WEBROOT®
Smarter Cybersecurity™

# Ready or Not:
## SMBs and the GDPR

# Introduction

The deadline for General Data Protection Regulation (GDPR) compliance draws closer for organisations across the world. With fewer than 12 months to ensure compliance with this radical new legislation, the issue must now be at the top of the agenda.

The full GDPR requirements are extensive, and many businesses will have to do considerable work to meet even the most basic among them. Indeed, one fifth of UK organisations have not even heard of GDPR, highlighting the work that remains to be done.

Companies of all kinds need to ensure that they have the right capabilities, from responding to data breaches in a timely manner to providing individuals with a clear outline of how their personal information is being used. Webroot surveyed 501 small- to medium-sized businesses (SMBs) in the UK to uncover actions and attitudes around the process of becoming compliant to GDPR.

# Who is impacted?

Due to the sheer scale of the GDPR, you might think its requirements apply only to large organisations that deal with huge masses of customer data each day—global brands such as Amazon and eBay, for example.

The reality is very different; any company that deals with the personal data of European Union (EU) citizens—regardless of size, industry or location—must comply with the new legislation. That includes ten person organizations up to the enterprises mentioned above.

Many small businesses may find adhering to the GDPR to be an intense burden. The complex regulations introduce a level of scrutiny around data management that many SMBs are unlikely to have experienced before. The risks for failing to comply are steep, with the maximum financial penalty of up to €20m or 4 percent of annual turnover (whichever is higher).

# About the survey

With so little time remaining before the GDPR takes hold, we wanted to explore the level of readiness—both actual and perceived—demonstrated by SMBs across the UK. To that end, we questioned 501 companies in the UK, of which more than 300 had active operations in another country within the EU. All of these companies will need to be fully compliant with this sweeping new legislation in 12 months, and will need to remain so after Brexit.

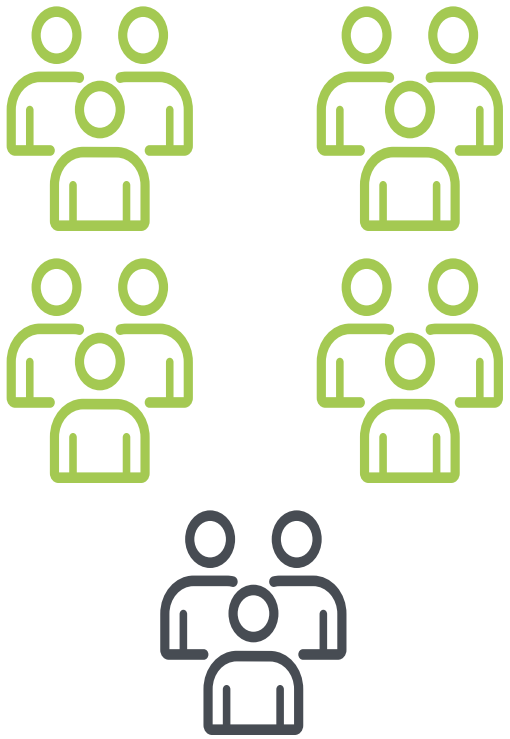
# Hidden misconceptions

Overall, basic knowledge about the GDPR is relatively high. Four in five of the companies surveyed (81 percent) had at least heard about the impending regulations. This leaves one-fifth who have not; a number which rises to 40 percent amongst companies with a turnover under £100k.

Scratch the surface and things become more problematic.

Of the 81 percent of survey respondents that said they are aware of the GDPR, only two-thirds were able to provide an accurate description of its purpose.

Around a quarter (26 percent), for instance, believe the GDPR is simply an advisory measure, and one that allows participating organisations to highlight their compliance online and in marketing material, rather than it being compulsory law. And nearly a tenth (8 percent) of SMBs believe the GDPR is applicable only to very large or multinational companies.



**1 in 5 companies haven't heard of GDPR**

# What about Brexit?

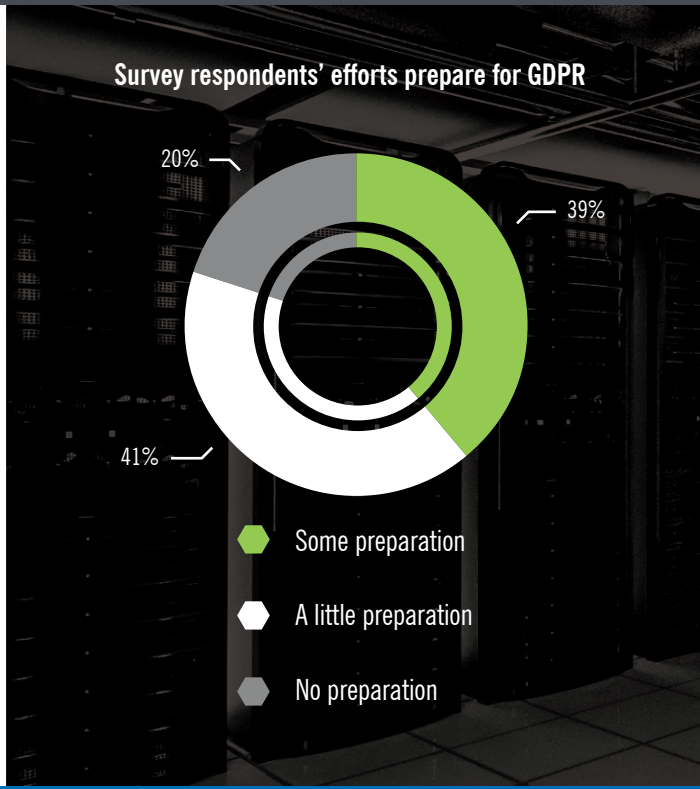
Unfortunately, the uncertainty about the full extent of the GDPR doesn't end with its applicability. Britain's continuing preparations to leave the European Union (EU) leave many respondents with even more questions; more than half (52 percent) believe they will no longer need to comply with the GDPR once Brexit negotiations conclude.

# Rushing to get ready

The confusion demonstrated by UK SMBs towards the GDPR may explain why many have yet to push ahead with their compliance preparations.

When asked what actions they had taken to adhere to the new regulations, some said they have put "several" (39 percent) or at least "one or two" (41 percent) processes in place. One fifth (20 percent) admitted that they haven't yet begun compliance work.

Considering the extensive checklist for GDPR preparation from the Information Commissioner's Office (ICO) takes the form of a comprehensive 12-step plan, it should come as little surprise the authority urges organisations to "start planning [their] approach to GDPR compliance as early as [they] can."[1]




[1] Preparing for the General Data Protection Regulation (GDPR) – Information Commissioner's Office, March 2016

The ICO goes on to note that the process of bringing a business into compliance with the new regulations can be complex, resource intensive and, in some cases, very expensive. With that in mind, it is troubling that only one-third of SMBs (29 percent) have allocated budget to help ensure they will be compliant when the GDPR comes into effect, particularly when we consider how many of those organisations believe the legislation is either inapplicable or simply advisory.

The apparent reticence to prepare is perhaps best explained by some underlying reservations that SMBs have. Although the regulations focus strongly on improving standards of protection around customer data, only a quarter of respondents (27 percent) believe the GDPR will actually make that information more secure.

Doubts about the effectiveness of the regulations translate into frustration. Almost one-fifth (19 percent) describe the GDPR as "an unnecessary hindrance on businesses", and more than a quarter (27 percent) consider it unfair to hold all businesses to the same standards, regardless of their size.

Much of the apprehension about the GDPR may stem from a generally lackadaisical attitude towards cybersecurity as a whole; almost half of the businesses surveyed (46 percent) said they don't believe their business is at risk of a cyberattack. This misconception couldn't be further from the truth.

> *...only one-third of SMBs (29 percent) have allocated budget...*

> *...a quarter of respondents (27 percent) believe the GDPR will actually make that information more secure.*

The Department for Culture, Media and Sport's (DCMS) Cyber Security Breaches Survey 2017 shows in the last 12 months, more than half of UK SMBs (52 percent) were targeted by attackers. Businesses that hold their customers' personal data are almost 15 percent more likely to be breached than those that do not (52 percent compared to 37 percent), and around a third of businesses (35 percent) that consider cybersecurity a low priority suffered a breach within the past year.

The DCMS report goes on to say, "breaches are still common even among businesses who do not consider cybersecurity to be a priority, or who may not think they are exposed to risk." Any organisations that do not consider cybersecurity a priority need only look at the widespread disruption caused by the recent WannaCry cyberattack as a case in point for putting it at the top of the agenda.

As the activation date for the GDPR comes closer into view, the culture of denial that this research found becomes ever more dangerous.

# Fear of failure dominates

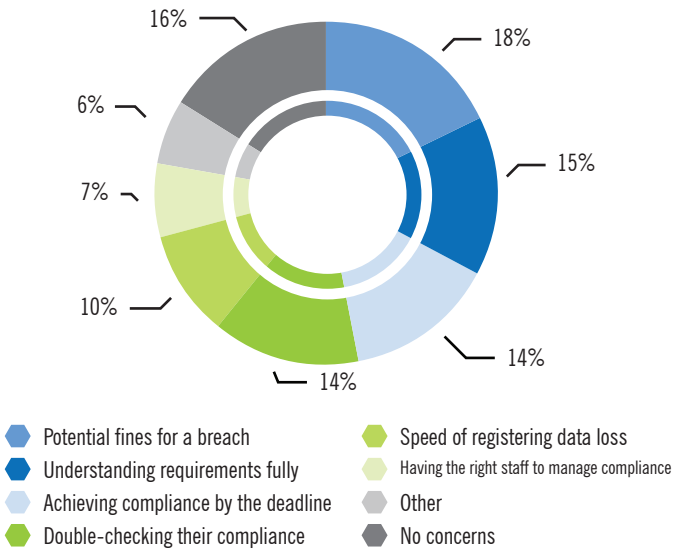
Although many SMBs seem to be complacent about their exposure to internet risks, they are more grounded when it comes to their likelihood of complying with the GDPR.

When asked about confidence in their organisation's ability to meet the full regulation requirements, only half (51 percent) said they were certain their business would be able to fulfil its obligations.

For the rest, the uncertainty around meeting the stringent GDPR criteria creates cause for concern. When asked what worried them most about failing to comply, almost a fifth (18 percent) said it was the potential fines they might owe in the event of a breach. This is unsurprising, given the major escalation of liability under the GDPR. More than a tenth of respondents cited anxiety about understanding the requirements of the regulation (15 percent), achieving compliance before the deadline (14 percent), and double-checking that they are in line with the regulations (also 14 percent)

**Confidence in ability to meet full regulation requirements**


**49% of respondents are not confident their organisation will be able to fulfil requirements. This graph represents factors contributing to their concern.**



Even beyond these issues, additional doubts linger. Thoughts about the speed with which they would need to register the loss of personal data (10 percent) and having the right staff in place to implement and manage compliance programmes (7 percent) continue to plague a number of SMBs.

In total, only a small number (16 percent) said they had no worries at all about their ability to comply.

## Work to be done, but context is key

It would be easy to dismiss Britain's SMBs for a lack of preparedness with regard to GDPR. However, to do so fails to take into account the complexity of the regulation and the myriad other issues that small businesses have to contend with in their daily running.

The GDPR seeks to better protect customers of all types within the European Union, an issue that SMBs should find indisputably relevant. At the same time, the finer details of the GDPR also are very complex, presenting small businesses and entrepreneurs with a variety of issues many never considered before.

## Tips for Businesses:

- **Act now.** This is the biggest change to data protection laws since the current EU Data Protection Directive was passed in 1995. Getting ready for the GDPR will require time and resources to implement new processes. It's crucial to get started now so your business is ready.
- **Know your data.** Find out what data and personal data your organisation has, where it's stored and in what systems. Planned audits and allocated resources for this work should be scheduled in sooner rather than later.
- **Delete.** Make sure that any data you do not need is deleted securely. There are legal requirements to maintain certain types of data. But when data retention is not required, professionally disposing of it with specialist equipment or software helps reduce risk.
- **Communicate.** With any process change, effective communication is essential. Proper internal communications to all employees and external communications to suppliers will help make them aware of changes and give them time to amend their own processes in good time.
- **Assess.** Consider a privacy impact assessment. When auditing the business's processing of personal data in relation GDPR, decide if a privacy impact assessment is required. Consider whether invasive means of collecting personal data are used and if the data is processed fairly and lawfully. Individuals must be informed about the purpose of use and how the business processes personal data transparently.


It might be unfair to judge SMBs for their seemingly limited comprehension around the upcoming regulations, but that does not negate the fact these regulations will become law within the next 12 months. Because of this, we believe the government and wider security industry as a whole must come together to support businesses on their journey towards compliance.

The UK is highly—and rightly—regarded for its powerful and influential small business economy. Ensuring this economy continues to be ready, willing, and able to thrive in the new world of cybersecurity should be top of everyone's agenda.

**About Webroot**

Webroot delivers network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at www.webroot.com.

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com