Globanet

2018 GLOBANET **GDPR REPORT**

CHAPTER 1:
Fears of Brand Damage, Job Loss, Company Livelihood Surface as Businesses Try to Come to Grips with GDPR Compliance

The deadline looms on the horizon: **25 May,2018**. That's the day the European Unionwill enact some of the most stringent data privacy regulations the world has ever seen. These regulations impact thousands of organizations around the globe - virtually any company that does business within the EU and holds personally identifiable information (personal data) on EU residents.

Despite that fast approaching deadline, research commissioned by Veritas Technologies shows that **86%** of organizations worldwide are concerned that a failure to adhere to the upcoming General Data Protection Regulation (GDPR) could have a major negative impact on their business. In addition, almost half **(47%)** of organizations fear they won't meet the requirements of the legislation, and many have critical concerns about what that could mean for their employees and their company as a whole.

Of course, organizations are worried about the significant fines that could be levied, which could be as high as **€20 million ($21.5m)**, or **4%** of annual revenue – whichever is greater. But, the research shows fears go much deeper.

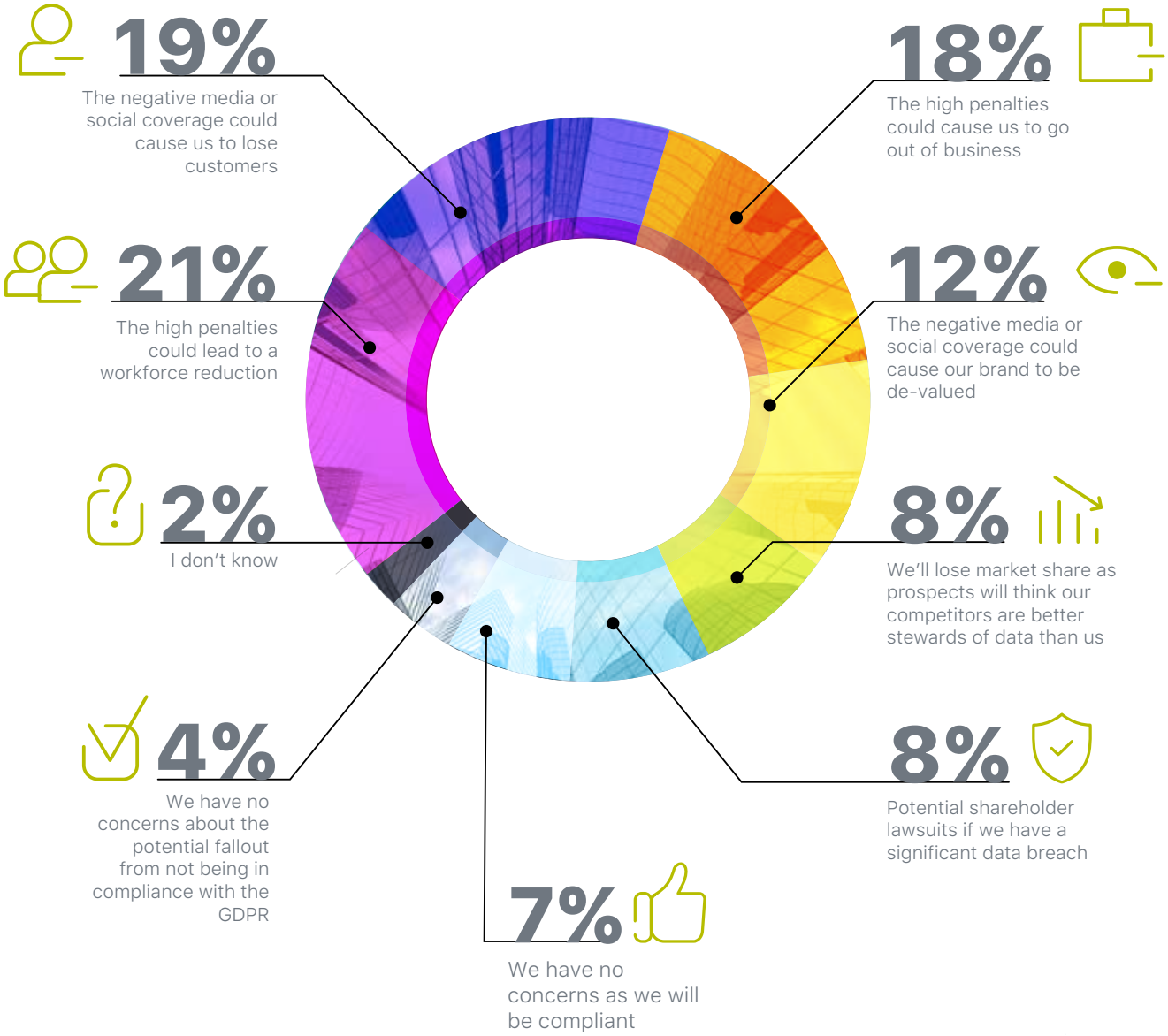
Nearly one in five **(18%)** respondents are worried that non-compliance could ultimately put their organization out of business. Additionally, one in five **(21%)** are very worried about potential layoffs, fearing that staff reductions may be an inevitable way to offset financial penalties incurred as a result of GDPR compliance failures.

Companies are also worried about the impact noncompliance could have on their brand image, especially if and when a compliance failure is made public, potentially as a result of the new obligations to notify data breaches to those affected. Nearly one in five **(19%)** surveyed fear that negative media or social coverage could cause their organization to lose customers. An additional one in ten **(12%)** are very concerned that their brand would be de-valued as a result of negative coverage.

Organizations are worried about the significant fines that could be levied, which could be as high as **€20 million ($21m)**, or **4%** of annual revenue – whichever is greater.

"What concerns you the most about the potential fallout from your organization not being in compliance with the GDPR?"

Asked to all 900 respondents



Lack of Technology Hindering GDPR Compliance

The research also highlights an important finding among those surveyed: many organizations don't have the proper technology to address the regulations. In fact, almost a third **(32%)** of respondents are worried their organization doesn't have the necessary technology to manage data effectively, something that could jeopardize their ability to search, discover and review data – all essential criteria for GDPR compliance.In addition, nearly forty percent **(39%)** of respondents are worried their organization isn't able to accurately identify and locate data.

This is a critical competency the regulation mandates considering that, when requested, businesses must be able to locate PII within a very short time frame.
Organizations are also extremely concerned about their ability to value data. More than four in ten **(42%)** report that they do not have a way to determine which data should be saved. Under GDPR, organizations can retain personal data as long as it being used for its original intent, but must delete it once it is no longer needed for that purpose. Failure to adhere could result in the top fine, which has substantial ramifications.

"What concerns you most about readying your business for GDPR?" Showing the top five concerns. Asked to all 900 respondents

In order to address these technology challenges, the research shows organizations are taking more of a proactive role in seeking outside assistance. Nearly two thirds **(65%)** of respondents say that their organization has worked, or is currently working with, third parties to support their GDPR efforts. And organizations are not afraid to assign a significant budget (albeit one that is still dwarfed by the size of potential fines for non-compliance) to support their GDPR readiness: on average, respondents expect their organization to have spent over one and a quarter million Euros **(€1,360,567)** or **$1,432,176** by **May**, **2018** in order to achieve full compliance. It's imperative that organizations around the world take immediate steps to achieve compliance. Now may be a good time to seek an advisory service to check readiness and create a path forward. The clock is ticking and it's not just fines that are at stake, but jobs, brand reputation and the livelihood of businesses globally.

13 KEY GDPR TERMS

1 **PERSONAL DATA** – This is the broad term for any information related to an individual or 'Data Subject', that can be used to directly or indirectly identify the person. This can be anything from a name or address to a fingerprint or banking details.

2 **BINDING CORPORATE RULES (BCRS)** - The set of internal rules adopted by multinational companies in to define their global policies on international data transfers within the same corporate group towards countries that don't share the same level of protection.

3 **PROCESSING** – An automated or manual action performed on personal data, for example collection, organization or recording. For processing of personal data to be lawful under the GDPR, businesses must identify a lawful basis for this action.

4 **DATA CONTROLLER** - Like the existing Data Protection Act (DPA), the GDPR applies to Data Controllers who process personal data. So first, who is the Data Controller? This is a person who decides the purpose for which any personal data is to be processed and the way in which it is to be processed. This can be decided by one person alone or jointly with other people.

5 **DATA PROCESSOR** - Unlike the DPA, the GDPR introduces specific responsibilities for the Data Processor. These are third parties that process data on behalf of the Data Controller and includes IT service providers.

6 **CONSENT** - The concept of "consent" is foundational to EU data protection law. In general, the validly obtained consent of the data subject will permit almost any type of processing activity, including Cross-Border Data Transfers.

7 **DATA PROTECTION OFFICER** - A Data Protection Officer is someone who is given formal responsibility for data protection compliance within a business. Not every business will need to appoint a data protection officer – you need to do so if:

- Your organization is a public authority; or

- You carry out large-scale systematic monitoring of individuals (for example, online behavior tracking); or

- You carry out large-scale processing of special categories of data or data relating to criminal convictions and offenses.

8 **DATA PROTECTION AUTHORITY (DPA)** – Every country will have its own DPA, a national authority responsible for the protection of data and privacy as well as implementing and enforcing data protection law. For example, in France it's the Commission nationale de l'informatique et des libertés (CNIL) and in the UK it's the Information Commissioner's Office (ICO).

9 **BIOMETRIC DATA** - Personal data that resulted from specific processing related to physical and behavioral features of a person, which allows the identification of that person.

10 **DATA SUBJECT** – When a piece of data relates to an individual, then they are known as the data subject. This could be you, me or anyone as long as they can be clearly identified from the data in question.

11 **RIGHT TO BE FORGOTTEN** - The right to erasure of personal data or 'the right to be forgotten' enables an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

12 **PSEUDONYMOUS DATA** - Some sets of data can be amended in such a way that no individuals can be identified from those data (whether directly or indirectly) without a "key" that allows the data to be re-identified. A good example of pseudonymous data is coded data sets used in clinical trials.

13 **CROSS-BORDER PROCESSING** - Processing of personal data when the controller or processor is established in more than one Member State, and the data processing takes place in more than one Member State, OR processing activities that take place in a single establishment in the Union, but that affects data subjects from more than one Member State.

Methodology

Globanet commissioned independent technology market research specialist Vanson Bourne to undertake the research upon which this report is based.

A total of **900** business decision makers were interviewed in **February** and **March 2017** across the US, the UK, France, Germany, Australia, Singapore, Japan and the Republic of Korea. The respondents were from organizations with at least **1,000** employees, and could be from any sector. To qualify for the research, respondents had to be from organizations which do at least some business within the EU.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates had the opportunity to participate.