

COMPLIANCE

General Data Protection Regulation (GDPR) and Rocket® Aldon Lifecycle Manager

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. Along with increased rights of the data subjects to control their information, the regulation also mandates technical security controls to protect the confidentiality, availability, and integrity of individuals’ data: ‘Data protection by design and by default’.

In typical implementations, personal data would never be stored within Rocket Aldon Lifecycle Manager directly. However, the scope of the regulation is broad, encompassing a number of organizational and procedural requirements in addition to technical security requirements, and the development of applications that store or process personal data directly impacts your overall ability to comply. Aldon Lifecycle Manager’s robust controls surrounding security, system development, and process management provide a strong foundation for GDPR compliance at your organization.

The specific Aldon Lifecycle Manager 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 articles of GDPR.





Article 5: Principles Relating to Personal Data Processing

GDPR REQUIREMENTS	ROCKET ALDON LIFECYCLE MANAGER CAPABILITIES
<p>1.f</p> <p>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').</p>	<p>Although Rocket Aldon Lifecycle Manager (IBM i Edition – LMi) and Rocket Aldon Lifecycle Manager (Enterprise Edition – LMe) do not directly store personal data, their role in the development of products that do is crucial to your ability to comply with GDPR and its concept of 'privacy of design'.</p> <p>Both products provide detailed, granular access rights management capabilities which allow you to specify individuals with read and write capabilities throughout the software and all development, test, and production environments that it touches.</p> <p>SDLC process controls, combined with the access rights management capabilities, allow you enforce segregation of duties and independent validation controls, ensuring the integrity and security of code developed to support the storage and processing of personal data.</p>
<p>2</p> <p>The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').</p>	<p>During an audit, you must show that your company is compliant. Audit logging can help. Customers can create reports from the audit log to answer questions which might arise, such as:</p> <ul style="list-style-type: none">• 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? <p>All actions within Aldon LMi and LMe and their associated modules, including code changes and promotions as well as administrative maintenance, are fully logged and reportable. This provides historical evidence to demonstrate the effective operation of controls protecting the integrity and confidentiality of personal data.</p>



Article 25: Data protection by design and by default

GDPR REQUIREMENTS	ROCKET ALDON LIFECYCLE MANAGER CAPABILITIES
<p>1</p> <p>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.</p>	<p>Aldon LMi and LMe would not typically store identifiable personal data, minimizing the volume and locations of data to be protected.</p> <p>In any circumstances where personal data is entered into Aldon Lifecycle Manager, all data transfers to and from the system are encrypted using state of the art protocols and ciphers to protect its confidentiality and integrity.</p>
<p>2</p> <p>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.</p>	<p>Access to personal data is restricted by permissions, and an audit trail provides all necessary information for compliance. This also reduces the risk that malicious code could be added to production systems that store personal data.</p> <p>Aldon LMi and LMe and their associated modules (Rocket Aldon Community Manager (CM) and Aldon Security Service Manager) support unique user IDs for all individuals accessing the systems.</p> <p>Administration of users and their roles is performed through the separate Security Service Manager module. Roles are customizable to meet an organization's specific controls requirements. Access to sensitive data and the environments that may house it can be restricted to the specific individuals who require such access.</p> <p>Individual user accounts and strong authentication requirements ensure that assigned permissions effectively protect sensitive data. Passwords are required for users to access each system. Aldon LMi also supports integration with IBM i user credentials, and Aldon CM supports LDAP integration with Active Directory credentials.</p>



Article 32: Security of processing

GDPR REQUIREMENTS

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.

ROCKET ALDON LIFECYCLE MANAGER CAPABILITIES

Although Rocket Aldon Lifecycle Manager (IBM i Edition – LMi) and Rocket Aldon Lifecycle Manager (Enterprise Edition – LMe) do not directly store personal data, their role in the development of products that do is crucial to your ability to comply with GDPR and its concept of ‘privacy of design’.

To protect the security and confidentiality of all data and code development, Aldon LMi and LMe and their associated modules (Aldon CM and Aldon Security Service Manager) support unique user IDs for all individuals accessing the systems.

Passwords are required for users to access each system. Aldon LMi also supports integration with IBM i user credentials, and Aldon MC supports LDAP integration with Active Directory credentials.

Detailed, customizable role-based access levels allow an organization to define the exact capabilities of each system user. Permissions are granular to support any organization’s business needs according to the rule of least privilege and segregation of duties.

Access to view or modify data is restricted to users specifically authorized within that development release and environment.

To ensure the security and integrity of code development, Aldon CM supports workflows for changes and development activities, which may include requests, approvals, testing, acceptance, and any other stages required by an organization’s policies.

Changes made to code are highlighted by the Aldon Harmonizer application, which supports formal, independent reviews of code changes before promotion to ensure that changes are in accordance with an approved work order.



 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