GDPR – A LAND OF OPPORTUNITY

John Fitzpatrick, information security officer at NGIT, offers some good news about the forthcoming EU GDPR regulations

Maybe you've already heard? GDPR is coming. And yes, you might be thinking, oh no, not another GDPARRRGHH! article.

I am not going to try and sell you technology, consultancy or any mythical silver bullet solution. Instead I am going to share some observations in relation to the new regulation, and give you some tips on where you should apply a bit of effort.

So with the date firmly set, the regulation sat on the starting line and a number of 'GDPR specialists' offering their services, what do you need to do to get ready?

Well the first thing is not to panic. That may seem strange and counter to what many other advisers are telling you, with a large part of their sales strategy reliant on reminding you that the date is just around the corner and the fines, the fines, oh my word, the fines are massive.

I am not suggesting you do not set any importance in getting to grips with what you need to do, but panic buying instant fixes from the myriad of opportunists that maybe knocking on your door is not going to help you get a clear understanding of what GDPR means to you.

MY FIRST TIPS:

- Get GDPR compliance on your risk register
- Appoint an accountable sponsor at the highest level possible within your company
- Think about data, not technology
- Start with the understanding that this will cause you to make changes within your company, if only minor, many of which I think will be positive
- It is a regulation. They do not often bring opportunity, but this one does.

So is GDPR brand new?

The answer is yes and no. The EU General Data Protection Regulation comes into force on 25 May 2018 and will repeal the current data protection regulation directive. The new regulation carries forward the original principles contained within Directive 95/46/EC, expands in certain areas, adds new where it makes sense (well to me anyway) and generally improves on the definitions, roles, responsibilities and the overall rights of the individual. However, there are some key changes. Most you have probably heard about, generally in a negative way. I hope to point you to the positives and possible opportunities.

SECOND TIPS:

- When processing personal data, you must do it lawfully, fairly, and with transparency. This gives you the opportunity to get to grips with what you store, and in some cases hoard, in terms of data.
- You can and should minimise the data you hold. This will lead to the smoother running systems, in terms of processing. Less data storage consumption also translates into lower costs and greater efficiency in your processing. Less data + better data classification = greater control and speed.

Less data stored = less cost

Data becomes a greater commodity than before. If you only hold the data you need, which is focused on the people you do business with, or intend to do business with, targeting services becomes much easier.

Holding data and processing data gives you a certain amount of control. Using predictive analytics will be a common part of the toolset of those businesses that want to continue to be successful, and categorising your data is a key first step in developing that capability.

NGIT positions itself as your one-stop shop for IT services. We provide services in the traditional sense of IT infrastructure, hosting, software, and the IT professional who just knows how to fix the things you use. But IT has expanded and compliance and management services, such as project and programme management and the ever-looming GDPR and its surrounding services, are now included in the scope of what most customers expect from an IT services provider.

Our private cloud environment and the services we provide around it tick all the right boxes. We host our clients' systems and data in local datacentres, and can therefore ensure end-to-end best practice is followed in everything we do. Added to this, we understand that our compliance and that of our customers is fundamentally tied together, and we are busy making sure that we are ready in our own compliance and in our ability to support you.

GDPR will require a review of your current procedures and processes to ensure they are suitable – we are already doing this for many clients. We are helping our clients ensure their internal procedures and processes are up to scratch through gap analysis and readiness reviews, and our new 'data protection officer as a service' offering.

So how do I get GDPR compliant?

That is the big question and the surprising answer is, you can't. The reason for this is two-fold. The law is not in force so you have time to prepare, but you cannot really comply. And secondly, directly compounded by the first, there are still unknowns and ambiguity and with no law in force, no precedence can be created. So what do you do? Well my only tip on this is simple:

Start a GDPR programme or project now and begin with a data mapping exercise followed by a gap analysis. Most importantly businesses need to be in a defensible position and be able to provide evidence that they have reviewed the regulation, and have taken reasonable steps to protect the personal data they hold.