GUIDE

McAfee
Together is power.

Navigating the General Data Protection Regulation Mini Guide

Introduction

The General Data Protection Regulation (GDPR) will deliver a long overdue modernization and harmonization of privacy and data protection laws across the EU. It replaces legislation that was drafted before phones became smart and the cloud came to transform business.

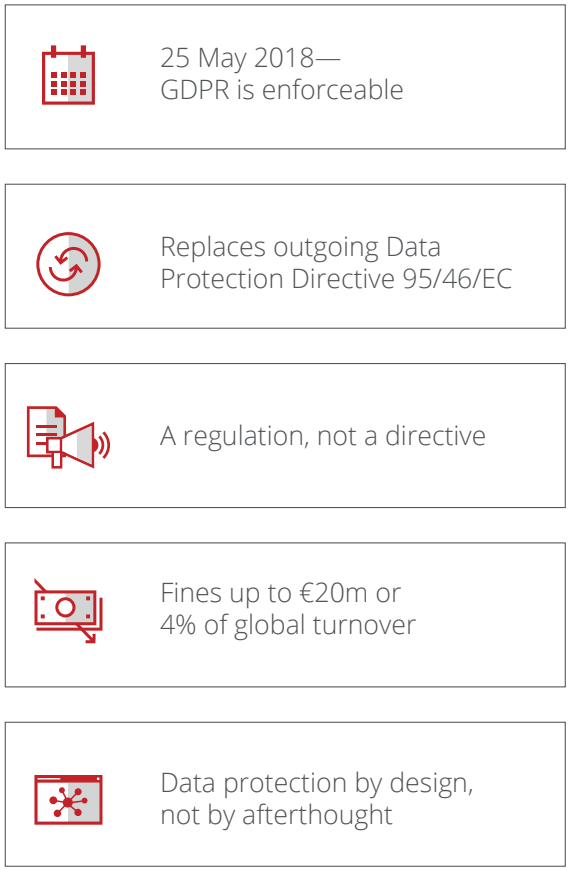
Much has been written about penalties associated with non-compliance with the GDPR—and they can be severe. But rather than focus on fines, security professionals should think about the GDPR as a golden opportunity. A chance to focus the C-suite on the best practice privacy and data protection practices we have been championing for years.

This guide will help you prepare for the GDPR. It outlines the key facts and figures, the questions organizations should ask to help assess their stage of readiness, and a comprehensive toolkit to help develop the capabilities needed to become GDPR-ready. Finally, we offer a short reference sheet covering the key information security professionals need to be prepared.

1. Need to know—the essential GDPR facts
2. How GDPR-ready is your organization? 10 questions to ask
3. The capabilities needed to become GDPR ready
4. Measuring security outcomes

1. Need to know—the essential GDPR facts

- The General Data Protection Regulation (GDPR) was approved by the EU Parliament on 14 April 2016. It will be enforceable on 25 May 2018.
- The GDPR replaces the Data Protection Directive 95/46/EC and was developed to harmonize data privacy laws across Europe and strengthen rights for individuals.
- As a regulation (not a directive), it will apply immediately in all EU territories. There is no need for countries to pass individual laws.
- The fines associated with breaching GDPR are considerable with the highest penalties resulting in fines of up to €20m or 4% of annual global turnover, whichever is greater.
- Data protection by design is a core principle for the GDPR. This means that data protection and privacy should be a priority in all organizations, not an afterthought.



2. How GDPR-ready is your organization?

The GDPR is a huge piece of legislation. Where does an organization start? We brought together a team of privacy, compliance, and technology experts to list the key questions any company should think about in relation to GDPR compliance.

For many organizations, the questions are: "Where to start?" and "Where do we prioritize?"

Business leaders and security executives should take a critical look at their existing data security programs and then ask the 10 questions below. Account managers and pre-sales engineers should use these discovery questions in conversations about GDPR with customers.

1. Is there a culture of data security and awareness in our organization?

It's essential that all people from executives to users, administrators, and developers be trained, certified, and ready to foster a culture of data security and privacy by design within the organization. In many circumstances, preparing for the new regulation requires the appointment of a data protection officer, who is responsible for organizational compliance and communication with supervisory authorities. This new role and executive sponsorship are essential to positive culture change in an organization.

2. Do we know what privacy-related data we collect and where it is stored?

An overriding principle of the GDPR is data minimization—only collect the data that is required to provide goods or services. By understanding what data an organization collects, the organization is able to better focus its compliance rather than applying a blanket, costly approach.

Secondly, you can't ensure the protection of data if you don't know the key repositories, applications, and business processes. Many data loss prevention programs fail because of this very issue. Data is everywhere today, and it is increasingly stored on mobile devices and cloud systems, creating more potential exposure to attack or misuse.

A key consideration should be to implement a continuous data discovery, inventory, and classification program that involves a cross-functional team of business data owners, security operations team members, and data security professionals.

For many organizations, the questions are: "Where to start?" and "Where do we prioritize?"

3. Do we employ encryption for data protection?

Encryption is a key mitigation factor for accidental and malicious data loss incidents and should be employed where possible to protect data at rest or in motion, particularly on mobile devices such as laptops, as well as data uploaded to cloud services. McAfee® research report, 'Building Trust in a Cloudy Sky,'[1] indicates that 74% of organizations store sensitive data in the cloud. Additionally, McAfee research on data exfiltration techniques indicates that over a third of data breaches have occurred in the cloud.

4. Is a data security project currently in place or is one planned for this year?

Establishing a data security program that includes host- and network-based control policy enforcement points is essential to prevent or detect accidental data loss or malicious data theft incidents. With the regulation coming into force in May 2018 and the complicated nature of implementing effective data security controls, organizations should allocate necessary resources as soon as possible.

5. Do we have an existing in-house application security program?

Many enterprises develop a significant number of their business applications in house. These applications are often internet-accessible and house private customer data. According to Verizon's 2016 Data Breach Investigations Report,[2] web application attacks represent the highest incident classification pattern.

As many organizations are implementing continuous DevOps, it is ever more important to build in a secure-by-design approach. Some key security controls to consider include secure coding practices and training for developers, application log collection, regular penetration testing, and perimeter network intrusion prevention systems.

6. Do we know where all of our databases are located and the types of data they store?

Databases often house the crown jewels of an organization—particularly customer-related data. However, too many organizations deploy only basic security controls, do not patch regularly because of application downtime, and rely on administrators for activity monitoring. Additionally, many databases are deployed for testing and development; production data in these creates another risk for sensitive data exposure.

For GDPR readiness, you should consider key actions such as discovery of on-premise and hosted databases, review of database security procedures, deployment of additional protection against vulnerability exploitation attacks, and creation of specific database breach use cases in security operations. For third-party hosted databases, a review of contracts with the hosting companies and assessment of their security posture is recommended.

Databases often house the crown jewels of an organization—particularly customer-related data

7. How do we account for cloud software-as-a-service applications that house private data?

Used by almost every organization, cloud applications range from business apps like Salesforce to cloud storage services like Box. While the cloud provider has responsibility for infrastructure security, the organization is still responsible for protecting data and monitoring user activity.

Two key GDPR-related security controls to consider here are Cloud Access Security Brokers (CASBs) and employment of user behavior analytics that can help control access as well as identify and respond to unusual account activity.

8. How are we controlling privileges and privileged user activity, particularly with cloud services?

According to Verizon's 2016 Data Breach Investigations Report,[3] privilege abuse is the top-reported type of insider threat. Insider actions are among the most difficult to detect, with the average organization taking months to discover such incidents. Additionally, cloud services are presenting an increasing attack surface: reducing, controlling, and monitoring privileged user activity is a key consideration for GDPR compliance and data protection in general.

9. What is the status of our advanced malware protection plans?

Verizon's 2016 Data Breach Investigations Report[4] found that almost 60% of malware incidents involved malware designed to steal or export data. Spear phishing is the most common way of delivering malware that gives an attacker persistent access to a system. Once inside the network, an attacker using this approach employs stolen credentials to access sensitive systems and encrypted channels to exfiltrate data.

In addition to advanced malware protection at the endpoint, consider protection solutions that can inspect HTTPS as the most common exfiltration channel.

10. Does Security Operations have pre-planned data breach detection use cases?

GDPR requires that an organization report a data breach within 72 hours. This implies the capability to identify a breach in that time frame. The recent SANS 2017 Incident Response Survey[5] found that just about 84% of organizations had at least one dedicated incident response team member, but only 53% of organizations considered themselves in a mature or maturing state for incident response. However, even in mature security operations centers, data breach incidents are difficult to identify, investigate, and respond to, especially at speed. A key consideration for GDPR readiness is to consolidate security data in a SIEM and employ user entity behavior analytics (UEBA) to identify anomalous behavior.

3. The capabilities needed to become GDPR ready

Getting ready for the GDPR is really about changing organizational culture as it relates to privacy, personal data protection, and cybersecurity in general. You can explore the background to this in more detail on the Securing Tomorrow blog. The organizational capabilities needed can be looked at in four main ways: governance, people, processes, and technology. We'll cover cybersecurity in more depth.

	Protection	Detection	Correction
Governance	■ Establish executive awareness and board-level support for cybersecurity and data protection ■ Appoint a data protection officer with appropriate authority to enforce compliance standards, to the extent that is necessary ■ Design a continuous compliance monitoring and assessment program for proactive compliance checks ■ Establish an information security management program based on industry-accepted frameworks (NIST, ISO27001, SABSA) and controls (SANS, etc.) ■ Foster a positive and collaborative culture of data security with the employees and business partners ■ Establish a security operations center and staff for 24/7 activity ■ Embed incident response and data protection language into cloud service provider and third-party supplier agreements		
People	■ Train and certify application developers on secure coding practices ■ Train and certify end users on data protection ■ Train and certify domain and technology administrators on secure configurations, responsibilities, and best practices ■ Train and certify domain and technology administrators on secure configurations	■ Train all users and administrators on data breach reporting procedures and responsibilities ■ Train and certify incident handlers on data breach reporting and handling requirements	■ Develop coaching mechanisms for positive reinforcement of data protection policies ■ Establish link between human resources and security for data protection policy violation handling ■ Establish a crisis action team to manage breach response actions
Processes	■ Establish a continuous application security testing process ■ Perform regular scans for databases and other sensitive data repositories ■ Embed data protection language into cloud provider and other third-party supplier agreements ■ Continuously review privileges and access rights to sensitive data repositories and applications ■ Develop a continuous data classification	■ Continuously monitor for data-at-rest encryption status across endpoints, data center, and cloud servers ■ Develop breach detection and response playbooks to identify accidental or malicious data loss scenarios ■ Continuously monitor for data breach scenarios ■ Develop reporting procedures to report data breaches to authorities within the required timeline ■ Embed incident detection language into cloud provider and other third-party supplier agreements	■ Exercise the crisis action team at least once per year ■ Develop response actions to isolate and fully understand the scope of a breach within four hours ■ Develop a continuously monitored vulnerability correction system for DevOps ■ Develop response action playbooks and rehearsals incorporating IT, SecOps, HR, PR, executive leadership, and business unit representatives
Technology	■ Advanced anti-malware solutions using signatures, intelligence, and behavioral analysis capability across end-user devices and servers ■ Encryption for data at rest on end-user devices, servers, and databases ■ Intrusion prevention systems for workload and application security ■ Network data loss prevention for data-in-motion security ■ Endpoint data loss prevention for data-in-use and in-motion security on end-user devices ■ Database Activity Monitoring to protect enterprise applications from exploit ■ Cloud Web Security Gateways for mobile data and threat prevention ■ Cloud Security Brokers to provide visibility and control of data in SaaS applications	■ Central visibility and policy management for data loss prevention and encryption tools ■ Security Information and Event Management system for real-time incident detection and forensics ■ Log collection system with capacity for at least six months but up to one-year storage for critical sensor and data sources ■ Secure evidence repository for data loss incident investigations ■ Endpoint detection and response tools with traffic and user activity history for incident triage ■ User behavior analytics to identify suspicious activity on enterprise and cloud applications	■ Automated policy-based encryption for data in motion on email, web, and cloud traffic ■ Response action tools capable of host, network, application, data, and user isolation to contain a breach

4. Measuring security outcomes

The table below provides a more comprehensive view on the key capabilities needed to meet the security outcomes of a GDPR-ready organization:

	Protection	Detection	Correction
Neutralize Threats	■ Prevent known or unknown malware installation on end-user devices, databases, and servers ■ Prevent application exploits that led to unauthorized access and data loss ■ Limit and control end-user and administrator privileges	■ Identify, investigate, and validate malware infections wherever they occur ■ Identify, investigate, and validate exploit attempts on applications that host private data ■ Identify, investigate, and validate exploit attempts on databases that host private data	■ Automatically share malware intelligence across sensors and control points ■ Isolate infected hosts or systems using pre-planned response and automated actions ■ Block malicious files on endpoints, network, and web channels using automated actions ■ Block command and control activity across network, web, or other channels using automated actions ■ Remove indicators of compromise from infected hosts or rebuild to prevent reinfection
Protect Data	■ Use automated discovery and classification tools to identify and mark private data ■ Protect private data in use, at rest, or in motion from accidental or policy-based loss incidents ■ Protect private data in use, at rest, or in motion from malicious loss incidents ■ Prevent exfiltration of private data to known or unknown locations ■ Prevent unauthorized access to private data ■ Use automated encryption to identify and protect data in motion	■ Identify, investigate, and validate policy-based data loss incidents ■ Identify, investigate, and validate malicious data exfiltration attempts ■ Identify, investigate, and validate exploit attempts on databases that host private data ■ Identify, investigate, and validate unauthorized access attempts to applications, databases, or servers that host private data	■ Automatically share data intelligence across sensors and control points ■ Isolate infected hosts or systems using pre-planned response and automated actions ■ Isolate user privileges and access to private data using pre-planned response and automated actions ■ Use automated encryption to identify and correct potential data loss scenarios
Protect Cloud Environments	■ Use automated discovery and classification tools to identify cloud applications and mark private data ■ Prevent known or unknown malware installation on cloud infrastructure-as-a-service servers ■ Prevent exploitation of cloud-hosted applications on infrastructure or platform ■ Protect private data in use, at rest, or in motion from accidental or malicious data loss incidents on cloud-hosted applications	■ Identify, investigate, and validate unauthorized access to cloud-based services ■ Identify, investigate, and validate breaches of private data security controls on software-as-a-service applications ■ Identify, investigate, and validate breaches of private data security controls on hosted applications	■ Automatically share data and malware intelligence across sensors and control points ■ Isolate infected hosts or systems using pre-planned response and automated actions ■ Isolate user privileges and access to private data using pre-planned response and automated actions ■ Use automated encryption to identify and correct potential data loss scenarios to cloud applications
Optimize Security Operations	■ Continuously scan to identify and classify private data and data repositories ■ Continuously reduce attack surface for vulnerability and application exploits through patching and vulnerability scanning ■ Continuously monitor for protection control status across all managed end-user devices, databases, and servers	■ Continuously monitor for indicators of compromise, particularly command and control activity ■ Continuously monitor for breaches of private data security controls ■ Continuously monitor for unauthorized access or privilege abuse attempts on systems with private data	■ Use automation and integrated technologies to adapt security postures to prevent reinfection and private data exposure ■ Use automation and integrated technologies to quickly triage suspected infections, insider activity, or data loss indicators

Summary

Getting ready for the GDPR will be on the minds of many enterprise business and security executives this year. Business executives and organizational security officers must prioritize investments and implement new programs or solutions that ensure the business is ready for the enhanced regulatory environment.

McAfee has a wide ranging and deep capability for the requirements of GDPR that protect data at rest and data in transit as well as provide visibility within the cloud.

To find out more, visit mcafee.com/GDPR

1. Building Trust in a Cloudy Sky
2. Verizon's 2016 Data Breach Investigations Report
3. Ibid.
4. Ibid.
5. SANS 2017 Incident Response Survey

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

3582_0917_gd-gdpr-mini-guide
SEPTEMBER 2017