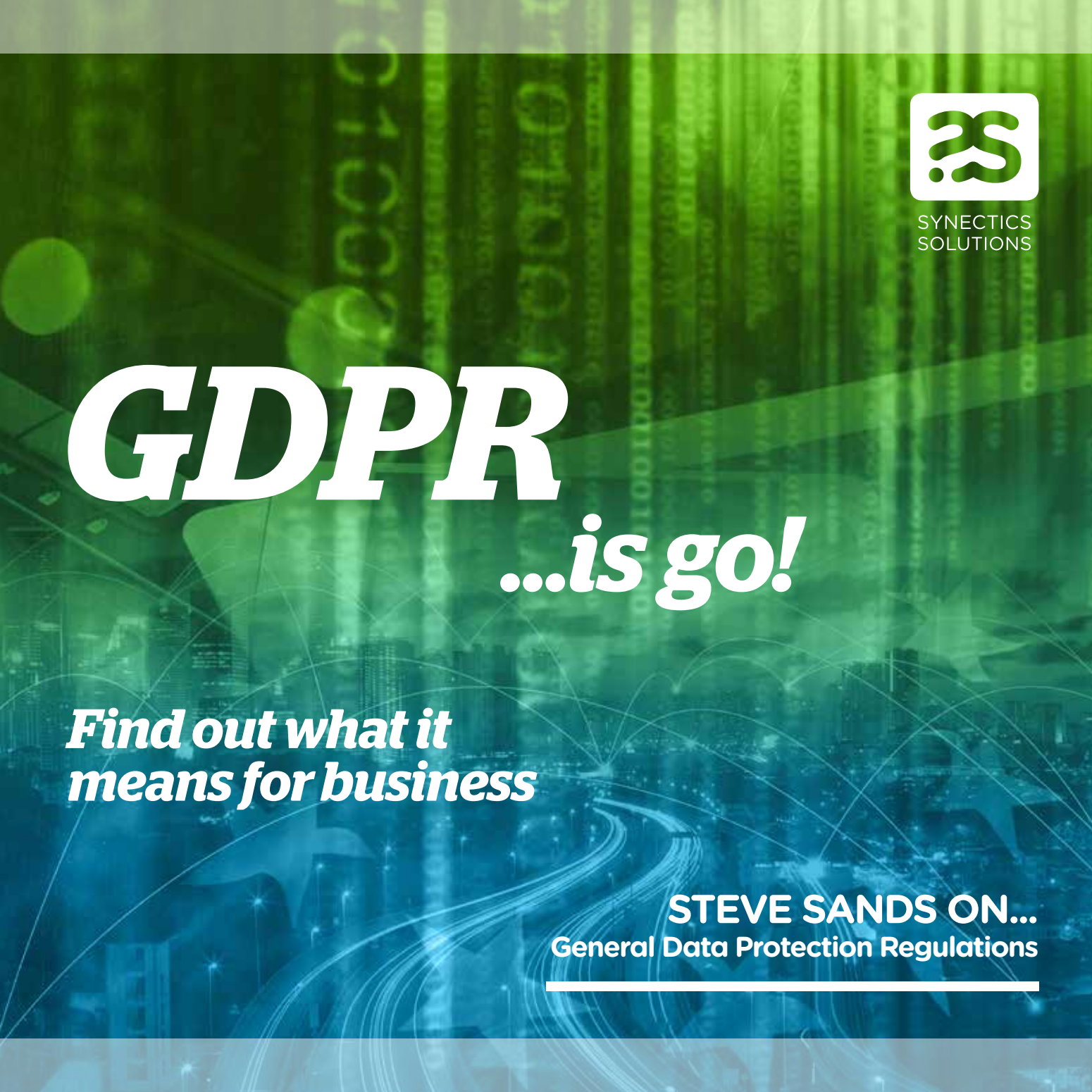
SYNECTICS
SOLUTIONS
GDPR
...is go!
Find out what it
means for business
STEVE SANDS ON...
General Data Protection Regulations

With GDPR now adopted into EU law, we speak to Steve Sands, Chief Information Security Officer (CISO) and Data Protection Officer (DPO) at Synectics Solutions to highlight how it differs from the Data Protection Act, and the implications for business.

The new regulations will bring significant changes in the coming 18 months and in the context of the UK's departure from the EU, the pros and cons of the legislation have been pulled sharply into focus.

Steve, can you start us off by explaining what the GDPR actually is?

Absolutely. The GDPR replaces the Data Protection Act (directive 95/46/EC) and affects all UK companies who collect or process personal information. It's focused on looking after the privacy and rights of the individual, and based on the premise that consumers and data subjects should have knowledge of what data is held about them and how it's used. Whilst it's designed to strengthen and unify data protection for individuals within the European Union, it does also deal with the transfer of personal data beyond the EU too.

What are the main differences between the GDPR and the Data Protection Act?

Well, we're down from eight principles to six now, but these are not radically different to the DPA. They focus on the intent with which any data is accessed and used being lawful, fair and transparent, and that it is for specified explicit and legitimate purposes. It's also focused on data being adequate, relevant and limited to what's necessary in relation to the purpose of the data access. Consideration is given to how accurate the data that's held is and how it's kept up-to-date, plus that it's only held in a form where the data subject could be identified for no longer than necessary. Finally it also looks for appropriate technical and organisational measures being in place in an organisation to protect against unlawful or unauthorised processing, as well as accidental loss or destruction.

So all positive then?

Well yes and no. One area of significant change is to the accountability requirements with the kind of sanctions and breach penalties that will make businesses sit up and take notice – fines can reach up to 4% of a business's turnover or €20m! And the penalties and sanctions will apply directly to data processors as well as data controllers. Inevitably, that will push data protection up the priority list, much as health and safety has over the last decade or two. There's also a much higher expectation around 'fair processing notices' which means that you need more details of where the processing is based, how long the data is retained, what purposes it's used for and the like. Transparency like this can only be a good thing for those consumers who are interested in their personal data.

There are pretty significant implications for organisations that are involved in data processing (and that's pretty much everyone these days). The GDPR affects both data controllers and data processors, and a Data Protection Officer with expert knowledge and a level of independence is required for bigger businesses (those with more than 250 employees or who process data for more than 5,000 subjects - and it doesn't take much to get to that level). Whilst it may be that the Data Protection Officer doesn't need to be full-time and in-house, we're likely to see a real shortage of expert consultants, and so legal teams are likely to be asked to step-in at first and pick up the slack. >>

With Brexit on the horizon, do we really need to worry about the GDPR?

We certainly do. Even if Article 50 is triggered in March as the Prime Minister has suggested, it will take two years for our exit from the EU to be agreed, and the **GDPR will become fully enforceable from 25th May 2018**. There are a number of different scenarios for after the UK leaves the European Union, but it's been suggested by some ministers that all current EU laws will become enshrined in UK law for ease, before the process of reviewing, debating if needed, and then keeping, refining, or dropping them starts. There appears to be a commitment to ensure that GDPR survives this process without any significant change so the risk of fines at 2 to 4% of turnover must be absolutely front of mind for businesses not planning to comply.

How is it all being 'policed'?

The Information Commissioner's Office (ICO) is leading on it and they have a reputation for being fair, but it'll be interesting to see how their funding evolves as we move forwards – after all, their role will massively increase and they've always avoided being funded from the proceeds of fines in the past. In terms of prosecutions, they could take action from the 25th May 2018, but I suspect they're more likely to choose their battles and initially focus on those wilfully not complying.

Is the GDPR fit for purpose?

It's early days and simply too early to tell. It's based on some solid principles and rights, and the Data Protection Act was certainly in need of an upgrade – in itself it was fine back in 1995 but we've evolved so much in the way that we generate, store, access and use data each and every day, that new guidance and protections absolutely had to be put in place. It's predicted that the volume of data held will grow more than tenfold in the next five years and we don't always know what uses our data is put to.

Do you foresee any problems?

Potentially yes. There's an enormous burden on data processors as well as data controllers, and that's never happened before. It will be interesting to see how some of the the big cloud providers deal with their requirement to check compliance. Fines are a percentage of turnover and they're likely to apply to them too, plus they have the reputational risk, after all as consumers we could hold both the data processor and the data controller responsible. And of course, all of that could see costs being passed on to the end users.

Also, Subject Access Requests used to carry a £10 charge but will now become free and that's likely to see an uplift in requests. Businesses need to prepare for this now! And finally, the GDPR enshrines the right of portability, which sees data, in theory, needing to be packaged up electronically and ported over to a new service provider, before being removed from the first company's system. I wonder how many have thought this through yet!

It's a case of watching and seeing how it all plays out but I strongly advise every business to consider how the GDPR will affect them, and to start planning for it now. At Synectics Solutions we're well advanced in our preparations, and we're supporting some of our clients with their own requirements.

STEVE SANDS

A risk and compliance professional, Steve leads on all aspects of cyber-security, privacy and data protection for Synectics Solutions.

A qualified ISO27001 Lead Auditor and a Data Protection Practitioner (PC.dp), Steve is a full member of several industry bodies including the Institute of Information Security Professionals (M.Inst. ISP), the British Computing Society, The Chartered Institute of IT (MBCS), the Information Systems Security Association (ISSA), and the Information Systems Audit and Control Association (ISACA).

Anyone seeking further information or support can call **01782 664 000**

Synectics Solutions Ltd, Synectics House, The Brampton
Newcastle-under-Lyme, Staffordshire, ST5 0QY

+44 (0) 1782 664000
info@synectics-solutions.com
www. synectics-solutions.com