The answer to GDPR

General Data Protection Regulation

atos.net/en/solutions/cyber-security/gdpr

GDPR Customer readiness

Is your company able to demonstrate compliance with the GDPR obligation?	- Atos GDPR visibility study	- Chapter IV - Section 1 - Articles 24, 30
Do you know where personal data is located in your infrastructure?	- Personal data catalogue creation service - Atos GDPR visibility study	- Chapter IV - Section 1 - Article 30
Has your company identified the risks related to personal data collection and processing?	- Atos GDPR visibility study	- Chapter IV - Section 2 - Article 32
Is your company able to process regularly data protection testing, to assess and evaluate effectiveness to ensure the security of personal data?	- Atos pen testing and data protection assessment services	- Chapter IV - Section 2 - Article 32.1 (d)
Is your company able to perform data protection impact assessment?	- Atos DPIA services	- Chapter IV - Section 3 - Article 35
Are your business lines fully aware of the impacts of the GDPR regulation?	- Atos GDPR customer workshop - Atos GDPR visibility study	- Chapter IV - Section 3 - Article 35
Are you aware of the GDPR impacts in your organization (from procurement to delivery?)	- Atos Consulting GDPR awareness & training services	- Chapter IV - Section 1 - Article 32.4 - Chapter IV - Section 4 - Article 39
Is your company complying with GDPR obligations when it transfers personal Data to Non-EU countries or process personal data cross-border?	- Data privacy risk analysis	- Chapter V - Articles 44, 45, 46

GDPR Customer data collection and rights management

Does your company implement appropriate measures to record and manage end-user consent when it collects personal data ?	- WL Consent management - Atos enforcement of new citizen's rights for data processing	- Chapter II - Article 6
Is your company able to provide transparent information, communication and terms when it collects personal data?	- WL e-contract	- Chapter III - Section 1 - Article 12
Is your company able to notify end-users on their new Digital rights ?	- WL e-identity - WL Messaging platform - Evidian Identity and Access Management	- Chapter III - Section2 - Articles 13, 15
Is your company able to implement appropriate measure to enforce end-users rights to erase and to be forgotten ?	- WL ID Center - Evidian Identity and Access Management	- Chapter III - Section 3 - Article 17
Does your company store, protect personal data and maintain privacy while allowing data monetization ?	- WL Token service provider - Trustway Data encryption at rest and in motion solutions	- Chapter II - Article 6.4 (e) - Chapter IV - Section 2 - Article 32.1 (a)

GDPR Privacy by design

Has your company defined and developed personal data management system to drive GDPR compliance?	- Atos Data Protection Management System (DPMS) for transparent modalities for GDPR exercise of rights	- Chapter III - Section 1 - Article 12
Is your company taking appropriate measures for personal data Integrity, availability and ability to restore?	- Atos lifecycle Data management (ILM) - WL e-safe - WL e-archiving	- Chapter IV - Section 2 - Article 32.1 (b)
Is your company considering to implement GDPR compliance for its SAP system?	- Atos SAP GDPR assessment	- Chapter IV - Section 3 - Article 35
Is your company able to design personal data protection safeguards at the time of application and processing design?	- Atos security consulting services	- Chapter IV - Section 1 - Article 25
Can your business lines or IT department take personal data privacy into account during the whole life cycle of the system or process development?	- Atos security consulting services	- Chapter IV - Section 1 - Article 25
Can you operationally demonstrate by default personal data privacy?	- Atos security consulting services	- Chapter IV - Section 1 - Article 25
Are you able to control and record access to personal data?	- Evidian Identity and Access Management	- Chapter IV - Section 1 - Article 25.2
Are you able to define and enforce access control policies to personal data?	- Evidian Identity and Access Management - Atos Privileged Administration Management solutions	- Chapter IV - Section 1 - Article 25.2

GDPR Privacy by design

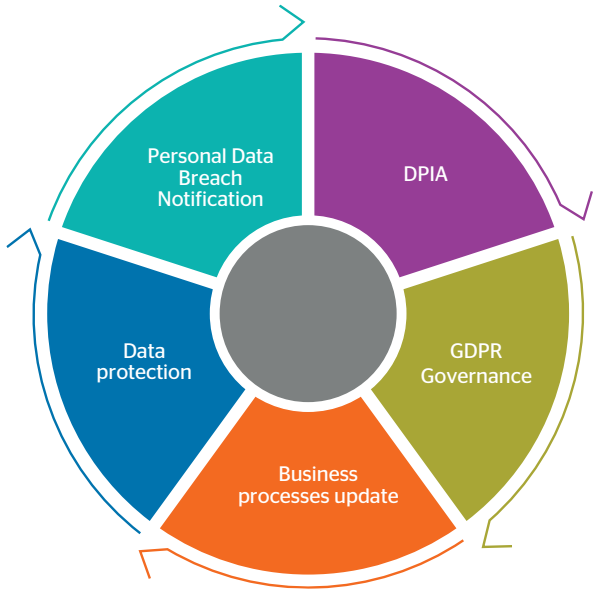
Can you identify/classify personal sensitive data and can you prevent un-authorized data sharing?	- Atos Data Loss Prevention solutions	- Chapter IV - Section 2 - Article 32.2
Is your company taking appropriate safeguard, such as encryption or pseudonymisation, to comply with lawfulness processing of personal data?	- Trustway Data encryption at rest and in motion solutions - WL Token service provider	- Chapter II - Article 6.4 (e) - Chapter IV - Section 2 - Article 32 (a)
Is your company leveraging encryption technologies to avoid the obligation to communicate personal data breach to end-users?	- Trustway Data encryption at rest and in motion solutions	- Chapter IV - Section 2 - Article 34.3 (a)

GDPR Breach detection and response

Are you able to detect whether personal data has been compromised?	- Atos Prescriptive SOC and CERT services	- Chapter IV - Section 2 - Article 33
Are you using public cloud services for personal data? If yes, can you demonstrate GDPR compliancy?	- Atos Prescriptive SOC and CERT services	- Chapter IV - Section 2 - Article 32
Can you report personal data breaches and notify the national authorities within 72 hours?	- Atos Prescriptive SOC and CERT services and reporting - WL Messaging platform	- Chapter IV - Section 2 - Article 33
Can you demonstrate GDPR compliancy and measures to avoid administrative fines?	- Atos GDPR structured and continuous improvement security	- Chapter IV - Section 5 - Articles 40 to 43

GDPR Atos approach

Atos uses its Continuous Improvement Cycle to deal with the wide-ranging impacts of GDPR:



To meet the regulatory challenges of GDPR, Atos implements a structured and continuous improvement approach. The Group offers both GDPR consulting and solutions to answer technical questions of the regulation. Using formal tools and reports, the compliance cycle makes it easier to upgrade from the initial Risk Assessment and DPIA to an ongoing managed security service ensuring end-to-end GDPR compliance.