COMPLIANCE

General Data Protection Regulation (GDPR) and Rocket® LegaSuite

The General Data Protection Regulation (GDPR) goes into effect on May 25, 2018 and is designed to “harmonize” data privacy laws across Europe as well as give greater protection and rights to individuals. GDPR provides for sweeping changes for the public as well as organizations that handle Personally Identifiable Information (PII). Individuals are given new powers over their data, with enhanced rights to access, rectify and erase their data as well as being able to freely request the transfer of their information to other platforms. The biggest change for organizations is the accountability principle (Article 5(2)), which requires companies to implement appropriate technical and organizational measures to protect personal data and to maintain relevant documentation of all processing activities.

Full compliance with GDPR cannot be achieved solely through technical means. The scope of the regulation is broad, encompassing a number of organizational and procedural requirements in addition to technical security requirements. For GDPR requirements concerning the security and integrity of electronic data, Rocket LegaSuite is designed to function in manner that allows your systems to comply with the relevant standards. LegaSuite will enable you to maintain compliance with the requirements listed below.

Article 5: Principles relating to personal data processing

GDPR REQUIREMENTS	LEGASUITE 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’).	Data storage and management exists within the underlying application systems, not within LegaSuite. However, LegaSuite overlays your application to enhance the user experience and facilitate the entry and updating of personal data to maintain its accuracy over time. LegaSuite also provides data entry configuration capabilities, such as data value restrictions and drop-down menu forms, which can help to ensure the accuracy of data being entered by users and prevent technical or clerical errors. All data transfers using LegaSuite are secured through encrypted protocols, including TLS1.2 and SSHv2. These protocols ensure the integrity of the data being transferred, ensuring the continuing accuracy of data within the system by preventing 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’).	LegaSuite does not store or cache data, limiting exposure to potential breaches.
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 LegaSuite are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for security and confidentiality of the data. The encryption protocols also ensure the integrity of the data being transferred to prevent technical errors or malicious interference. LegaSuite leverages user credentials, access rights, and authentication mechanisms defined by your host system O/S, extending those security controls to your web platform. LegaSuite also supports single sign-on authentication. Credentials are transmitted in encrypted form. LegaSuite provides configuration options that can further limit data values and form types presented to end users. This can be used to provide additional confidentiality for sensitive data and to protect the integrity of data in the system from invalid inputs. Any changes to LegaSuite data presentation configurations must be developed and compiled through your IDE; they cannot be edited directly within a LegaSuite production environment. This prevents accidental or unauthorized changes that could impair the integrity of data input or presentation.

Article 25: Data protection by design and by default

GDPR REQUIREMENTS	LEGASUITE 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.	All data transfers using LegaSuite are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for security and confidentiality of the data. LegaSuite leverages user credentials, access rights, and authentication mechanisms defined by your host system O/S, extending those security controls to your web platform. LegaSuite also supports single sign-on authentication. Credentials are transmitted in encrypted form. LegaSuite's data presentation configuration options can support masking and pseudonymization of sensitive data, as well as additional data access restrictions.
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.	LegaSuite's data presentation configuration options can restrict the data available to end users in various use cases in your web platform, enhancing built-in host system access rights to specifically enforce confidentiality restrictions based on the method of the data access.

Article 32: Security of processing

GDPR REQUIREMENTS	LEGASUITE CAPABILITIES
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 pseudonymization and encryption of personal data.	LegaSuite's data presentation configuration options can support masking and pseudonymization of sensitive data, as well as additional data access restrictions. All data transfers using LegaSuite are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for security and confidentiality of the data.
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.	LegaSuite leverages user credentials, access rights, and authentication mechanisms defined by your host system O/S, extending those security controls to your web platform. LegaSuite also supports single sign-on authentication. Credentials are transmitted in encrypted form. LegaSuite provides configuration options that can further limit data values and form types presented to end users. This can be used to provide additional confidentiality for sensitive data and to protect the integrity of data in the system from invalid inputs. Any changes to LegaSuite data presentation configurations must be developed and compiled through your IDE; they cannot be edited directly within a LegaSuite production environment. This prevents accidental or unauthorized changes that could impair the integrity of data input or presentation.

Article 34: Notification of a personal data breach to the data subject

GDPR REQUIREMENTS	LEGASUITE CAPABILITIES
3 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 LegaSuite are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for security and confidentiality of the data, rendering it unintelligible to unauthorized persons. LegaSuite's data presentation configuration options can support masking and pseudonymization of sensitive data, limiting its exposure in an identifiable format.

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