Top Line

Ready or Not? GDPR Maturity Across Vertical Industries

Sponsored by: BlackBerry

Duncan Brown
April 2017

GDPR CHANGES THE GAME

Much has been written of the incoming General Data Protection Regulation (GDPR). There is a lot of hype, and a not inconsiderable amount of myth and misunderstanding, none of which negates the fact that GDPR represents a fundamental shift in the risk associated with processing personal data.

Why is GDPR such a big deal? Essentially, the principles and core objectives of GDPR are the same as those in the existing 95/46/EC data protection directive currently in force. While there are some new requirements to consider, GDPR represents more of a continuation of existing regulatory intentions, rather than a step change in requirements. The main difference between the existing and new law is what happens when things go wrong.

Regulators, also known as supervisory authorities, in charge of data protection wield a number of hefty sticks with which to enforce the new regime under GDPR. These include (but are not limited to):

- Substantial fines for non-compliance, up to 4% of global annual revenue
- Mandatory breach notification, which could affect company reputation
- The right of data subjects to be represented by a third-party body in the pursuit of a complaint, similar to class action lawsuits
- A suspension of the right to conduct personal data processing (which could severely restrain a company from operating)

The net effect of these sanctions is that the processing of personal data now represents a substantial risk to the operations of most businesses. It is the intention of the regulation that these sanctions force a change in behavior towards processing personal data. Companies will be incentivized no longer to treat personal data protection as a minor issue: it will now feature highly on every company's risk register.

The scope of GDPR is extensive: the definition of personal data includes any attributes that do – or can – identify an individual. This includes the possibility of characteristics that separately would not be identifiers, but combined have that effect. For example, an IP address combined with some other information, such as cookie data, can identify an individual computer, and therefore a person. In addition, GDPR defines special categories of data that require additional protection. These are sensitive data types, and include health, racial or ethnic origin, political opinions, genetic data, and so on.

GDPR also has an extensive geographical scope. Basically, the law follows the data, making the location of processing irrelevant. This means that data moved outside the geographic boundary of the EU – a so-called data transfer – remains within the scope of GDPR. This extra-territoriality

clause extends the jurisdiction of the EU to any corner of the world that is processing data relating to people in the EU (including temporary visitors). There are strict rules on the mechanisms for legally transferring data beyond the EU, in order to make sure that the destination country or individual processor applies rules similar to those prescribed in GDPR.

Much of GDPR is about process. But some elements can only be enabled by technology, and others are made manageable or cost-effective only through technology. GDPR is not specific about the types of technologies an organization should deploy. This is deliberate: the legislators want to avoid a situation where technology advances mean that GDPR is out of date. So the text of GDPR is vague and generic in many places. One of the areas that is particularly loosely defined is the concept of state of the art (Articles 25 and 32). Companies are obliged to "take into account" the state of the art in determining which technology to deploy. Note that they are not obliged to implement state of the art: instead they must balance the benefits against the cost of a particular technology and the risks associated with the data being processed, along with other contextual attributes that pertain to each company. It is up to each company, therefore, to define what state of the art means to it, and to document why it has (or has not) implemented it.

Companies have a lot to do to reach compliance with GDPR. But the clock is ticking: the law was signed into force in April 2016, and with a two-year transition period will be applied (enforced) from May 25, 2018.

IDC has conducted an extensive survey of organizations across Europe to determine their approaches and plans for implementing GDPR. This paper provides some insight into what different types of company are doing to ready themselves for compliance.

IN A STATE OF READINESS — OR PANIC?

How are companies approaching GDPR? In many ways, the answer depends on their starting point. Companies that have a strong understanding of personal data throughout the organization, with rigorous data management processes and controls, are generally at a good starting point with regard to GDPR. Companies that have been less focused on personal data and have been loose in their adherence to existing laws will struggle. This starting point is influenced by a number of factors, the main ones being:

- Industry: Companies that operate in a regulated industry are generally more prepared for GDPR, mainly because they understand the process of compliance. Even though they may not have an ideal resume with regards to data management, they have a mechanism for reaching compliance. Clearly, those industries that do focus on personal data as well have a greater advantage.
- Size: Generally speaking, larger firms tend to have more resources to apply to obligations like GDPR and have a greater standard of process and technology maturity.
- Location: Some countries in the EU have a robust set of data protection rules that correspond closely with the incoming GDPR. Other countries in the EU have a much lighter data protection regime. These variances also exist beyond the EU. Companies operating predominantly from one country will naturally assume the required level of data protection prevalent in that country. GDPR changes this situation by unifying (to a large but not complete extent) the rules and their application across all EU countries. Extra-territoriality also extends the application of the law globally.

Is GDPR an Obstacle or an Opportunity?

For some companies, GDPR represents the chance to re-architect their information governance regimes, orientating the management of personal data around recognized best practices. The motivation for this could be a desire to operate efficiently and cost-effectively, or even to create competitive advantage by processing customer data appropriately. For other companies, GDPR is a chore, a distraction from other business priorities that must be addressed, but with the minimum effort.

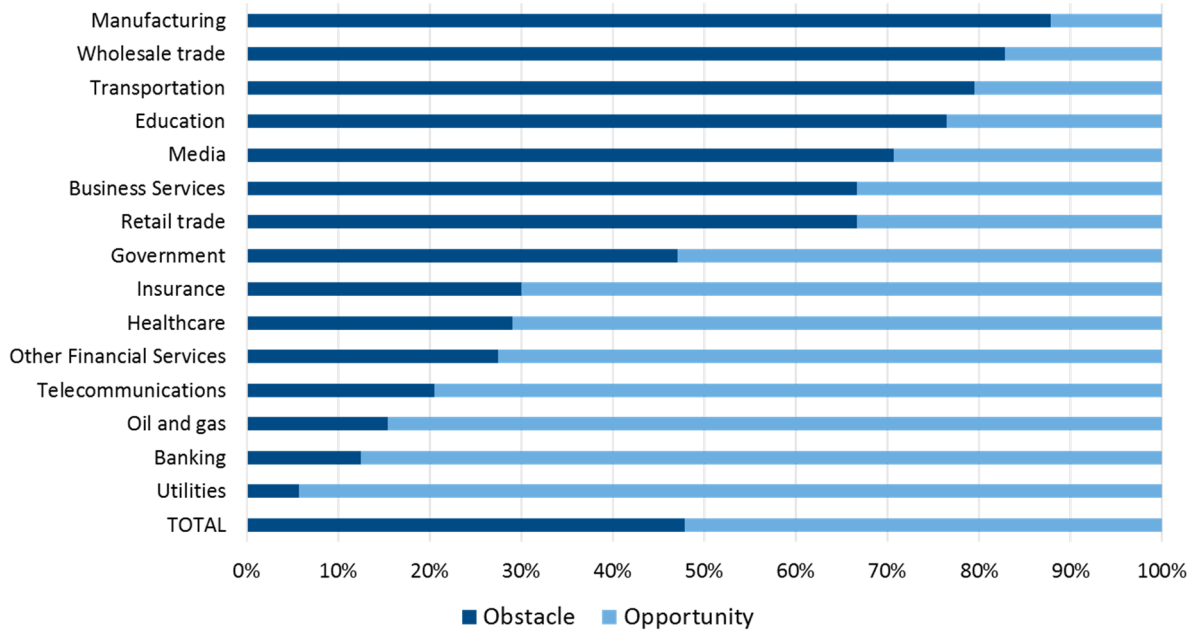
Overall, the split between those companies seeing GDPR as an opportunity and those regarding it as an obstacle is remarkably even, almost 50:50 (see Figure 1). But this even spread masks a high degree of variance between industries. There is a world of difference in the approach of companies in regulated industries such as utilities, banking, oil and gas, and telecommunications: these companies tend to be GDPR "Opportunists." In contrast, manufacturing, wholesale trade, transport, media, and (worryingly) education are much more GDPR "Obstaclers."

Another driver in the overall approach to GDPR is the personnel involved. Is GDPR an IT issue or a legal and compliance concern? The answer is both, and in fact is broader still. The impact of GDPR is far-reaching, and should involve sales, marketing, HR, lines of business, and, of course, the board. The leadership of GDPR may also then depend on who within a company has the prevailing authority and gravitas, and their vision will influence the company's approach.

FIGURE 1

Does GDPR Represent an Opportunity or an Obstacle?

Q1. Which of the following best describes your organization's approach to GDPR compliance?



Respondents were given range of options, which were then classified by IDC into two broad categories

Source: IDC EMEA GDPR Survey, 2017. n=560

Of course, it's not quite completely black and white: there are shades of grey. There is a middle ground that appears to be hedging their options. The primary "hedger" is government, most likely torn between adopting best practice and working within the constraints of public finances. We'd like to see retail and business services (such as legal and accounting) also move into this position. Firms in these sectors are typically not the most mature in information governance and security, but they do recognize the importance of GDPR to their business. Each of them processes substantial personal data, much of it sensitive.

What Drives the Overriding Approach to GDPR?

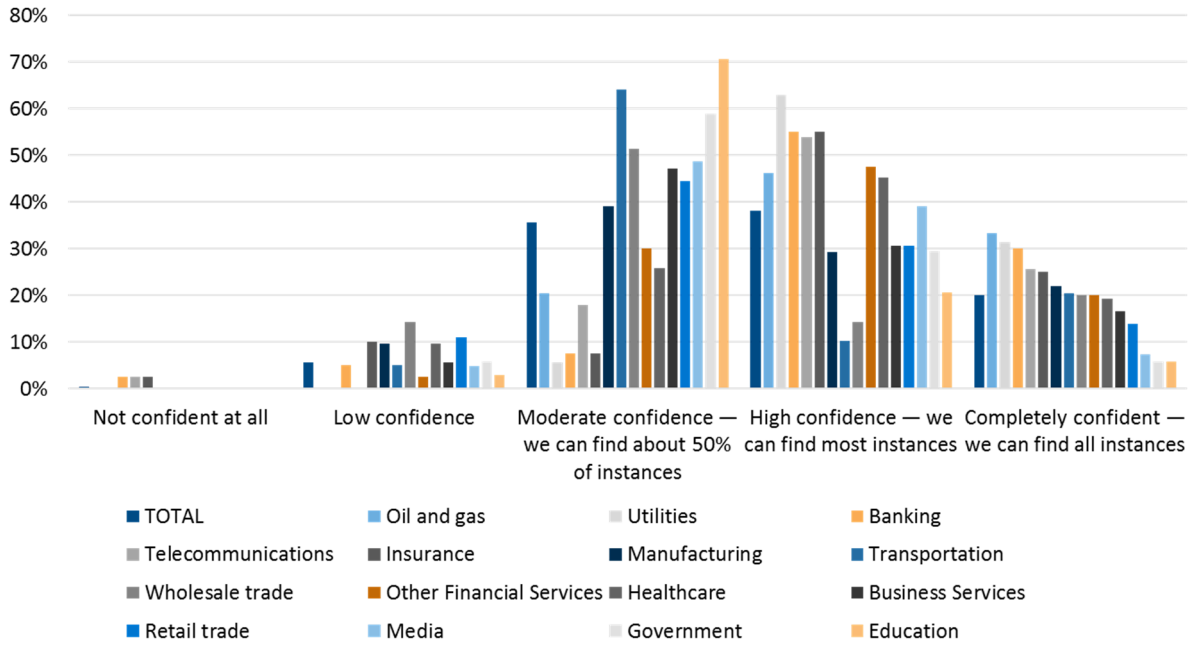
What are the factors in an organization deciding how to approach GDPR? Our research indicates that the starting point is the primary deciding factor in determining companies' view of GDPR as an opportunity or an obstacle. One way of measuring the company's initial position with regard to information governance is to assess its ability to identify and locate personal data in the organization. This is a requirement of GDPR (article 30, Records of processing activities), and is also a prerequisite for subsequent rights of access (article 15), rectification (article 16), and erasure (the right to be forgotten, article 17) (there are other rights too). So, it's a good proxy for readiness.

Our research shows that there is a strong correlation between the confidence of companies to identify and locate all instances of personal data and the attitude towards GDPR as an opportunity (See Figure 2). On the other hand, more wholesale trade companies have low confidence in their ability to find personal data than in any other sector, and there are fewer educational organizations confident of finding all personal data than in any other industry.

FIGURE 2

Where's my Data?

Q5. How confident are you that you can identify and locate every instance of an individual's personal data in your systems in the event of an individual requesting removal?



Source: IDC EMEA GDPR Survey, 2017. n=560

Let's remind ourselves of what this chart shows. On average, 42% of companies in Europe think they can find – at best – half the instances of personal data in their organization. In education, it's 73%, and in transportation it's 69%. Knowing what data you have is step one on the road to GDPR compliance, and yet many companies admit they have no idea where half of it is.

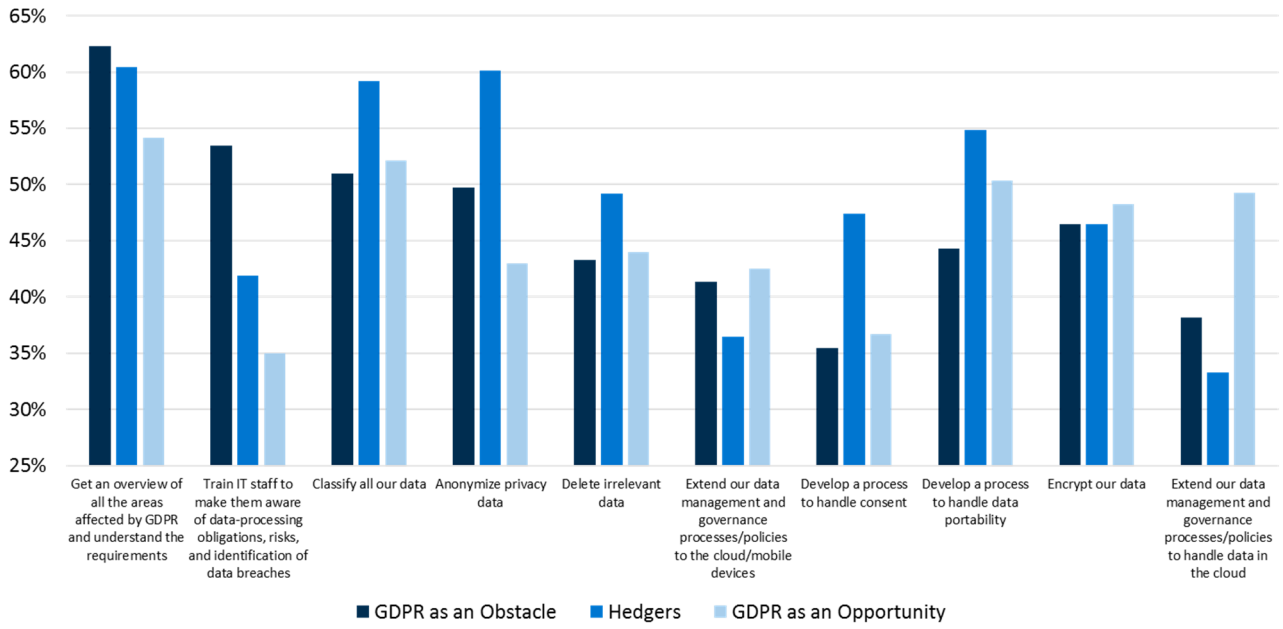
What are the GDPR Priorities of Companies?

What should companies focus on to be best positioned for GDPR? Factoring in sector tendencies towards seeing GDPR as an opportunity or obstacle, and with an understanding of their starting point, our research reveals that companies with low ambitions recognize the need to start with the basics (see Figure 3). It is no surprise that manufacturing and media companies are most likely to be focused on just getting an overview of the impact of GDPR on their business. We are relieved to see that healthcare and business services (including legal) companies are focusing strongly on deleting irrelevant data and handling consent. Advanced companies with great maturity and an opportunistic vision, such as banking, telecommunications and utilities tend to focus on the detail of GDPR, such as data portability, consent, and moving data governance processes to cloud and mobile devices.

FIGURE 3

What are Companies Focusing on?

Q7. Which compliance actions do you think will be the most challenging to execute?



Some responses have been removed for clarity

Source: IDC EMEA GDPR Survey, 2017. n=560

Note also that Obstaclers are more likely to be doing nothing at all, so their overall interest and activity in each of the compliance actions is lower than average.

Obstaclers focus on the basics, including training IT staff in data breaches (but not so much on educating all staff on the impact of GDPR). Hedgers are interested in these, but also in anonymizing data and deleting redundant and irrelevant data. Opportunists focus on detailed requirements, such as data portability, encryption, and extending information governance to the cloud and mobile platforms.

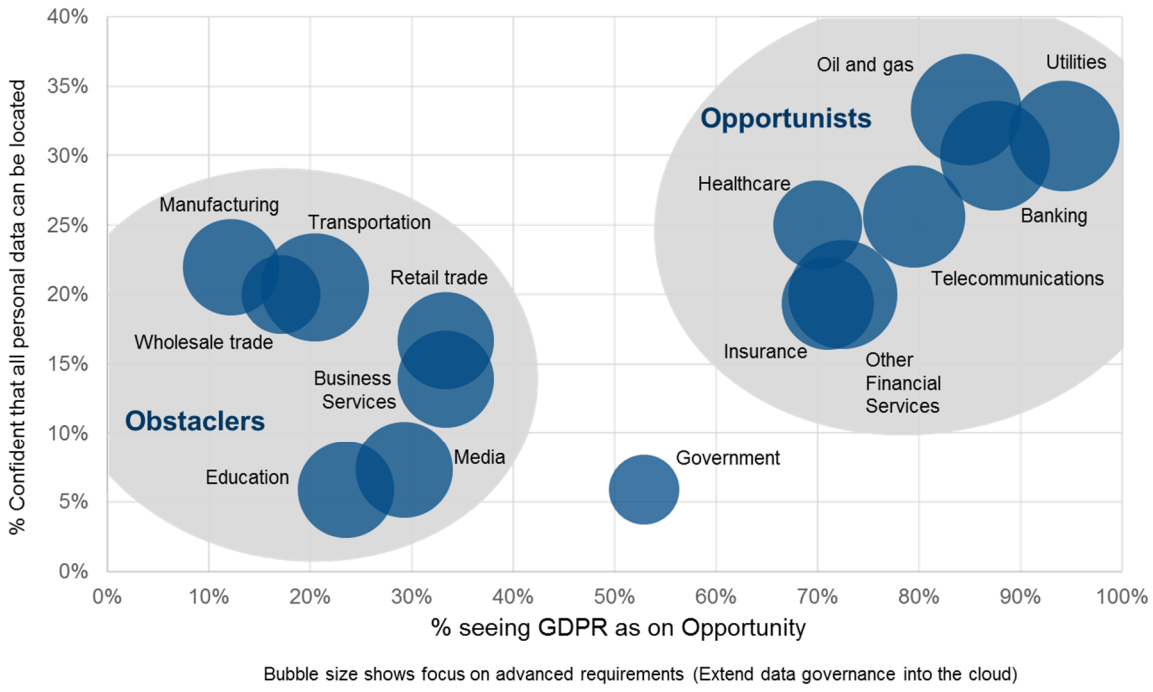
Overall GDPR Maturity Assessment by Vertical

Overall, there are two broad camps of readiness with regard to GDPR (see Figure 4). Opportunists are starting from a position of relative advantage. They generally have better information governance processes in place and are more likely to have more mature security capabilities. They seek to leverage these attributes, adopting best data protection practices and perhaps even establishing competitive advantage. Obstaclers, on the other hand, see GDPR as a hurdle to normal business, something to be surmounted but which is in the way of their strategic goals.

Neither of these approaches is wrong. Companies can take either position, as long as they do so consciously and have taken a risk-based path to determining their approach. The fact that GDPR is not prescriptive creates this flexibility, so it can be many things to many organizations. But GDPR requires that organizations understand their obligations and responsibilities, and document their processing decisions based on an assessment of risk.

FIGURE 4

GDPR Readiness by Industry



Bubble size shows focus on advanced requirements (Extend data governance into the cloud)

Source: IDC EMEA GDPR Survey, 2017. n=560

CALL TO ACTION: GET MOVING ON GDPR

Companies in all sectors are faced with substantial challenges to prepare for GDPR. Although there are wide differences between sectors, we think there are basic steps that most companies can follow to be successful in their GDPR programs:

1. Understand the strategic aim of your GDPR program. Are you an Obstacler or an Opportunist? Deciding which you are is key, as it determines the broad approach to compliance and will define your end goals. It may depend on your starting point related to your existing security and information governance capabilities. But budget and an assessment of the risk of personal data to your organization are also key factors.
2. Have a view on state of the art. Remember: you're not obliged to implement state of the art technologies and processes, but you do need to know what these are in order to make informed risk-based choices.
3. Find your data. Even in the most mature and sophisticated companies only one-third is confident they know where 100% of their personal data resides. Knowing where personal data is located is a pre-requisite for compliance with the core principles of GDPR (see Article 5), and for the enforcement of rights of access, rectification, and erasure.
4. Prioritize data protection activities. This will depend on your starting point, so you need to identify this position early on in your activities. What data or business process represents the greatest risk? Knowing this will direct your early actions and map out the remainder of your program toward May 2018.
5. Document everything. Any decision that you make regarding GDPR provides a narrative of your strategic objectives, and underpins a risk-based assessment of the situation in your company. You must be able to evidence this, particularly where possible non-compliance is being investigated.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015
www.idc.com

Copyright 2017 IDC. Reproduction is forbidden unless authorized. All rights reserved.