Navigating the European Union's

GLOBAL DATA PROTECTION REGULATION

What you need to know in the evolving global regulatory environment

ca technologies | VERACODE

EYE ON COMPLIANCE

It has become painfully apparent in recent years that there are no boundaries or barriers to cyberthreats in the digital age. As the frequency of attacks rises and the sophistication level of cybercriminals grows, every organization is at risk.

But cybersecurity isn't the only challenge. It's also necessary to deal with emerging regulations that attempt to curb risks. Among the most notable: the European General Data Protection Regulation (GDPR), which is scheduled to take effect in May 2018.[1]

The initiative applies to any and all businesses that control or manage the personal data of residents of the European Union. It also widens the traditional definition of "personal data" to include any information that can be used to directly or indirectly identify a person — including a computer IP address, a name, a photo, an email address, bank details, posts on social networking sites or medical information.

Organizations that fail to comply with the GDPR risk fines as high as 4 percent of global turnover, at a maximum of €20 million. Yet despite the potentially high price tag, more than 50 percent of companies affected by the GDPR won't be in full compliance with its requirements by the end of 2018, according to consulting firm Gartner.[2]

If your organization competes globally, it's critical to begin preparing for the GDPR and construct a framework that delivers the necessary level of compliance. Boosting cybersecurity protections, including application security, is at the center of everything.

KEY REQUIREMENTS

An organization must have a cybersecurity program in place to deal with the provisions of the GDPR. Core requirements include:

- A cybersecurity policy that protects the integrity of data
- A breach notification plan
- Appropriate technical and organizational solutions and safeguards
- A clear vendor vetting policy
- Clearly defined methods for validating data integrity, including testing, assessing and evaluating the effectiveness of security policies
- Impact assessments

Get the Key Takeaways

MOVING BEYOND RISKY BUSINESS

It's no secret that cyberattacks have changed the way organizations both large and small approach cybersecurity. A January 2017 report from consulting firm Risk Based Security revealed that 4,149 data breaches exposed more than 4.2 billion records in 2016.[3] These events occurred in more than 100 countries. Overall, 50.4 percent of data breaches exposed between one and 10,000 records.

The EU mandate introduces new and more stringent requirements for data protection, including some that affect application security practices.

Although business leaders often view regulations and compliance as obstacles, they can actually serve as the foundation for a more strategic approach to cybersecurity. The EU mandate introduces new and more stringent requirements for data protection, including some that affect application security practices. These requirements touch on such tasks as identifying application security flaws, conducting code reviews, establishing remediation strategies and scaling practices to meet the needs of different groups across the organization.

Unfortunately, many organizations will struggle to meet GDPR standards for code review and partner verification due to lack of time, budget and staff. Thus, it's critical to tap solutions that can address key GDPR requirements, including application security and secure development, without juggling a spate of tools or hiring additional staff. It's vital to move beyond a check-box approach, which may not meet the needs of an auditor, and embrace a best-practice compliance framework.

4 KEY **BEST PRACTICES**

1 **Track code flaws, reviews and compliance through a single platform.** Best-practice organizations create a single, central repository for information about software weaknesses, as well as proposed, accepted and rejected mitigations. This approach both streamlines compliance and maximizes the effectiveness of security assessments by consolidating the results of multiple testing methods (for instance, static analysis, dynamic analysis and manual penetration testing) in one place.

2 **Achieve continuous compliance monitoring.** It's vital to recognize that compliance isn't the end goal. Ultimately, regulations are part of an overall security framework to better protect systems and data. Thus, an organization's cybersecurity initiative must rely on continuous and ongoing compliance. In terms of application security, ongoing compliance results from the following:

- Security testing that integrates with the software development lifecycle
- Regular discovery scans of web applications within an organization's domain, including temporary marketing sites, international domains, and sites obtained via mergers and acquisitions
- Continuous monitoring of production web applications for vulnerabilities
- Virtual patching for web application firewalls based on the security intelligence from application assessments
- Auditing and protection during actual cybersecurity events that take aim at common vulnerabilities

3 **Keep nonpublic data safe, whether in internal applications or vendor systems.** A key aspect of the EU GDPR is the provision that an organization must protect personal data managed both internally and by a contractor or vendor. Consequently, a business must ensure that cryptography used by an application remains intact and is implemented correctly, and it must work towards a program that holds third-party software to the same security standards as internally developed software.

4 **Automate and audit compliance workflows.** A platform that automates workflows, reduces communication overhead and delivers a secure audit trail for compliance processes is key. This, in turn, necessitates the need for a robust policy management framework to document and communicate a security policy. The ability to integrate with other key systems to share critical information, such as application security scores, listings of all discovered flaws and flaw status information (new, open, fixed or re-opened), also facilitates this process.

BY THE BOOK

Complying with the EU GDPR will create challenges for many organizations. Limited staff, time and budgets are often the culprits. Today, as attacks proliferate, many organizations are stretched thin.

Not surprisingly, the right strategic and tactical framework can simplify things. For instance, the Veracode Application Security Platform allows your organization to monitor three mission-critical tasks from one central location:

A wide variety of methods to assess application security

Compliance and development team reporting

Secure development training

In addition, Veracode services help enterprises develop effective cybersecurity strategies and deliver risk-reduction results — without the need to hire additional staff or dramatically expand a cybersecurity budget.

GETTING DOWN TO BUSINESS (AND SECURITY)

Here's a look at **seven critical GDPR regulations** and how Veracode can help you specifically address the challenge.

REGULATION 1

GDPR Chapter II, Article 5
(Principles Relating to Processing of Personal Data)

SUMMARY

Provides the fundamental guidelines for processing, handling and protecting personal data.

KEY PROVISIONS

Section 1: Personal data must be:

(a) "processed lawfully, fairly and in a transparent manner in relation to the data subject."

(b) "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes..."

(e) "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed..."

(f) "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures..."

KEY SOLUTIONS

Veracode Static Analysis
This SaaS-based service allows developers to quickly identify and remediate application security flaws without having to manage a tool. It analyzes major frameworks and languages without requiring source code.

Veracode Web Application Scanning
This service delivers testing and evaluation of a program by executing data in real-time. It simulates the way an attacker would inspect applications and identifies vulnerabilities.

Veracode Manual Penetration Testing
This service complements Veracode's automated scanning technologies with best-in-class penetration testing services.

Veracode Software Composition Analysis
Building an inventory of open source and commercial code components helps your organization identify and remediate vulnerabilities.

REGULATION 2

GDPR Chapter IV, Section 1, Article 24
(Responsibility of the Controller)

SUMMARY

Addresses how an enterprise will be able to demonstrate that it is meeting compliance with this regulation.

KEY PROVISIONS

Section 1: "...the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

Section 3: "Adherence to approved codes of conduct... or approved certification mechanisms... may be used as an element by which to demonstrate compliance with the obligations of the controller."

KEY SOLUTIONS

Veracode Application Security Platform
This solution offers a holistic, scalable way to manage security risk across your entire application portfolio. Security program managers work with you to define policies and success criteria, thus producing a strategic, repeatable way to tackle application security risk.

Veracode Security Program Management
This service helps enterprises map out a security strategy and deliver best-practice results. It ensures that your program stays on track to meet strategic goals.

REGULATION 3

GDPR Chapter IV, Section 1, Article 25
(Data Protection by Design and By Default)

SUMMARY

Mandates that an organization include security considerations in the design phase of systems and that data processing always defaults to the most privacy-focused method.

KEY PROVISIONS

Section 1: "Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, adopt appropriate technical and organizational solutions in such a way that the processing of data will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

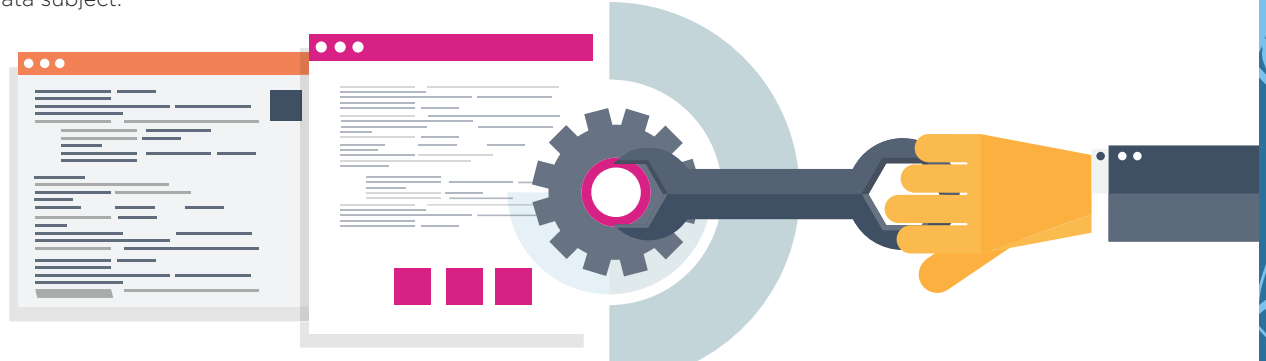
KEY SOLUTIONS

Veracode Static Analysis

Veracode Greenlight
This solution offers instant scanning for developers — right in the IDE.

Veracode Remediation Advisory Solutions
This service provides one-on-one consultations with secure development experts.

Veracode Manual Penetration Testing
This solution taps a security consultant who manually tests applications for vulnerabilities, without visibility into their inner workings, and addresses the requirement for "pseudonymisation" of data.



REGULATION 4

GDPR Chapter IV, Section 1, Article 28
(Processor)

SUMMARY

Establishes guidelines for organizations using third parties to process data.

KEY PROVISION

Section 1: "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

KEY SOLUTION

Veracode Vendor Application Security Testing
This solution provides security testing of outsourced and vendor code without compromising vendor intellectual property.

REGULATION 5

GDPR Chapter IV, Section 2, Article 32
(Security of Processing)

SUMMARY

This provision requires the controller and processor to implement technical and organizational measures to enforce a security policy commensurate with risk. It spans data validation surrounding the integrity of personal data. It also addresses confidentiality, integrity, availability, and resilience of systems and services processing critical data.

KEY PROVISIONS

Section 1 (d): "a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."

KEY SOLUTIONS

- **Veracode Static Analysis**
- **Veracode Web Application Scanning**
- **Veracode Software Composition Analysis**
- **Veracode Vendor Application Security Testing**
- **Veracode Manual Penetration Testing**

REGULATION 6

GDPR Chapter IV, Section 2, Article 33
(Notification of a Personal Data Breach to the Supervisory Authority)

SUMMARY

Lays out mandatory provisions for data breach notifications.

KEY PROVISIONS

Section 1: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority...Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Section 3 (a): "describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned."

KEY SOLUTION

Veracode Runtime Protection
This solution defends against application-layer attacks in real time. In monitoring mode, it delivers alerts about active threats and logs an audit trail. In blocking mode, Veracode Runtime Protection also prevents the attack from being executed.

REGULATION 7

GDPR Chapter IV, Section 3, Article 35
(Data Protection Impact Assessment)

SUMMARY

Every two years, or when there is a change to specific risks, the controller must immediately carry out a compliance review to ensure that data processing is in compliance with the Data Protection Impact Assessment (DPIA).

KEY PROVISIONS

Section 7 (c): "an assessment of the risks to the rights and freedoms of data subjects..."

Section 11: "Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations."

KEY SOLUTIONS

Veracode Static Analysis

Veracode Web Application Scanning

Veracode Manual Penetration Testing

5 DATA PROTECTION **BEST PRACTICES**

According to Gartner, organizations should focus on the following key issues when establishing a GDPR framework:[4]

1
Fully understand your organization's role and relationship with GDPR requirements.

2
Appoint a data protection officer.

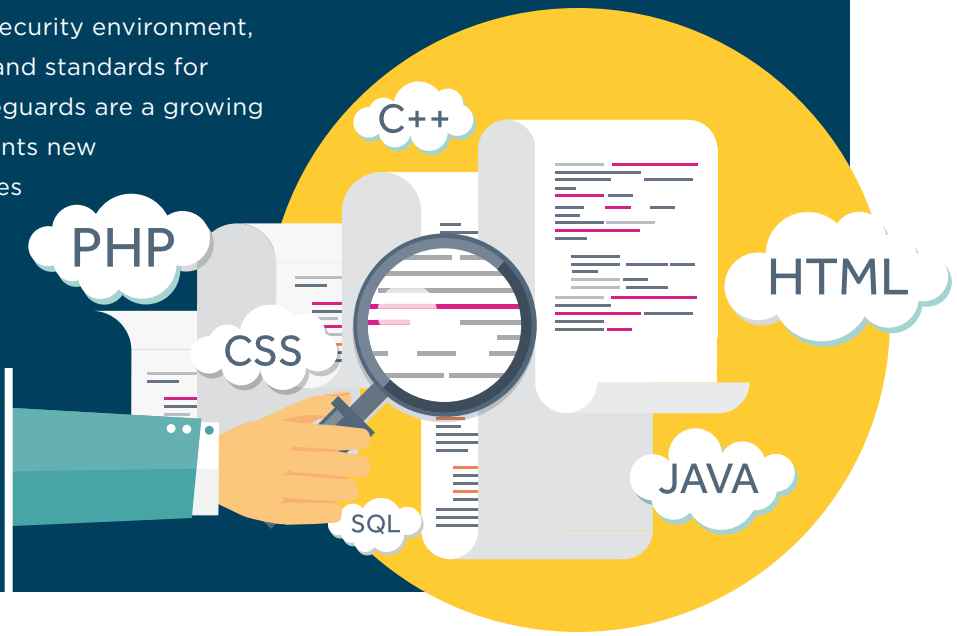
3
Demonstrate accountability for all processes that touch data privacy.

4
Check cross-border data flows using appropriate safeguards such as Binding Corporate Rules (BCRs) and standard contractual clauses.

5
Prepare for data subjects exercising their rights, including data portability and being informed.

THINKING BEYOND REGULATIONS

Amid an increasingly complex cybersecurity environment, one thing is clear: Rules, regulations and standards for overseeing data and establishing safeguards are a growing part of the picture. While this represents new challenges for organizations of all sizes and across industries, the common denominator is that a sound strategy and the right tools and solutions, including application security, are paramount. Together, this provides a foundation for a compliant and secure enterprise.



FOR MORE INFORMATION

Get the Key Takeaways

- Sign up for our weekly platform demo.
- Contact us.

SOURCES:

1 Regulation (EU) 2016/679 of the European Parliament and of the Council. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

2 Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation. https://www.gartner.com/newsroom/id/3701117

3 2016 Reported Data Breaches Expose Over 4 Billion Records. https://www.riskbasedsecurity.com/2017/01/2016-reported-data-breaches-expose-over-4-billion-records/

4 Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation. https://www.gartner.com/newsroom/id/3701117

ca technologies | VERACODE

Veracode's cloud-based service and systematic approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobile and third-party applications. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world's largest global enterprises, including 3 of the top 4 banks in the Fortune 100 and 20+ of Forbes' 100 Most Valuable Brands.

LEARN MORE AT WWW.VERACODE.COM, ON THE VERACODE BLOG, AND ON TWITTER.