syncsort

# Three Imperatives for Keeping IBM i Environments in Compliance with GDPR

KANTION

# Introduction

The European Union's General Data Protection Regulation (GDPR), which begins enforcement on May 25, 2018, is about giving individuals control over their personally identifiable information that is stored, processed and shared by companies, as well as making companies responsible to adequately protect personal data from theft and misuse. But if you think that just because your company doesn't have offices in the E.U. it doesn't need to be concerned with GDPR, think again. GDPR applies to every organization that stores, processes or otherwise uses data relating to E.U. citizens, and there are stiff penalties for non-compliance that can be as high as 4 million Euros or 4% of revenue, whichever is higher.

## GDPR: It's About Respecting and Protecting Personal Data

There is no shortage of information available about GDPR with a multitude of websites and white papers detailing and interpreting the specifics of the regulation. The essence of GDPR boils down to the following requirements for organizations regarding personal data:

- Keep or otherwise use an individual's data only with the consent of the individual and within a specifically defined scope

# Introduction

- Know where each individual's data resides so that it can be identified upon request of the individual or an auditor. Companies must provide an individual with their personal data upon request along with a description of how the data is being used. In addition, an individual may make reasonable requests to have his/her data changed and, in certain cases, have the data deleted (the "right to be forgotten")
- Protect the individual's data from theft or unauthorized access
- Promptly notify individuals, as well as the proper authorities, if an individual's personal data is stolen

## Processes Are as Important as Technologies

Certainly technology plays a critical role in preventing theft or misuse of personal data, and we'll look closely at this in the next section. However, it's important to emphasize that security technologies are only a piece of an overall GDPR-compliance effort. Another significant piece is the implementation of all necessary processes and procedures to meet compliance across your organization. These processes and procedures include (but aren't limited to):

- Defining, disseminating and enforcing clear security and privacy policies
- Keeping proper documentation about how data is used and where data resides in IT systems
- Responding to individuals who request their data
- Obtaining and tracking data-usage permissions

Effectively implementing these policies requires buy-in at the highest levels of management.

# The Three IT Imperatives for Complying with GDPR

Now that you have a gist of GDPR, let's discuss how this relates to the storage and usage of personal data on IBM i environments. The information technology imperatives of GDPR generally fall into three main categories:

1) **Protect data**
2) **Track activity/detect violations**
3) **Assess risks**

## 1 Imperative #1: Protect Data

Data protection is the broadest IT-related requirement that results from the myriad of GDPR regulations. In essence, each company must make a reasonable determination of the data protection measures it needs to implement in light of the sensitivity and potential vulnerability of its data. At minimum this includes preventing an individual's personally identifiable data from being stolen, from being seen by an unauthorized person, or from being used in a way that is out of the scope of an individual's consent.

### The key elements of data protection on IBM i include:

- Global access control - Prevent unauthorized access to systems and data through the comprehensive management of object authorities, network protocols (ODBC, DDM, DRDA, NetServer, TELNET, etc.), open-source protocols (JSON, Node.js, Python, Ruby, etc.), PASE, SQL statements, file opens, command usage, login security and more. This includes the use of technologies that define and manage exit programs, rules-based access requirements, multi-factor authentication, user session timeout, and more.

- Sensitive data protection - Ensure unauthorized individuals are not able to view the contents of sensitive data fields; e.g.: credit card numbers, social security numbers, etc. This is done through encryption, masking or pseudonymization technologies that render these fields unreadable to all but authorized users.

- Elevated authority management – Restrict the use of powerful profiles, therefore eliminating an otherwise significant security vulnerability. In lieu of giving users powerful profiles, it is best to provide users with only the authorities they need to do their jobs, and if a higher authority is required for a task, grant that authority within very specific, time-based parameters. Add-on technologies are essential to streamline this functionality and track all activity under the elevated profile.

# The Three IT Imperatives for Complying with GDPR

## 2 Imperative #2: Track Activity/Detect Violations

GDPR requires that organizations have mechanisms in place to track how personal data is used and how that data is accessed within systems. In addition, organizations must be able to quickly detect and remediate a breach or inappropriate use of an individual's data, then report the extent of that breach in a timely manner should one occur.

### Examples of information that can be tracked with journaling:

- Data changes outside of normal business hours
- Changes to specific fields within the database (credit limits, discount rates, etc.)
- Changes to system values, user profiles, authorization lists, etc.
- Access attempts (authentication and object access)
- Object transfer to production libraries and IFS directories
- Access to, or use of, sensitive files, programs, menus, etc.

### Activity tracking and violation detection on the IBM i is done in a variety of ways:

- System activity log/trace – The most efficient way to log system access and sensitive data activity on the IBM i is to utilize the journaling function that's integrated within the IBM i OS. Journals are reliable, they collect everything within their defined scope, and they cannot be falsified or otherwise manipulated by any user or process. When tracing suspicious activity, add-on technologies are essential to render the cryptic information contained in journals into a readable format. Once this is done it is much easier for administrators and security officers to perform searches on journaled data and to generate actionable reports and violation alerts.
- Policy compliance management – As a means to proactively find IBM i object and configuration settings that may be in violation of your security policies, it is valuable to use technologies that map your security policies across all object and system configuration settings. This allows comparing policies with your settings in order to discover and correct any discrepancies.
- Global access control - The accesscontrol technologies described earlier provide an added benefit when they also include mechanisms that alert administrators and security officers in the event of an access violation, while at the same time tracking all activity of the offending user.

# The Three IT Imperatives for Complying with GDPR

## 3 Imperative #3: Assess Risks

A comprehensive IT security program for IBM i requires proactively taking steps to seek out and address security vulnerabilities through an in-depth risk assessment process. In fact, several provisions within GDPR—as well as within many other compliance regulations—mandate that security risk assessments be performed on a regular basis. In addition, many compliance regulations (not to mention general security best practices) include separation-of-duties requirements, which means assessments must be conducted by a person or process that is independent from the IT staff members that manage or otherwise use the system.

An IBM i security risk assessment should comprehensively analyze security in the designated environment(s), comparing system configurations with known security best practices. The analysis should present a clear picture to management and staff of security vulnerabilities along with specific recommendations for remediation. Some of the key areas of vulnerability on the IBM i that should be addressed by the risk assessment include:

- System values
- Default passwords
- Disabled users
- Command line users
- Distribution of powerful users
- Library authorities
- Open ports
- Exit-point programs

# GDPR as a Competitive Advantage

Instead of looking at GDPR as yet another regulatory burden, it is worth considering it from the perspective of doing the right thing both for individuals and for your business. Once GDPR compliance is fully implemented, the potential benefits to your organization are many:

- Gain the goodwill and trust from customers, prospects, vendors, employees and other constituents when they see that your company is making efforts to respect the privacy and security of their personal information
- Reduce the possibility of fines and lost reputation by implementing robust measures to secure against a data breach
- Improve the quality of your data as individuals take the opportunity to review and update their personal data. To learn more, read the Syncsort eBook, *GDPR and Data Quality*.
- Improve the understanding of each individual's activities and preferences by virtue of having a better view of where all of an individual's data resides across platforms and applications
- Expand business opportunities through partnerships with other companies for whom GDPR compliance is a requirement of their partners.

# Syncsort Can Help

Syncsort and our specialist Partners offer a comprehensive suite of technologies and services for managing security and compliance on IBM i. With best-of-breed technologies and a team of seasoned IBM i security and compliance professionals, we're here to help your organization implement the data protection, activity tracking and risk assessment disciplines it needs to comply with even the most stringent requirements. Syncsort technologies and services include:

- Global Access Control – Secure object authorities, network protocols, open source protocols, SQL statements, file opens, command usage, login security and more
- Sensitive Data Protection – Prevent the unauthorized reading of sensitive data fields through encryption, masking and pseudonymization
- Elevated Authority Management - Restrict the use of powerful profiles through time-based provisioning of authorities for specifically defined tasks, while logging all activity of the elevated user.
- System Activity Log/Trace – Enhance the readability of IBM i journals so it's easier to find and trace suspicious activity and create actionable reports and violation alerts for management.
- Policy Compliance Management - Compare company security policies with IBM i system and object configuration settings to more easily discover and correct discrepancies
- Security Risk Assessment – Proactively identify potential security and compliance vulnerabilities with the help of a Kantion IBM i security expert
- Managed Security Services – Put our experts to work year-round monitoring and optimizing your IBM i security. A range of service levels are available.

To learn more about Syncsort's security technologies and services for IBM i, visit: www.syncsort.com/Assure
For more information on Kantion, visit: www.kantionit.com

## About Syncsort

Syncsort is the global leader in Big Iron to Big Data software. We organize data everywhere to keep the world working – the same data that powers machine learning, AI and predictive analytics. We use our decades of experience so that more than 7,000 customers, including 84 of the Fortune 100, can quickly extract value from their critical data anytime, anywhere. Our products provide a simple way to optimize, assure, integrate, and advance data, helping to solve for the present and prepare for the future. Learn more at syncsort.com.

**www.syncsort.com**

## About Kantion

As a proud Syncsort Partner, Kantion provides data availability and security solutions and services across Asia Pacific, Australia and New Zealand.  Our customers range from the largest banking and financial institutions to small and medium size companies, all benefiting from our 25+ years of expertise.  Learn more at www.kantionit.com or call +61 (0)3 9558 5592.

**www.kantionit.com**