COMPLIANCE

# General Data Protection Regulation (GDPR) and Rocket® OpenTech

The General Data Protection Regulation (GDPR) that went into effect on May 25, 2018 was designed to "harmonize" data privacy laws across Europe as well as give individuals greater protection and rights. GDPR provides for sweeping changes for the public and 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, as well as the ability to freely request the transfer of their information to other platforms. Along with the data subjects' increased rights to control their information, the regulation also mandates technical security controls to protect individuals' data confidentiality, availability, and integrity: "Data protection by design and by default."

GDPR requires that you protect your PII from loss, destruction, or other unavailability, all while maintaining security and confidentiality. Rocket® OpenTech products give you the ability to do that. They provide you with all the tools you need to implement a strong backup management program and availability controls for your entire IBM® z/OS® environment—from executing backup and migration jobs, to monitoring job statuses, to simulating restoration events, and more. The Rocket OpenTech portfolio includes Rocket DR/Xpert, Rocket DASD Backup Supervisor, Rocket Tape/Copy, Rocket Virtual Data Recovery, and Rocket CopyExport Manager.

Relevant OpenTech security controls and specifications, along with the GDPR articles they satisfy, are described below. However, GDPR compliance cannot be attained solely through technical means. 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 | OPENTECH CAPABILITIES |
|---|---|
| 1.f<br>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'). | OpenTech products provide a robust suite of tools to protect your PII against accidental loss or destruction.<br><br>All OpenTech products leverage native IBM user credentials, authentication, and access rights management functions to restrict access to data and protect the confidentiality of PII. |
| 2<br>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. Audit Logging can help. OpenTech products use native IBM functions to record all actions within the system. All actions performed through OpenTech products against backup jobs and datasets, as well as all modifications to user accounts, roles, and assigned permissions, are logged and traceable to individual users executing the function. This provides historical evidence to demonstrate the effective operation of controls protecting the integrity and confidentiality of personal data. |

## **Article 25:** Data protection by design and by default

| GDPR REQUIREMENTS | OPENTECH CAPABILITIES |
|---|---|
| 1<br>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. | DR/Xpert helps analyze your production batch jobs and datasets to automatically identify those that are critical, and continuously monitors for changes. Datasets identified as critical can be compared to your Data Protection Impact (DPIA) Assessment to ensure that all your high-risk PII is covered in your backup processes. DR/Xpert can then ensure that these critical datasets have current backed-up or mirrored datasets available.<br><br>All OpenTech products leverage native IBM z/OS functionality to provide security and confidentiality of the data being processed. User credentials, authentication, permissions, and logging capabilities are inherited from the operating system, allowing your key mainframe logical security controls to extend to the application.<br><br>DR/Xpert, DASD Backup Supervisor, and Tape/Copy also leverage the Integrated Cryptographic Services Facility (ICSF), and can also support RSA encryption, to protect backup data during transit between storage locations. |

## **Article 32:** Security of processing

| GDPR REQUIREMENTS | OPENTECH CAPABILITIES |
|---|---|
| 1.b<br><br>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. | OpenTech products leverage the logged-in user credentials of the native IBM TSO function. TSO credentials, and all authentication mechanisms tied to that login, are inherited by OpenTech products.<br><br>IBM Security Authorization Facility (SAF) provides standard access controls over data based on the TSO login. OpenTech product functions validate that the user has SAF rights and cannot bypass mainframe access restrictions.<br><br>While certain features such as the Tape/Copy tape browse function allow access to data within backup volumes, this access is still restricted by the SAF permissions for the logged-in user.<br><br>All relevant changes to user accounts, roles, and assigned permissions through the SAF are fully logged through the IBM System Management Facility (SMF). Reporting and alerting on such actions can be configured through the mainframe functions.<br><br>All actions performed through OpenTech products against backup jobs and datasets are traceable to individual users executing the function. Detailed logging is available through the IBM Resource Access Control Facility (RACF).<br><br>DR/Xpert centrally manages your backup utilities (such as Tape/Copy) to generate backup jobs automatically, along with restoration jobs for when they're needed, and integrate them with your job scheduling.<br><br>It also helps you identify all critical data, or enables you to view data by other categories such as department or application in accordance with your DPIA, to ensure that adequate backups are being performed on the selected data.<br><br>DASD Backup Supervisor continuously monitors for new or modified volumes and maintains backup jobs to ensure that they are reliably backed up.<br><br>Tape/Copy executes the backup process from tapes to other media, and builds in error reporting and recovery features to ensure all your data volumes remain intact.<br><br>For data volumes in your virtual tape library, Virtual Data Recovery automatically detects data differentials and backs them up for archival to a consolidated medium for efficient storage and restore ability. |

## **Article 32:** Security of processing

| GDPR REQUIREMENTS | OPENTECH CAPABILITIES |
| --- | --- |
| 1.c<br><br>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 restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. | DR/Xpert provides facilities in the event of a disaster recovery incident for managing restoration tasks, and allows prioritization of recovery according to your RTOs. Combined with the storage and recovery efficiency features of other OpenTech products, this enables you to minimize system downtime in a recovery event.<br><br>DASD Backup Supervisor generates automated recovery jobs associated with its backup tapes to be stored alongside the data. This allows for quick, simple, and efficient restoration in a test or a real disaster recovery scenario.<br><br>DR/Xpert monitors backup data for all critical datasets to ensure you are within your Recovery Point Objective (RPO) windows. |



Rocket

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