Solution Brief

Protecting Personal Data Under the General Data Protection Regulation?

EU Regulation 2016/679 (the General Data Protection Regulation or the GDPR), which was agreed by the European Union in December 2015, will come fully into force on 25 May 2018. This Regulation will require higher levels of data protection and data security, and companies are expected to implement appropriate technical and organisational measures designed to implement data protection principles in an effective manner.

In the event of serious non-compliance entities will be exposed to fines of up to 20 million Euro or up to 4% of a company's global annual turnover.

Background

The General Data Protection Regulation (GDPR) is a new European Union (EU) regulation that aims to strengthen privacy protection and enhance trust and confidence in how personal data is used and managed. It supplants the existing Data Directive 95/46/EC that has been in place since the mid-1990s and will unify the EU's approach to the processing and transfer of personal data. It is intended to be one of the key regulatory cornerstones for Europe's ambition to be a leading global digital economy. The regulation covers how personal data is gathered, stored, shared, processed and used. Member States and organisations including private and public sector will need to comply by May 2018, when the new regulation will fully apply.

Its main aim is 'to allow people to regain control of their personal data.' The new rules strengthen existing rights and broaden data protection obligations for data controllers (meaning the person who determines the purposes and means of the processing of personal data) and data processors (the persons who process personal data on behalf of a data controller) so that European citizens' personal information is protected—no matter where it is sent, processed, or stored—even outside the EU. For example, every entity that holds or uses personal data in the EU, or which targets the EU for goods, services, or online profiling, will be regulated.

intel Security

The reforms include:

- **Integrity and confidentiality:** Personal data must be processed in a manner which ensures the appropriate security of the data. Controllers will be required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- **Accountability:** Entities must be able to proactively demonstrate compliance with the regulation's data principles.
- **Data breach reporting:** Mandatory breach notifications will have to be made within 72 hours by organisations discovering a personal data breach.
- **Data protection by design and by default:** Data protection safeguards will be built into products and services from the earliest stage of development, and it is likely privacy-friendly default settings will be the norm.
- **Increased visibility of personal data:** Entities must maintain a record of personal data processing activities under their control.
- **Right to data portability:** Individuals, in certain circumstances, will have the right to receive their personal data in a structured, commonly used, machine readable format in order to transmit them to another controller (for example, another service provider).
- **Erasure (commonly referred to as the "right to be forgotten"):** Individuals, in certain circumstances, have the right to request from a controller the erasure of the personal data that is held about them and the controller shall communicate this request to recipients of such personal data.

Intel Security offers a number of leading technology solutions that enable your organisation to improve its overall security posture thereby more effectively protecting its valuable data.

Solutions that save you time and reduce your security and privacy risks

Security and privacy risks can be significantly mitigated by employing effective technology solutions:

Data Loss Prevention

The unauthorized access to, or exfiltration of, your organization's sensitive information can be catastrophic. Our Data Loss Prevention technology provides multi-layered protection for data regardless of where it resides—on the network, in the cloud, or at the endpoint.

Database Security

Our Database Security Products are designed to secure business-critical databases from external, internal, and intra-database threats in real time with no architecture changes, costly hardware, or database downtime required. Our solutions give you visibility into your overall database landscape and corresponding security posture and fully align database internal security policy practices.

Cyber Protection (Threat Defense Lifecycle)
A breach could also be caused by a malware infection or another cyber-related exploit. We are continually raising the bar for security; building technologies that help you fight advanced threats more efficiently. Here are our core components to simplifying the Threat Defense Lifecycle:

- McAfee Active Response: A leading innovation in the endpoint detection and response market.
- McAfee Data Exchange Layer (DXL): A superhighway for sharing threat information, enabling easy integration with both McAfee products and third-party solutions.
- McAfee Endpoint Security: Speeds threat detection and remediation with a framework that enables fast scanning, instant threat updates, and maximized CPU performance.
- McAfee Enterprise Security Manager: At the core of our SIEM offering, it delivers the performance, actionable intelligence, and real-time situational awareness required to identify, understand, and respond to stealthy threats, while the embedded framework simplifies compliance.
- McAfee Threat Intelligence Exchange: Optimizes threat detection and response by delivering protection to all points in your enterprise as new threats emerge

For more information please contact gordon.morrison@intel.com.

Legal Disclaimer

No computer system can be absolutely secure. Intel Security does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

This publication is for information purposes only and it does not constitute legal advice or advice on how to achieve operational privacy and security. If you require legal advice on the requirements of the General Data Protection Regulation, or any other law, or advice on the extent to which Intel Security technologies can assist you to achieve compliance with the regulation or any other law, you are advised to consult a suitably qualified legal professional. If you require advice on the nature of the technical and organisational measures that are required to deliver operational privacy and security in your organisation, you should consult a suitably qualified privacy and security professional. No liability is accepted to any party for any harms or losses suffered in reliance on the contents of this publication.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com