iSecurity

DATASHEET

IBM i GDPR Compliance Simplified

Get ready for May 25, 2018

What is GDPR?

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation that strengthens and unifies data protection for all individuals within the European Union (EU). It is intended to protect personal data and establishes how organizations process, store, and ultimately destroy it when the data is no longer required. The regulation becomes enforceable from May 25, 2018 and affects all organizations, companies and entities worldwide that processes personal data of individuals within the EU. Non-compliance will result in fines of up to EUR 20 million or 4% of the global annual corporate revenue, whichever is greater.

Impact on companies

Data Subject Rights

The GDPR gives individuals the right to request a copy of their personal data, to seek erasure, modification or portability of their data and (in certain cases) withdraw consent/object to certain types of processing activity. EU based organizations will expect systems and processes offered by companies to be designed to help comply with these requirements. Companies should build supporting functionality into systems.

Security Measures

Companies will have direct responsibility to ensure appropriate data security measures are adopted when processing data. Previously this responsibility sat exclusively with the customer (controller), but will now need to be actively managed jointly in co-operation with the customer on a mutually agreed basis.

Record Keeping

Companies must maintain a full record of all ‘processing operations’ which they carry out on behalf of their customer involving the processing of personal data. This means keeping an up-to-date register of services being performed on each category of customer originating data.

Supply Chain Management

Customers will be required to conduct more robust risk assessments before engaging third party providers to process data. They will apply more robust contract protections and conduct regular audits. Companies should be prepared to respond positively to this evolving regime, especially during tender processes and contract negotiations to mitigate risk and create a competitive advantage.

Notification of Data Breach

Companies will be required to notify the customer (controller) ‘without undue delay’ as soon as it becomes aware of a data breach involving loss of personal data. Customers are likely to expand on this in contractual arrangements, to meet their own obligations to notify regulators within 72 hours of a breach.

iSecurity | Your GDPR Solution for IBM i

Table: Mapping Key GDPR Requirements

	ARTICLE	HIGHLIGHTS	DATA SECURITY REQUIREMENTS	iSecurity
ASSESS	Data protection impact assessment *Art. 35 and 84	Assessment of the purpose, scope and risk associated with processing personal data	Inventory of personal data across organization, access rights to data, and risk associated with that access	Assessment Audit Compliance Evaluator Visualizer
PREVENT	Security of processing *Art. 5, 6, 25, 28, 29, 32, 64 and 83	Implement appropriate technical and organizational security controls to protect personal data	• Pseudonymization and encryption • Ongoing protection • Regular testing and verification	Anti-Virus Action Encryption Firewall Authority on Demand Screen
DETECT	Data breach notification *Art. 30, 33 and 34	72 hour notification to Data Protection Authority following discovery of data breach, and notification to affected individuals	Breach report that includes: • what happened • numbers of affected individual • • what data was breached	AP-Journal Audit Action Capture Compliance Evaluator Visualizer

Summary

GDPR will impact much of an organization– from IT, legal, marketing, customer service, to even HR. While the scope of impact may be large, there is still time for you to prepare for the new regulations. iSecurity can help you accelerate compliance with several GDPR obligations, including data subject 's rights, security measures, record keeping, supply chain management, and data breach notification. With iSecurity, you have the visibility into who is accessing what data, and when.

Why Raz-Lee?

Raz-Lee Security is the leader in security and compliance solutions that guard business-critical information on IBM i servers. We are committed to providing the best and most comprehensive solutions for compliance, auditing, and protection from threats and ransomware. We have developed cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

Raz-Lee's flagship iSecurity suite of products is comprised of solutions that help your company safeguard and monitor valuable information assets against intrusions. Our state-of-the-art products protect your files and databases from both theft and extortion attacks. Our technology provides visibility into how users access data and applications, and uses sophisticated user tracking and classification to detect and block cyberattacks, unauthorized users and malicious insiders.

With over 30 years of exclusive IBM i security focus, Raz-Lee has achieved outstanding development capabilities and expertise. We work hard to help your company achieve the highest security and regulatory compliance.