COMPLIANCE

General Data Protection Regulation (GDPR) and Rocket Servergraph

The General Data Protection Regulation (GDPR) that goes into effect on May 25 2018 is designed to "harmonize" data privacy laws across Europe and give individuals greater protection and rights. GDPR drives sweeping changes for the public and for organizations that handle Personally Identifiable Information (PII). The regulation gives individuals new powers over their data, with enhanced rights to access, rectify, and erase it, and the ability to freely request the transfer of their information to other platforms. Along with data subjects' increased rights to control their information, GDPR also mandates technical security controls to protect the confidentiality, availability, and integrity of individuals' data: 'Data protection by design and by default'.

You cannot achieve full compliance with GDPR solely through technical means. The regulation's scope is broad, encompassing organizational, procedural, and technical security requirements. Rocket® Servergraph helps you comply with the GDPR requirements surrounding personal data confidentiality, integrity, and availability by giving you tools to ensure these principles apply consistently throughout your backup environment. The specific GDPR security controls and specifications, along with the GDPR articles they satisfy, are described below. However, GDPR compliance will ultimately depend on an effective implementation of these capabilities, as well as other organizational and procedural controls to address all GDPR articles.

Article 5: Principles Relating to Personal Data Processing

GDPR REQUIREMENTS	ROCKET SERVERGRAPH CAPABILITIES
1.e Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’).	Rocket Servergraph only collects metadata, not the actual data being backed up. This minimizes the storage of personal data to be protected.
1.f Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').	Servergraph collects information from backup software, hardware, and processes in your environment to provide evidence that data backups are operating in accordance with your organizational policies. Traps, reports, and alerts capture relevant information for all your backup systems—including processing errors—to ensure the completeness, accuracy, and integrity of data stored in backups.
2 The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).	Backup collection logs and reports are retained within Servergraph for a fully configurable duration to maintain historical evidence of the controls, and to provide accountability for all related activities.

Article 25: Data Protection by Default and by Design

GDPR REQUIREMENTS	ROCKET SERVERGRAPH CAPABILITIES
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 intervention to an indefinite number of natural persons.	Servergraph only collects metadata, not the actual data being backed up. This minimizes the storage of personal data to be protected. The Servergraph administration platform’s detailed, configurable user access permissions support the rule of least privilege, limit unauthorized access to backup configurations, and prevent modification of storage destinations that could affect data subjects’ confidentiality.

Article 32: Security of Processing

GDPR REQUIREMENTS	ROCKET SERVERGRAPH CAPABILITIES
1.b 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 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.	Servergraph supports unique user IDs for all individuals accessing the system, and uses LDAP integration with Active Directory credentials to ensure access security and confidentiality for all systems and data with which Servergraph interacts. Detailed, customizable permissions can be configured for each user to support the rule of least privilege and segregation of duties. Servergraph is agentless and merely requires a read-only service account to operate, preventing unintentional or unauthorized modification of network systems and data.

Article 32: Security of Processing - continued

GDPR REQUIREMENTS	ROCKET SERVERGRAPH CAPABILITIES
	System administration is performed through the separate administration client, with access restricted to designated administrative users. The Server Monitor feature shows real-time statistics and alerts for backup systems, such as storage utilization and disk capacity, ensuring that these systems will be available and operating in the event of a business continuity incident. Servergraph reports can alert you to any processing errors that could impair the completeness, accuracy, or integrity of data stored in backups.
1.c 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 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.	Servergraph collects information from backup software, hardware, and processes in your environment to provide evidence that data backups are operating in accordance with your organizational policies, including Recovery Point Objectives (RPOs) and other critical metrics in a data recovery scenario. Servergraph offers dashboards that allow users to monitor the status of your backup systems in real time. Traps, reports, and alerts are customizable to capture relevant information for all your backup control requirements, so you can ensure that each backup job completes successfully to make data available for recovery.

Rocket®

rocketsoftware.com

info@rocketsoftware.com

US: 1 855 577 4323
EMEA: 0800 520 0439
APAC: 612 9412 5400

twitter.com/rocket

www.linkedin.com/company/rocket-software

www.facebook.com/RocketSoftwareInc

blog.rocketsoftware.com