Executive summary

EU General Data Protection Regulation (GDPR)

A practical approach to securing personal data and avoiding non-compliance fines

Introduction

The European Union’s General Data Protection Regulation (GDPR) aims to improve protection of data that can be directly or indirectly linked to individuals. Taking effect on 25 May 2018, this regulation applies to all organizations that control or process the personal data of EU citizens, including communications service providers (CSPs). Organizations that fail to comply with the GDPR will face heavy fines in the event of a data breach.

At its heart, the GDPR provides a mandate for organizations to manage and protect access to their customers’ personal data. This briefing note describes strategies that can help CSPs and other organizations fulfill this mandate. It provides practical steps for protecting access to personal data, rapidly detecting and responding to data breaches, and demonstrating GDPR compliance.

77% of the time, attackers combined hacking, malware and social engineering to steal credentials in order to advance their attacks.

Contents

What does the GDPR require if a data breach occurs? 3
Protecting access with identity and access security 3
Ensuring a rapid response to personal data breaches 4
Demonstrating compliance with operational controls 4
Summary 5
What does the GDPR require if a data breach occurs?

Chapter 4 of the GDPR describes what data controllers and processors need to do protect personal data and how they need to react if a breach occurs.

GDPR Article 25 specifies that organizations must protect personal data by design and by default. This requires the ability to specify which privileged users – including employees, third parties, applications, or processes – have access to any customer’s personal data. The GDPR makes organizations responsible for controlling who and what has privileged access to all personal data in their care.

Article 33 specifies that controllers must notify a supervisory authority (SA) within 72 hours of discovering a breach. They must also notify affected customers without undue delay.

It is not enough to comply with the GDPR. Organizations must also be able to demonstrate compliance by producing accurate, reliable reports that show which users have privileged access to critical accounts, when they require this access, and what actions they perform. These reports are becoming essential because of the proliferation of privileged accounts across enterprises, and the often unrestricted, anonymous access to these accounts.

Protecting access with identity and access security

Organizations must protect access to personal data to comply with the GDPR. But compliance will be difficult to achieve without a strong identity and access management strategy. This strategy must include solutions that safeguard privileged accounts that have access to systems and applications containing personal data.

An identity and access security solution should allow an organization to enforce the GDPR’s privileged credential usage control requirements with capabilities such as live user activity monitoring and session recording. It should also isolate privileged sessions, especially those that come from outside the network or from unmanaged third-party devices. Further, it should ensure individual accountability with privileged access to help the organization meet the GDPR’s notification and reporting requirements.

With an effective identity and access security solution, an organization can:

• Ensure that all partners and third-party ecosystem members comply with the GDPR’s access protection requirements
• Improve its overall security posture by securing personal data and other valuable or mission-critical corporate information, including customer data, financial information, contracts, and legal documents
Ensuring a rapid response to personal data breaches

Once the GDPR takes effect, the risks associated with non-compliance will include loss of goodwill and fines that could equal up to 4 percent of an organization’s global turnover. In 2016, the UK-based mobile operator TalkTalk was fined £100,000 for security failings that allowed hackers to access customer data. Had the GDPR been in place, the penalty could have been as high as £59 million.

The desire to avoid major fines will inspire organizations to develop strategies for complying with the rapid breach detection and response requirements laid out in the GDPR. But a strong detection and response solution does more than help an organization avoid fiscal pain.

Organizations should deploy a cyberthreat detection and mitigation solution that uses automation to support proactive anomaly detection and access blocking. This type of early detection is different from that offered by perimeter defenses because it uses analytics and traffic profile anomaly detection to identify unknown cyberthreats and attacks. With a solution that profiles and analyzes user and entity behavior in real time and delivers prioritized alerts when it finds abnormal activity, an organization can detect and respond to breaches early.

Demonstrating compliance with operational controls

Organizations need the ability to demonstrate GDPR compliance to avoid fines. As with strong personal data protection and the ability to respond rapidly to a breach, effectively demonstrating compliance can bring strategic business benefits.

For example, demonstrating compliance shows that an organization has operational controls that keep personal data secure. This protects and enhances the organization’s brand, enabling it to attract new employees, better partners, and more business. An organization that proves its ability to provide strong personal data security in collaboration with partners can use these partnerships to pursue new market opportunities.

An audit and compliance management solution enables organizations to identify exactly who and what accessed personal data. Solutions that support tamper-resistant audit logs and session recordings enhance overall security and provide the detailed data organizations need to demonstrate GDPR compliance.
Summary

The GDPR provides a comprehensive mandate for securing the personal data of EU citizens. It will be enforced starting 25 May 2018. Organizations can take important steps toward GDPR compliance by deploying solutions that enable them to:

• Monitor access to privileged accounts and establish individual accountability by requiring users to “check out” shared account credentials
• Assess environmental risks and distinguish between normal and abnormal user and entity behavior
• Generate audit logs that show exactly which people, applications, or processes accessed personal data
• Provide tamper-resistant audit logs and session recordings to demonstrate compliance

Nokia NetGuard provides a portfolio of security products and professional services that can help organizations assess their state of GDPR readiness and implement measures to ensure ongoing compliance. Read our white paper for insights and recommendations that can help your organization prepare for GDPR enforcement.