COMPLIANCE

General Data Protection Regulation (GDPR) and Rocket® Mainstar® Catalog RecoveryPlus

The General Data Protection Regulation (GDPR) that went into effect on May 25, 2018 is designed to "harmonize" data privacy laws across Europe as well as give individuals greater protection and rights. GDPR provides for sweeping changes for the public and 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® Catalog RecoveryPlus (CR+) does not directly store or process PII. However, it strengthens your IBM® z/OS® data protection strategy by providing enhanced ICF Catalog management, backup, and recovery capabilities. These are key to ensuring the integrity of data in your mainframe environment, preventing data loss, and quickly and reliably restoring data availability.

Relevant CR+ 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	CR+ 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').	CR+ provides enhanced ICF Catalog management capabilities for your IBM z/OS environment, helping you ensure data integrity and prevent accidental loss. CR+ leverages native IBM z/OS user credentials, authentication, and access rights management functions to restrict access to data and protect the confidentiality of PII. It also expands the native access management capabilities to define additional function-based access controls, enabling you to further protect both the confidentiality and integrity of your data.
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. While CR+ interfaces with ICF catalogs, which are metadata that would not include PII, its administrative functions could impact PII availability and recovery. All relevant actions performed through CR+, as well as changes to user accounts, roles, and assigned permissions, are logged and traceable to individual users executing the function. Reporting and alerting on such actions can be configured through the mainframe functions.

Article 25: Data protection by design and by default

GDPR REQUIREMENTS	CR+ 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.	CR+ does not store or process PII directly, nor does it allow any user access to PII. There is no exposure to confidentiality risk. Because CR+ provides assurance over your data availability requirements, security of the application's administrative functions is critical. The application leverages native IBM z/OS functionality for user credentials, authentication, permissions, and logging capabilities. CR+ also expands on these native capabilities by adding function-level permissions and customizable, role-based permissions management.

Article 32: Security of processing

GDPR REQUIREMENTS	CR+ 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.	CR+ leverages the logged-in user credentials of the native IBM TSO function of z/OS. TSO credentials, and all authentication mechanisms tied to that login, are leveraged by CR+. Detailed, customizable permissions can be configured for each user to support the rule of least privilege and segregation of duties. Permissions can apply to both the data being accessed and the function being performed. IBM Security Authorization Facility (SAF) provides the standard access controls over data. CR+ defines new profiles that add function-based access controls, and supports role-based permissions management for consistent application of user rights. Specific reports are available from the application showing the function-level permissions granted through its access profiles. You can use these to validate the appropriateness of assigned rights.
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	CR+ monitors your ICF catalogs enterprise-wide to verify that they're appropriately backed up and recoverable. It also analyzes your disaster recovery site's ICF catalogs and synchronizes them with your production data. CR+ performs diagnostics of relationships between data sets and ICF catalogs to identify integrity problems that could impair your data recovery capabilities, and automatically generates fix commands. Verifying backup and recoverability status of ICF catalogs in your production and DR environments helps prevent data sets from being destroyed or losing integrity. CR+ also allows routine maintenance of ICF catalogs during operation without outages, reducing downtime and supporting 24x7 high-availability environments.

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