Rocket

COMPLIANCE

General Data Protection Regulation (GDPR) and Rocket MultiValue Databases

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 provides for 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 their data, and the ability to freely request the transfer of their information to other platforms. The biggest change for organizations is the accountability principle (Article 5(2)). It requires companies to implement appropriate technical and organizational measures to protect personal data and maintain relevant documentation of all processing activities.

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 UniVerse, Rocket UniData and Rocket D3, collectively known as the Rocket MultiValue Application Platform (Rocket MV), provide the capabilities you need to fulfill many of these requirements, as described in this document. However, GDPR compliance will ultimately depend on an effective application of these capabilities throughout your product design and implementation, as well as other organizational and procedural controls to address all articles of the regulation.

Article 5: Principles Relating to Personal Data Processing

GDPR REQUIREMENTS	MULTIVALUE CAPABILITIES
1.d Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which it is processed, is erased or rectified without delay (“accuracy”).	Data “accuracy,” where validity is already established, is protected from malicious or unauthorized alteration through role-based, Active Directory-integrated access rights management. Rocket MultiValue can enforce granular write/update access for individual users. OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. This encryption also protects the integrity of data being sent and received to prevent inaccuracies. Parties can be certain they are talking to the intended party, and that data has not been corrupted or maliciously altered during transmission.
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”).	Rocker MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured on a more granular level to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited to authorized users. The operating system performs user authentication and passes it to the database. Rocket MV supports username and password sets from Microsoft and Unix systems, as well as token-based single sign-on (SSO). OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. Open source implementation of the SSL and TLS protocols lets you send and receive encrypted information. When combined with the correct—and validated—certificate, parties can be certain they are talking to the intended party, and that data has not been maliciously changed during transmission. Rocket MV supports robust password and encryption key management solutions for Automatic Data Encryption. Policies can be defined for individual keys. Rocket MV supports the latest implementation of the Transport Layer Security (TLS) encryption protocol, TLS 1.2, for maximum security. Delayed Standby Replication lets you protect a subscriber from malicious damage caused by a compromise to the publisher. Real-time replication may introduce the same damage from the publisher to the subscriber, exposing you to potential data loss. Keeping the subscriber a defined interval behind the publisher (such as six hours) protects the business and assists in addressing “clear record” events. Recoverable File System (RFS) helps maintain physical integrity of data at rest and ensure recovery from hardware failures. Audit logs can provide a secure record of any data access or updates, whether authorized or unauthorized. Audit logging configuration is stored in an encrypted file that can be password-protected, and is only modifiable by authorized users.
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. With Audit Logging, customers can create reports from the audit log to answer questions such as: • Who updated, deleted, or changed an account? • When did a specific user log in or out of an account? • Which users have access to specific data, and when did they access the data?

Article 25: Data Protection by Design and by Default

GDPR REQUIREMENTS	MULTIVALUE 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 organizational measures**, such as pseudonymization, that are **designed to implement data-protection principles**, such as data minimization, 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.	Data "accuracy," where validity is already established, is protected from malicious or unauthorized alteration through role-based, Active Directory-integrated access rights management. Rocket MV can enforce granular write/update access for individual users. OpenSSL-based Automatic Data Encryption protects data in-transit, in-use, and at rest. This encryption also protects the integrity of the data being sent and received to prevent inaccuracies. Parties can be certain they are talking to the intended party, and that data has not been corrupted or maliciously altered during transmission. Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured granularly to support your confidentiality requirements and protect sensitive information. Information-access and disclosure is limited to authorized users.
2 The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed. That obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility. In particular, such measures shall ensure that by default personal data is not made accessible without the individual's intervention to an indefinite number of natural persons.	Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured granularly to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited to authorized users.

Article 30: Records of Processing Activities

GDPR REQUIREMENTS	MULTIVALUE CAPABILITIES
1.c Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain a description of the categories of data subjects and of the categories of personal data.	Metadata concerning data subjects can be stored in any product designed and produced using Rocket MV (and subsequently retrieved therefrom) through the inclusion of an appropriate data-field associated with the subject's record. Audit logging can be configured to record any updates to the metadata associated with data subjects, and can be used to generate reports.
1.g Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain, where possible, a general description of the technical and organizational security measures.	Rocket Software technical security documentation for its Rocket MV products will help you describe the technical security measures protecting your data.
3 The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	Audit logs produce an electronic copy of the records and processing activities required by this article. Rocket Software technical security documentation surrounding Rocket MV is available in electronic format.
4 The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.	Rocket MV can fulfill this requirement for all data stored within the database through appropriately designed queries and reports of a data subject's records. Processing activities surrounding a data subject's records can be evidenced through audit logs and reported on to show all access to and modification of such records.

Article 32: Security of Processing

GDPR REQUIREMENTS	MULTIVALUE CAPABILITIES
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:	
1.a the pseudonymization and encryption of personal data;	OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. This encryption also protects the integrity of data being sent and received to prevent inaccuracies. Parties can be certain they are talking to the intended party, and that data has not been corrupted or maliciously altered during transmission.
1.b the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured on a more granular level to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited to authorized users. The operating system performs user authentication and passes it to the database. Rocket MV supports username and password sets from Microsoft and Unix systems, as well as token-based single sign-on (SSO). OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. This encryption also protects the integrity of the data being sent and received to prevent inaccuracies. Parties can be certain they are talking to the intended party, and that data has not been corrupted or maliciously altered during transmission.
1.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;	Delayed Standby Replication lets you protect a subscriber from malicious damage caused by a compromise to the publisher. Real-time replication may introduce the same damage from the publisher to the subscriber, exposing you to a potential for data loss. Keeping the subscriber a defined interval behind the publisher (such as six hours) protects the business and assists in addressing ‘clear record’ events. Recoverable File System (RFS) helps maintain physical integrity of data at rest and ensures recovery from hardware failures. Rocket MV provides account backup and restore utilities that can assist with the restoration of a database to its last known good state.

Article 33: Notification of a Personal Data Breach to the Supervisory Authority

GDPR REQUIREMENTS	MULTIVALUE CAPABILITIES
3.a Notification of a breach provided to a supervisory authority shall 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.	Detailed audit logging and reporting capabilities let you determine exactly what records were accessed, when, and by whom. This will aid in a forensic investigation into the extent of a data breach and the number of affected records. Audit logging configuration is stored in an encrypted file that can be password-protected, and is only modifiable by authorized users.
5 The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects, and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.	Audit logs and reports can provide documented evidence supporting your breach reporting actions, and allow supervisory authorities to verify compliance.

Article 34: Notification of a Personal Data Breach to the Data Subject

GDPR REQUIREMENTS	MULTIVALUE CAPABILITIES
3.a Notification of a personal data breach to the data subject shall not be required if the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.	OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. Access to database files or their storage media by an unauthorized party without encryption keys will not result in a breach. Rocket MV supports the latest implementation of the Transport Layer Security (TLS) encryption protocol, TLS 1.2. Data intercepted in transit will be unintelligible to any unauthorized party.

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/comp rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com