General Data Protection Regulation Compliance

Allow our security specialists to help you with GDPR compliance

General Data Protection Regulation (GDPR) is an overarching regulation for organizations that process EU citizen data either outside and/or inside of the EU to protect the data of those individuals. It is important to note that this regulation does not supersede national law, but adds to it. GDPR requires that if you process data on EU citizens, no matter your geographical location, you must comply with this regulation.

GDPR Assessment Methodology:

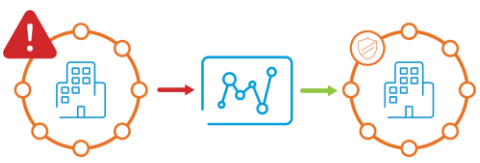
To prepare, we provide a phased approach that incorporates GDPR's core requirements.

Phase one: Know the data. Map out data flows of personal data within the organization.

Phase two: Conduct an assessment against the GDPR requirements.

Phase three: Take the information that was learned from the assessment and build a program. Our managed security team will provide policies, services, and Data Protection Officers, who ensure an entity's compliance.

Phase four: Ongoing testing, operating, and managing of the GDPR programmed approach. This includes conducting regular penetration testing, table top breach exercises, and having the right elements in place to help detect a breach.



As part of regulation under GDPR, you are required to disclose any personal data breaches within 72 hours of detection to a regulator.

If your organization is infringing that can result in a fine up to 20 million euros, or 4% of your company's global annual turnover from the previous year –whichever is greater.

Whether your organization is in need of filling a temporary vacancy or providing continuous expert advice, AT&T Cybersecurity Consulting is your extended arm and resource to help pursue strategies that best suit your organization.

AT&T Business

	GDPR Compliance Requirements	AT&T Security Solutions
Prevent	• Data Protection Impact Assessment	• Data Privacy • Risk-Based Security Assessment Services
	• Determine software vulnerabilities	• Application Security Testing • Vulnerability Scanning Service (VSS)
	• Comply with main data quality principles • Implement appropriate protection • Advisory and development services	• GDPR Gap Analysis • Data Classification • Security Strategy and Roadmap Service
Detect	• Near-time analysis to help detect and respond to a breach	• TMLA (Threat Manager - Log Analysis)
	• Storage for system logs in preparation for an audit	• Threat Manager
	• Provides protection and support of consistent security policies	• Premise/Network-Based Firewall • Cloud Web Security Services (CWSS) • DDoS Defense
Respond	• Incident Response planning and analysis • Forensic Retainer Services • Data Breach Simulations	• Incident Response Plan Development • Incident Response Plan Testing • Incident Response Retainer Services • Forensic and Electronic Discovery

People — Process — Technology

GDPR Compliance Action Plan:

Gap Assessment

Assessing your organization's readiness begins with learning the scope of the impact. If you are processing this data you must know where PII data is, why you have it, how you are using it, who is accessing it, how it is being protected, and be able to demonstrate this to an external regulator to comply. Utilizing the GDPR Readiness Assessment can guide you through the core requirements.

Privacy Impact Analysis

GDPR requires you to conduct PIAs (Private Impact Assessment) for "high risk" activities which could potentially cause serious harm. Being continuously proactive will allow your organization to implement components with long-term timelines and collect data inventory that can be mapped to comply with Article 30.

Incident Response and Notification

When your organization is processing personal data, it is vital that it is processed appropriately. GDPR contains a section on breach notifications as well. If your organization is breached, an efficient incident response plan should be in place to handle the breach and help limit further damage.