irwinmitchell

GDPR 2018

Getting Ready

For The New **Data Protection Challenge**

YouGov®

A report for Irwin Mitchell

Contents

Welcome to the latest business study from Irwin Mitchell.

In this in-depth report, we are examining the new far-reaching data protection law which comes into force on 25 May 2018.

Joanne Bone

Stuart Padgham

The General Data Protection Regulation, or GDPR for short, has the potential to have an impact on businesses worldwide and in particular those in the UK and Europe. Although for many, its introduction might seem a long way off, the changes are considerable and the fines for non-compliance could reach €20m or 4% of annual worldwide turnover – whichever is bigger.

Although there are many organisations that have taken proactive steps towards compliance, the conversations that we have had with businesses in recent months reveal a concerning misunderstanding about the new regulations and a lack of activity towards compliance.

To understand if this is the case and the possible reasons for it, we commissioned international market research firm, YouGov, to question over 2,000 senior business decision-makers to assess just how ready they are, what action they have taken to date, and (if so) why they haven't done anything yet.

We wanted to see what the levels of awareness around GDPR are, how easily they think that they would be able to identify a data breach and what the likely damage would be to their business.

We are also interested in finding out what businesses think about data protection rules in general, in particular whether they see them as a threat or an opportunity in the short and long-term.

The results, which have been analysed at different levels according to size of organisation and the sector that they operate in, reveal some worrying trends and it's clear that there is a big job still to be done in order to raise awareness of what has changed and just what is at stake post 25 May 2018.

We hope you find this report and the insights from some of our clients and experts useful in terms of helping steer your business in the right direction on this new and complex legal reform. If you would like to discuss any concerns about GDPR, then please do get in touch.

We'll be with you every step of the way.

GDPR – a summary

All businesses that use personal data have until **25 May 2018** to comply with GDPR. Non-compliance can lead to potential fines of up to €20m or 4% of annual worldwide turnover – whichever is bigger.

Some of the key changes to be introduced by the GDPR include:

Compulsory notification of data breaches

Data breaches which impact on privacy will have to be notified to the Information Commissioner ("ICO"), the UK data protection regulator, within 72 hours of it happening. There is also an obligation to notify individuals affected in certain circumstances. Breaches can range from a customer database being hacked, to putting a letter in the wrong envelope. Organisations will need to monitor their systems to know whether or not there has been a breach.

Obligation to be more transparent in how personal data is used

Organisations will need to be open with individuals about what data they collect and what is being done with it. Fair processing notices and privacy policies will need to be updated.

The right to be forgotten

Individuals can require businesses to erase their personal data and whilst businesses need to have a process to action this, the right is not wide-ranging. It will be important for businesses to understand its scope, their obligations and how they need to reply to requests.

Increased rights given to individuals

The rights that individuals already have in relation to accessing the data that businesses hold will be extended. Additional information will need to be provided and generally in a shorter timescale. It will also no longer be possible to charge a fee.

Consent

Not all use of personal data needs consent. If a business relies on consent then its consents need to be looked at. Consent will be harder to obtain and maintain under GDPR.

Key findings

Less than half **38%** of the senior decision-makers are aware of the new GDPR rules

Only **14%** felt that the new rules will have a positive impact on their business

Just **29%** have started preparing for GDPR despite the compliance deadline being less than 12 months away

Over a **third** believe GDPR is not an issue for the sector they work in

2/3 are not reviewing their consents regularly enough to comply with the new GDPR

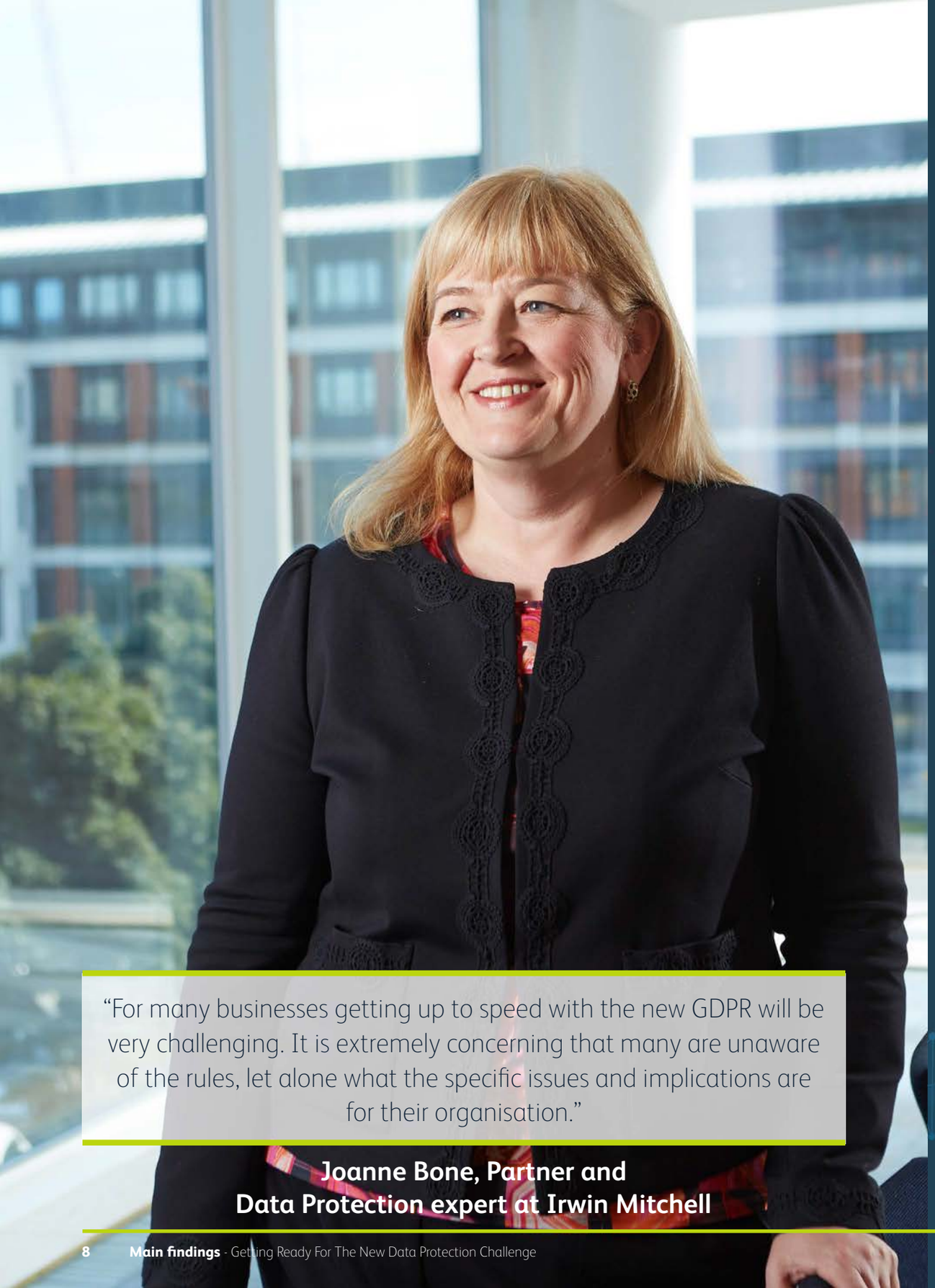
31% say that 'performing regular detailed reviews of data collection / use' will be the most important factor regarding the new rules

Four in **10** would have to cut staff or go out of business if they suffered the maximum fine

Over **2/3** are not aware they could be **fined up to €20m** or **4%** of their global turnover for non-compliance with GDPR

About the research

This GDPR survey was completed by 2,129 senior decision-makers within businesses. The fieldwork was undertaken between 18 and 27 April 2017 and carried out online by YouGov. The figures have been weighted and are representative of all GB businesses in terms of size (i.e. employees).



"For many businesses getting up to speed with the new GDPR will be very challenging. It is extremely concerning that many are unaware of the rules, let alone what the specific issues and implications are for their organisation."

Joanne Bone, Partner and Data Protection expert at Irwin Mitchell

Main findings

GDPR awareness

To set the context for the study and our analysis, we wanted to first of all establish the level of awareness amongst senior decision-makers in relation to the new data protection regulations.

Respondents were asked if they have heard about GDPR, but despite the far-reaching implications and the potential to affect the vast majority of organisations, 62 % of businesses said they had not.

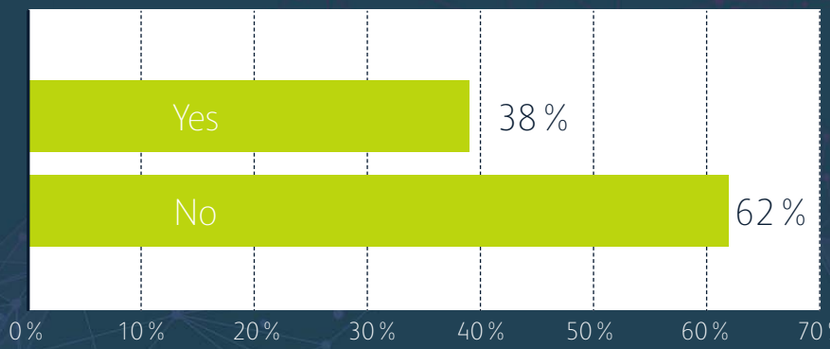


Figure 1 - *Proportion of businesses that are aware of GDPR*

We analysed this response according to company size and it is clear that awareness levels are lower amongst smaller organisations. Less than a quarter (22 %) of small businesses said they have heard of the rules and this figure rose to 43 % and 56 % for medium and large companies respectively.

Examining the data on a sector basis, awareness levels are unsurprisingly higher in industries which generate and hold a lot of data. However, the levels in areas such as financial services (57 %), medical (51 %) and media, marketing, advertising, PR & sales (38 %) are much lower than we expected to see.

New punishments

One of the key changes under the new data protection regime will be the heavy fines that will be introduced. Currently UK businesses can receive a maximum penalty of £500,000 for data protection non-compliance – however this is due to change from 25 May 2018.

To understand whether this crucial point is understood amongst senior decision-makers within UK companies, we asked whether they were aware they could be fined up to €20m or 4 % of their global turnover for non-compliance with GDPR.

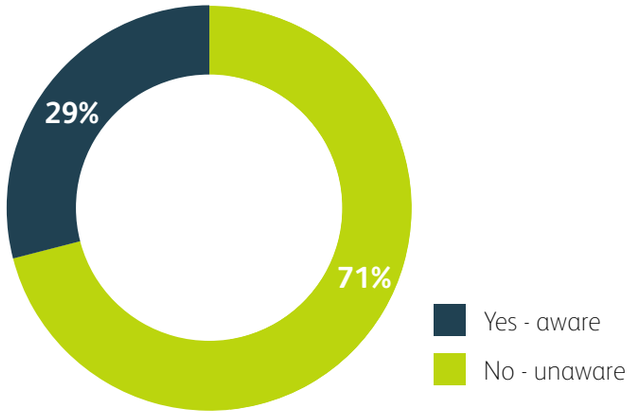


Figure 2 - *Proportion of firms aware they could be fined up to €20m or 4% of global turnover for GDPR non-compliance*

The fact that almost three quarters are not aware of the level of fines is a striking and concerning finding from this survey. In addition to 71 % of firms not knowing what the new level of fines will be, the study revealed this trend is more pronounced amongst smaller firms where 86 % said they are unaware.

The survey once again reveals some worrying levels of understanding within industry sectors where it should be much higher, such as retail (26 %), hospitality & leisure (30 %) and accountancy (40 %).

It is also worth highlighting that smaller firms cannot afford to be complacent, particularly as the ICO has recently shown an appetite for clamping down on smaller concerns.

In May 2017, the ICO issued a fine of £55,000 to a business which is small enough to have to file only limited accounts at Companies House. This is a stark reminder that small firms are definitely on the radar as far as the ICO is concerned.

To understand how powerful these fines could be for businesses, we asked what the impact would be if their company was fined 4 % of global turnover. Here, 18 % said that they would go out of business, whilst almost one third (31 %) revealed they would be forced into reducing headcount.

Seven per cent of businesses said they would be affected in different ways with some claiming their cash flow would be severely hit. Others said that they would have to cut back on new machinery purchases and put a freeze on new recruitment.

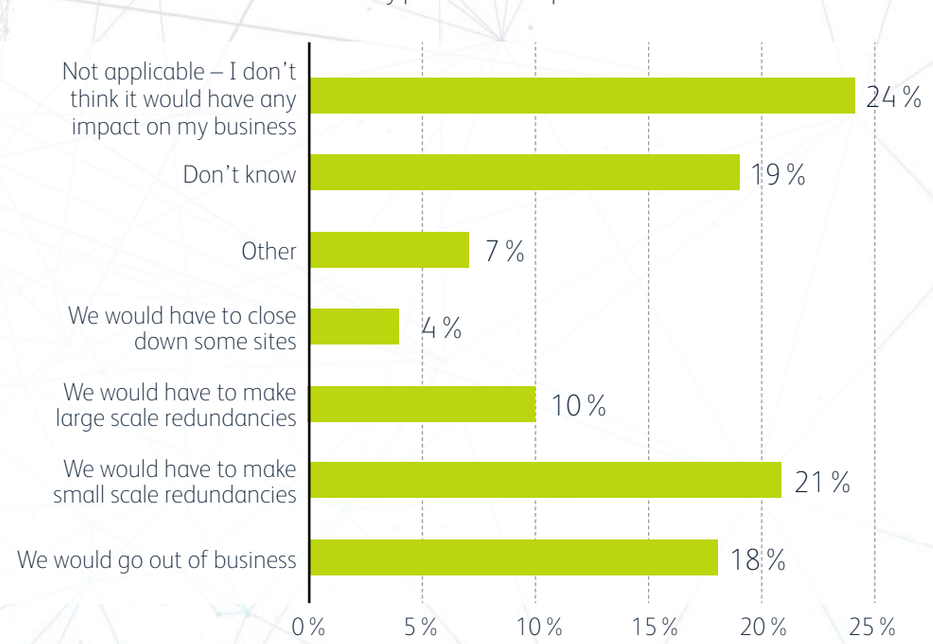


Figure 3 - *Expected impact on businesses if fined 4% of turnover following non-compliance with GDPR*

Despite the regime of new penalties, Irwin Mitchell believes early action in relation to GDPR can ensure a business can use the new rules in a positive way to generate rewards for their business. With this in mind, we asked respondents what their perception towards the new law is.

Here we found that more perceive a negative impact instead of a positive one, however what was also interesting is the 41% that think the rules will have no impact at all on their business. Although this is unsurprising based on the answers to earlier questions, it points to an emerging theme of very low awareness of how far reaching these new rules will be and suggests a lack of prioritisation amongst senior management.

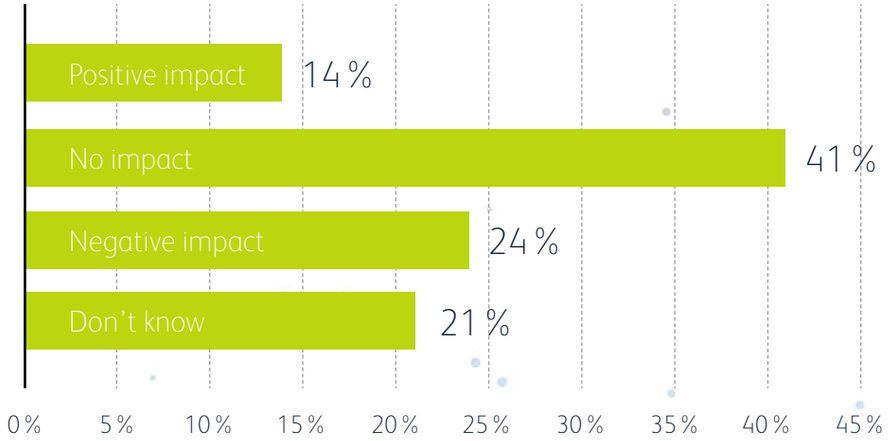


Figure 4 - *Proportion of businesses describing impact of GDPR on their organisation*

"GDPR is a board level issue and compliance should not be the sole responsibility of HR, marketing or IT. Proper GDPR compliance requires a joined up approach across the business as it affects all strands."

Joanne Bone

Partner and Data Protection expert at Irwin Mitchell

The perception towards GDPR will clearly have an impact on how businesses will deal with it and the survey asked whether companies of all sizes view GDPR as a threat or an opportunity. Here it was pleasing to see that almost one in five think it presents an opportunity to their business, however it was disappointing to see that slightly more view it as a threat.

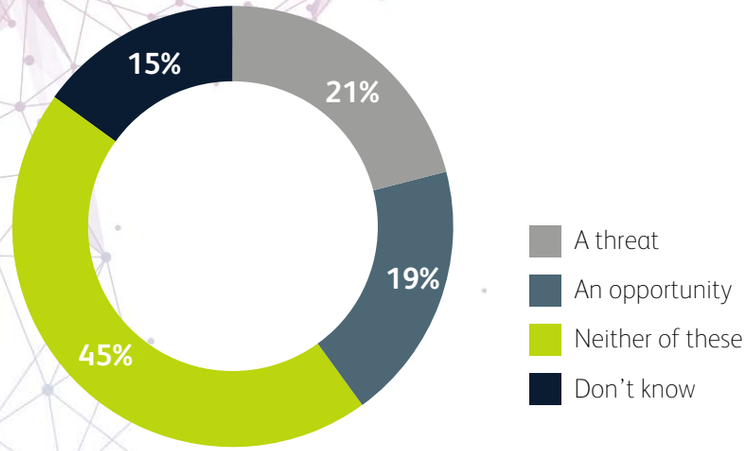


Figure 5 - *Proportion of businesses that see GDPR as a threat or an opportunity*

Stuart Padgham

Partner and National Head of Commercial at Irwin Mitchell

"It is important to recognise that taking a proactive approach towards GDPR compliance will potentially reap financial benefits. Good data governance can build customer trust and the right permissions can also help you take advantage of the Big Data Revolution and enable you to commercialise your data for competitive advantage."

With four out of 10 companies stating that the new rules will have no impact, the survey explored why this is the case.

Analysis in this area once again reveals some interesting and worrying results, with only a third of companies stating GDPR is not an issue for their sector or industry. Almost a quarter said it is not relevant as they're not a consumer-facing organisation. This appears to be one of the major misconceptions relating to GDPR and is explored in more detail below, but there are others. One in 10 said they think GDPR is irrelevant as it's an EU law and the UK will soon no longer be a member.

"It's important to understand that Brexit does not mean that GDPR compliance efforts can stop. The government has made it clear that GDPR will be the law in the UK both before and after Brexit. Any businesses that have put their compliance efforts on hold following the referendum result should restart them immediately."

Daniel Hedley

Partner in Commercial and Data Protection at Irwin Mitchell

Amongst the sectors where decision-makers don't feel GDPR is relevant to them, hospitality & leisure (45 %), retail (43 %) and manufacturing (34 %) score the highest.

These results in hospitality & leisure and retail are amongst the most concerning because not only will these sectors be greatly affected by GDPR, they reinforce one of our key themes about the low awareness of GDPR that exists.

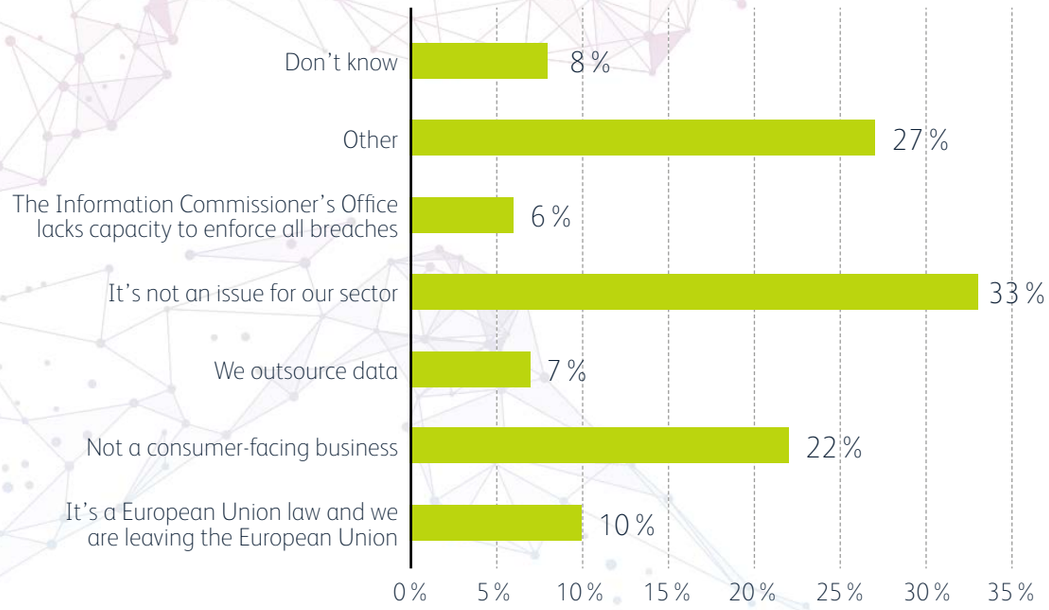


Figure 6 - *Reasons why businesses think GDPR will have no impact on their business*

Almost a quarter of businesses say GDPR will have no impact on their business because they are not consumer-facing. This is perhaps one of the biggest misunderstandings about GDPR because the reality is that the rules encompass a wide range of personal data including employee data, payroll and pension records. They also apply to data in a business context where individuals are concerned, such as sole traders and partnerships. The data that a construction business holds in relation to a plumber that it sub-contracts to, for example, will also be included in GDPR.

"Contrary to popular belief, personal data is not just consumer information. Business data relating to suppliers and customers who are sole traders and partnerships will for example be caught and should be analysed with the same degree of importance as consumer data."

Joanne Bone

Partner and Data Protection expert at Irwin Mitchell

Early preparation

Due to the far-reaching impacts of GDPR, we strongly recommend that businesses take proactive steps to ensure they are ready for 25 May 2018. The amount of work required will of course depend on a number of factors including the size of company, the sector in which it operates and also how much work has been done in the past in relation to data protection compliance.

Despite the many variables, we wanted to understand through this survey what the current levels of engagement with GDPR are with less than 12 months left to the deadline.

Perhaps with the low levels of awareness and high proportion of firms thinking the impact of GDPR will be low, it isn't surprising that just over half of businesses haven't yet started work on their compliance and a further 20 % are not sure as to whether any steps have been put in place.

Whether they are surprising or not, these results are concerning, because with the May 2018 deadline fast approaching and with so much at stake, our study reveals there is a very real possibility that the majority of organisations will not be compliant in time.

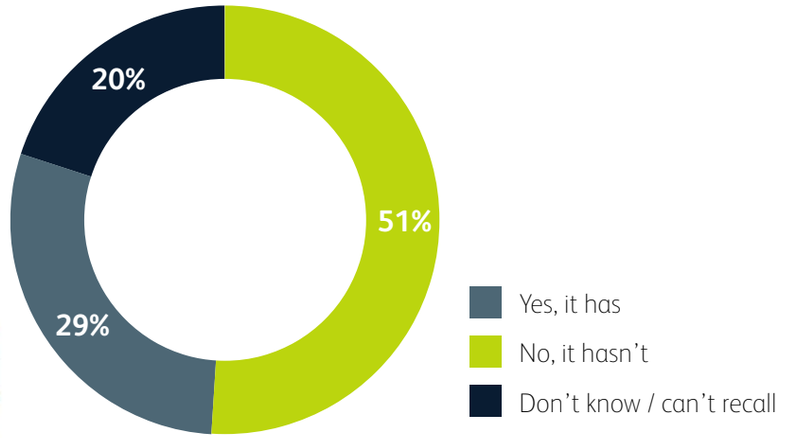


Figure 7 - *Proportion of organisations which have started preparing for the new data protection rules*

We have also detected a significant difference between activity levels and the size of company. In the case of small businesses, 78 % of organisations have not taken any action so far, whilst the proportion is much lower amongst larger organisations.

Main market listed client

"GDPR is an opportunity to strengthen customers' trust and confidence in our brand."

"As a leader in credit management services, Lowell takes data compliance very seriously. We have worked in compliance with the DPA since the formative days of the business and have taken a similarly proactive approach towards GDPR. This stance saw us begin work on GDPR very early, with the aim of being compliant well-ahead of its introduction in May 2018."

Kerry Smith, Solicitor (Technology & Data) at Lowell Group

Data Breach

The compulsory notification of a data breach is a key aspect of GDPR and will mean that the ICO will need to be told about certain data breaches within 72 hours. Individuals affected will also need to be notified in some circumstances.

This aspect of GDPR is potentially one of the most challenging hurdles but in order to establish how businesses will cope, we asked if they are currently in a position to detect data breaches.

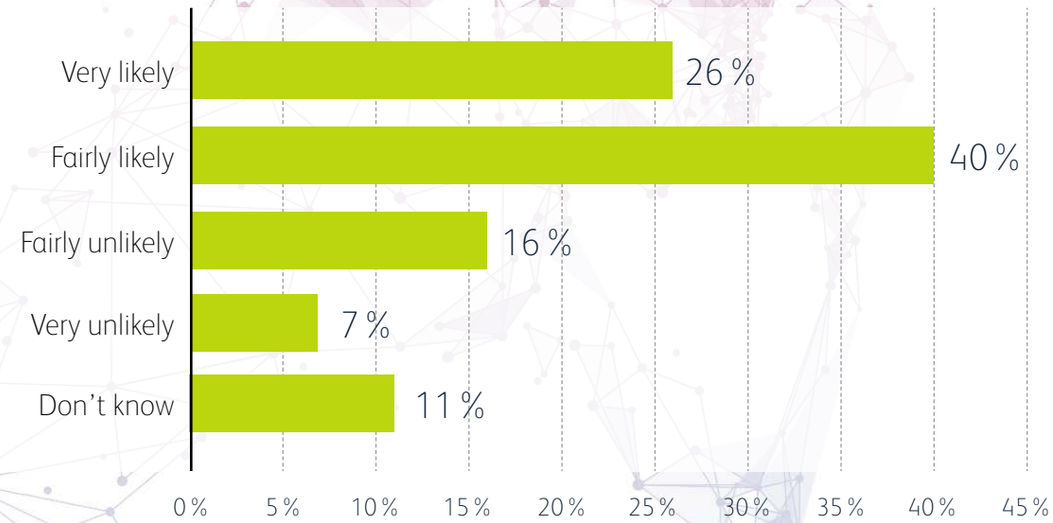


Figure 8 - *Likelihood of businesses being aware that a data breach had occurred*

Although a reassuring 66 % claim to be confident in this area, only a quarter are certain and a worrying 23 % think it's unlikely.

We then asked businesses to forecast with their current systems in place how long after finding out about a data breach would it take to investigate and report it to the ICO.

Significantly, only a third think they would be able to report it within the new three day timescale set by the ICO, with four out of 10 admitting that they would report it after three days and therefore fall foul of GDPR. Highlighting the need for greater awareness for the new laws, a worrying 10 % say they wouldn't even report a data breach.

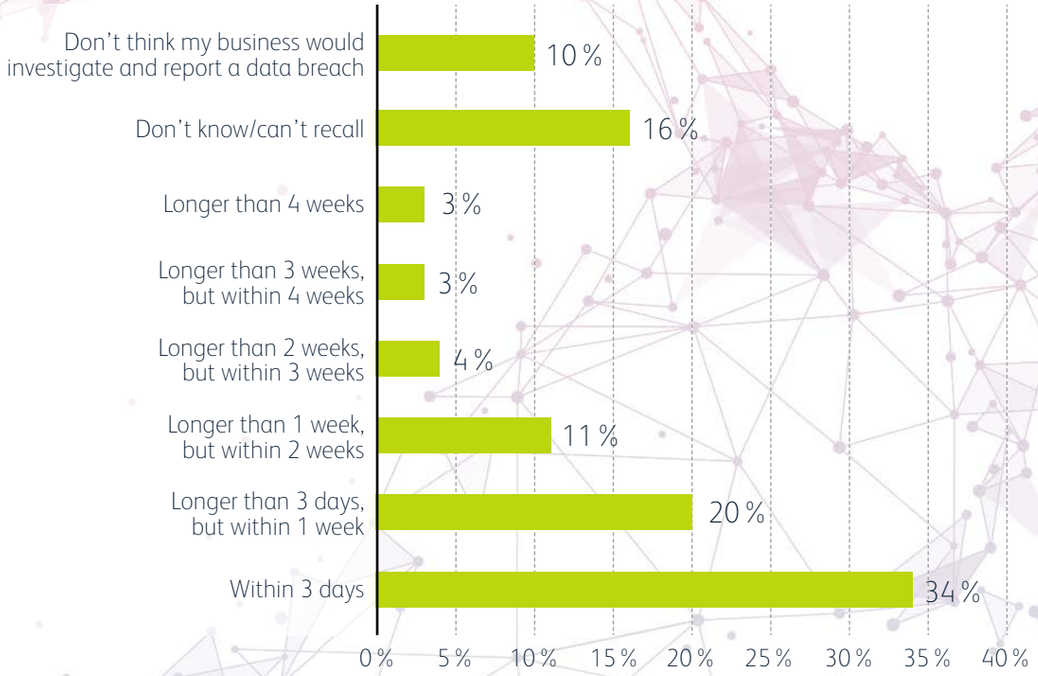


Figure 9 - *Timescales businesses say they would be able to report data breaches*

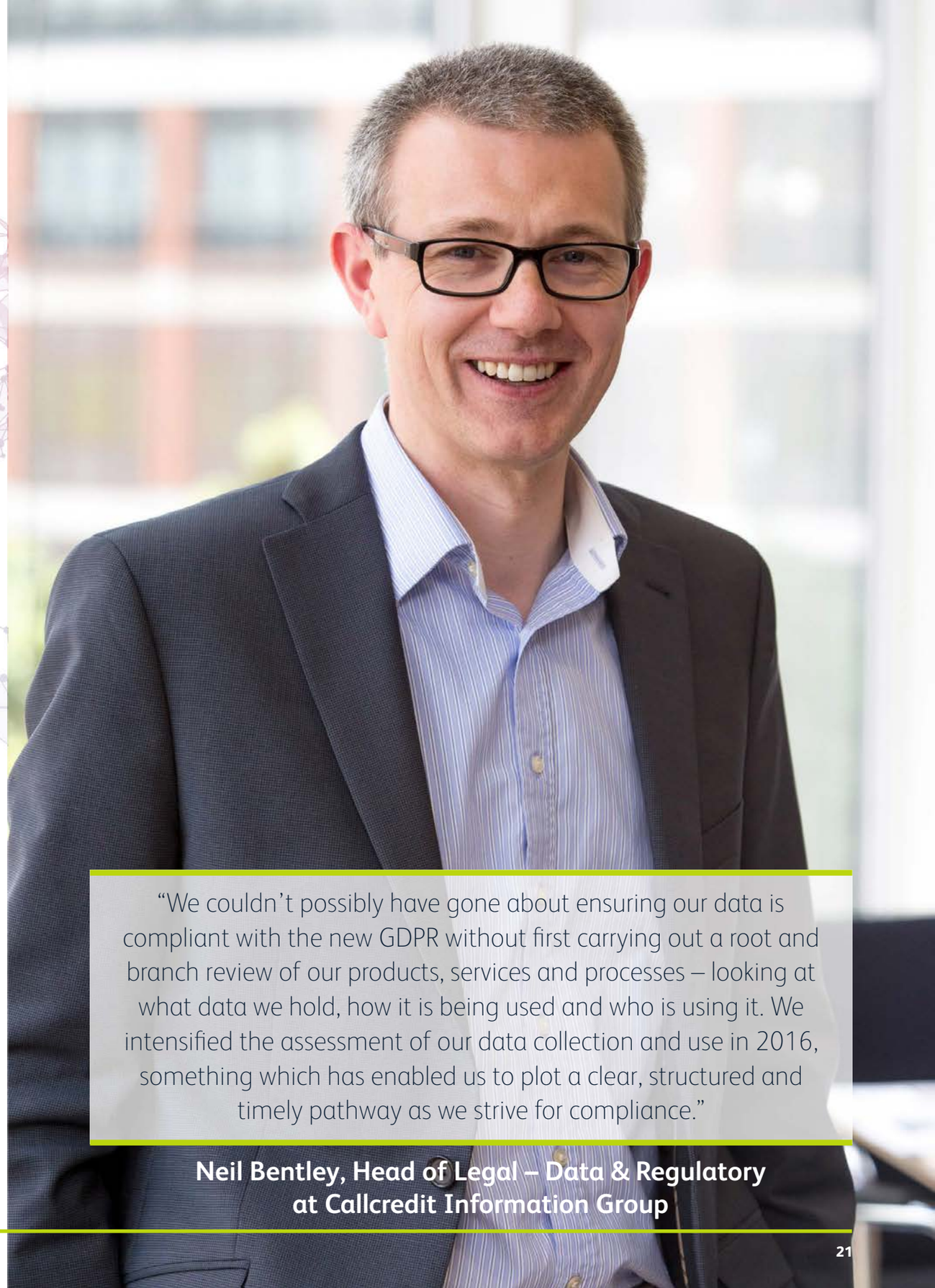
Priorities

We asked businesses what their GDPR priorities are between now and May 2018 and this revealed some very interesting results. We provided a wide range of options and invited all 2,129 respondents to indicate which are highly relevant to their business.

What we found is that no one area takes priority, with businesses seeming to take a broad approach. We anticipated that the 'regular detailed reviews of data collection and use' would be the number one priority and although this was the case, we expected it would be much higher than it is in this survey.

It was also clear that a relatively high number of small companies are appointing Data Protection Officers (DPO). A DPO is certainly a necessity if an organisation crunches lots of data, however for it to be so high amongst SMEs is consistent with a common misconception that such an appointment is a quick fix to dealing with GDPR's complexities.

Overall, the answers to this question highlight a possible lack of focus and reveal that the majority of businesses are currently focussed in the wrong areas.



"We couldn't possibly have gone about ensuring our data is compliant with the new GDPR without first carrying out a root and branch review of our products, services and processes – looking at what data we hold, how it is being used and who is using it. We intensified the assessment of our data collection and use in 2016, something which has enabled us to plot a clear, structured and timely pathway as we strive for compliance."

Neil Bentley, Head of Legal – Data & Regulatory at Callcredit Information Group

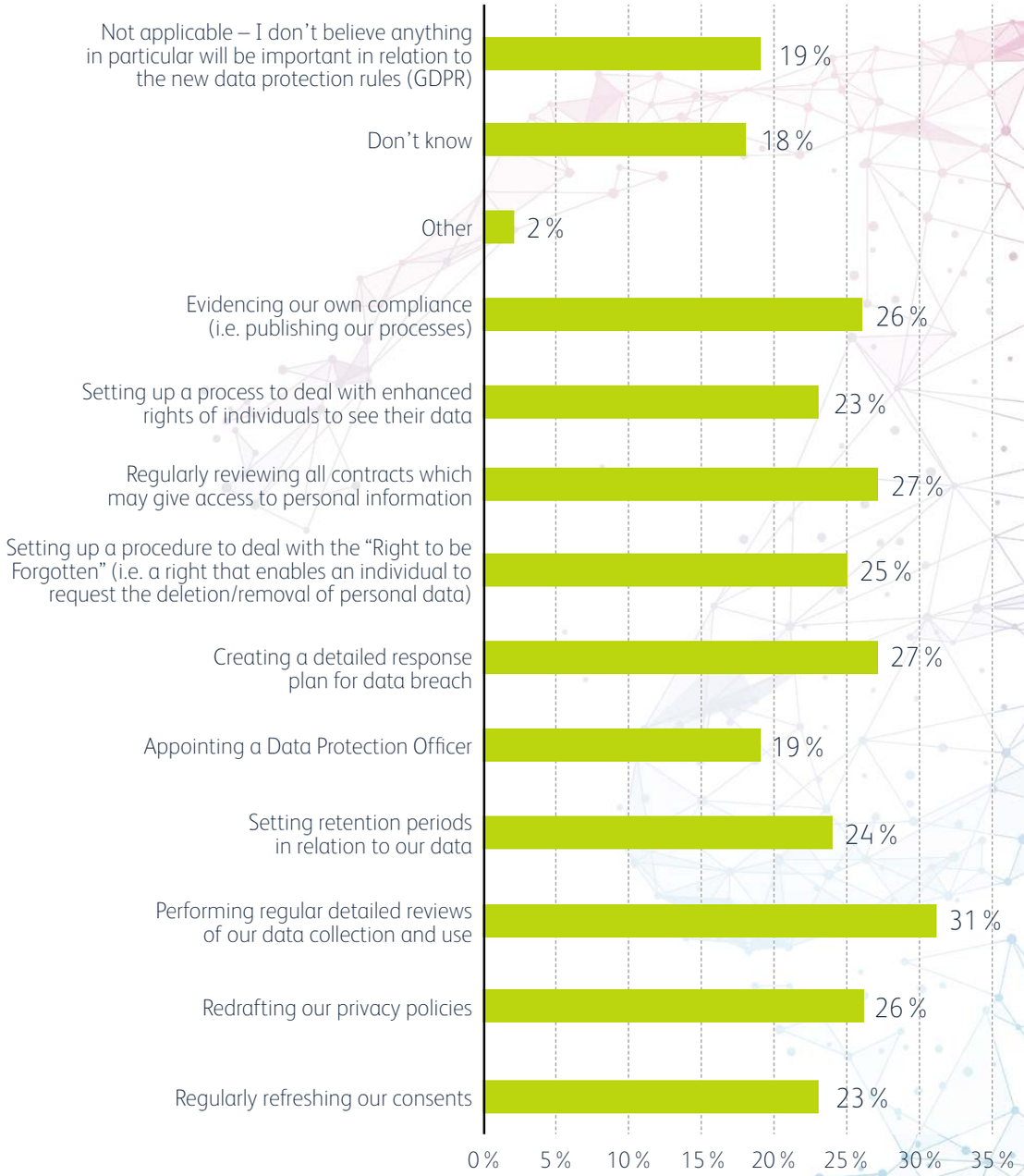


Figure 10 - *Top GDPR priorities for businesses*

Marketing consents

Consent for marketing activity will be harder to obtain and maintain under GDPR and it's vital businesses update their activity in this area on a regular basis. Businesses can no longer rely on implied consent or pre-ticked boxes – consent must be unambiguous, freely given and will require clear affirmative action as well as all third parties being clearly named.

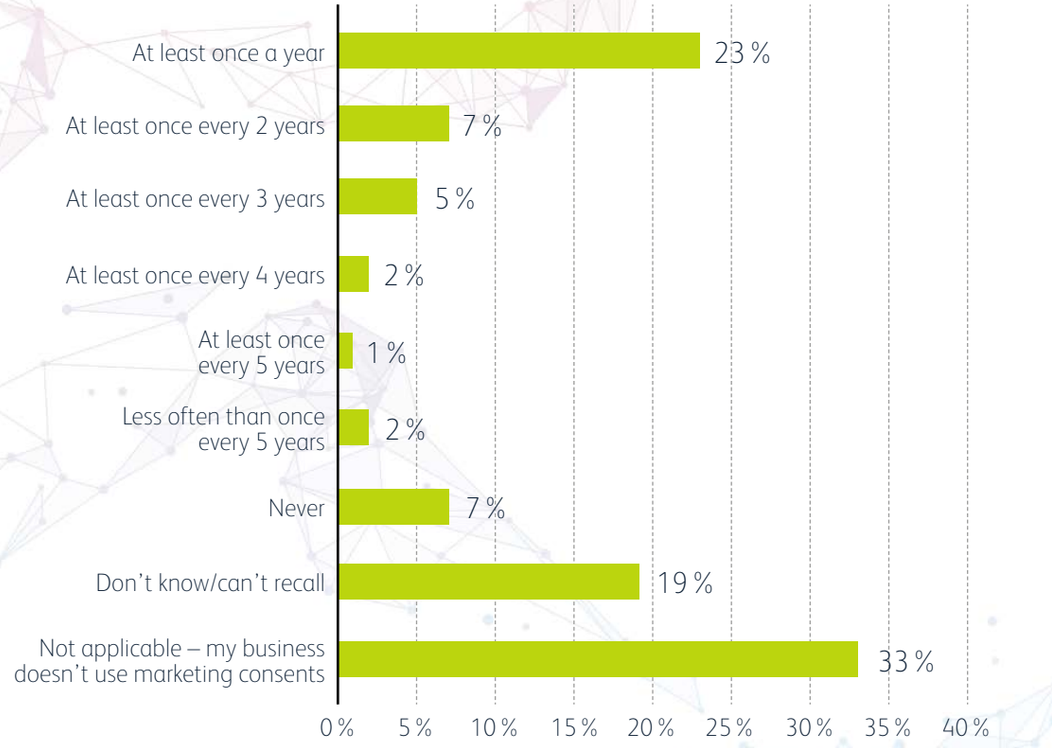


Figure 11 - *Frequency of how often businesses review their marketing consents*

Our report reveals that 30 % are already doing what they need to do, whilst over a third are not or don't know. One third say they don't use marketing consents which although will be the case for many of the businesses surveyed, the response rate amongst some industry sectors where the use of marketing consents is almost ubiquitous, such as retail and hospitality & leisure, is concerning and points to a serious misunderstanding of the rules.

We also think these businesses are missing an opportunity. Margins are tight in retail, hospitality & leisure and good data governance will enable them to personalise the customer experience, build trust and confidence and ultimately gain competitive advantage.

Conclusion

It is hard to think of a business today that does not use personal data. Whether you have employee data, customer data or supplier data – if the data relates to an individual you will be caught by the new data protection laws.

With this in mind, there appears to be a distinct and concerning lack of awareness and action towards compliance.

There is clearly much more work to be done in terms of raising awareness of GDPR, especially in relation to what it means, the hefty fines for non-compliance and also that it doesn't just affect consumer-facing organisations. There are other misconceptions that need to be tackled, such as the fact that despite Brexit the regulations and changes incorporated within GDPR will still be introduced on 25 May 2018, and will remain in place long after then.

Those businesses that are aware of GDPR are generally not enthusiastic about it. Many think it will have a negative impact on their business and in some cases appear to be burying their heads in the sand.

We have however spoken to and advised a number of businesses that are looking at GDPR in a different way. They are viewing it as something positive and a piece of legislation that provides an opportunity to differentiate their organisation, build trust with their stakeholders, enhance their brand and gain a valuable competitive advantage.

The view is that if the GDPR was in force last year the fines issued by the ICO would have been around 79 times higher. Taking this into account, businesses need a true specialist to help navigate them through to compliance. General advice in this area will not be enough. GDPR compliance should be treated like a marathon, not a sprint, and compliance requires long-term planning and preparation.

GDPR
it's a **marathon**
not a **sprint**

Action points

Action points

for **businesses**

Whilst the results show that many businesses are not sure of what their GDPR compliance requirements are, there are some key issues which need to be considered on the pathway to compliance.

These are as follows:

- Carry out a data audit – you need to understand what personal data you have and how you use it in order to begin a compliance program.
- Review what permissions apply to your use and collection of personal data – the GDPR has defined lawful purposes that you need to bring yourself within in order to use personal data. You need to assess which of these apply and document this.
- Review your consents – if you use consent to collect and use personal data you need to review the content of your consents as the GDPR has changed what consent will look like going forward. You should not rely on implied consent. Consent should be unambiguous and given via clear affirmative action. You should avoid pre-ticked boxes.
- A key part of the GDPR is transparency. This involves being clear with individuals how their personal data is used. You therefore need to review your fair processing notices which tell people how their data is used and your privacy policies.
- Set a Data Retention Policy and stick to it.
- Review your contracts – contracts which relate to data sharing or which appoint a third party to process personal data on your behalf need to be reviewed as there are new requirements relating to these. Similarly if you use personal data on behalf of third parties you need to review the contracts under which you do this.
- Carry out staff training – consider what training your staff need and whether certain staff need enhanced data protection training.
- Consider whether you need to appoint a data protection officer. Not all businesses will need to do this but you should consider whether the requirements apply to you.
- Set policies and procedures for dealing with enhanced rights of individuals such as subject access, the right to be forgotten and data portability.
- Notification of certain data breaches will be compulsory and so you should set a data breach policy and procedure which is tested.
- Evidence what compliance actions you take. Under the GDPR not only do you have to do the right thing but you should also evidence the fact that you have done the right thing.

Don't be slow out of the blocks

There is **less than one year to go** until

GDPR

comes into force **on 25 May 2018.**

Our data protection experts can help you over the finish line.

Key contacts

Joanne Bone

Joanne has been advising businesses and other lawyers on data protection for almost 20 years, including specialist advice on the new GDPR regulations since 2015. Joanne has a wealth of experience and is our key contact for the North and Midlands.

T: +44 (0)113 218 6429
E: joanne.bone@irwinmitchell.com

Stuart Padgham

Stuart is the national head of Irwin Mitchell's Commercial team, based in our Gatwick office. He has over 15 years' experience working on data protection issues as well as IT and other commercial arrangements and is our key contact for the South.

T: +44 (0)129 374 2768
E: stuart.padgham@irwinmitchell.com


WORLD
Para Athletics
CHAMPIONSHIPS
LONDON
2017™
NATIONAL SUPPLIER
irwinmitchell.com/gdpr-2018
Irwin Mitchell LLP is authorised and regulated by the Solicitors Regulation Authority.
BLS-GDPR-0005