DATA SHEET

Total Security Management GDPR Compliance Guide

Beginning on May 25th 2018, all organizations within the European Union (EU) and organizations doing business within the EU will need to meet the General Data Protection (GDPR) compliance. GDPR was designed to create a unified security framework and set up principles to protect the personal data of European citizens. Any organization that handles Personal Identifiable Information (PII) must follow these guidelines to prevent unauthorized distribution of EU citizen data. Non-compliance will result in fines of up to $20 million or 4% of an organizations revenue.

The GDPR is a collection of 11 chapters, 99 articles, and 173 focused on increasing privacy through organizational best practices and secure network architectures. A key component of this compliance is on the role of the data controller and the data processor. Per the GDPR, the 'controller' is defined as the person, authority, agency, or other body that determines why and how personal data is processed. The 'processor' is defined as the person, authority, agency, or other body that processes personal data on behalf of the controller. The controller is responsible for implementing effective measures to ensure privacy and compliance with GDPR. They are also responsible for demonstrating that the processor acting on their behalf is following those measures. Both the controller and the processor must maintain an accurate record of all activities involving the processing of personal data, including what type of data is being processed, why it is being processed, who it is being shared with, how long the data is being retained, and how the data is being protected. The GDPR can be summarized into a few key principles:

- Personal data should be processed lawfully, fairly, and transparently
- Personal data should only be collected for specific, explicit, and legitimate purposes
- Data processing should not exceed what is

necessary to satisfy the given purpose
- Data Controllers must ensure that information remains accurate and valid
- Personal data should not be kept longer than what is necessary to satisfy the given purpose
- All personal data should be processed in a manner that ensures security and confidentiality
- Organizations must be able to demonstrate compliance

RackFoundry TSM helps organizations meet these principles by including several key security tools within a singular platform. Specifically, RackFoundry TSM helps address the below articles within the GDPR:

GDPR Article	Recital	Example of how RackFoundry TSM Helps
Chapter 4: 3		
Article 24: Responsibility of the controller	1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	This article refers to having appropriate technical controls in place to detect and prevent cybersecurity threats. RackFoundry TSM helps address this control by including the following essential cybersecurity tools: • Security Information Event Management (SIEM) • Log Manager • 4 Threat Intelligence Feeds • Vulnerability Scanner • File Integrity Monitoring (FIM) • Intrusion Prevention System/Intrusion Detection System (IPS/IDS) • Web Application Firewall (WAF) • Asset Inventory and Discovery • Stateful Firewall • VPN • Behavioral Monitoring • Compliance Reporting • 24/7 Security Operations Center (SOC)
Article 25: Data protection by design and by default	2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's	Continuous network monitoring and anomaly detection helps users track personal data and detect if it is made accessible without approval by the data subject. RackFoundry TSM stores an accurate audit log of the collection and processing of personal data for further review.

GDPR Article	Recital	Example of how RackFoundry TSM Helps
	intervention to an indefinite number of natural persons.	
Article 29: Processing under the authority of the controller or processor	1. The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	RackFoundry TSM stores an accurate audit log of the processing of personal data to help enforce this article.
Article 32: Security of processing	1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: a. the pseudonymisation and encryption of personal data; b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 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; d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is	RackFoundry TSM's SIEM provides real time threat intelligence to detect cybersecurity threats and notify users to facilitate rapid remediation. Vulnerability Scanning and Asset Inventory tools help users asses the security posture of their environment and identify and address vulnerable areas before a breach occurs. RackFoundry's IPS, WAF, and Stateful Firewall protect the boundary against cybersecurity threats that could affect the confidentiality, integrity, and availability of personal data. RackFoundry's VPN ensures the encryption of personal data in transit. RackFoundry TSM's SIEM and Behavioral Monitoring tools monitor user activity and network traffic for unauthorized access to personal data, changes to account privileges, and unusual user activity.

GDPR Article	Recital	Example of how RackFoundry TSM Helps
	required to do so by Union or Member State law.	
Article 33: Notification of a personal data breach to the supervisory authority	1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. 2Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. 3. The notification referred to in paragraph 1 shall at least: a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; c. describe the likely consequences of the personal data breach; d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.	RackFoundry TSM helps users comply with this article of GDPR by providing continuous network monitoring, real time threat detection, and automated alert notifications. 4 threat intelligence feeds provide advanced event correlation to identify security breaches during the early stages and help mitigate any effects of the compromise. Alert notifications summarize threat information including threat description, affected devices, compromised data, threat severity, time/date of breach, and remediation procedures. This helps users notify the appropriate independent public authorities when a breach does occur. RackFoundry's 24/7 Security Operations Centers (SOC) helps triage security incidents, assess severity, and determine appropriate remediation procedures. RackFoundry's Vulnerability Scanner and perimeter protection tools (IPS, WAF, Stateful Firewall) help minimize cybersecurity breaches.
Article 34: Communication of a personal data breach to the data subject	1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	RackFoundry's SIEM supports forensic investigations to help users assess threat severity and appropriate actions that may be required. RackFoundry's SOC provides rapid forensic analysis and alert notifications for critical/high risk cybersecurity threats. This helps users notify the involved data subject without undue delay.

GDPR Article	Recital	Example of how RackFoundry TSM Helps
Article 35: Data protection impact assessment	1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.	RackFoundry TSM's Vulnerability Scanner helps users assess their processing environment for cybersecurity risks. Asset Discovery scans help users identify network assets to better understand where personal data is being processed and associated risks.
Chapter 5: Transfers of personal data to third countries or international organizations		
Article 44: General principle for transfers	1. Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.	RackFoundry TSM helps organizations abide to this article by monitoring network traffic and notifying users of possible transfers of personal data, especially international transfers.

As you can see, RackFoundry TSM addresses several articles within GDPR. With its layered approach to network security, TSM combines essential threat detection and prevention tools such as SIEM, Web Application Firewall (WAF), File Integrity Monitoring (FIM), Vulnerability Scanning, and IDS/IPS. Furthermore, RackFoundry's Security Operations Centers (SOC) is staffed 24/7/365 to provide continuous network monitoring and security expertise. Overall, RackFoundry TSM provides the needed visibility and prevention to ensure the highest level of security for compliance.

About RackFoundry

RackFoundry, the maker of Total Security Management (TSM), is a leader in complete coverage security appliances, secure cloud services and professional services such as SecurityXpert that provides security expertise to organizations of all sizes and industries. The RackFoundry security team, FortressLabs™, help find new vulnerabilities in the wild, mitigate any found vulnerabilities, and head up the RackFoundry Security Operations Center.

For more information visit us at www.rackfoundry.com.