GDPR COMPLIANCE OVERVIEW

protiviti®
Face the Future with Confidence

An EU Data Regulation Requirement

What is GDPR?

The General Data Protection Regulation (GDPR) was adopted on April 27, 2016, to replace the European Union's 1995 Data Protection Directive (DPD). **GDPR goes into effect May 25, 2018** and will be immediately enforced as law in all member states of the European Union. This updated legislation provides a unified set of rules designed to give European citizens more control over their private information across all digital forms. The key driver for this change is increased risk of exposing EU citizen data through increased use of mobile devices, adoption of big data analytics, and increased volumes of personal data being digitally generated, processed and shared across the globe.

Key Considerations

Does GDPR apply to you?

- The scope of the new regulation has been extended to ALL organizations collecting and processing personal data of individuals residing in the EU, regardless of the company's physical location.

Why comply with GDPR?

- Failure to comply will result in fines up to **4% of global revenue** or **$20 million** (whichever is higher).

Do you know your data?

- GDPR reinforces an organization's need to possess a heightened awareness of the personal data being collected and accountability for how such data is generated, processed, and stored.
- Organizations must also have a firm understanding of how their vendors handle their data.

Are you able to support the Data Subject's Rights, if enforced?

- GDPR provides data subjects with a set of privacy rights that can be enforced against an organization that processes their personal data. These rights may limit your organization's ability to lawfully process personal data, and may significantly impact your current business model.

What is GDPR Personal Data?

GDPR defines Personal Data as any information relating to any person (data subject) who can be identified, directly or indirectly, in particular by reference to an identifier. **The including of publicly available information (name and address) and common technical data (MAC addresses and Cookies) introduces new scope that companies need to be aware of.**

Examples of GDPR Personal Data

- Name
- Address
- Phone Number
- Email Address
- Passport Number
- Financial & Bank Info
- Date of Birth
- Healthcare Data
- Biometric Data
- Employee ID
- IP Address (static or dynamic)
- Mac Address
- Cookies
- GPS Data
- Financial & Bank Account Info

GDPR COMPLIANCE OVERVIEW

protiviti®
Face the Future with Confidence

An EU Data Regulation Requirement

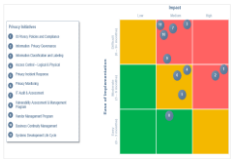
Key GDPR Requirements

Breach Notification	Requirement to report Privacy breaches to the regulator within **72 hours** and potentially to the data subject.
Privacy By Design & By Default	Firms must consider privacy at the start of any new project and ensure that the right security controls are in place throughout all development phases.
Data Subject's Rights	New rights include the right to be forgotten, right to data portability, and the right to object to profiling.
Consent	Requirement to gain unambiguous consent (i.e. explicit).
Data Protection Officer (DPO)	DPO required for 'government bodies' and organizations conducting mass surveillance or mass processing of Special Categories of data.

How Protiviti Can Assist

0 Discovery & Planning

Inventory of GDPR Data sources with their Criticality Template

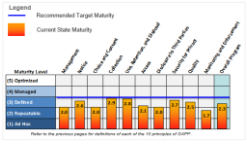


1 Current State

Current State Analysis

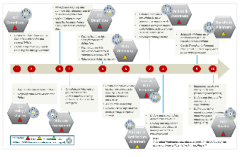
2 GDPR Gap Analysis

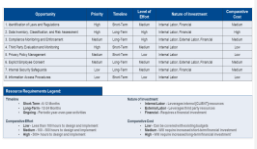
GDPR Gap Analysis Results



3 Compliance Roadmap

Compliance Roadmap & Supporting Report





4 Gap Remediation

Remediate & Implement Solutions