GDPR Compliancy

A Global Change Is On Its Way

Pascal Greenens

As Cyber Security Evangelist for Radware, Pascal helps execute the company's thought leadership on today's security threat landscape for EMEA, Central and Latin America. Pascal brings over two decades of experience in many aspects of Information Technology and holds a degree in Civil Engineering from the Free University of Brussels, specializing in electronics with a finalization in parallel computing.

David Hobbs

As Director of Security Solutions, David Hobbs is responsible for developing, managing, and increasing Radware's security practice in APAC. Before joining Radware, David was at one of the leading Breach Investigation Firms in the US. David has worked in the Security and Engineering arena for over 20 years and during this time has helped various government agencies and world governments in various cyber security issues across all sectors.

WHAT IS THE GENERAL DATA PROTECTION REGULATION?

In January 2012, the European Commission (EU) proposed a comprehensive reform of the data protection rules in the EU. The General Data Protection Regulation (GDPR) is the largest reform in data protection law in 20 years. The regulation provides protection concerning the processing of personal data and the free movement of such data. It entered into force on May 24, 2016 and it will apply from May 25, 2018.

What is meant by "personal data?" Personal data is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. Personal data can include:

- Name
- Phone Number
- Physical, genetic or physiological information
- Cultural identity
- Bank details
- Cookies
- Email address
- Social media posts
- Medical information
- Location
- IP address

HOW WILL GDPR IMPACT ORGANIZATIONS?

GDPR contains many requirements about how you collect, store, and use personal information. This means not only how you identify and secure the personal data in your systems but also how you accommodate new transparency requirements, how you detect and report personal data breaches, and how you train privacy personnel and employees.

Given how much is involved, you should not wait until the regulation takes effect to prepare. You need to begin reviewing your privacy and data management practices now. Failure to comply with the GDPR could prove costly, as companies that do not meet the requirements and obligations could face substantial fines and reputational harm.

MARKETING TO CUSTOMERS AND PUBLIC TRUST

Consumer research[1] in the last year shows a decline in trust and an increase in levels of concern about the protection and processing of their personal data and this is believed to have an influence on the future growth of digital technologies.

1 https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf

The GDPR provides EU residents with control over their personal data through a set of "data subject rights." This includes the right to:

- Access readily-available information in plain language about how personal data is used
- Object to processing of data for specific uses, such as marketing or profiling
- Access personal data
- Have incorrect personal data deleted or corrected
- Have personal data rectified and erased in certain circumstances (sometimes referred to as the "right to be forgotten")
- Restrict or object to processing of personal data
- Receive a copy of personal data

For the EU citizen, the GDPR means a reinforcement of their individual rights, while businesses restore the trust of their consumers. The GDPR is creating a compliance model that takes into account many of the compliance initiatives in other countries similar to PCI and HIPAA. However, GDPR has much broader scope and complexity to the handling and sharing of personal identifying information.

ENFORCEMENT ACTIONS

Not abiding to the GDPR will result in enforced action, including fines of up to € 20,000,000 or 4% of an organization's annual worldwide revenue when facing a breach of the data protection rules. The GDPR includes provisions that promote accountability and governance that can be audited with non-compliance leading to administrative fines of up to € 10,000,000 or 2% of annual worldwide revenue.

GLOBAL ACTIONS

Whenever a company wants to trade or do business with one or several of the EU Member States, it will have to prove adequacy – in other words its data protection standards would have to be equivalent to the EU's GDPR starting May of 2018. This virtually makes GDPR a global, worldwide regulation affecting organizations and businesses around the globe. Examples of companies doing business outside of the EU with data from EU citizens: hotels, airlines, insurance, banking, travel companies, e-commerce websites, SAS platforms, retailers who ship or store EU customer data, etc.

WHAT DOES IT MEAN FOR ONLINE BUSINESS AND CLOUD SERVICE PROVIDERS?

For online businesses and cloud service providers, GDPR compliance means adherence to the principles of "*Privacy by Design*" and "*Data Protection by Design*" during the design, development, implementation and deployment of web applications or services and any components or services associated with them. With the rapid adoption of cloud services, there is a heightened concern with regard to the readiness of these applications and services. A recent study conducted by Symantec/Bluecoat shows that 98% of today's cloud applications do not even come close to being GDPR ready.

WAF, DDOS AND THE GDPR

Based on recital 39 of the GDPR, personal data should be processed in a manner that ensures appropriate security and confidentiality, including preventing unauthorized access to or use of personal data and the equipment used for the processing. Recital 49 goes further by requiring the ability of a network or an information system to resist accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems. The recital literally says "*This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.*" This would include brute force login attempts and automated mitigation techniques outlined in the OWASP Top 10 requirement for PCI compliance.

Most businesses will face the urgent need for increasing protection on published applications and services on all topics and purposes of data leak prevention, access control, web-based attack prevention and denial of service prevention. Leading providers of cloud and on-premise web application and API protection services as well as on-demand, always-on cloud and hybrid denial of service mitigation services do provide an adequate solution for this acute need. A fully managed WAF and DDoS Cloud service provides a fast route to check off one of the regulatory compliance boxes and a worry-free GDPR compliance strategy.

Curious what C-level executives think about these changing regulations, in addition to global attack trends, security automation, how to effectively manage security?

Download the *Cyber-Security Perceptions & Realities: A View from the C-Suite* to learn more.
