COMPLIANCE

General Data Protection Regulation (GDPR) and Rocket® Mainstar® Backup and Recovery Manager Suite

The General Data Protection Regulation (GDPR) that went into effect on May 25, 2018 is designed to "harmonize" data privacy laws across Europe and give individuals greater protection and rights. GDPR provides for sweeping changes for the public as well as 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, as well as the ability to freely request the transfer of their information to other platforms. Along with the data subjects' increased rights to control their information, the regulation also mandates technical security controls to protect individuals' data confidentiality, availability, and integrity: 'Data protection by design and by default'.

Rocket® Mainstar® Backup and Recovery Manager Suite (BRMS) centralizes your backup and recovery management processes for an IBM® z/OS® environment. Where GDPR requires you to identify all data storage and data flows, BRMS gives you an effective tool to quickly identify where all your critical data is stored and archived. It also provides a powerful tool to ensure the availability of personal data in light of the regulation's data protection requirements.

BRMS security controls and specifications, along with the GDPR articles they satisfy, are described below. However, GDPR compliance cannot be attained solely through technical means. Compliance will ultimately depend on an effective implementation of these capabilities, as well as other organizational and procedural controls to address all articles of GDPR.

Article 5: Principles Relating to Personal Data Processing

GDPR REQUIREMENTS	BRMS CAPABILITIES
1.f Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').	BRMS leverages native IBM z/OS user credentials, authentication, and access rights management functions to restrict access to data and protect the confidentiality of PII. BRMS analyzes your critical datasets to determine whether they're included in your backup processes, or whether they're omitted or outdated, and ensures that they are successfully backed up without errors.
2 The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	During an audit, you must show that your company is compliant. Audit Logging can help. BRMS utilizes native IBM z/OS functions to record all actions within the system. All actions performed through BRMS against backup jobs and datasets, as well as all modifications to user accounts, roles, and assigned permissions, are logged and traceable to individual users executing the function. This provides historical evidence to demonstrate the effective operation of controls protecting the integrity and confidentiality of personal data.

Article 25: Data protection by design and by default

GDPR REQUIREMENTS	BRMS CAPABILITIES
1 Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	BRMS does not directly store PII; it facilitates the effective management of such data in your IBM z/OS and archival environments. This helps you identify all critical data and ensures its integrity and availability. BRMS leverages native IBM z/OS functionality to provide security and confidentiality for the data being processed. User credentials, authentication, permissions, and logging capabilities are inherited from the operating system, allowing your key mainframe logical security controls to extend to the application. BRMS also enhances the capabilities of native ABARS facilities to ensure that restored files cannot have modified security permissions, protecting the confidentiality of data within the restored files.

Article 32: Security of processing

GDPR REQUIREMENTS	BRMS 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 organisational 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.	BRMS leverages your TSO credentials and all associated authentication mechanisms. There is no need to maintain a separate user account list in BRMS. IBM Security Authorization Facility (SAF) provides standard access controls over data based on the TSO login. BRMS security functions validate that the user has SAF rights and cannot bypass mainframe access restrictions. All relevant changes to user accounts, roles, and assigned permissions through the SAF are fully logged through the IBM System Management Facility (SMF). Reporting and alerting on such actions can be configured through the mainframe functions. All actions performed against backup jobs and datasets are traceable to individual users executing the function. Detailed logging is available through the IBM Resource Access Control Facility (RACF).
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 organisational 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.	BRMS performs analysis to identify all critical datasets and determine whether they're included in your backup processes, or whether they're omitted or outdated. BRMS provides a centralized management interface to configure, monitor, and report on the various predefined backup jobs executed by all your backup software for the entire IBM z/OS environment. Interfaces with your backup software allow BRMS to generate backup jobs to cover any missing datasets. Reporting functionality shows the status of each dataset and each backup or restoration task, to ensure successful completion and data integrity. BRMS automatically generates jobs to restore datasets that can be used for periodic testing requirements.

Rocket

rocketsoftware.com
info@rocketsoftware.com
US: 1 877 577 4323
EMEA: 0800 520 0439
APAC: 1800 823 405
twitter.com/rocket
www.linkedin.com/company/rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com