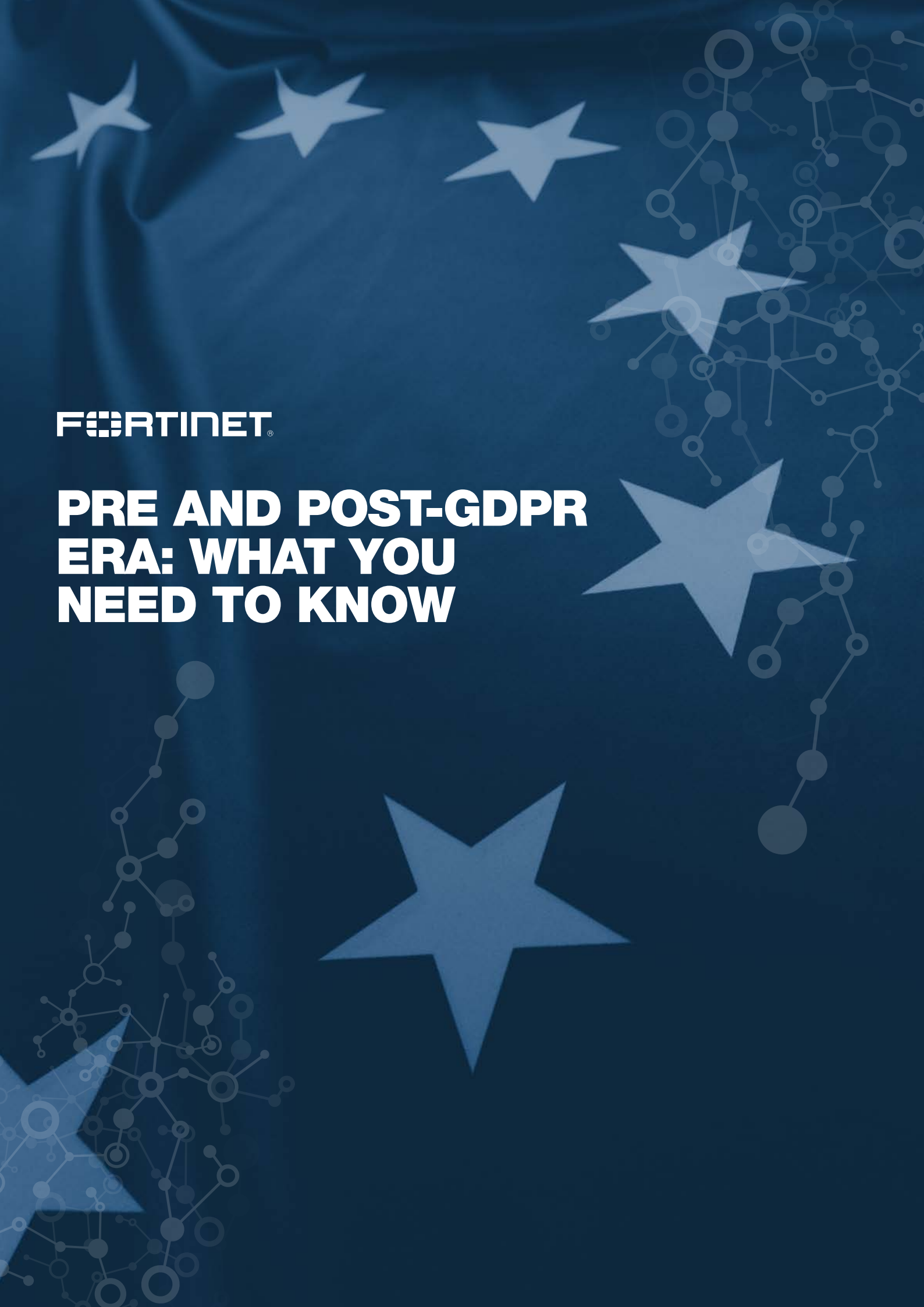


PRE AND POST-GDPR ERA: WHAT YOU NEED TO KNOW

A lot has been said and written about the GDPR from a multitude of perspectives: analysis of its many articles, projections into the potential impact of the regulation and more than a fair share of dire predictions and claims about how an organization's GDPR compliance efforts could simply be resolved by investing in product "X".

Now that May 25 2018 has come and gone without the world having come to an end or leaving the Internet devoid of interesting content - social media somehow survived however – this is a good time to reflect on why something as dramatic as GDPR was thought to be necessary and provide insight on what organizations still need to be aware of in a GDPR governed digital world.

HOW DID DATA PROTECTION BECOME SUCH A BIG DEAL?

The short answer? Very slowly and over many years.

When the pre-GDPR data protection regulations were first developed, the concept of user data in a digital format was in its infancy. In the mid-1990s, most users were part of closed communities/ services like AOL if they were connected at all. And like with any new technology the focus was on what they could do rather than the possible consequences.

But as technology evolved and reliable, high speed Internet access became more widely available, the range of options and different services continued to grow. Companies like Google, Facebook and others built their whole business model on the collection, analysis and manipulation of user data. All of this accelerated with the introduction of smartphones and the massive adoption of "apps", liberating the Internet surfer from the confines of their home or work computers.

While all of this was happening on the "plus" side, on the "minus" side the hackers and cybercriminals were waking up to the value of this personal data. Let's be clear about this, stealing personal information is not new. But given the sheer volume of data, the lack of awareness by the data subject, and the minimal attention to securing the data by companies collecting it were creating a perfect storm that could easily be taken advantage of.

The third aspect of "why GDPR" is that even when there were high profile data breaches, the regulatory consequences for the companies at the heart of the breach were minimal or non-existent. Even though a serious data breach has a tangible cost – both direct, indirect as well as reputational costs – most breached organizations survived the storm and continued with business as usual. Quite simply put, whatever the costs of a data breach, including fines from regulators, there was not enough of an incentive – let's call it a "stick" – to make a difference. Experiencing a data breach was a calculated and manageable business risk when compared to the value of user data, data that could be used over and over again.

It was in this environment that what we now know as the GDPR was born and it was designed to address all of these issues and raise the question 'Why is data protection so important?'

WHAT DOES THE GDPR MEAN TO THE AVERAGE USER?

While the GDPR seems to have "snuck up" on the average user, as well as the typical organization, the impact of what it was supposed to do was very much brought to the forefront just before the May 25, 2018 effective date by the Cambridge Analytica and Facebook incident, where 87 million Facebook users personal data was secretly harvested for political purposes in 2016. Although unfortunate, here was a stark reminder of why greater awareness by the data subjects was needed in regards to the collection of their personal data and much greater attention to detail by the organization's collecting and using that data.

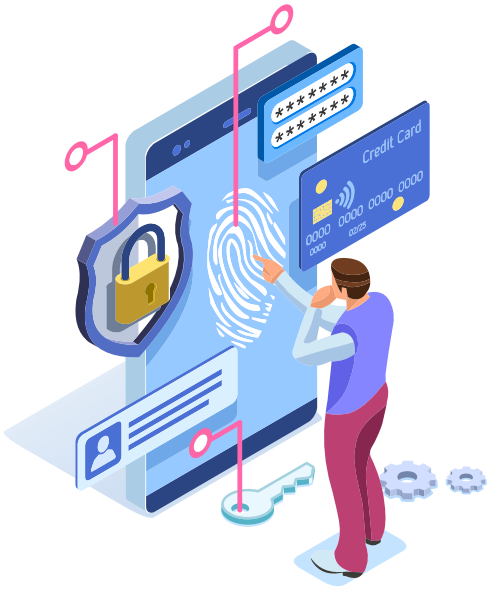
The $64,000 question however is whether or not this increased awareness will remain, especially by the data subject, or will we sink back into the mindset of the past? That remains to be seen but for the organizations collecting the data, this incident happening in the midst of the escalating GDPR hype certainly drove home the point that there will be consequences for violations of the regulation.

WHAT DOES THE GDPR MEAN TO THE AVERAGE EU BASED ORGANIZATION?

Despite a nearly two year grace period before its entry in force on May 25, 2018, only a very small share of businesses felt they were ready to face the implications set by this regulation. There may be any number of valid reasons for this but organizations are out of time, they must now take an honest look at their rationale, processes and procedures for collecting user personal data.

Because of the rapid growth of the online market combined with lack of effective data protection regulations prior to the GDPR, most organizations developed their data collection procedures in a haphazard

manner even with multiple entities within the same organization collecting the same personal data. This approach naturally led to a lack of awareness as to what data and from whom they had and how they were using it.



The GDPR now forces organizations to think of data collection from a "Rights vs Responsibilities" perspective. Prior to the GDPR, collection of user data was taken by default and in extreme cases it was very difficult for the data subject not to agree to its collection. With the GDPR the tables are turned. It's the data user who's in control and owns the rights to their personal data and controls who can collect it and who can't. Organizations who now wish to collect personal data must respect that right and be upfront about how and why they will collect their personal data. Once permission is obtained, and the GDPR requires that it must be just as easy for the data subject to withdraw that permission as it was to give it, a number of responsibilities that the data collecting company must respect come into play.

In order to meet these responsibilities, organizations have had to rationalize their data collection strategies beginning with how they obtained the data subject's permission. Once obtained, it becomes critical that an organization can identify and manage the personal data it has collected, bringing together disparate systems to have a consolidated view on what information they have and how it is being used. This consolidated view is absolutely necessary when responding to requests to either transfer a data subject's personal data or to erase it completely. Besides illustrating who's in control of the data, this is probably the greatest challenge that the GDPR has presented to organizations.

Further down the list of responsibilities but no less important is protection of the collected data from cyber attacks and breaches. This is the component of the GDPR that got most of the attention prior to it becoming effective due to the potentially eye-watering fines that can result from a data breach. Where the previous regulations had little to no "stick" aspect to it, the GDPR certainly contains a large one. Maybe this is the first time where not getting hit with the stick is actually the carrot.

In the event of a data breach, organizations have a window of a maximum of 72 hours after its discovery to report it. An interesting twist in the regulation however, is that the organization can make a decision as to whether or not the data breach is actually severe enough to report it, that is "the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons,". Should it decide to report the breach - and reporting a breach does not automatically equate to a fine – a significant amount of information needs to accompany the notification. This makes knowing where personal data is located even more important than ever and increased the challenge to organizations preparing for the GDPR.

The significant fines associated with the GDPR – 4% of annual global turnover or $20M - are designed to keep organizations attention on their obligations to keep collected data safe. Although no one can predict how individual data protection agencies will react when the first major data breach occurs in the post-GDPR era, the regulations finally have a strong enforcement potential that was lacking in the previous regulations. In fact, in some EU member states the maximum pre-GDPR era fines that could be assessed were actually limited by the regulations themselves.

WHAT DOES THE GDPR MEAN TO NON-EU BASED ORGANIZATIONS?

This is probably the most contentious, as well as the most interesting, aspect of the GDPR. Based on the assumption that personal data is owned by the data subject, the EU decided that anyone resident in any of the EU member states – citizen or not – was protected by the provisions of the regulation. The physical location of the organization collecting that data was immaterial. However, the enforcement of the regulations, and potential fines in case of a data breach, is still an open question and most likely has teams of lawyers preparing for the first major challenge to the GDPR.

In the case of large, multi-national firms with operations in the EU the scenario is reasonably straightforward and there is a history of the EU assessing fines against these organizations. The real question however concerns those organizations who are able to offer goods or services to an EU resident but do not have a physical presence inside of the EU.

"ON THE INTERNET, NOBODY KNOWS YOU'RE A DOG." (THE NEW YORKER, 1993)

In the same way that the Internet inspired the above cartoon line, it has also opened significant business opportunities to all sizes of organizations but particularly for small and medium business. In terms of data protection however, these same organizations are statistically more vulnerable to cyberattacks and data breaches.

Fortunately, the EU does make a distinction between those organizations whose websites make their goods and services available globally from those organizations which make an effort to solicit business from EU residents. These efforts can include offering goods and services in local currency, language or domain names as well as tracking/ monitoring the behavior of online visitors.

However, in these early days no one is completely sure of how the EU will approach dealing with a non-EU organization which has violated the regulation.

Despite the significant fines and reputational damage associated with GDPR non-compliance, some companies (EU or non EU based organizations) may still be tempted to not disclose when a data breach has occured or the full extent of it. This would be a huge mistake. It's important to remember that the GDPR is all about forcing organizations to be more transparent and responsible.

WHAT ARE THE EARLY OBSERVATIONS OF THE POST-GDPR ERA?

So far, for most of us the most visible sign of the GDPR taking effect is the number of emails requesting that you either review the organization's revised data privacy policy and/or explicitly opt-in in to continue to receive information from the organization.

An interesting side-effect that has occurred as a result of the GDPR is the number of non-EU websites which have decided to block their content from EU based readers. Whether this will be permanent or a temporary strategy while the organization has a better feel for how the GDPR will play out, only time will tell.

IT'S MAY 26. WHAT SHOULD ORGANIZATIONS DO NOW?

For most organizations it's about fixing the most obvious deficiencies first. And for most organizations that means making sure that the most visible part of the organization, their web site, conforms to the regulations. If it's an organization that uses personal data as part of the outbound marketing activities, it's imperative that they have reached out to their installed base to re-obtain their permission to continue to hold and use their personal data.

Behind the scenes however, each organization needs to take stock of their data collection process and procedures and work on the much harder task of identifying and organizing the personal data that they hold. We can assume (hope) for a moment that new data, that is the data obtained after May 25 2018, are treated in a GDPR appropriate manner. Depending upon any number of factors including what sort of legacy IT systems are still in use and/or an organization's cloud strategy this process could be significant.

But there is one other aspect where organizations might be playing a dangerous game and that's with their cyber defenses. Since most organizations, and certainly the larger enterprises, service providers and government entities already have network security technologies in place, they are inclined to rely on existing capabilities while they address other aspects of GDPR compliance.

The problem with this approach is whether or not their current capabilities can meet the challenge of both preventing attacks from becoming a data breach and being able to meet the 72-hour reporting window. Because organizations are more likely to be fined for a data breach than any other form of non-compliance, organizations should be looking at their current capabilities much more closely, identifying those areas which require attention and developing a comprehensive plan to address these issues.

But more importantly organizations should take advantage of the GDPR as the opportunity to initiate a much larger review of their cyber security capabilities from a more holistic approach rather than which products/technologies/vendors they have and which one they need to get.

In this environment of increased scrutiny and regulations and a threat landscape that has increased both in volume and complexity, organizations must have absolute confidence that their network security infrastructure has the ability to comprehensively protect their network. This means blocking as many attacks as possible, regardless of where they occur, and quickly detecting any intrusions that do make it through the first line of defense. Once detected, it should be able to respond to the intrusion to minimize any potential damage. By doing so organizations will be better able to determine if reporting of the incident to the appropriate data protection authority is warranted or not.

However, there is no one technology which can do all of this. Organizations reviewing their operational capabilities in light of meeting the stringent requirements of the GDPR should take this opportunity to look beyond just what the GDPR calls for. In particular, organizations should look as to whether their current network security posture can fully support their current business requirements and foreseeable future requirements.

CONCLUSION

To some, the GDPR signals the beginning of a new era that resets the relationship between data subject and data collector in favor of the data subject. To others, it's another example of an unnecessary and over-reaching regulation, particularly in the eyes of non-EU organizations. While only time will tell how effective the GDPR will be, the expectation is that increased awareness about the collection, use and protection of personal data is very much an improvement on current practices.

The other important thing is that organizations should take advantage of the GDPR as a business opportunity rather than a one-off compliance effort. GDPR compliance is a continuous process that will need to be constantly evaluated and adjusted over time.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

August 10, 2018 9:01 AM 245116 0 1 EN

Public:01_BROCHURES:17_MISCELLANEOUS:Manifesto_GDPR:manifesto_GDPR-A4.indd