



COMPLIANCE

General Data Protection Regulation (GDPR) and Rocket BlueZone

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® BlueZone is designed to minimize regulatory exposure to GDPR's articles, while providing strong, built-in technical capabilities that allow you to easily conform to applicable articles. The specific BlueZone 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

1.d

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').

ROCKET BLUEZONE CAPABILITIES

Rocket BlueZone provides communication between clients and back-end mainframe systems by utilizing user access permissions inherent to the back-end mainframe environment. BlueZone cannot provide any capability for data access that is not already specifically authorized within your mainframe O/S to the logged-in user.

All data transfers to and from the mainframe environment are encrypted to protect against unauthorized access to the data in transit, or disclosure of user credentials that could be utilized for unauthorized system access.

Article 30: Records of Processing Activities

GDPR REQUIREMENTS

1

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- b) the purposes of the processing;
- c) a description of the categories of data subjects and of the categories of personal data;
- d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
- e) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- f) where possible, the envisaged time limits for erasure of the different categories of data;
- g) where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

ROCKET BLUEZONE CAPABILITIES

The built-in logging mechanisms inherent to your mainframe environment record all activities initiated through BlueZone sessions. These logs may include all the necessary information, depending on your configurations. There is no need to maintain a separate log management function specifically for BlueZone.

As a supplemental logging mechanism, Rocket® BlueZone Web records a log of all client connections to the web server. This does not record commands issued through the sessions, which would be logged through built-in mainframe functionality, but provides an additional layer of security by showing which endpoints are connecting, when, and from what source.

Article 32: Security of Processing

GDPR REQUIREMENTS

1.a

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 pseudonymisation and encryption of personal data.

ROCKET BLUEZONE CAPABILITIES

BlueZone products support state-of-the-art encryption methods for all communications between clients and the back-end mainframe environment, including TLS1.2 and SSHv2 protocols with FIPS-compliant encryption algorithms.

BlueZone Web applies this level of encryption to both the end user-to-web server session, and the web server-to-mainframe session.

While support for older protocols is available to be used for legacy systems, this support can be disabled entirely to prevent any potential security vulnerabilities.

In environments where the mainframe cannot support encrypted sessions, the optional Security Server allows for plain text communications to be isolated within a secure, local network with mainframe, while applying strong encryption methods to all external connections with clients.



Article 32: Security of Processing - continued

GDPR REQUIREMENTS

ROCKET BLUEZONE 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.

BlueZone leverages the built-in authentication mechanisms and user access permissions schemas within your mainframe environment, and can support multifactor authentication methods. There is no need to maintain a separate access rights management function for BlueZone, as your existing mainframe controls will apply.

BlueZone also offers optional X.509 certificates to authentication endpoint devices attempting to connect to the mainframe.

Encryption of all data in transit to and from the mainframe prevents unauthorized access through eavesdropping, and protects the administrative credentials used to establish sessions.

Encryption of data in transit also protects data integrity, preventing technical errors, corruption, or malicious alteration in transit that could impair data accuracy and reliability.

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.

The distributed nature of BlueZone architecture lets administrators connect to the mainframe environment from anywhere to perform routine maintenance or emergency corrections. During a technical incident or disaster scenario, BlueZone can help continue or restore operations and data access.


BlueZone clients can specify alternate hosts for instant cut-over to disaster recovery facilities.

BlueZone Web can support redundant web servers to withstand a technical incident and continue operating in other environments, while allowing administrators from any location to continue working.



 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](https://www.linkedin.com/company/rocket-software)

 [www.facebook.com/
RocketSoftwareInc](https://www.facebook.com/RocketSoftwareInc)

 blog.rocketsoftware.com