COMPLIANCE

General Data Protection Regulation (GDPR) and Rocket API

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. One of the biggest changes 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. For GDPR requirements concerning the security and integrity of electronic data, Rocket® API is designed to help your systems comply with the relevant standards. Rocket API will enable you to maintain compliance with the requirements listed below.

Article 5: Principles Relating to Personal Data Processing

GDPR REQUIREMENTS	ROCKET API CAPABILITIES
1.d Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').	All data transfers using Rocket API are secured through encrypted protocols, including TLS1.2 and SSHv2. These protocols ensure the integrity of the data being transferred, to prevent technical errors or malicious interference.
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; ('storage limitation').	Rocket API does not by default store any data involved with API calls, limiting the storage of such data. Customers can cache common API calls for performance reasons. This cached data is retained in memory only, not written to any permanent storage mechanism. It is erased when the Rocket API service is stopped, or at preconfigured time intervals. Rocket API supports data masking and anonymization capabilities to limit the exposure of data in a personally identifiable form.
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').	All data transfers using Rocket API are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for data security and confidentiality. The encryption protocols also ensure the integrity of data being transferred, to prevent technical errors or malicious interference. Rocket API leverages access credentials from the back-end mainframe operating system, inheriting all access rights and restrictions associated with those credentials. These include read and write capabilities. In addition to access rights controlled through the back-end mainframe, Rocket API provides application-layer security that can further restrict API calls by user, by function, and by data being accessed. Data transfers are strictly between the back-end mainframe and the front-end system calling the API. There is no capability for data to be leaked, forwarded, or otherwise redirected through Rocket API. Audit logging functionality can record all API calls, showing details of the user accessing the function, data being accessed, and data values being read and/or written. The Rocket Access and Connectivity Hub (RACH) management interface, which manages the inventory of APIs and deployment to API gateways, enforces granular user access controls that are configurable by each customer. RACH uses LDAP authentication to leverage the password controls and other mechanisms that authenticate your users. RACH audit logging records all user activity within the application—including uploading and deployment of compiled APIs as well as administration of the application itself— providing individual accountability for all access and activity.
2 The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	Audit logging functionality can record all API calls, showing details of the user accessing the function, data being accessed, and data values being read and/or written. RACH audit logging records all user activity within the application—including uploading and deployment of compiled APIs as well as administration of the application itself—providing individual accountability for all access and activity.

Article 25: Data Protection by Design and by Default

GDPR REQUIREMENTS	ROCKET API 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, which 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.	Rocket API supports data masking and anonymization capabilities to limit the exposure of data in a personally identifiable form. All data transfers using Rocket API are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for data security and confidentiality. The encryption protocols also ensure the integrity of data being transferred, to prevent technical errors or malicious interference. Rocket API leverages access credentials from the back-end mainframe operating system, inheriting all access rights and restrictions associated with the credentials. These include read and write capabilities. In addition to the access rights controlled through the back-end mainframe, Rocket API provides application-layer security that can further restrict API calls by user, by function, and by data being accessed.
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.	Rocket API leverages access credentials from the back-end mainframe operating system, inheriting all access rights and restrictions associated with the credentials. These include read and write capabilities. In addition to the access rights controlled through the back-end mainframe, Rocket API provides application-layer security that can further restrict API calls by user, by function, and by data being accessed. Data transfers are strictly between the back-end mainframe and the front-end system calling the API. There is no capability for data to be leaked, forwarded, or otherwise redirected through Rocket API.

Article 32: Security of Processing

GDPR REQUIREMENTS	ROCKET API 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;	Rocket API supports data masking and anonymization capabilities to limit the exposure of data in a personally identifiable form. All data transfers using Rocket API are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for data security and confidentiality.
1.b The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	Rocket API leverages access credentials from the back-end mainframe operating system, inheriting all access rights and restrictions associated with the credentials. These include read and write capabilities. In addition to the access rights controlled through the back-end mainframe, Rocket API provides application-layer security that can further restrict API calls by user, by function, and by data being accessed. The Rocket Access and Connectivity Hub (RACH) management interface, which manages the inventory of APIs and deployment to API gateways, enforces granular user access controls that are configurable by each customer. RACH uses LDAP authentication to leverage the password controls and other mechanisms that authenticate your users.

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

GDPR REQUIREMENTS	ROCKET API CAPABILITIES
3.a [Notification of a personal data breach to the supervisory authority] shall at least 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.	Audit logging functionality can record all API calls, showing details of the user accessing the function, data being accessed, and data values being read and/or written. This would serve as a formal record of the nature and extent of a breach involving API calls. RACH audit logging records all user activity within the application—including uploading and deployment of compiled APIs as well as administration of the application itself—providing individual accountability for all access and activity.

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

GDPR REQUIREMENTS	ROCKET API 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.	All data transfers using Rocket API are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for data security and confidentiality, rendering it unintelligible to unauthorized persons. Rocket API supports data masking and anonymization capabilities to limit the exposure of data in a personally identifiable form.

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