WhiteSource

# GDPR

## FRIEND OR FOE?

# THE COUNTDOWN IS ON


On May 25, 2018 — less than four months from now — the European Union's General Data Protection Regulations (GDPR) will replace the Data Protection Directives. The GDPR is a comprehensive collection of highly nuanced regulations that aim to strengthen and harmonize how data is collected, held, and protected across the European Union (EU). The regulations will give individuals far greater control over their own data — a right that, unfortunately, has been trampled by the "big data = more money" mindset that many, if not most, organizations have adopted in recent years.

And don't assume that you're off the hook if your organization isn't located within EU borders. Once the new laws come into effect, they will apply to any organizations that conduct business with anyone residing in the EU. So, regardless of whether you're based in the good 'ol US of A, Tokyo, or anywhere else in the world, if you collect or process data on EU-based residents, you'll be responsible for adhering to the new regulations.

In this white paper, we explore some of the key GDPR regulations, the consequences of non-compliance, and how organizations can use the GDPR to re-examine and upgrade their security posture.

# CONTENTS

# A GDPR PRIMER

A quick look at some of the most important articles within the regulations clearly shows that the overarching goal of GDPR is to inculcate a stance of "privacy-by-design" among organizations that conduct business within EU borders. With 99 articles and more than 250 pages of text, we can't possibly address every topic here, but some of the most relevant rights that compliant businesses will have to uphold include:

01

### THE RIGHT TO BE ERASED/FORGOTTEN:

This article provides individuals with the right to have their data erased from all systems where it's being held or processed without delay in cases where that data is no longer needed for the intended purposes, when data was processed unlawfully, and in a few other circumstances.

02

### THE RIGHT OF ACCESS TO DATA:

This article provides the individual with the right to know if his or her data is being processed, to access that data, and to obtain more information about how that information will be processed.

03

### THE RIGHT TO BE INFORMED OF HOW DATA IS BEING USED:

Each person has the right to know how and why their data is being used.

04

### THE RIGHT TO RESTRICT DATA PROCESSING:

This right allows the individual to demand that the information stored about him or her will not be used in any way.

05

### THE RIGHT TO OBJECT TO HOW DATA IS PROCESSED:

This provision allows the individual to object to data being used for direct marketing purposes or for scientific and research purposes. In the case of processing data for direct marketing purposes, once the person objects, data may no longer be processed under any circumstances. In the case of objecting to processing data for scientific/research purposes, there must be "grounds relating to the particular situation."

06

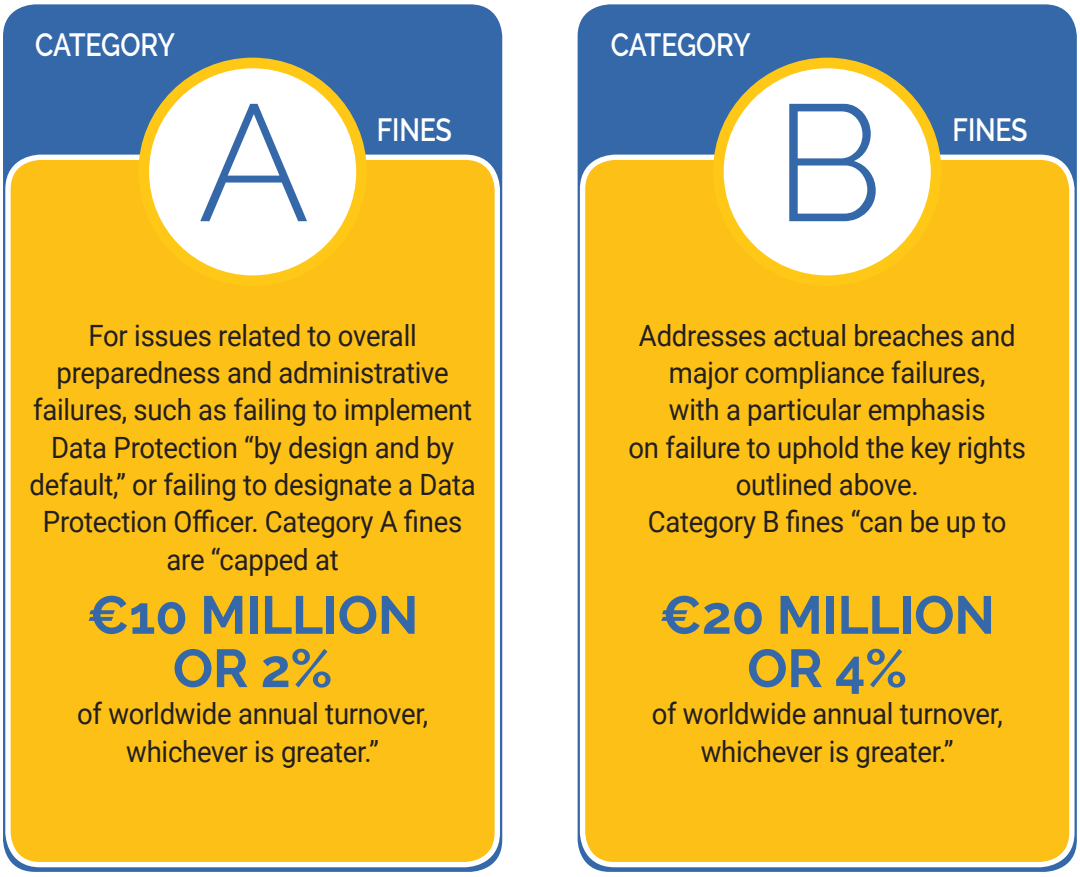
### THE RIGHT TO BE INFORMED OF ANY DATA BREACH WITHOUT UNDUE DELAY:

Article 33 outlines that data breaches must be reported to supervisory boards within 72 hours of discovering the breach. Article 34 states that any compromised individuals must be informed of a breach as soon as possible.

# THE COST OF NON-COMPLIANCE

As overwhelming as the regulations may seem, they are being put into place to correct some long-standing wrongs regarding the handling of personal data. The rights granted by the GDPR are obviously a big win for individuals and their data. The GDPR also helps businesses by providing clearer and more consistent guidelines for data collection, storage, and processing — and for harmonizing those guidelines across all EU countries.

The GDPR also comes with teeth. Article 83 outlines two categories of fines that can be levied for failure to comply with the new regulations:




In addition to these financial penalties, the Data Protection Authorities (DPAs) also have the power to temporarily ban data processing by an organization suspected of non-compliance. If the non-compliance is not corrected, the DPA can prevent the organization from using the data. For some companies, a temporary or definitive ban of this nature could mean the end of their business operations.

Major efforts are being made to ensure that these non-compliance penalties will be administered in a similar manner across all member states. It is also worth noting that individual member states can levy their own penalties for GDPR-related breaches in order to close the gaps between the GDPR regulations and their local laws. Last but not least, individuals can bring civil suits in their own, local jurisdictions against organizations that they feel have breached their rights as defined in the GDPR.

# GDPR MUST HAVES


The onerous fines and penalties described here are certainly strong motivators for organizations to ensure that they are GDPR-compliant by May 25th. But let's put the stick aside for the moment, and look at the carrot. In today's digital economy, it is simply good business to implement data security policies that will win the trust of your customers. Becoming GDPR-compliant provides organizations with the opportunity to rebuild and strengthen their security posture from the bottom-up.

## ESTABLISH ACCOUNTABILITY

For most businesses, the IT or IT security teams are responsible for developing and implementing data security policies. However, for GDPR compliance to become a strategic advantage for your organization, it is important that key decision makers — up to and including the board of directors — are involved. There needs to be a clear, corporate message that security is at the heart of all business operations.

The GDPR **requires** public authorities and companies that carry out large-scale monitoring of individuals or large-scale processing of data to appoint a Data Protection Officer (DPO). Whether an in-house employee or an external consultant, the DPO must have the authority to act independently. The minimum tasks of the DPO are to inform and advise about organizational and employee compliance obligations, to monitor compliance, and to be the point of contact for supervisory authorities.

But even if your organization is not required to appoint a DPO, we highly recommend that you establish a DPO-like position that reports directly to management and is responsible for implementing and maintaining GDPR compliance requirements.

## DO YOU REALLY NEED ALL THAT DATA?

Companies often have a tendency to hoard data, creating unnecessary risk — not to mention needless costs. Getting ready for GDPR compliance is a great opportunity to intimately understand the data that you collect, and why you collect it. If you aren't using your collected data on a regular basis, for example, then perhaps it no longer serves a core business purpose. This is also a good time to ensure that your consent mechanisms meet the GDPR requirements, which require specific, informed, and unambiguous consent.

## DATA VISIBILITY

The GDPR grants data subjects the "right to be forgotten." When this right is exercised, you have to be able to track and delete every instance of a data subject's records, whether online or offline. In today's complex, hybrid IT environments, your data may travel frequently among on-premises data centers and one or more public cloud providers. You have to understand in-depth how and when your data travels, and where your sensitive data is located at all times. Moreover, the more data storage and access silos you have in your organization, the harder it's going to be to meet this requirement.

Now is the time to verify that your data management tools and procedures are well-documented, that they minimize data duplication, and that they provide effective data visibility across the entire organization. Upgrade your tools and procedures as necessary.

## DATA CONTROLLER VS. DATA PROCESSOR

The GDPR differentiates between data controllers and data processors. The data controller is the entity "...which, alone or jointly with others, determines the purposes and means of the processing of personal data. " The data processor is an entity other than the data controller's employees "...which processes personal data on behalf of the controller." Good examples of data processors are third-party data storage or data analytics providers.

According to the GDPR, it is the data controller who is responsible for compliant collection, processing, and protection of personal data. However, the GDPR explicitly outlines certain responsibilities for which the data processor is liable, such as:


If you are a data controller, it is important that you ensure that all of the third parties you use to process, store, and manage your data can clearly demonstrate that they meet the standards of the GDPR. You must be confident that you can audit their compliance independently, if required.

## ROBUST DISASTER RECOVERY PLAN

Article 32 of the GDPR focuses on the security of processing. Among its provisions, the article requires compliant organizations to be able to ensure "...the ongoing confidentiality, integrity, **availability and resilience of processing systems and services,**" as well as "...the ability **to restore the availability and access to personal data** in a timely manner in the event of a physical or technical incident".

Both of these provisions translate into the need for a robust disaster recovery plan that can restore data and business processes within a reasonable but undefined timeframe. EU regulations had given companies up to seven days to restore data after a disaster. By today's standards, seven days is clearly unacceptable and, over time, GDPR regulators will set benchmarks that are more suitable.

Also, if you use a third-party DR service provider, it will be considered a data processor by the GDPR, and you will have to show that it is GDPR-compliant.

## DON'T FORGET THE BASICS

At the end of the day, getting ready for GDPR means making sure that all of the data protection basics are in place — network access is protected, operating systems and applications are up-to-date, sensitive data is encrypted and properly backed up, and employees are well-informed about security risks such as phishing, malware types, and other social engineering attacks. It is critical that regular vulnerability assessments are performed across the organization's tools, technologies, and processes.

# APPLICATION SECURITY AND GDPR

Whether an organization is a data controller or processor, the GDPR lays out responsibility in Articles 25 and 32 for taking the "appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with this Regulation."

This requirement has a significant impact on how organizations are expected to secure the applications that they use for the storing and processing of personal data. While it is far too often not given the proper emphasis as a security priority, the application layer is by far the most common target for attackers seeking to pilfer valuable user data. The Global Risk Management Survey conducted in 2016 found that 84% of cyber attacks targeted the application layer, out in front of the network layer.

Applications facilitate the flow of information between the user and the backend where the data is stored, providing the interface for interactions. Constructed out of mountains of code, each line in an application presents another opportunity for a critical flaw that a hacker can exploit to execute their breach and reach the data on the other side. Add to this that penetrations of the application layer do not require actions like clicking on a phishing email by someone inside the organization, and can go easily unnoticed for months on end — as was seen in the Equifax case which was only uncovered two to three months after the attack began — making them a ripe target for exploitation.

When it comes to implementing application security practices, organizations need to think about how they can use tools to catch issues in real-time, monitor the code throughout the software development lifecycle, and keep their products protected post-deployment. Automation is key to keeping applications secure, especially at scale when large teams of developers are writing and compiling enormous quantities of code for their products.

In regards to the requirements under GDPR, organizations are expected to take reasonable measures to ensure that the applications they are using as the gateways to their data are secured. On the most basic level, this means ensuring that their applications are built with code that is tested for vulnerabilities, and that they monitor for new vulnerabilities that could be discovered in the future.

# OPEN SOURCE AND GDPR

Open source components have become the main building blocks in modern applications, accounting for 60% to 80% of the code base on average. Therefore, when it comes to implementing application vulnerability management processes to comply with the GDPR requirement open source vulnerabilities should be at the top of the to do list.

The need to automate the detection and remediation of open source vulnerabilities does not only comes from the rise in open source usage, but also due to the rise in the publications of CVEs and the increased focus of hackers on open source vulnerabilities as an entry point to breach applications.

In 2017 the number of new CVEs more than doubled, mainly due to CVEs that were reported in popular open source projects. This trend, which continues to accelerate in 2018, is likely due to an increased awareness of security for open source projects.

Another reason is that hackers understand how lucrative open source vulnerabilities can as one vulnerability can have millions of victims. Open source components are a favorite target for hackers for two primary reasons. First is that a popular component are used across multiple organizations, sometimes reaching millions of users. Second is the fact that while a hacker could spend months looking through a project for a "0-day" vulnerability, the information on vulnerabilities in open source projects  are publically available

One of the first challenges when it comes to open source security is simply knowing which components are in your applications. Since most developers are tracking their usage manually, if at all, far too many software teams do not have a good grasp of their open source inventory.

Moreover, they are unable to control whether components with known vulnerabilities are being used in their products. Simply put, you cannot patch what you do not know that you have. Therefore, it is essential to have a solution in place that can continuously monitor which open source components you have in your environment, as well as your products that have been deployed.

A prime example for this need can be seen with the Equifax case wherein the company was caught unaware by the fact that they had a vulnerable version of Apache Struts 2 in one of their deployed web applications, and therefore was vulnerable to exploitation by hackers who targeted them more than two months after the vulnerability was announced. The resulting attack compromised the personally identifiable information belonging to over 145.9 million people, representing the largest theft of data to date. Had they been monitoring their open source components continuously using a solution like Software Composition Analysis, then they would have received an alert that they were using the vulnerable version and could have implemented the necessary fix.

One of the valuable lessons that was learned from the outcry after the Equifax breach was that the public held the company responsible for the theft of their data, even though the compromised component was not written by them. From the public's perspective, Equifax's developers had included it in their product, failed to keep track of it and update when the warning came out, and most importantly, exposed their data to criminals. They were less inclined to hear that it was the fault of the Apache Foundation. If Equifax used it, then they were responsible.

There are growing expectations from the industry regarding how companies are supposed to manage their open source component usage.

OWASP's famous Top 10 Application Security Risks relates specifically to the importance of avoiding components with known vulnerabilities with their A9 entry where they warn that "Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts."

While the GDPR is less specific in its wording regarding what their expectations are for how exactly organizations are supposed to protect themselves, executives should be conscious of the kinds of questions that can arise should a breach occur.

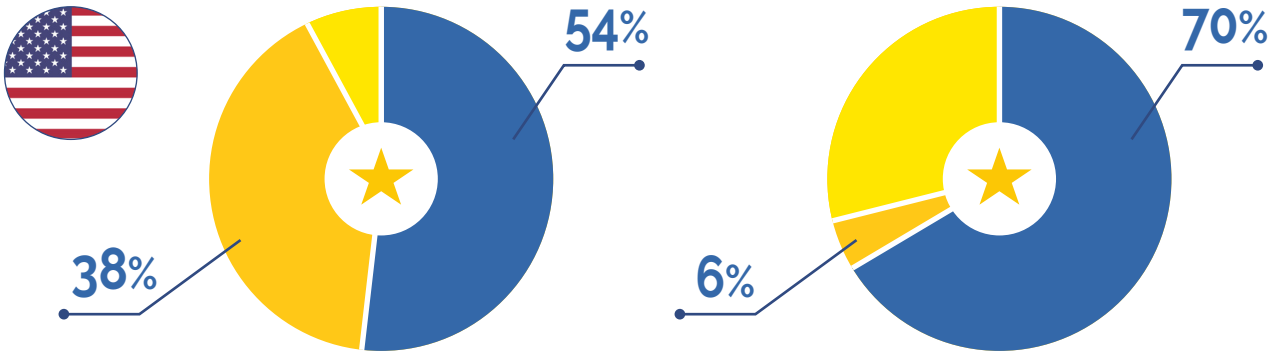
Did they stand up to industry best practices? Were the proper technologies implemented? Did their developers have the tools that they needed for building and maintaining secure products?

The European Union does not appear to be gearing up for intensive audits at this stage in the game, due in part to the enormous scale that they would have to contend with. The commission will likely focus their efforts on those who are in blatant violation of regulations and are actively abusing the data in their possession. However, they are laying the groundwork to initiate sizable proceedings against those companies that should have taken basic steps to guard themselves, but were negligent and did not make good faith efforts to protect themselves and the public's data.

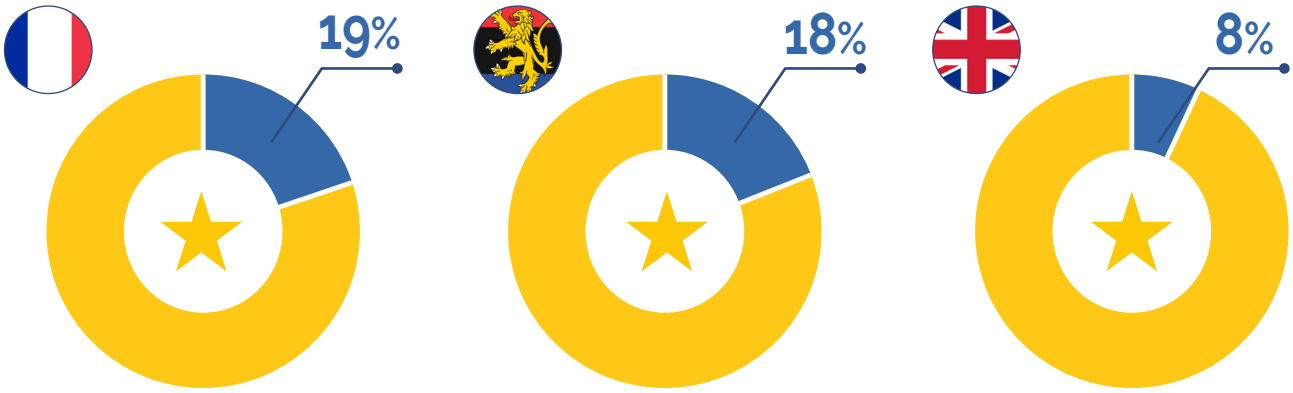
In our reading of the GDPR as it relates to securing data through design and continual maintenance operations, their expectations are for organizations to develop software applications in accordance with best practices throughout the software development lifecycle, implying that if companies want to be in line with the regulations, then they need to put solutions in place to ensure that vulnerable components are not used from the earliest stages of development, during the building of the application, and that newly discovered vulnerabilities are alerted on post-deployment.

# ARE WE THERE YET?

In a recent PwC survey of C-level executives from large U.S. multinational companies (more than 500 employees), 54% reported that GDPR readiness is at the top of their data-privacy and security agenda, and another 38% placed GDPR as one of several top priorities. A little more than 70% have begun — and 6% have completed — their GDPR preparation. Given the penalties that could be incurred for non-compliance, unprecedented budgets have been allocated for this activity, with 68% indicating that they will invest between $1 million and $10 million, while 9% expect to spend over $10 million.




In Europe as well, businesses are ramping up their GDPR preparedness, with 19% of French businesses, 18% of Benelux businesses, and 8% of British businesses already claiming to be fully GDPR-compliant.




PwC GDPR Series puls survey 2017 [8]

There's no question that getting ready for GDPR is a complex process that requires widespread recruitment of resources and leadership. However, rather than regarding GDPR as a foe, winning enterprises will use GDPR as a springboard to fix what is broken and become a true "security-by-design" company. Clearly demonstrated respect for data privacy positions a company as worthy of its customers' trust, and can be leveraged as a competitive advantage.

References

[1] Final GDPR document (English)

[2] Eight Ways Board Directors Should Be Preparing for the GDPR Right Now, Diligent

[3] Penalties for Non-Compliance with GDPR, Winterhawk Consulting

[4] Michelle Drolet, How much will non-compliance with GDPR cost you?, CSO, October 2017

[5] Petter Nordwall, Coming, ready or not: The cost of GDPR non-compliance, SC Media, September 2017

[6] Data protection officers, ICO

[7] Carla Bouca, EU GDPR controller vs. processor – What are the differences?, EU GDPR Knowledge Base

[8] Pulse Survey: US Companies ramping up General Data Protection Regulation (GDPR) budgets, PwC, 2017