoked by Atos internal SPRING program and related organizational changes
- Article 27 - EU Representatives
  Objective: review the way Atos has so far nominated EU representatives, at the same time investigate if and how external EU representatives can be replaced by Atos-internal representatives
- Communication new policies
  Objective: defining a standard on how to communicate new and changed policies affecting Data Protection
- DP related Data Sovereignty
  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
- DP related incident management process
  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
  Objective: do preparation work for potential ISO 27701 certification – structure existing policies, guidelines, and organization, provide gap analysis of the existing Atos organization compared to the standard
- eSO working group
  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
- GDPR-related processes on Office365 / SharePoint
  Objective: investigate what can be stored how and where with SharePoint online considering data protection requirements, especially as set out in GDPR
- Transfer of employee data in matrix org
  Objective: investigate how employee data can be lawfully shared between different legal entities within matrix organizations, assess different roles (Data Controller, Data Processor, Joint Controllers) and lawful basis for transfer of employee data within the matrix organization

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 meetings at regular intervals. Results have been shared and agreed with the Data Protection community members.

Projects and internal developments

Trainings & awareness

Data Protection training, communication and awareness is one of the main activities in the Atos Group Data Protection Office. This rubric is so important since one of the most common ways data breaches occur are due to human errors. This means, that one of the main sources of a data breach in a company is due to an employee error. Therefore, a considerable number of data breaches could be prevented if employees have knowledge about how to protect personal data.

The Group Data Protection Office's mission in this area is to have training and communication that are relevant, clear, attractive, and effective to create an impact on employee behavior when working with personal data.

In this context, all Atos employees must complete the global mandatory e-Learning training on Data Protection including GDPR rules. In this training, Atos' employees learn Atos' approach on Data Protection, the tools available for them to reach compliance, as well as the rights and obligations a Data Subject has.

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 preformed further trainings and webinars during the year:

From 27 to 31 of January, we celebrated the International Data Protection Day (January 28) with an entire Data Protection Week full of activities. Each day during the week publications were posted with tips on how to protect personal data. A "Virtual Coffee with GDPO" were organized to solve employees' questions in an informal talk. Different activities were performed in countries and in the end of the week a webinar in the Atos University Learning Friday was presented with the subject: "Not yet again Data Protection!", mainly addressing privacy as a basic human right, the potential difficulties in implementing data protection by default in daily routines and how to still energize data protection in Atos.

In March, during Atos Innovation week the Atos Group Data Protection team presented a demo on how to use the new MyCADP online tool.

In November, the Data Protection Awareness Week. Different awareness sessions were organized in the Community with new relevant and attractive topics:

- Schrems II: "Crossing borders - Atos solutions which can help you when exporting personal data from the EU"
- Lights, Camera, Action - Sharing Pictures and Videos online
- Data Protection - Not Again!
- Coffee and Conversation - DPO's and DPLE's - APAC/India
- Coffee and Conversations - DPO's and DPLE's – NAO
- Social Media - The Good, The Bad, and the Ugly

Due to the pandemic context, a communication email was shared with employees to remind them what to keep in mind to protect personal data when working from home. This has been done in coordination with other security-related awareness messages and communication activities driven by the internal crisis management team.

During the year several awareness sessions have been facilitated in Atos local organizations, as far as requested these have been supported by Atos Group Data Protection team with content and guest speakers.

COVID-19

During the reporting period, several documents and support have been delivered regarding the COVID-19 outbreak. In fact, the pandemic did not only create consequences on health of individuals, but also on their freedom and rights, including the right to privacy. Approaching and analyzing that angle, giving support and informing managers and employees on that topic is considered at the utmost importance for Atos.

In that regard, the GDPO team provided guidance, consultancy, and support regarding the processing of personal data in the context of COVID-19. It consisted of for example the publication in April 2020 of the document "Covid-19 and Data Protection Guidelines" explaining the Data Protection requirements per country for the processing of personal data in an employer-employee relationship, as well as support for the global crisis management teams and the support regarding back to office applications.

Schrems II

When the decision was issued, the immediate reaction was to communicate and inform the management about the ruling and its implications for Atos, followed by the design of a compliance strategy not only to align with the ruling, but also with the European data protection board's recommendations (EDPB hereinafter) that have been published later. The action plan was divided into three main parts:

- First, creating a maximum transparency in providing clear and complete information about the new situation while fostering the already existing data protection-aware culture and ecosystem;
- Second, strengthening and updating the assessment and compliance tools and reviewing processing activities that required updates;
- Third, developing a twofold strategy to support Atos' customers where relevant and needed.

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' 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.

The Schrems II situation has thus found Atos with a mature and well-established network that has enabled us to communicate easily on the subject and organize the trainings meaninglessly during such a critical time. Atos data protection teams have organized and animated at all levels of the company specific Schrems II webinars to raise awareness about the ruling and its consequences, providing guidelines, as well as FAQs to help colleagues, on their level, to comply with the ruling and recommendations from authorities. These actions have allowed Atos to identify all processing operations that needed to be updated including assessment and compliance tools.

Projects and internal developments

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 2.9) 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.

Atos has been striving to take and keep a leading role in data protection, playing a role of an innovator in the field. Atos' purpose is to constantly create new standards that provide a safer and more trustworthy informational space. In that regard, Atos is the first European company that has put in its legal status as its raison d'être the engagement to help design the informational space, and part of that is to make it as safe as it can reasonably be. Atos is the first company to have received a validation for its Binding corporate rules (hereinafter: BCRs) from European data protection authorities. In addition to that, Atos has designed the first BCRs register called BCR-001 that was afterwards validated by Atos' lead authority, the French Commission National Informatique & Libertés (CNIL), to help companies comply with their obligation to record personal data processes in the context of international transfers using BCRs. In consequence, part of the Atos strategy is to dedicate human and technical resources to shape the future of data protection and particularly in areas where laws and regulations do not especially provide satisfying solutions. It is animated by that spirit that as soon as the Schrems II decision was published, even before the EDPB's recommendations, Atos teams have put in place a series of additional measures to make personal data transfers as secure as possible, raising the already high standards where necessary in the light of the Schrems II ruling. In parallel, it was ensured that partners' and clients' personal data are treated with the highest level of security and care. To that end, Atos has also reviewed and updated the data protection addenda as well as the technical and organizational measures to reflect the new situation.

The role of Atos data protection teams in the context of the ruling was therefore to accompany collaborators in updating those assessment and compliance tools making them not only compliant with the Schrems II decision but also with the EDPB recommendations, easing at the same time, the review and update of processing activities where Atos acted as Controller, but also our partners' processing activities where Atos acted as Processor.

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.

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.

Projects and internal developments

Specific Schrems II strategy for customers

Complying with the Schrems II decision and the EDPB recommendations merely 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.

Brexit

With Brexit personal data transfers from EU to the UK and vice versa would become transfers to a third country, hence these could require – unlike before – a valid transfer mechanism that complied with GDPR (for EU personal data transfers). However, this would not be applicable in the event of an adequacy decision by the EU (for EU personal data) in respect of the UK. With regard to transfers into the UK, the UK government had already stated that (in respect of UK personal data) it would allow such transfers.

As Atos can base internal personal data transfers on its Binding Corporate Rules, this transfer mechanism had been identified as an alternative for all such EU personal data transfers to the UK in case Brexit would be concluded without any EU adequacy decision for the UK. To also use this mechanism for UK personal data, Atos prepared for Atos UK BCR, inspired by the Atos Group BCR approach and model. This could then also cover internal transfers of UK personal data to any other jurisdiction. By end of the reporting period, preparation work on Atos UK BCR had still been ongoing. Based on the decision to accept each other as adequate countries for an intermediate period of 4 months, which could be extended by additional 2 months, such data transfers were still possible without additional transfer mechanisms by end of the reporting period.

During preparation for Brexit, Atos also reviewed and adapted the nomination of its data protection representatives. While on the one hand a UK representative to cover requirements as set out in UK Data Protection Act has been nominated by end of the reporting period, a working group took the task to review how to improve nominating EU representatives as required in Art. 27 GDPR.

Projects and internal developments

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

MyCADP Business Review Meeting (BRM):
The MyCADP project board organizes and schedules regular BRM calls with main DPOs (Business review Meeting Data Protection) to ensure that this valuable tool remains well managed. The BRM focuses on significant changes (i.e. large change) and corresponding business requirements. The "Large Change Requests" are discussed in the BRM. Incidents & small changes are managed via the normal GIT Service Management Processes and not discussed in the BRM (reporting via separate Service Meeting can be arranged

Migration project:
The MyCADP project board organized a common migration process to migrate in a harmonized manner all the existing CADP-Cs in the Excel template into the new MyCADP tool template (stored as a record in the MyCADP tool).

From February 2020, DPOs began sending migration batches to the project migration team, who then confirmed when the batch had been migrated and issued an invitation to start reviewing.

From April 2020, on the other hand, for Global CADP-C, the migration is managed by the DPC (or GDPO team when no DPC designated) who coordinates a specific domain (HR, FINANCE, IT, etc.) and sends a similar migration batch to follow the same migration process. To speed up the migration from a template to another, it is planned to divide the review work between GDPO team and a small team of key-reviewers in the DPO-network who have enough capacity to join.

MyCADP template release:
The MyCADP project started in January 2020 with Template version 4 and implemented an iterative process to collect DPO's feedbacks but not only. Respondents teams and processing owners were interviewed to adapt the MyCADP template to their usages.
By the end of 2020, the project was using template version 42.
As an example, an answer in the MyCADP questionnaire (section General) could now specify the location of data subjects in particular jurisdictions, such as California, Brazil, Germany, Spain, Portugal, as a result of which MyCADP will then populate the questionnaire with a set of additional questions, according to the selection. The additional questions allow the respondent to answer specific requirements in the assessment of personal data processing in these countries by their data protection authority.

MyCADP mandatory questions:
It is decided to highlight a limited amount of questions in the MyCADP questionnaire.

Red stars mark the mandatory questions selected by the Group DPO. You can "save and exit" the assessment before finalization, but you cannot submit your assessment to DPO without having answered all mandatory questions.

Record ID vs Excel file name:
One of the main advantages among others of the MyCADP tool is the unique and simple identification of a processing with an identification number called Record ID

Stage vs Status
In the CADP process acting as controller, the manual workflow status (submitted by automatic collect via SP, incomplete, final) were replaced by automation workflow stages (initiated, in progress, under review, completed)

Number of assessments / statistics:
750 records created during 2020 (initialization of a compliance assessment questionnaire)

305 records completed during 2020 (compliance assessment review finalized in 2020)

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

The Atos data protection community has been defining and exploring for many years new inclusive ways to work together regardless of locations or legal entities. In that sense, several working groups were created, comprised of small groups of data protection experts from all entities to tackle and undertake data protection projects and needs. In that sense, Atos has tackled in 2020 one of the major projects that was updating the Compliance Assessment tool of Data Processing where Atos acts as Processor (CADP-P hereinafter). Besides regular updates and improvements the objective had been set to optimize the assessment. In that sense, each item in the CADP-P has been checked for obsolescence while ensuring the assessment still covers all relevant questions and information to appraise the risk level of each processing activity. Such exercise helped the overall Atos Data Protection Community in better understanding clients' and collaborators' needs when assessing what should be built in services and processing activities. Atos data protection teams have published 2 updated versions of the CADP-P in 2020.

At the completion of the project, data protection teams achieved to provide a more usable, practical, and efficient version of the assessment tool. They also made sure that it can be used in a way that provides more clarity of information, allowing to enhance user experience and better supporting the review of data protection requirements during solution design and sales process. The focus on practicality and efficiency has also increased and secured the acceptance rate of the tool from our collaborators.

The need for updating the tool stemmed also from feedbacks that data protection teams had received from users and that have been treated with the utmost importance. Such feedbacks related mainly to the usability of the tool, but also to the understandability of the sets of information that it displays. With the 2020 updates of the CADP-P tool Atos also ensured the ease of use improved readability and understanding of its content.

For 2021 a major update of the CADP-P to its version 3.0 has been scheduled. Atos data protection teams foresee to completely overhaul the graphical user interface within the first release of the CADP-P in 2021 and to revise the overall structure to increase usability.

Projects and internal developments

Book of internal controls

The BIC update was also one of the major improvements within Atos data protection teams in 2020. Pursuant the global action plan, a working group had been established to make the Book of internal controls (hereinafter: BIC) more practical and more comprehensible.

The BIC review has mainly been aiming at reducing the number of controls while ensuring that none of the risks to be covered would be ignored or missed. At the same time, the wording of the existing BIC did not in all cases allow collaborators to easily understand what controls are necessary where, how, with whom and why they should be conducted.

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 that. 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.

The review of the BIC had still been ongoing by end of 2020 with final results to be expected in the first semester 2021.

Human Resources

Personal Administration

In 2020 Atos has started the renewal process for their Personal Administration solution moving to SAP SuccessFactors Employee Central. The project has been accompanied by the Data Protection Coordinator for Human Resources, supported by several Data Protection Officers and the Atos Group Data Protection Office.

The processing activity "Personnel Administration" has been assessed via a Compliance Assessment of Data Processing acting as Controller (CADP-C ID 1685). The assessment led to the result that no additional Data Protection Impact Assessment (DPIA) as defined in Art. 35 GDPR would be required. Nevertheless, Atos decided to do an additional DPIA in order to add the highest level of check for risks to the rights and freedoms to privacy of the Atos employees. As the CADP-C before, the DPIA showed only acceptable residual risks for the data subjects.

Mandatory e-Learning

Atos is requiring its employees to attend an e-Learning on Data Protection. The e-Learning had been reworked in the course of the Atos GDPR Compliance Program in 2018 – the next release is foreseen for 2021, together with the move to a new training platform. To successfully attend 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 e-Learning must be re-taken on an annual basis.

By end of 2020, 94,3% of the total of Atos employees have successfully attended to the mandatory e-Learning on Data Protection.

Cooperation with HEC Paris

Atos has established a relation with HEC Paris regarding Data Protection. The purpose of this collaboration is to create a long-term partnership to push the knowledge of Artificial Intelligence technologies and law forward while addressing some of the pressing challenges Atos faces today and that are likely to benefit from LegalTech solutions.

As a first step of the collaboration, Atos co-delivers the TechLaw course offered by HEC Paris in the LLM. /MS. Droit et management International master. This course is taught by Professor David Restrepo (Associate Professor of Law and AI, HEC Paris, Data IA). The Group Data Protection Office with the General Secretary and the Atos Head of AI co-delivered a total of 18 hours of sessions during 2020.

The course covered the following topics:

- Introduction to AI technologies: data analytics, machine learning, and visualization.
- Automated decisions making
- Accountability, explainability and Ethics of AI
- Transformation of legal professions

As a second step, Atos and HEC collaborate with a team of professionals and students to set up a joint project to use technology to solve Atos Data Protection challenges. The topic chosen by the team is "Data Protection compliance in the data supply chain".

While delivering its services, Atos is often involved in long supply chains, acting both in a role as processor of the data received by its clients and in the role of a client providing data to be processed by its suppliers.

In this context, Atos has the challenge to ensure compliance through all the data supply chain by protecting at each stage of the data flow the privacy and security of personal data. This involves both compliance with data protection instructions contractually engaged, with the legal rules established in the Data Protection regulations including the GDPR, and the effective auditing of the flowing data.

To face the challenge and ensure compliance, the team is working on designing a Smart Contract & AI-based compliance tool that could help Data Controllers and Data Processors monitor the data supply chain in data protection contracts and risk assessments.

Projects and internal developments

Upcoming challenges

2020 has been an overall challenging year when it comes to data protection. In addition to the Schrems II ruling, the Covid-19 outbreak has also been a global topic that will, with other important topics, be challenges to take in 2021.

The first key foreseeable data protection challenge related to the Schrems II decision is data globalization after Schrems II. Indeed, in many situations, the Schrems II ruling as well as Authorities' recommendations do unfortunately not help find suitable solutions to ensure safe personal data transfers in some countries and mainly in the U.S., but also draw a clear picture as to what is compliant and what is not. Video conferencing tools and office applications give a great example of the lack of a clear of harmonized interpretation of the Schrems II ruling and its meaning. Microsoft, being one if not the major supplier for such solutions, is currently campaigning to keep European personal data in Europe by end of 2022, hence not leaving any doubt to comply fully with the Schrems II ruling's implications by that time. Until then current discussions on telemetry data, definition of personal data and definition of data transfers will most likely continue and lead to different interpretations and opinions. The root cause is yet not inherent to Microsoft or any other supplier, but a point to be seriously and permanently re-discussed in all areas where relevant business solutions can hardly be obtained in Europe if not via U.S. suppliers who need access to data in clear in order to provide their services.

The Brexit effect is also another key challenge in data protection. On 19 February 2021, the European Commission issued a much-anticipated draft adequacy decision regarding data flows between the EU and the UK. Unsurprisingly, the EU commission did include terms or conditions acknowledging the Schrems II decision confirming that existing UK law is already sufficient without the need to implement additional safeguards when transferring personal data from the EU to the UK. However, the adoption of the EU commission's proposal will mean that the UK and the EU are subject to different regulatory regimes. Therefore, while processing personal data in the EU and the UK, organizations must consider and comply with both, the EU GDPR and the UK GDPR. Furthermore, depending on their activities, organizations may need to take certain measures as appointing representatives or face some challenges as identifying their lead authorities for example.

Another major challenge for data protection is the Covid-19 outbreak for which many organizations were unprepared and its aftermath. If certain challenges have already been dealt with within the company as the implications of working from home and data protection as well as trainings and communications that were needed to raise awareness about the topic, more are yet to come related for instance to the aftermath of vaccines or recovered persons and the respective consequences for employers and employees in the workplace.

4 Conclusion and outlook

Conclusion and outlook

During 2020 Atos improved and enhanced its data protection activities. Despite external challenges, such as Covid-19, Brexit and Schrems II, the Atos Data Protection teams managed to provide support and guidance where requested and played an increasing role in supervising activities regarding the processing of personal data. With the introduction of a new technical environment to create Compliance Assessments of Data Processing when acting as Data Controller, Atos opened a new chapter in assessing and documenting the processing activities it performs for its own purposes. At the same time the Atos Data Protection Community has evolved into a more mature and massively collaborative ecosystem that allows Atos to tackle data protection challenges based on the knowledge of its close to 100 members from all over the world. Roles have been clarified and the foundation has been set to enhance process organization in the next step.

For 2021 the focus will hence be moved from organizational structure to process organization. As a result, Atos entities will benefit from global blueprint processes that support a globally consistent level of quality for processing assessments, personal data breach handling and data subjects' requests. This way, any kind of potential certification of Atos data protection activities will already be prepared. At the same time, and as the assessments of processing activities performed as a Data Controller are now based on sufficient tooling, the environment to assess such activities when acting as Data Processor will be reviewed and enhanced. As a first step CADP-P version 3.0 is planned to be published in the first semester 2021. Additional steps to prepare the decision for and subsequent move to a more sophisticated tooling will be done during the second half of 2021.

In parallel, Atos will grow its Data Protection Community, continue to raise and keep awareness for data protection, and pursue the continuous improvement of its systems that refer to or encompass the processing of personal data.

About Atos

Atos is a global leader in digital transformation with 110,000 employees and annual revenue of € 12 billion. European number one in cybersecurity, cloud and high performance computing, the group provides tailored end-to-end solutions for all industries in 73 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos operates under the brands Atos and Atos|Syntel. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

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

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

Let's start a discussion together

Atos, the Atos logo, Atos|Syntel are registered trademarks of the Atos group. © 2021 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.