
GDPR Data Risk Assessment



Understand your GDPR data protection risks

GDPR compliance is a board level issue

The EU General Data Protection Regulation (GDPR) applies to any organisation that processes and stores the personal data of EU citizens. With provisions including fines of up to 4% of global annual turnover or €20 million (whichever is higher) data protection compliance is now a board-level issue with real implications for those not prepared. GDPR comes into effect May 2018, which means that organisations must be preparing for compliance now according to business needs, as they occurred, with multiple databases instances of various versions.

5 Key Questions

Effective compliance starts with knowing what personal data you have, how it flows, and how it leaves your enterprise.

Five simple questions can indicate the impact that GDPR will present to your organization.

- What EU resident personal data do we already hold?
- How sensitive is it?
- Are we able to perform an effective **Data Protection Impact Assessment (DPIA)** as recommended by GDPR?
- How does data flow through-out the organisation and outside it?
- How is it used or shared?

Get visibility and an action plan for compliance

Many enterprises simply do not know where their data is, and with the cloud and data sharing so prevalent, this issue is expanding daily. The Atos GDPR Data Risk Assessment is a software-driven assessment that answers these 5 essential questions, providing you with a clear understanding of your GDPR data protection risks. It is particularly beneficial in completing the mandatory data protection impact assessment GDPR requires, and includes recommendations on what data protection procedures and controls you need. After completing the assessment, you will be positioned to understand what steps you need to take to meet the data protection principles of GDPR.

Atos uses Digital Guardian's data protection platform to perform the assessment. The software is deployed as a virtual appliance. It can be installed and operational quickly, typically less than an hour. The full assessment can be executed in two weeks and requires minimal customer resources.



The Atos DPIA & Data Risk Assessment

Stage 1: Understand Where Personal Data Resides - Data at Rest Risk Analysis

This analysis includes discovering EU residents' personal data across your network shares, databases and cloud storage repositories. This analysis discovers and fingerprints common GDPR data patterns and detects this data either on site or in the cloud.

Digital Guardian's threat aware data protection platform scans repositories to identify:

- Personal data types
- Sensitivity levels of the data
- Which repositories contain sensitive data.

Stage 2: Understand How Data Flows - Data in Motion Risk Analysis

This analysis identifies how EU residents' personal data flows and how it leaves your organisation. This analysis uses the same data patterns and fingerprints used in the Data at Rest Risk Analysis and identifies:

- Personal data types in motion
- Sensitivity levels of the data in motion
- Channels by which personal data is leaving your network, e.g. web or email.

Stage 3: Understand Your Next Steps - Report and Recommendations

Once these two analyses are complete Atos will provide you with the data and insights you need to determine where you're most at risk and what your next steps should be. The deliverables in stage 3 include:

- Executive Summary of risks
- Detailed data analysis report
- In-depth review of findings
- Data protection strategy recommendations.

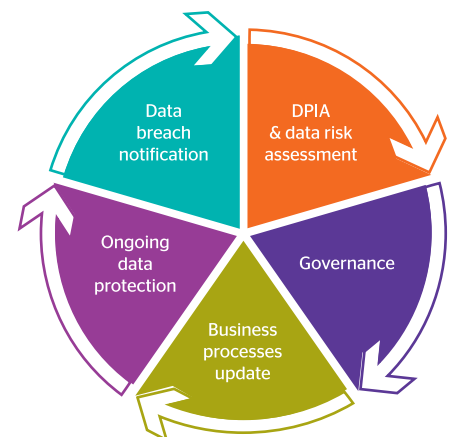
Upgrade to the Atos Data Privacy By Design Framework for Rapid Compliance and Increased Confidence.

It is easy to upgrade from the initial Risk Assessment to an ongoing managed security service ensuring GDPR compliance on an ongoing basis



Meet the GDPR Protection Principles with Atos Data Privacy by Design Framework

- **DPIA & Data Risk Assessment:** Gain clear visibility of where your sensitive data is, and how it is being used and shared both inside and outside your company. An assessment of the likelihood and severity of risk including the measures, safeguards and processes to be used for mitigating risk and ensuring personal data protection
- **Internal and external governance:** Extending from the DPO to external partners and suppliers, ensuring all meet GDPR obligations
- **GDPR Business Process Update:** Including updates of legal forms for consent, erasure, and modifications; cross service delivery processes for IT, security and privacy (DPO)
- **Ongoing Data Protection:** Deploy Digital Guardian DLP, Evidian Identity & Access Management & TrustWay Encryption. With Atos 24/7 SOC/CERT services on alert to detect any misalignment with GDPR regulation & potential threats to data privacy
- **Data Breach Notification:** Based on Bull advanced analytics, compliance is measured and documented continuously, enabling 72 hour breach notification.



DPIA: Data Protection Impact Assessment

Three non-limitative situations in which a DPIA is required (article 35, 3° of the GDPR):

- (1) an automated processing of personal aspects relating to the data subject which have legal effects on him or her or similarly significantly affect him or her,
- (2) processing on a large scale of sensitive data or of personal data relating to criminal convictions and offences or,
- (3) a systematic monitoring of a publicly accessible area on a large scale.

About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of over € 12 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies and industry knowledge, Atos supports the digital transformation of its clients across all business sectors. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, Unify and Worldline. Atos is listed on the CAC40 Paris stock index.

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

Let's start a discussion together



About Digital Guardian

Digital Guardian provides the industry's only data protection platform that is purpose-built to stop data theft from both insiders and external adversaries. The Digital Guardian Data Protection Platform performs across the corporate network, traditional endpoints, and cloud applications. It's buttressed by the DG Cloud, a big data security analytics backend that sees and blocks all threats to sensitive information. For more than 15 years, it has enabled data-rich organizations to protect their most valuable assets with a choice of on premises, SaaS or managed service deployment.

Digital Guardian's unique data awareness, combined with threat detection and response, enables organizations to protect data without slowing the pace of their business.

Find out more about us
digitalguardian.com

For more information: marketing@atos.net

Atos, the Atos logo, Atos Syntel, Unify, and Worldline are registered trademarks of the Atos group. February 2019. © 2019 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.