General Data Protection Regulations (GDPR): Dispelling the fear and embracing pragmatism

Zoe Wallis, Winning Moves Ltd | T: +44(0)121 285 3800 | E: zoew@winningmoves.com

We need to talk about data protection. Yes, you heard me correctly. Now don't fall asleep; this is important.

We've all got certain subjects that we'd rather reserve for those evenings when we just can't sleep; something so 'fantastically thrilling' that it sends us off in to that elusive slumber. Well, I'm telling you now, protecting the data you store and fulfilling your legal obligations to do so, doesn't need to be one of them. Five years of legal education, coupled with ten years in enterprise, has taught me that it's possible for compliance not to be boring. Trust me – I'm not a lawyer….I'm a pragmatist.

As the Operations Director of a small business, it's not just my job to make sure we're compliant, but also to make sure that we **can** still operate. It's possible to be compliant to the nth degree, to guard against every single eventuality,
but I guarantee you two things if you do this:

1. You'll never get any work done; and
2. You'll never be profitable.

Let me be abundantly clear: I'm not saying don't comply at all; I'm saying apply some common sense.

WINNING MOVES®

It is incredibly easy to get caught up in what I believe to be significant fear and hype about the change in data protection legislation. The General Data Protection Regulations (GDPR) becomes enforceable from 25th May 2018 and replaces the existing Data Protection Acts of 1993 and 1998 (DPA), including equivalent law in Scotland and Northern Ireland.

I've sat through the briefings where the attempt has been made to terrify the individuals sat in the room so that they wholeheartedly grab the call to action to employ these consultants on a lucrative retainer. And, truth be told, all that fear comes from the unknown. Unknown because it's 'new' law and unknown because it's not therefore tested. Let me be more obvious – it's a sales pitch. It's one of the oldest tricks in the book: selling with FUD (fear, uncertainty and doubt) and it's very compelling.

But how 'new' is GDPR really. Let's face it we've had data protection laws for years, I'm not denying there are some changes as a result of the GDPR, however it's not like we've never had to do anything to protect data. It's not like we never had to make sure our information was secure for the benefit of our customers and for our commercial activities. So what are we all so afraid of?

My intention, should you choose to keep reading, is two-fold: firstly to make you appreciate what the key changes are; and secondly to dispel any fear you may have and enable you to get yourself prepared for the changes ahead. You will have some work to do, but it is not as scary as you think.

It's not like we never had to make sure our information was secure for the benefit of our customers and for our commercial activities. So what are we all so afraid of?

WINNING MOVES®

Key differences in a nutshell

	DPA	GDPR
Scope	Reactive review in event of a breach occurring	Must proactively demonstrate endeavouring to prevent breaches. All breaches should be reported within 72 hours if likely to impact on individuals affected
Personal Data	Wide reaching but did not embrace technological changes	Widened definition to include biometric and geographical information
Geography	United Kingdom (through respective statutory instruments)	Any organisation that processes data of European Union citizens, wherever the organisation is based
Roles and Responsibilities	Previously, Data Controllers were responsible for breaches	Creates new role of Data Protection Officer for some organisations. Either/both Data Controller and Data Processor can be held liable for breach
Rights of Data Subjects	Enshrined in 8 key principles: • Auto opt-in allowed • Charge for data subject access requests • 40 days to respond to data subject access request	Now 7 principles amended so that : • Opt in must be positive (cannot be assumed) • Can only keep data as long as you have a legitimate interst to hold it • Generally cannot charge for data subject access requests • Respond to data subject access request within 1 month
Penalties	£500,000 maximum	Maximum €20million or 4% global turnover

WINNING MOVES®

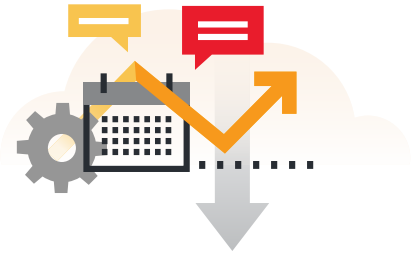
What about Brexit?

The Information Commissioners Office has stated clearly that the U.K. will comply, Brexit or not. This means that come 25th May 2018, we all need to be confident that we have taken steps to show that we are actively endeavouring to comply with the law.

From a business point of view, it makes sense. The scope of the GDPR covers not just companies in the European Union, but any other Country in the world who processes the data of European Union citizens. This means, that UK SMEs will need give assurance to their European Union neighbours that they both respect and protect their fundamental freedoms to the same level as is provided in their own country, making it easier for us to continue to trade with them.

The Information Commissioners Office has stated clearly that the U.K. will comply, Brexit or not.

But I don't process personal data...



Yes, you do. You need to be aware of the obligations because let's face it – **we all process personal data**; I am yet to meet a business that doesn't. Some areas of personal data processing are obvious e.g. payroll and HR data, some less so. In the internet age, we will all hold customer or supplier email addresses and yes, this constitutes personal data too- even if it's a work email address. Do you:

- have pictures of your staff on your corporate website?
- Have the ability to track where laptops are and therefore where your employees are?
- Have location services enabled on mobile phones to enable remote wiping

Yes? That's personal data too.

WINNING MOVES®

So what do you need to do?

It's quite simple, really. You need to demonstrate that you are doing all you can to guard against a data breach in your organisation. That is not to say a breach may never happen. Rather, it's that in the event of the worst happening, you can demonstrate you did all you could to prevent the breach and to prevent harm to the fundamental rights and freedoms of individuals.

And how do you do this?

The ICO has issued a 12-point plan that all businesses should follow to ensure their compliance. This includes making sure you have mapped out your data flows within your business, ensuring data is safeguarded in all instances, and communicating with individuals whose data you have to get their consent to hold it.

As a small business owner myself, I can tell you now, it's not rocket science to do this – your main challenge will be making the time to do this – and it's important that you do. That's where we can help. We've developed a 2 day, hands-on training course that will get you ready for the GDPR. I'll tell you now - we won't require you to take a multiple choice exam and then give you a certificate at the end of it, that you can wave about to demonstrate you've attended and that you've read the legislation.

There's no value in that. What we will help you do is:

- Understand the personal data you have in your business
- Understand and map out your data flows
- Review the protections and controls you have in place to protect your data
- Review and update your policies, terms and conditions so that you're compliant
- Determine if you need to appoint a DPO

In a short space of time, we will guide you through the 12 point plan the ICO has laid out so that you're ready for 25th May 2018. All for the cost of £995. *As the saying goes, teach a man to fish….*

Winning Moves has supported SMEs for 21 years helping them to start, develop and grow. We believe that you are the best person to make changes in your business and we believe in sharing knowledge and best practice. This is what we do and we're good at it. You don't need a consultant on a retainer to do this for you, you can do it yourself. But you need to make time to do it. If you'd like to find out more, please contact us on 01785 827600 or email info@winningmoves.com.

GET IN TOUCH

Ground Floor, Baskerville House, Centenary Square,
Broad Street Birmingham B1 2ND

T +44 (0)121 285 3800
E info@winningmoves.com

winningmoves.com