FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Tripwire and GDPR

Achieve Compliance Using Foundational Controls

The recently-enacted European Union General Data Protection Regulation (GDPR) requires organizations to take adequate measures to ensure the security and privacy of personal data of any European citizen. This supersedes the previous Data Protection directive. As a regulation—as opposed to a mere directive—it directly imposes a uniform data security law regime on organizations that need to comply.

MAKING COMPLIANCE COMPELLING

> *The hefty fines and penalties for infringement not only encourage accountability, they may be the single most eye-catching feature of the Regulation, causing multinationals and local companies to invest more in compliance.*
>
> **— IAPP-Top 10 Operational Impacts of the GDPR: Part 10 — Consequences for GDPR Violations**

Who Needs to Comply?

The GDPR is explicit on who needs to comply: the regulation states any organization touching and managing (collects, stores, processes and/or shares) the personal data of EU individuals. Personal data includes "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." This is an extensive definition. For IT professionals, this could include MAC or IP addresses. Essentially, those who must comply are any data owners ("Data Controllers") and data processors. This has a global reach, for affected organizations do not need to be located in Europe.

Why Should You Care?

Data breaches alone can impact your customer base and drive negative publicity with long-lasting effects. The financial consequences of failing to comply with the GDPR are also steep, with fines of up to 20 million euro or 4% of global annual turnover. Interestingly, in the Ovum research report, *Data Privacy Laws*: *Cutting the Red Tape*, two-thirds of the respondents say they expect the legislation to force changes in their European business strategy.

Planning for Compliance

While organizations have some controls in place to secure their data, many are not prepared for GDPR. In research from before implementation and enforcement, over two thirds of IT professionals surveyed say they need to invest in new technologies or services to help prepare their business for the impact of GDPR. This compliance standard touches across all departments and personnel. Planning for GDPR compliance should start right away by assessing the current situation and the gaps that exist. For more advice on how to get started, read Tripwire white paper "*Getting Up to Speed on GDPR.*"

How Tripwire Can Help

Tripwire is a leading provider of foundational controls for compliance, security and IT operations. GDPR requires that organizations implement adequate security measures to protect EU citizens' data. Tripwire's comprehensive foundational security controls deliver capabilities that are essential to the standard of adequate protection, including automation and integration to enhance the operational efficiency of these controls and maintain a high integrity state.

Tripwire makes demonstrating compliance with GDPR easy. Implementing the controls isn't enough. You also have to be able to continuously demonstrate compliance. Tripwire can assess compliance of systems against these standards, and provide audit-ready reporting. Tripwire can do so continuously, so you're always prepared for an audit. Organizations can be confident, knowing that Tripwire already has a solid compliance track record with standards like PCI DSS, NERC, NIST and many others. Tripwire's integrated solutions portfolio includes file integrity monitoring, configuration management, asset discovery, vulnerability management, and log collection. These capabilities support popular industry-standard frameworks like the Center for Internet Security (CIS) Controls and ISO/IEC 27001/27002.

Much of GDPR requires visibility and monitoring of assets. Tripwire delivers continuous monitoring of cyber assets. Tripwire offers the ability to discover data that is not encrypted or identify unknown assets and their vulnerability and risk levels. Tripwire also offers audit trails to assist with investigations and to remediate back to pre-attack status.

Tripwire Responds to GDPR Requirements

Article	Tripwire Response	Tripwire Enterprise	Tripwire IP360	Tripwire LogCenter
Article 25 (page 48) *Data protection by design and by default* "2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."	Tripwire can *support* this requirement by identifying and alerting on system changes that might affect what data is processed.	Supports		Supports
Article 30 (page 50) *Records of processing activities* "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility."	Tripwire® LogCenter® can collect logs from the systems processing data to comply with this requirement.			Provides
Article 32 (page 52) *Security of processing* "1. .....shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: ...... (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"	Tripwire's suite of products provides the ability to measure and manage risk, ensuring confidentiality, integrity and availability. When applied to processing systems, Tripwire can monitor systems against security policies, identify and track vulnerabilities, and provide the ability to investigate activity through log data.	Provides	Provides	Provides
(a) the pseudonymisation and encryption of personal data;				Validates

Tripwire Responds to GDPR Requirements

Article	Tripwire Response	Tripwire Enterprise	Tripwire IP360	Tripwire LogCenter
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	Tripwire's suite of products provides the ability to measure and manage risk, ensuring confidentiality, integrity and availability. When applied to processing systems, Tripwire can monitor systems against security policies, identify and track vulnerabilities, and provide the ability to investigate activity through log data.	Provides	Provides	Provides
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;	By baselining systems and tracking their changes, Tripwire Enterprise can be used to more effectively bring systems back online after an outage. Tripwire Enteprise customers can review how a deployed system has changed in production in order to ensure that restored backups meet operational requirements.	Supports		
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Tripwire IP360™ can be used to identify vulnerabilities in processing systems. Tripwire Enterprise can be used to identify security related misconfigurations in processing systems.	Provides	Provides	
Article 35 (page 53) *Data protection impact assessment* "7. (d) he measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."	By identifying where data exists using asset tags, Tripwire Enterprise can assist organizations efforts to assess the impact of security mechanisms and measures.	Supports		
Article 39 (page 56) *Tasks of the data protection officer* "1. The data protection officer shall have at least the following tasks: … (b) to monitor compliance with this Regulation, …"	Tripwire Enterprise and Tripwire LogCenter can provide data and reports to validate that appropriate security measures have been put in place and continue to operate.	Validates		Validates
Article 57 (page 68) *Tasks* "Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: … (h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;"	Tripwire products can provide a wealth of information for investigations. Tripwire Enterprise can provide detailed data about how assets have changed. TripwireIP360 can detail how assets are and were vulnerabile, as well as software inventory information. Tripwire LogCenter can provide a history of an assets activity in log events for detailed investigations.	Supports	Supports	Supports
Article 59 (page 70) *Activity reports* "Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). …"	The results from Tripwire's suite of products can be used to contribute to an annual report. Contributions would include evidence of infringements, supporting data for investigations, and validation of compliance.	Supports	Supports	Supports

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.