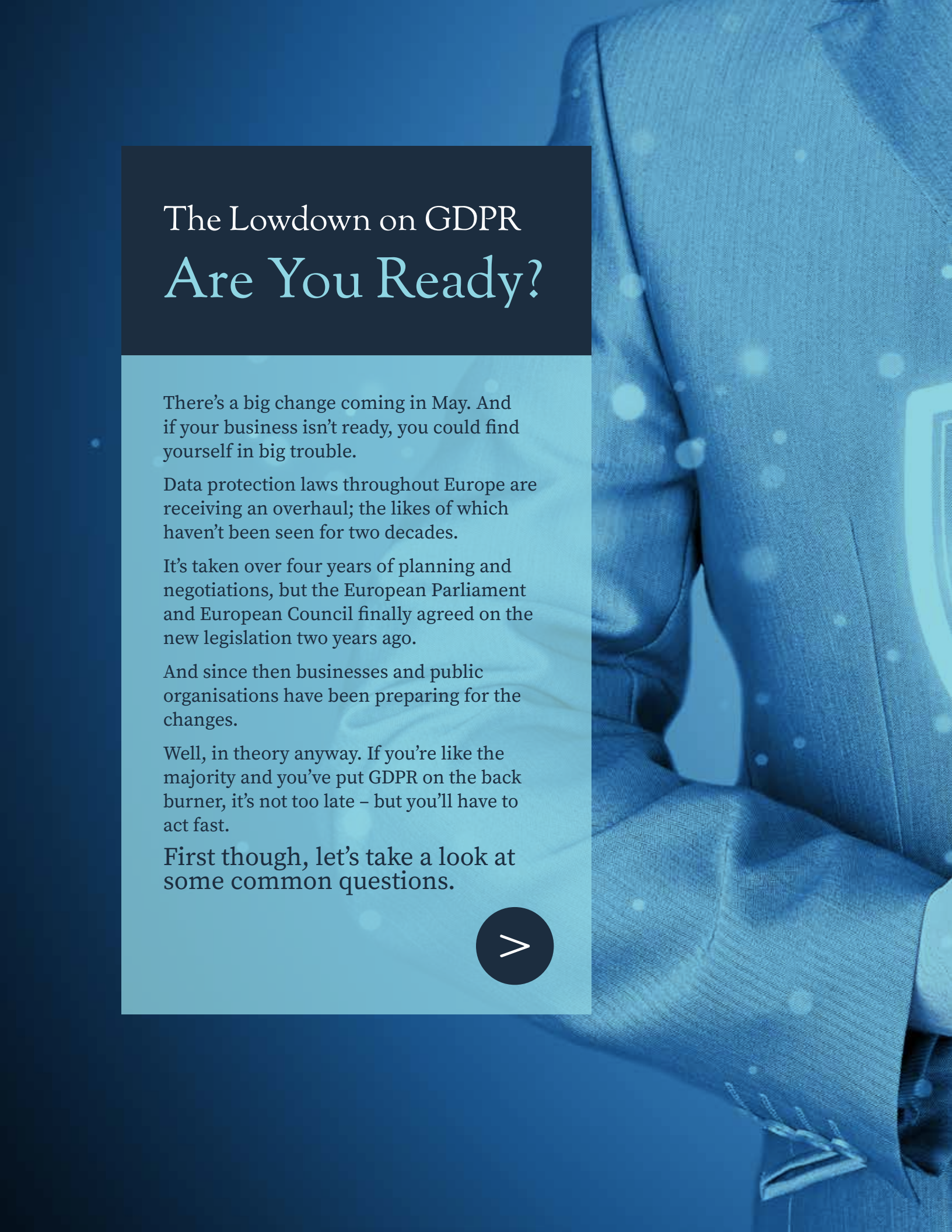
The Lowdown on GDPR
Are You Ready?



The Lowdown on GDPR
Are You Ready?

There's a big change coming in May. And if your business isn't ready, you could find yourself in big trouble.

Data protection laws throughout Europe are receiving an overhaul; the likes of which haven't been seen for two decades.

It's taken over four years of planning and negotiations, but the European Parliament and European Council finally agreed on the new legislation two years ago.

And since then businesses and public organisations have been preparing for the changes.

Well, in theory anyway. If you're like the majority and you've put GDPR on the back burner, it's not too late – but you'll have to act fast.

First though, let's take a look at some common questions.

>

What exactly is the GDPR?

The European General Data Protection Regulation (GDPR) is the new, improved version of the Data Protection Act. It comes into force on 25th May 2018, and it will change the way organisations collect and manage the information they collect about customers.

The regulation is the new framework for data protection across the whole of Europe. According to the governing bodies behind it, the GDPR has been designed to harmonise data privacy laws and protect the rights of individuals.

We already have data protection laws. Why do we need more?

Yes we do, but things have changed a lot since the last laws were passed. It's hard to imagine now, but back 1998 there was no such thing as smartphones and Mark Zuckerberg was just a 14 year old who hadn't even considered the idea of Facebook yet. Let's face it, the world is a very different place now and the change is long overdue. We're creating and collecting huge amounts of digital information every second, and the laws created twenty years ago just don't cut it any more.

Is my business going to be affected?

Yep. All organisations that collect data – even just a name and number – will have to comply with the GDPR. There are more hefty requirements for businesses employing 250 staff or more, but all organisations that collect any kind of personal data are going to be affected.

You will also have an obligation to erase the data of any individual who exercises their "right to be forgotten". At any time, your customers can withdraw their consent to your storing or using their personal data and insist that you delete it.

What kind of data does it cover?

The regulation encompasses both basic personal data (names, addresses, dates of birth etc.) and sensitive data (sexual orientation, genetics, religion etc.).

True, this information has already been covered under the previous data protection laws, but one big change is that anonymous data is also included now. In fact, the GDPR positively encourages the pseudonymisation of data, and there will be incentives for controllers to use this more secure method of collection.

The GDPR defines pseudonymisation as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." To pseudonymise a data set, the "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person."

In layman's terms, it's a way to keep information private and store different data sets separately.

My business is B2B and doesn't collect customer data, so I don't need to worry, right?

Wrong! Any company with employees located in the EU is obligated to comply. You might not collect customer data, but you'll still have information about partners and employees, and that information must all be stored in line with the requirements outlined.

Voluntary groups, member clubs and charities are also going to be affected by the GDPR.

Will there be a UK specific version?

Sort of. There has been some flexibility in terms of how individual countries choose to implement the GDPR, but they all have to adhere to the overall principles.

The UK Government introduced its own new data protection legislation to the House of Lords in September. The Data Protection Bill 2017 will:

- Make our data protection laws fit for the digital age in which an ever increasing amount of data is being processed.
- Empower people to take control of their data.
- Support UK businesses and organisations through the change.
- Ensure that the UK is prepared for the future after we have left the EU

It covers all the main areas of the EU regulations, but with some exemptions. These include added protection for journalists, anti-doping agencies, scientific and historical researchers who handle personal data.

The UK bill also states that parental consent must be required for all information about anyone under 13.


PASSWORD3Q
8#1X?M%PASSWORD
B#1X?M%PASSWORD3Q

What's the nitty gritty?

The full GDPR paper contains 99 articles which all set out the rights of individuals and the obligations of organisations. Trust us, you don't want to read them!

In a nutshell, here are the main things you need to be aware of.

Accountability and Compliance

The GDPR means that all organisations that handle people's personal information will be more accountable for that data. This includes things like clear data protection policies, risk assessments and developing documents that outline the what, how and why of the data you collect.

With cyber-crime at an all-time high and huge data breaches hitting the headlines, the risks of not looking after client information have been well documented. With large, well established organisations like the NHS, Yahoo, LinkedIn and T-Mobile all falling prey to cyber-attacks, nobody can afford to be complacent.

The Information Commissioner's Office has to be informed of any breach within 72 hours, and this information has to be

made public. The repercussions of this aren't just financial or legal… damage to reputation is often a lot harder to recover from.

Companies that process a lot of sensitive data or undertake "regular and systematic monitoring" of individuals at a large scale are now required by law to employ a data protection officer. Arguably this could be an add-on to an existing role, but for a lot of bigger companies it's going to mean employing a completely new member of staff.

Organisations are also going to have to obtain consent to process data in certain situations. If you're relying on consent to lawfully use someone's information you'll have to clearly explain that consent has been given, either in writing or through a "positive opt-in."

Access to Data

The GDPR gives individuals a lot more power to access – and request the deletion of – any data that's held about them. Until now a Subject Access Request (SAR) enabled businesses to charge a fee of £10 for someone to view the data that was held about them. Under the new regulations, the SAR has been completely scrapped.

Now, anyone will be able to request their personal information completely free of charge, and this information must be provided within a month. In addition, the ICO states that all individuals have "the right not to be subject to a decision" that has a significant effect on them. Basically, organisations are no longer able to make automatic decisions based just on personal data and any decisions that are made must be clearly explained.

Fines

All laws have to be enforceable, and the GDPR is no exception. Any organisation that fails to comply with the regulation will face significant financial penalties. That means you can be fined if you:

- Don't process an individual's data in the correct way
- Fail to employ a data protection officer if required
- Suffer a security breach

How much you will be fined depends on the individual circumstances, but even smaller offences could result in a fine of up to €10 million or 2% of your global turnover (whichever is greater). In the case of major breaches which have a seriously detrimental effect on an individual or group, the fines could be as much as €20 million or 4% cent of a firm's global turnover (whichever is greater).

As you can see, the people behind the GDPR mean business. If you fail to comply, we're definitely not just talking about a tap on the wrist.

Have we scared you? Thought so. We didn't mean to. We just believe that forewarned is forearmed

The vast majority of smaller businesses simply won't be able to recover from fines like these, not to mention the damage to their reputation. The good news is, it's not too late to get your business GDPR ready… as long as you act now.

How to prepare your business for GDPR

If you've got the time, you can read and familiarise yourself with all 99 articles (it's OK. We know you're very unlikely to do that).

So if you haven't got time, it's important to have a clear idea of what's expected of your individual organisation. For example, you might not need to employ a data protection officer.

A lot of the main concepts and principles of the GDPR are similar to those outlined in the Data Protection Act, but this is a revamped version for the digital age.

Don't make the mistake of thinking there's a grace period during which you'll be forgiven a few teething problems and oversights. When the 25th May arrives you'll be expected to be fully compliant and to be able to prove it. No excuses!

The best thing you can do to ensure you've got everything covered is to enlist a data expert to come in and support you through the process. If it feels like an unnecessary expense, ask yourself how you'd feel about being fined, spending valuable time in court and having your name splashed all over the headlines. Getting your GDPR paperwork and procedures right is an investment that will save your time, money and reputation in the long run.

This is happening. And you can't afford to waste any more time.

We are able to help you with the data security aspects of GDPR. We can ensure that you have an appropriate level of protection on your network, using strategies such as a firewall, vulnerability scanning, and off-site backups of critical data.

Call us on 01689 422522 if you need any advice or help in getting ready for the new GDPR.

IT Support (UK) Ltd