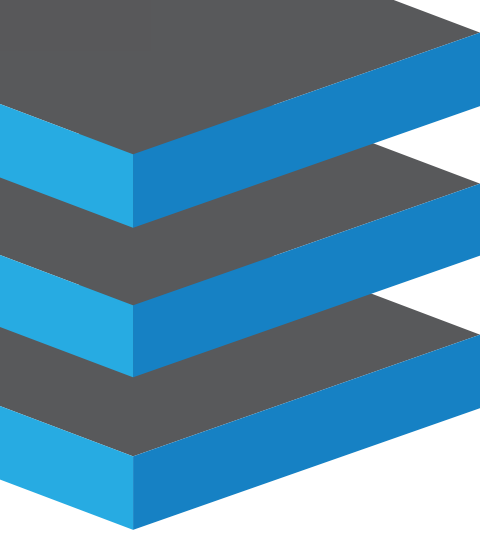

Supporting GDPR on the IBM i

Contents

Overview

The General Data Protection Regulation (GDPR) is an upcoming Regulation (EU) 2016/679 of The European Parliament and the Council of the European Union. It is about giving individuals ('natural persons') control over information concerning them ('personal data') and the protection of that information with respect to processing and movement of data. It was adopted on April 27, 2016 and comes into force on May 25, 2018.

The reform is seen as an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the "Digital Single Market".

A European parliament "regulation" is a binding legislative act. It must be applied in its entirety across the EU. A "directive" is a legislative act that sets out a goal that all EU countries must achieve. Member States are under an obligation to update their legal frameworks to conform to Directive (EU) 2016/680 by May 6, 2018. . However, it is up to the individual countries to devise their own laws on how to reach these goals.

Non-compliance can lead to penalties including fines. Penalties can be severe: failure to protect data can in certain cases result in fines of up to million Euro or 2% of the world wide revenue of the organization involved.

Who Does it Apply To?

The regulation applies to two categories of organization:

Controllers: Organizations of any kind or individuals that transmit, maintain, or process personal information.

Processors: Organizations of any kind or individuals that "process personal data on behalf of the controller. For example if personal data is stored or transmitted through a system under your control you are a Processor. Or if you provide personal information to other organizations likes third party IT service providers or organizations that host their own clouds you are a Processor.

Fines

Non-compliance can lead to penalties including fines. Penalties can be severe: failure to protect data can in certain cases result i fines of up to million Euro or 2% of the world wide revenue.

The Purpose of This Document

The paragraphs of the GDPR cover a range of subjects including the kind of data that may be processed, the providing of access to individuals regarding their data and other procedures, and additionally refers to the protection of data.

The purpose of this document is to pinpoint the appropriate sections of the regulation that relate to data protection and to illustrate the functions of Enforcive/Enterprise Security that can help achieve it.

This document will therefore not cover procedural obligations such as lawfulness of processing, the type of data processed, place of processing, agreement by the individuals whose data is processed and the like.

The Regulation

The GDPR is structured in 173 'recitals' that set out the reasons for the contents of the enacting terms (i.e. the articles), followed by 99 articles. Of these, 13 recitals and 11 articles mention or imply the need for data protection technologies, which can be grouped into the following categories:

- Protection of Data
- Privacy and Confidentiality of Data
- Integrity of Data
- Encryption and Pseudonymization
- Access Control, Malicious and Accidental Damage
- Compliance to Regulations
- Risk Assessment
- Logging and Auditing
- Security Settings and Policy

Section in GDPR	Category
Recital (6)	Protection
Recital (7)	Protection
Recital (15)	Protection
Recital (28)	Encryption
Recital (39)	Privacy, Access control
Recital (49)	Damage, Integrity, Access control
Recital (71)	Privacy, Risk
Recital (78)	Compliance, Encryption
Recital (83)	Risk, Encryption, Damage, Privacy, Integrity, Access Control
Recital (84)	Risk
Recital (87)	Settings, Log/Audit
Recital (90)	Risk, Settings, Protection, Compliance
Recital (108)	Protection
Recital (162)	Access Control
Article 5 1(f)	Integrity, Privacy, Damage
Article 6 4(e)	Encryption
Article 24	All categories
Article 25	Protection, Encryption, Access Control
Article 28	All categories
Article 30	Log/Audit, Security settings
Article 32	Risk, Encryption, Integrity, Security settings, Damage, Privacy, Access Control
Article 34	Encryption
Article 35	Risk, Settings
Article 47	Integrity, Protection
Article 71	Security Settings

Figure 1: Original Sections of the GDPR and Their Corresponding Categories

Protection of Data

Protection of data is expressly mentioned or strongly implied in recitals 6, 7, 15, 90, and 108; and in articles 24, 25, 28, and 47, in which the regulation mandates technical and organizational measures shall be employed to implement data protection policies. The responsibility for data protection falls on both the controller and the processor (see definitions in Who Does it Apply To?. Techniques and data protection principles mentioned to achieve the protection of data included pseudonymization, purpose limitation, data minimization, limited storage periods and data quality.

Enforcive/Enterprise Security contains a range of functions that address the requirement of data protection including:

- Application Access Control including File Protection
- Encryption
- Firewall and IP Packet Filtering
- Session Timeout

Privacy and Confidentiality of Data

The privacy or confidentiality of data is mentioned or strongly implied in recitals 39, 71 and 83; and in articles 5, 28 and 32 in which the regulation states the requirement for preventing unauthorized disclosure of or access to such data and that personal data should be processed in a manner that ensures appropriate security and confidentiality using appropriate technical or organizational measures. The most prominent functions of Enterprise Security the help achieve this are:

- Encryption
- Session Timeout
- Application Access Control including File Protection

Integrity of Data

Data integrity comes up in recitals 49 and 83; and in articles 5, 32 and 47. Among the references is the requirement to incorporate technical measures to ensure integrity and to protect personal data against accidental loss destruction or damage. The issue of integrity is addressed through both audit/alerting and also protection measures Enterprise Security functions that help maintain the integrity of data are:

- Application Access Control including File Protection and Application Audit
- Central Audit consolidates logs from different audit sources - Exit Points, QAUDJRN, File Journal, SQL statements, etc.
- Alert Center
- Report Generator
- File Audit

Encryption and Pseudonymization

The need for encryption and pseudonymization is referred to repeatedly in the GDPR regulation, appearing in recitals 28, 78 and 83; and articles 6, 25, 32 and 34. Enterprise Security's Encryption module contains the capability of addressing both of these approaches. It can physically encrypt selected database fields using a secured multi-part key and one of many encryption algorithms or a field can be masked or scrambled - two techniques for providing applications with replacement characters or digits in one or more positions, which is the requirement of pseudonymization. It is also possible to combine both techniques, i.e., field encryption with masking or scrambling. In addition, the update function for field can be denied to users based on role.

Access Control, Malicious and Accidental Damage

Access Control is a central component of any data protection requirement and can be considered an implicit part of it. In addition to this however, a number of explicit references to access control exist in the GDPR, in recitals 39 49, and 162; and article 25 where technical and organizational measures are mentioned for ensuring that personal data is accessible for processing only when necessary. This implies access control with respect to when, where and two whom access to the data is allowed. Access Control can be implemented, based on need to know. A similar strategy is adopted to prevent both intentional and unintentional damage Enterprise Security features access control in a preventative capacity in the following:

- Policy Compliance Manager (checks and fixes authorities and system settings)
- Application Access Control including file protection
- Firewall
- Session Timeout

Monitoring and auditing functions for control access are covered in:

- Alert Center
- File Audit
- Report Generator

Compliance to Regulations

While every paragraph in the regulation implicitly mandates compliance and recital 78 mentions the need for appropriate technical and organizational measures to be taken it is recital 90 that talks about assessment of compliance with the regulation. The Enterprise Security features that help demonstrate compliance are:

- Policy Compliance Manager (checks and fixes authorities and system settings)
- Application Access Control including File Protection
- Central Audit consolidates logs from different audit sources
- Cross Platform Audit consolidates logs from multiple IBM i servers/LPARs into a single repository located on a dedicated server

Risk Assessment

Recitals 71, 83, 84, and 90; and articles 32 and 35 refer to risk assessment, including the measures taken against risks, as a necessary step in determining the level of security required. To this end the stand-alone Enforcive Security Risk Assessment product can be run to provide a comprehensive report of the risks in the system.

Logging and Auditing

Article 30 - 'Records of processing Activities' mandates maintaining a record of processing activities and this is requirement is addressed by the many audits operating in Enterprise Security. That includes the Central Audit, the built-in audit in the firewall and the Report Generator.

Security Settings and Policy

Articles 30, 32, 35, and 71 relate to the maintenance and reporting of a security policy and an assessment of that policy. The Policy Compliance module, stand-alone Security Risk Assessment and Report Generator are the main tools that address this requirement.

GDPR Category	Enterprise Security Function									
	Compliance	Application Access Control	Encryption	Central Audit	Firewall	Session Timeout	Security risk assess-ment	Alert Center	Report Generator	File Audit
Protection of Data		✓	✓		✓	✓				
Privacy / Confidentiality			✓			✓				
Integrity of Data		✓		✓				✓	✓	✓
Encryption / pseudonym-isation			✓							
Access Control, Malicious / Accidental Damage	✓	✓	✓	✓	✓	✓		✓	✓	✓
Compliance to Regulations	✓		✓	✓						
Risk Assessment							✓			
Logging and Auditing				✓	✓				✓	✓
Security Settings and Policy	✓						✓		✓	

Figure 2: Enterprise Security Functions Mapped to GDPR Regulation Categories

Description of Enterprise Security Functions

The Enterprise Security Product is comprised of the security-related main functions listed below:

1 - Policy Compliance Manager
2 - Application Access Control including file protection
3 - Encryption
4 - Central Audit including audits from all sources - system, history, SQL and more
5 - File Audit
6 - Firewall and IP Packet Filtering
7 - Session Timeout
8 - Security risk assessment
9 - Alert Center
10 - Report Generator

1. Policy Compliance Manager

Description
A template-based tool to create and document a security policy for your organization. Once defined, the policy or template can be checked against the actual definitions in the system. The check produces a report showing any deviations from your policy template(s). After checking the deviations, you have the option of aligning the actual definitions in the system with the specified policy through a fix function.

Architecture
- Different policies possible for different target groups of users and objects. Wide target range possible
- Templates on a local IBM i can be used to check object characteristics on local and remote servers
- Fix option to bring deviations in line with desired policy

Highlights
- Wide scope of IBM i compliance checking capabilities including: Object authority(also IFS), user profiles, system values, TCP/IP port status, authorization lists, object integrity (also IFS), user auditing, object auditing, adopted authority and group members
- Object and IFS file integrity (using MD5 algorithm)
- Cross server/LPAR template definition and deviation reporting
- High granularity in specifying OS parameters

Organizational Benefits
- User-friendly, rapid definition of IBM i security policy
- Takes the "pain" out of regulatory compliance by automating the proof of the existence of controls required by regulations
- Alerts following deviations from policy
- Automatic fix process to restore required policy
- Policies can be run manually or on a scheduled basis
- Implementation of policy on remote IBM i computers

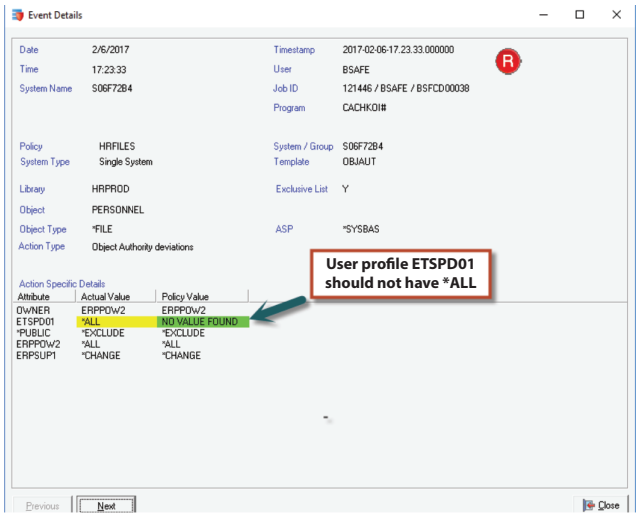

Figure 3: Policy Compliance Manager Event Details

2. Application Access Control

Description
This module provides protection from unauthorized activity coming from the TCP/IP network using tools like FTP, ODBC, JDBC, REMOTE COMMAND, IFS, etc., blocks intruders and malicious users, and reduces the chance of corruption of data.

Architecture
- Permissions definitions via desktop manager
- Activation of protection and auditing is done on the green screen menu
- Server based exit point management using proprietary exit programs

Highlights
- Provides an additional layer of protection on top of the operating system's object authority
- Role Based Management: Defines permissions for most users under a general system policy; users with special requirements are placed in user groups according to role, with the appropriate permissions
- Intuitive: Rapid roll-out of granular permissions by user or group, exit point, function, library and object
- Protection of commands
- Authority swapping – a controlled way of granting elevated authority on a temporary basis
- Simulation mode for safe and phased implementation
- Regulates exit point activity by IP address
- Replication of definitions across servers/partitions

Organizational Benefits
- Supports role based security
- Prevents power user authority misuse
- Protects against data theft, database manipulation
- Protects against tampering with objects
- Prevents authorized users from manipulating data through unauthorized communications channels
- Improves privacy, security and robustness of IBM i
- Facilitates regulatory compliance

Description of the Enterprise Security Functions (continued)

3. Encryption

Description
Enterprise Security Field Encryption is a mechanism that allows encryption and masking of selected fields in an existing information system, without the need to change HLL or CL application programs and without the need to change your database.

Architecture
- The original field value is replaced with a token value (not the encrypted value) with which the system transparently retrieves the encrypted value, stored elsewhere, before decrypting it and making it available to the user
- For v7.1 and higher
- The original field values are encrypted and kept in a separate object
- Decryption will only occur if the user has the required authority.

Highlights
- Role-based key management
- Full or partial masking, by character position
- Two-tier encryption
- Unlimited multiple keys
- User-entered or automatically generated string
- Choice of Encryption Algorithm
- Customer Control of Object Placement
- GUI simplicity for IBM i Server Protection
- User-defined Access
- Can replace Field Masking in versions 7.1 and higher

Organizational Benefits
- High security solution
- Fast and simple
- Answers compliance requirements
- Application Independent
- Integrates with Enterprise Security Manager

4. Central Audit

Description
The Central Audit consolidates events from different logs and journals of a single iBM i server or LPAR into one consolidated log.

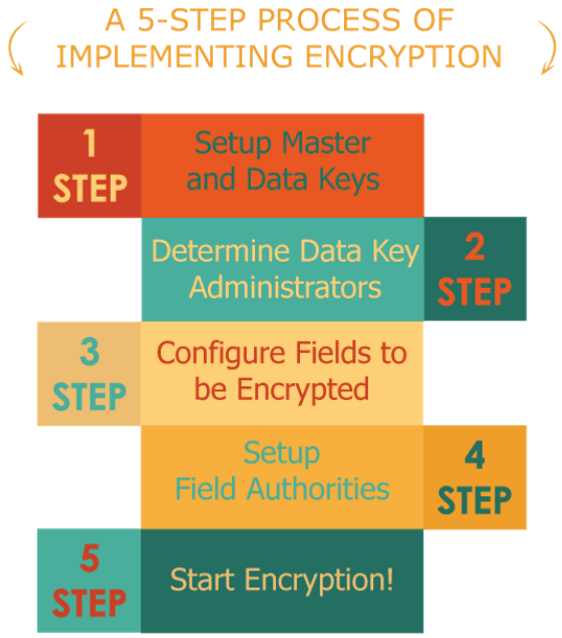

Figure 4: Enforcive Steps to Encryption

Architecture
- A consolidated list of diverse audit events, which have been created in the various auditing modules of the product.
- The data is contained in separate partitions delimited by amount of data or by period

Highlights
- Audit logs covered: Application Audit, System Audit, Message Queue Monitor, History Monitor, File Audit, SQL Statement Audit, Policy Compliance Manager Log, IP packet filtering log, Alerts
- Fine control of audit data collection policy
- Audit event detail specific to event type (access attempt, SQL statement, system event etc.)
- View Data Monitor: Read events at field level
- Administrator Audit: Activity of Enforcive Administrators
- Filtering of diverse audit events on common criteria
- Built-in predefined reports
- Configurable data partition rollover behavior
- IASP library storage option
- Provides for export to CPA or SYSLOG server

Organizational Benefits
- Wide-angled view of security-related system activity
- Filtering of diverse audit events on common criteria
- Makes organizations independent of OS/400 journals by storing relevant events on IBM i even after the journals in which these events were originally captured have been detached
- Meets regulatory compliance requirements
- Improves visibility of security incidents

Description of the Enterprise Security Functions (continued)

5. File Audit

Description
A database integrity mechanism which allows you to monitor changes in the database at the file or field level and provides GUI-based control of file journal management functions.

Architecture
- Proprietary real-time viewing engine for IBM file journal receiver objects
- GUI-controlled journal functions including receiver management and user-defined reports

Highlights
- A visual and intuitive way of tracking changes at field level in the File Journal
- Details of database events including who made the change and with what program
- Before/After images at the field level
- Field values before and after the change
- Rich on-line filtering
- User-defined audit reports
- Receiver management including attachment and deletion

Organizational Benefits
- Easy investigation of file, record, and field changes in the database. Text displayed for action type and group
- An easy-to-use tool for tracking data changes, that doesn't require green screen expertise
- Clearly defined data monitoring controls that help meet compliance demands

6. Firewall

Description
A purpose-built firewall for the IBM i family of servers. Firewall Manager's user-friendly GUI screens make securing your computer's ports a simple admin task.

Architecture
- The protection software resides on the target IBM i computer it is meant to protect
- 1 computer protected per installation
- Definitions made in Enterprise Security Manger
- Control of incoming and outgoing requests handled by exit point architecture

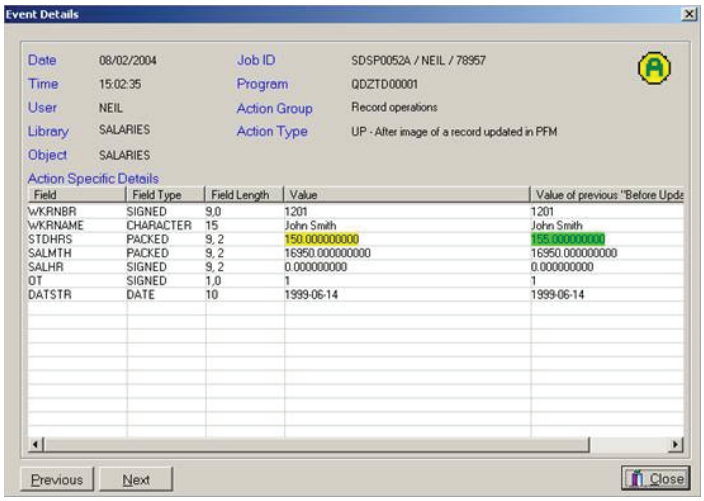

Figure 5: File Audit - After Image of Record Update

Highlights
- Easy to set up and maintain
- Fully integrated into Enterprise Security
- Controls incoming and outgoing network traffic
- Controls the ports permitted to be in listening mode
- Includes audit log of connection attempts
- Rules defined at user and group levels
- Outgoing communication can be conditional according to IBM i user or user group

Organizational Benefits
- A full featured firewall integrated into Enterprise Security
- Simple to set up and maintain

7. Session Timeout

Description
A flexible policy for forcing session timeouts in native, green screen sessions.

Architecture
- Management of session timeout events through a proprietary system of users and groups and operating system parameters

Highlights
- Different session timeout criteria for different user groups (as opposed to the 'one size fits all' option provides in the OS)
- System defaults for users without specific definitions
- Specifying of permitted idle time
- Specifying of action to take when timeout occurs
- Optional sending of message to system administrator

Organizational Benefits
- Allows the organization to easily implement important security best practices, which would otherwise be highly time-consuming tasks

Description of the Enterprise Security Functions (continued)

8. Security Risk Assessment

Description
A tool that reviews and analyzes security settings on IBM i computers and reports strengths and weaknesses and levels of risk.

Highlights
- Port activity map
- Security policy summary
- Password policy summary
- Audit policy summary
- Pinpointing of deviations from recommended values
- Application server protection run-down
- A breakdown of power-users by special authorities
- A management report summarizing vulnerability

9. Alert Center

Description
Rich and unique system of alerts, following a wide range of IBM i system conditions and events. Alert delivery can take a number of different forms including email, on-screen display and others.

Architecture
- Alerting of a variety of events including authorized and non-authorized access at exit point level, compliance checks, system health checks, database field changes, message queue messages and system journal events
- Handling of collected event information by IBM i or by Windows-based alert handler
- Events covered: Exit point, system journal, file journal, message queues, Policy Compliance Manager deviations, SQL Statements

Highlights
- Granular condition definition. Alerts can be conditioned from general to highly specific triggering criteria such as specific SQL statements or FTP sub-functions on a specific library or file
- Multiple alert actions including email, writing to Windows event log, displaying on screen, SNMP traps and output to syslog
- Multiple pro-active alert actions including calling a program, disabling users, changing user authority etc.
- Database field value change alert

Organizational Benefits
- Automatic alerting of breaches
- Fast reaction to security incidents
- Automatic blocking of suspicious users
- More control of events in system
- Meeting of regulatory compliance requirements

10. Report Generator

Description
A tool for the creation of a wide range of security and audit reports. It contains a number of different report templates that define the type of information to display and can be tailored to the information and format you require. It incorporates report management features to run, schedule and view the reports created.

Architecture
- Combination of on-the-fly processing and the use of information collected previously by Enterprise Security
- Definition in GUI, run natively on IBM i

Highlights
- Group definitions using report groups
- Column selection, multiple view definitions
- Scheduling and manual running options
- Main selection criteria tailored to report type
- Flexible filtering on all fields
- Option of adding SQL statement
- Various different export formats including Office (HTML), CSV and PDF
- Varied report types:
- Reports can be defined to run across multiple servers/partitions
- More than 250 predefined reports ready-to-go or samples
- Automatic email send option

Organizational Benefits
- Avoids the need to write custom reports
- Saves time and money

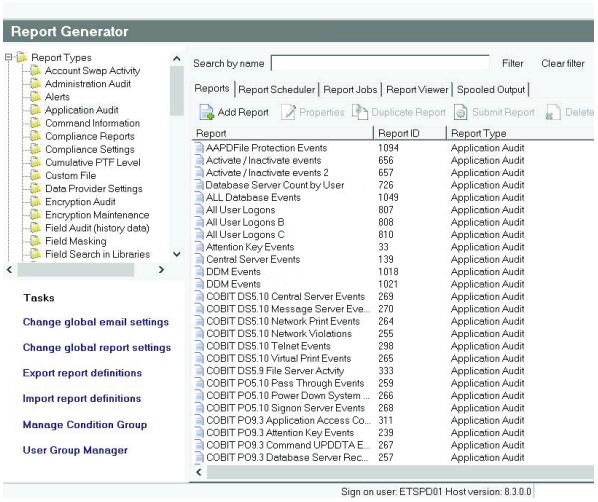

Figure 6: Report Generator's Application Audit Reports

About Enforcive, Inc.
Enforcive provides comprehensive security solutions to help businesses reduce workloads, satisfy auditors and improve responsiveness to security threats. For over three decades, Enforcive has been providing solutions within mission critical environments using platforms including IBM i, System z, AIX, Linux and Windows. Our expertise and commitment to innovation enables us to offer the best of breed solutions to our customers.

Enforcive Enterprise Security™ for IBM i:
Enterprise Security for IBM i is a comprehensive security, encryption and compliance management solution for IBM's Power i (AS400). With intuitive GUI-controlled security, encryption, reporting and compliance modules, this software suite enables system administrators and auditors to easily manage security and compliance tasks efficiently and effectively. Enforcive Enterprise Security has been synonymous with ease of use, providing security and compliance solutions within mission critical environments.

Enforcive, Inc.
www.enforcive.com

North America
Tel: 1-877-237-8024
E-mail: info@enforcive.com

International
Tel: (+972)9-9610400
Email: info-eu@enforcive.com

Enforcive™
Data respected.