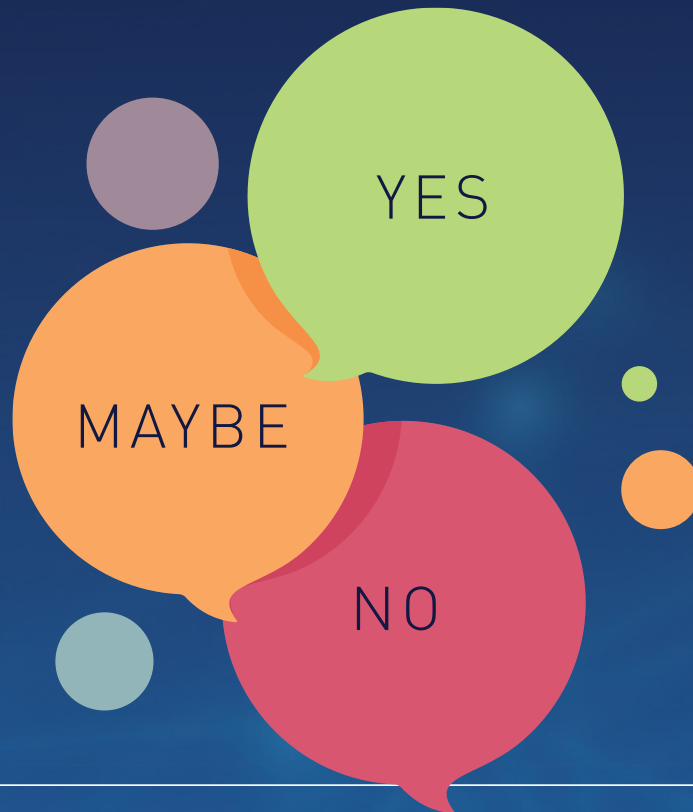




Excellence through experience

GDPR COMPLIANT?

BE PREPARED FOR THE 25TH MAY 2018



FIND OUT FOR JUST
£399*

Answer 60 probing questions to create a gap analysis report showing how close to compliance you are. And what steps you need to take.

- Simple to use online portal
- 60 data protection questions
- Tailored gap analysis report
- Reviewed by UK Data Protection lawyers

POWERED BY



* Price Excludes VAT

0333 222 4334

www.quiss.co.uk

BRAVE THE DATA

It seems like a long time coming, or at least it does for me as we've been covering the General Data Protection Regulation for the last two years. For law firms, and most businesses for that matter, I imagine they are wishing for a little bit more time to prepare. But as we understand it, as long as firms can prove they have plans in place and are starting to fix systems and processes as soon as possible, we won't be hearing about too many fines hitting companies.

Unfortunately, the hard part has really only just begun – don't think for a second that once you become compliant you can just sit back and focus on building the business. Without a doubt, we'll be seeing rules change as issues hit courts. But it's not all work and no play – I'm reminded by one of the interviewees just how important the GDPR is. Ultimately it's here to protect everyone's information. Our world will only continue to become more digital and with the amount of data and information swimming around the internet, now is the time for businesses to capture the trust of their clients.

Kayli Olson, acting editor
@LPMmag | kaylio@lpmmag.co.uk

FEATURE

05 What steps have firms taken to become GDPR compliant before the big day?

INDUSTRY VIEWS

12 Simon Ghent at Accesspoint, gives some practical advice for GDPR

16 Nick Hayne at Quiss, talks how to stay compliant well after the GDPR deadline

18 Natasha Rawley at ADDS, on how firms can change their document processes

About us

LPM magazine is published by Burlington Media. Burlington is a company focused solely on people in legal business services and management – whatever size or type of legal services provider they work for.

We run LinkedIn groups with thousands of members, across several areas, from legal IT to legal process outsourcing. Find our LPM group at bit.ly/lpmmag. Our sister brand LSN's website is where you can find news, views and resources from the established legal news providers

and hundreds of suppliers to the legal industry, all rolled into one useful information feed:

www.lsn.co.uk. We also run the popular **Legal Practice Management conferences**,

tailored specifically for anyone working in management in SME law firms and ABSs. Sign up for our weekly practice management e-newsletters, which bring you the best of our practice management content and our social feeds, every week: www.lsn.co.uk/subscribe/ezone

Contact us



Rupert Collins-White is editor-in-chief of LPM magazine. He has written about the legal sector since 2005, before which he endured years as an IT hack until he tunnelled out with a plastic fork.
rupertw@lpmmag.co.uk





Kayli Olson is acting editor. A Kingston graduate, she has spent most of her time in the UK picking up British slang, playing board games, drinking bitter and showing us 'how it's done'.
kaylio@lpmmag.co.uk




Emily Nash is LPM's client services contact – and resident musician. Want to advertise in LPM magazine or feature in our awesome advertorial section? Then get in touch with her.
emilyn@lpmmag.co.uk

 **0870 112 5058 or LPM@LPMAG.CO.UK**
Burlington Media Group, 20 Mortlake High Street, London SW14 8JN

 **www.lsn.co.uk/practice-management**
Find practice management blogs, news, resources, white papers, case studies, video and audio and much more online

 **@LPMmag**
We're listening, and we also have plenty to say. We love Twitter – and if you love Twitter too, share your thoughts with us

 **bit.ly/lpmmag**
We run LinkedIn groups for thousands of people in legal business services, and we run a dedicated LPM group, too

**Archive
Document
Data
Storage**



**View our free
GDPR toolkit:**

archivestorage.net/news/gdpr

**“Let us help your firm prepare
for the GDPR Legislation.”**

The File Queen, ADDS



**GDPR Record
Management Consultation**



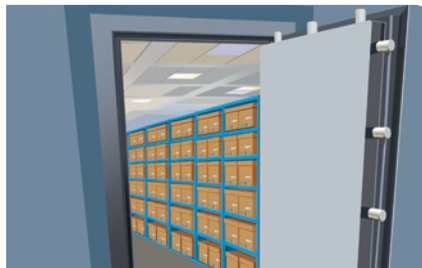
**Secure Destruction
of Files & Hardware**



**File Barcoding
Tracking Software**



**IT Asset Management
Software**



**Secure Matter File,
Deed & Will Storage**



File Scanning

Contact us now for a free consultation

☎ 0800 328 0272 | 🌐 www.archivestorage.net | ✉ filequeen@archivestorage.net



Certificate Number
4075-QM8-001
ISO 9001 : 2008



Certificate Number
4075-ISM-001
ISO 27001 : 2013



Certificate Number
4075-EMS-001
ISO 14001 : 2004



Criminal Disclosure
Checks



DVLA
Report – UK



SO NEAR, YET SO GDPR

The GDPR clock is moving closer to midnight. How prepared are SME law firms for the new data protection laws? Kayli Olson reports

Recital 4 (Article 1) of the General Data Protection Regulation (GDPR) states: “The processing of personal data should be designed to serve mankind.” Sounds like something out of a dystopian science-fiction novel, only it’s not fiction and hopefully won’t see the start of businesses going bust.

Despite worry from firms, of all shapes and sizes, on the impact that GDPR will have on their operations, believe it or not, the GDPR isn’t out for businesses’ throats, but rather is a punch at an answer to the question of data usage and rights.

Justin Ellis, co-founder and partner at

London-based law firm Northwall Cyber, points out that we’re in an environment that’s very different from 20 years ago when the last Data Protection Act was brought to the UK. Data usage in 1998 was at a very early stage.

“We’ve got a lot of data at our disposal and we need to be using that in a positive way. The thing to keep in the back of your mind when you’re embarking on compliance is to make sure data isn’t being used in a negative way, but that is being used in a way that will serve the people it’s supposed to be serving.”

A report in November 2017 from the



“In very broad brushstrokes the two main buckets of GDPR are information security and ‘everything else’. And that everything else bit is what is most daunting for businesses.”

Justin Ellis, director at iLaw and partner at Northwall Cyber

Information Commissioner’s Office (ICO) found that only 20% of citizens said they trust companies with their data. That’s a huge gap for businesses to fill – and long gone are the days when people’s information wasn’t looked after with the utmost care.

IT IS WHAT IT ISN’T

Unfortunately, even this late in the game, there are still misconceptions to clear up about what GDPR looks like in practice and how firms can actually prepare.

Ellis says: “If you drew a venn diagram of data protection and information security, they would form overlapping circles – they both have important elements to do with each other but they’re two distinct areas. In very broad brushstrokes the two main buckets of GDPR are information security and ‘everything else’. And that everything else bit is what is most daunting for businesses.”

Martin Lake, head of IT at Lester Aldridge, agrees: “GDPR is not just an IT problem, it’s a business-wide problem and requires active engagement from the entire organisation.

“We’re taking GDPR as an opportunity to improve our relationships with our clients by giving their personal data the same level of care and professionalism as the legal advice they receive.”

His firm engaged with an external consultancy, which came in to do a full analysis of the firm’s systems, processes and people. From there, Lester Aldridge was able to put together a remediation roadmap focused on delivering the

process, technology and training changes required to achieve compliance.

Things such as a data-mapping exercise, data protection impact assessment (DPIA), building in data protection ‘by design’ into systems and creating a response plan are all steps that should be explored.

Lake says: “It was important for us to document our processes and ensure they’re aligned to GDPR. And so, if the time ever came to deal with a data breach, rather than running around like headless chickens, we can follow our data breach policy and focus people on dealing with the respective tasks effectively, such as communicating with the rest of the business or making sure we don’t forget to tell the ICO or miss out on a key part of GDPR requirements.

“The firm has a ‘know-mantra’ – know what personal data we have, why we have it, where it is, what we can do with it, who can access it and how to gather it all together.”

KEEP IT SIMPLE, STUPID

Alistair Sloan, solicitor at Scottish law firm Inksters, says: “Do a paper exercise and think about what the business does, why it does it and then match that against the legislation.”

Sloan is structuring the firm’s general data-protection policy, which will act as a high-level overview of data-protection practices and will contain detailed information about areas where it wouldn’t be sensible to have in a separate or distinct policy, but the general policy will point people in the right direction to policies they need to refer to.



LPM FIRM FACTS

Fletchers

Statutory turnover: £26m estimated

Corporate status: Ltd

227 fee earners, 375 total staff

Offices: Southport and Manchester

LPM FIRM FACTS

Inksters

Revenue: Undisclosed

Corporate status: LLP

13 fee earners, 18 total staff

Offices: Glasgow, Forfar, Inverness, Wick, Lerwick, Portee

LPM FIRM FACTS

Lester Aldridge

Revenue: £21m

Corporate status: LLP

124 fee earners, 310 total staff

Offices: Bournemouth, Southampton, London

LPM FIRM FACTS

Northwall Cyber

Revenue: Still in first financial year

Corporate status: LLP

4 fee earners, 6 total staff

Offices: London



Adrian Denson, chief legal officer at Fletchers Solicitors, a Manchester-based medical negligence and serious injury law firm

With just over a month to go until the GDPR comes into force, which will affect the use of personally identifiable data (PID), law firms should now have their affairs in order, so they are ready to comply with the new laws. However, for those businesses that have left it until now, they may well find that they are frantically rushing around to get themselves on track. With this in mind, here are five essential tips that these firms should take on board before 25 May 2018 to avoid the imposition of heavy fines.

1 Assign a leader who will manage all things GDPR – The Regulations are far reaching, and too much for someone to do on their own part time, whilst doing their day job. So, firms should assign an individual who will take the lead and responsibility for data protection compliance. Having an individual that is dedicated to GDPR will ensure that businesses give the regulations the necessary attention that is needed, while being supported by specialists in their own areas, such as their IT department.

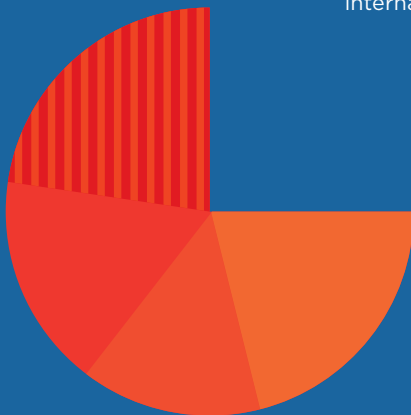
2 Map what data is on file, where it goes and what it is used for – Data mapping is time consuming, but it means that firms will know the risks, what changes need to be made, what they will lose the right to use after 25 May, and ideally, where to start with their changes. It will also help with planning and delegation of changes.

3 Ensure that all data is processed in a compliant way – GDPR will set a higher standard for consent, so if a law firm is relying on previous permissions as a lawful basis to process data, it is important to check that it is valid under the new regulations. If it isn't, then the onus is on the firm to re-approach individuals to regain consent or they may have to stop doing what they are doing. There are six processing options that make the use of PID lawful. Decide which one to rely upon and document it internally - and tell the data subject.

4 Update policies and procedures – It is vital that, come 25 May, a law firm's data protection policies and procedures have been updated to consider the new regulations. Time must be spent on reading through the regulations, so that policies can be swiftly updated accordingly. Do staff know what to do if a person asks for their details to be deleted, for example? Keep records of any decisions made to process data, even if it turns out to be the wrong decision – at least then firms can show why they reached the decision they did.

5 Train staff and carry out internal audits – Businesses should consider 'drip training' staff on GDPR laws by offering more than just one session to each of them. They also mustn't forget to tell staff what changes they are having to make to their processes. Train employees to follow 'red-flag' processes so they report issues with holding and using data, this will enable changes to be made to maintain compliance with the new laws. Once staff are trained to carry out continuous internal audits on the data that the firm holds, they need to make sure that all elements of the business are operating compliantly.

Law firms have had two years to prepare themselves for the impending GDPR regulations and the date of implementation is now fast approaching. Very soon, the way in which data is stored and processed will be revolutionised. For those law firms that have yet to update their data handling, there is still time to comply and prepare to avoid that knock on the door.



“One of the biggest challenges we’ve had is just dealing with the volume of work and variety of data that we hold as a multi-practice firm. The DPO and GDPR project team will be vital for us to keep on top of compliance.”

Martin Lake, head of IT, Lester Aldridge

“For example, if someone is going to send personal data out of the business, there’s a separate policy which sets out the steps needed to do that – we have a draft of handling and transfer policy. We’ve revamped our home working policy because there’s a lot of flexibility in the firm for people to work out of the office, whether at home, or court, and so on.

“So, rather than having one mammoth-like policy, it’s being split into different subject matters, which will be easier for our employees and consultants to use and find the information they need to ensure they’re compliant – hopefully, keeping the firm on the right side of the law,” says Sloan.

Firms must also remember to include process improvement and auditability for their physical files as well as digital. And for a historically paper-heavy industry like legal, that could prove to be quite difficult.

Lake at Lester Aldridge says the firm is adopting a clear-desk policy. “We also have lockable storage cabinets rather than open shelves.

“Fundamentally, we’re being asked to look after someone else’s personal data. I think it’s a bit sad that it’s taken some fairly robust legislation in terms of the GDPR to actually make businesses think about their data handling and put in the right processes to do this.”

THERE’S A SNAKE IN MY BOOT

One of the most important processes to put in place, after security and data handling is nailed down one way or another, is an incident response plan.

Lake says his firm has just finalised its own. “As with our disaster recovery and business continuity plans, it’s been trialled and will be regularly

tested. Because it’s one thing having a perfect document on paper, but it isn’t until you try it out that you realise you forgot a bit in the middle where the miracle occurs, as it were.”

There are some very strict time limits within the GDPR as to how and when the ICO or individuals affected by a breach need to be notified, adds Ellis at Northwall Cyber.

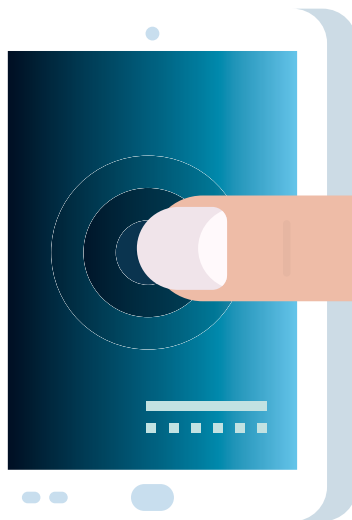
“Reporting an incident is one part of the procedure. The other part is more technology-oriented – looking into how the breach occurred and what steps are needed to make sure it doesn’t happen again.

“We have to have systems that are robust and enable us to continue processing even if we have some sort of information system disaster. Ultimately, though, it’ll be the combination of security, policies and procedures that firms need to have in place to enable them to comply,” Ellis says.

It’ll only be a minority of law firms that will be able to say they are completely compliant with GDPR on 25 May, he points out, and Lake and Sloan agree. Not everyone is going to get hit on day one.

“Therefore, in the time left, it’s all about getting the easy wins. Put the firm in a position where if the Information Commissioner came knocking on your door because she received a complaint then you should be able to at least point to a thought on the matter – a lot of thought. Know the main risks that your organisation is facing and how you’re going to deal with them, and try to have some solutions already in place,” says Ellis.

And even once you’ve got everything in place, Ellis says, you’ll still have to keep it under review to make sure that you have an ongoing





compliance programme.

TIME TO TAKE RESPONSIBILITY

To keep the boat afloat, firms need to understand the accountability requirements of the GDPR. Sloan at Inksters says it's about looking at individuals' job roles and working out where responsibilities sit within the existing structure so far as possible.

Sloan says: "We're thinking about our subject access handling policy and considering whether it might be better to have someone from the administrative team responsible for logging and monitoring them, as opposed to someone in the legal team. We need to make sure that the right person at the right level has the right responsibility."

"There needs to be a clear structure to identify who in the firm has what responsibility. Our firm is not of the size to need to appoint a data protection officer. So, at our May firm-wide gathering – where we get together to discuss important issues – obviously GDPR and data protection awareness is on that agenda."

Lake at Lester Aldridge says his firm has appointed a data protection officer (DPO) and has also set up a GDPR project team – consisting of the managing partner, DPO, deputy DPO, head

of compliance and himself as head of IT.

"One of the biggest challenges we've had is just dealing with the volume of work and variety of data that we hold as a multi-practice firm. The DPO and GDPR project team will be vital for us to keep on top of compliance."

From there the firm will have ongoing staff awareness and training, with aid from legal trainer Socrates. And on top of all that, Lake says the firm has a communication matrix so that staff know who they should be communicating incidents to, all the way from a missent email through to a major hack.

Ellis at Northwall Cyber agrees: "Training is going to be absolutely imperative because everyone in a law firm has to at least be aware of how to spot an issue."

Sloan says many firms think that the GDPR is only going to hinder them – that's understandable when looking at the effort needed to prepare and stay on top of it – but in reality, it's going to build a lot of trust and confidence, both with clients and employees.

As a profession, trust is essential to creating lasting relationships between client and law firm. The GDPR is there for the protection of your clients' data, and that will only strengthen their trust in your whole business. **LPM**

LPM

LEGAL PRACTICE MANAGEMENT

ONE-DAY CONFERENCE MANCHESTER

THURSDAY 17 MAY 2018
HOLIDAY INN, CENTRAL MANCHESTER

**THE ONLY EVENT IN
MANCHESTER FOR SENIOR
MANAGERS IN SME LAW FIRMS**

**"THANKS TO ALL INVOLVED IN PUTTING THIS TOGETHER.
IT IS THE 'MUST ATTEND' EVENT FOR PRACTICE MANAGERS."**

Simon Longhurst
Practice director, Teacher Stern

Sponsored by:

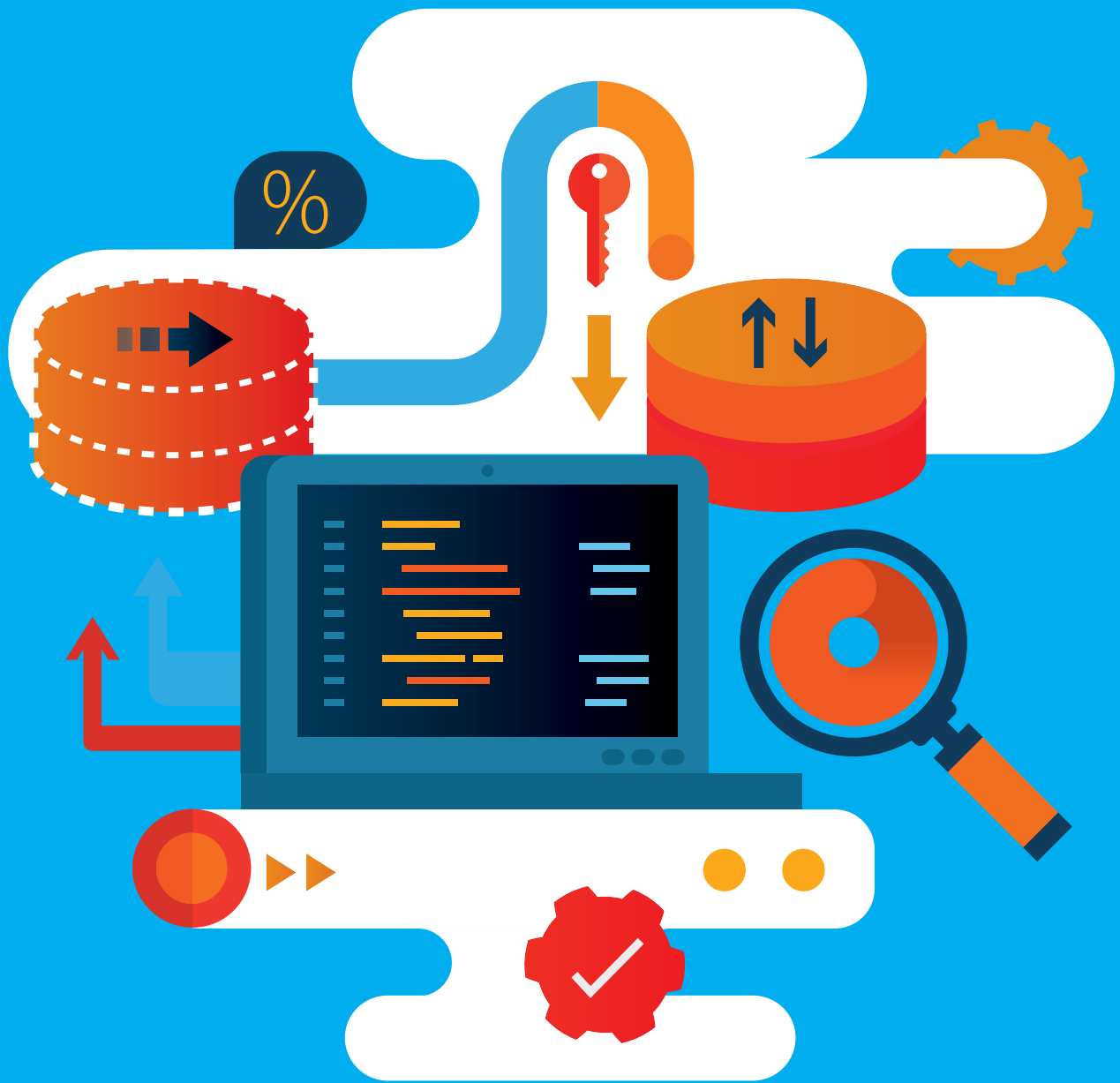


BOOK NOW

LSN.CO.UK/LPM2018

CALL 0870 112 5058

EMAIL EVENTS@LPMMAG.CO.UK



INDUSTRY VIEWS INDEX

DATA NOW

12 INDUSTRY ANALYSIS

Ready or not?

Simon Ghent, specialist GDPR consultant at **Accesspoint Legal Services** gives some practical advice for law firms making the journey through the GDPR forest

18 INTERVIEW

Here it comes

Natasha Rawley, the file queen at **Archive Document Data Storage**, gives firms the GDPR breakdown for improving data management

16 INDUSTRY ANALYSIS

After the 'finish' line

Nick Hayne, head of professional services at **Quiss**, talks about how compliance is not an end-all but an ongoing challenge



READY OR NOT?



Simon Ghent, specialist GDPR consultant for Accesspoint Legal Services, provides practical advice for law firms who can't see the GDPR wood for the trees

Data protection is now high on the agenda for businesses that are taking the imminent arrival of the General Data Protection Regulations (GDPR) seriously. Many have attended seminars – some have even read the regulations. However, based on our experience, many law firms cannot see the wood for the trees. As a result, many are ill-prepared for the first fundamental shift in data protection law in the last 20 years.

It isn't too late though. Don't fall for scaremongering. The Information Commissioner's Office (ICO) is not seeking to heavily penalise firms that take data protection seriously. Nor is establishing a readiness stance onerous. Rather, by approaching data protection in a methodical manner, legal firms can greatly benefit.

WHY WE NEED TO CHANGE

The way we work has changed dramatically since the Data Protection Act became law back in 1998. Back then, Google was still relatively new, our workplace heavily paper based and things like cloud computing, biometric data and digital marketing were in their infancy.

Despite the DPA giving us a framework, where personal data was identified and protected, it was often ignored. The ICO had neither sufficient powers or the resources to effectively enforce it.



This meant that many firms were able to pay lip service rather than demonstrate a proactive approach to data protection.

Fast forward 20 years and businesses can hold and process vast amounts of data for a relatively low cost. This technology revolution has changed the way we gather and handle data. The adoption of mobile devices and use of electronic bundles is changing the way many legal firms operate; rather than carrying around huge files, they are increasingly using cloud services and data centres like Accesspoint's to deliver secure access to documents, HR systems and practice management systems. Courts are even starting to provide secure WiFi.

At the same time, the threats to our data have rapidly increased. Some high-profile organisations have misused or lost people's information. Facebook and Cambridge Analytica recently hit the headlines for misusing people's information. Legal firms have suffered data breaches and are increasingly becoming targets for fraud.

Think about your own information and who it is shared with. When we consider all the apps we use and the businesses we share information with, it amounts to a surprisingly large number. Consider how much data they hold about you and what they can do with that information.

You would likely be shocked at how much

information is stored and how it has been traded as a commodity without our knowledge or permission. At the same time, malicious attacks and user error have been rapidly increasing, leaving our information extremely vulnerable.

We live in an unprecedented information age, so the GDPR, along with the Data Protection Bill that codifies the GDPR into UK law, should be welcomed as a result. The "protection of the fundamental rights and freedoms of individual persons, in particular, the protection of personal data" (Article 1) is certainly a noble objective. In a nutshell, this law is telling us all to play fairly and carefully with each other's data. If we don't, the results could be harsh.

HOW WE NEED TO CHANGE

Legal firms should be at the forefront of this change as they are perceived by the general public to be the ones who know about GDPR and what it stands for. Yes, perhaps a misconception but true and, after all, you are often dealing with distressed or vulnerable people. You may carry information about children or be involved with criminal proceedings. It's likely that data you hold would harm your client if it were freely available. Therefore, the information you hold is often sensitive or, to put it in GDPR-speak, a 'special category' of data.

ABOUT THE SPONSOR

Accesspoint is an independent legal IT specialist that consults on a variety of information technology-related issues, offering the best in IT solutions to help firms work more effectively.

www.theaccesspoint.co.uk

Accesspoint

Legal Services

Where knowledge makes the difference

Sadly, many view data protection as an IT problem and have assumed the outsourced IT company will deal with it. Others believe that it is something that can be solved by updating policy templates that no one reads. Hence why Accesspoint is often called into firms with poor IT security, little awareness of data protection principles and, in some cases, significant breaches and mismanagement of data.

For legal practices that want to demonstrate care and respect for their clients' information, it is vital that data protection becomes part of the culture. Everyone across your firm should understand and work within a framework where people's information is protected.

Firms that don't embrace this change face potential reputational damage, compensation claims, disruption to business operations, fines and, in extreme cases, criminal proceedings. So, it is worth getting it right.

WHAT SHOULD YOU DO?

It's important to take an orderly and systematic approach to your compliance journey, thus ensuring you review all areas of your data processing activities. Not forgetting your responsibilities as employers and all your personnel data.

The GDPR is not a one-time audit of 'compliance' and it shouldn't be ignored. You have an obligation to demonstrate how you are protecting data in line with the regulation. You should consider your 'legitimate reasons' for data collection, storage and subsequent use.

You should have a good governance structure in place that challenges all those who you entrust your data with and enforce high standards through awareness training and controls across your business. With the support of the senior management team, someone should have responsibility for data protection to drive changes and ensure that you are ready for the many aspects of the GDPR.

In some cases, a data protection officer (DPO) may be required. Three criteria are set for organisations when determining if a DPO is required. Legal firms will need to consider the third criteria carefully. If "the core activities of the controller or the processor consist of processing ... personal data relating to criminal convictions and offences" then you may conclude that you need a DPO. If so, you need to analyse if this

position should be internal or outsourced. Cases have already demonstrated that the DPO cannot have conflicts of interest. Even if you don't need a DPO you may consider it prudent to appoint someone who can fulfil the control tasks you're obligated to carry out.

Understanding your data is another crucial step. Establishing who "controllers" and "processors" are should be established first. In a nutshell, you're a controller if your firm "determines the purposes and means of the processing of personal data". When you receive an enquiry, gain a new client or employ a new member of staff, it will mean that you control their data. A "processor" handles that data on the controller's behalf. For most firms, processors may include cost consultants, barristers, IT companies, archive storage companies or hosting and IT companies, like Accesspoint.

This is important because as controllers under Article 24, you are responsible for the data. As such, you have an obligation to ensure the organisations you work with are ready for the GDPR and have a robust cybersecurity position. Don't assume they will. Many don't in our experience. Send questionnaires and carry out audits to establish this. If you use hosted applications ask if they have staff in "third countries" and if so ensure they have the necessary contractual clauses in place and that these have been approved.

As data controllers, you are required to "implement appropriate technical and organisational measures ... in an effective way ... in order to meet the requirements of this regulation and protect the rights of data subjects." This is especially important when handling "special categories of data" such as child data or data relating to criminal convictions. This principle of "privacy by design" means that you should understand how data enters, gets processed and then disposed of.

Imagine a factory. Normally every part of the factory has documentation highlighting all the inflows, outflows, valves and controls. This enables critical areas of weakness to be highlighted and control methods put in place to mitigate risk.

Data that you control and process is similar. If you don't understand your data, you cannot manage it. You can carry out this exercise using spreadsheets, flow diagrams or software tools



designed to assist you, like Accesspoint's bespoke GDPR auditing software platform.

If you're changing systems or processes you may need to carry out data protection impact assessments (DPIAs). These can highlight potential risks and vulnerabilities to data, which you can then seek to address and therefore mitigate risk.

Once you have established what data you have and how it flows in and flows out, and how it is processed and finally destroyed, you can then focus on the legal basis you have for processing this data.

Consent has been widely discussed, with some claiming that consent is always needed. Although they're not a get-out-of-jail card, other legal bases for processing exist. In many cases you will hold people's data for contractual necessity. You may have a legal obligation to hold this data. For example: the SRA and HMRC provide retention guidelines. These do not conflict with the GDPR. You will have data where the legal basis to hold it will change over time. Whatever legal basis you use, you should be mindful that you still need to be transparent and uphold the fundamental rights of the data subject.

TRANSPARENCY IN PRACTICE

What does transparency mean practically? We have all clicked 'next' when downloading an update without reading the terms or conditions. How many users actually understand what they signed up for? In many cases businesses bury onerous clauses that give them carte blanche to do as they wish with your information. Some client care letters and terms of service have at times been very poor and ambiguous.

That will now change with the GDPR. It's only right for people to understand who, why and for how long their data is being processed. This includes knowing, and in some cases consenting to, how data is shared with others.

As data controllers, legal firms need to ensure that when they collect information data subjects are clearly informed. Recital 58 defines this as "concise, easily accessible, clear and in plain language."

This typically will mean privacy notices, client engagement forms, client care letters and employee contracts – which should be reviewed. You will also want to ensure that the contact forms on your websites clearly tell people what

you will do with the information received.

Another key principle is that data will be "processed in an appropriate manner to maintain security." Elizabeth Denham, the Information Commissioner, stated that "cybersecurity and data protection are inextricably linked."

With cyber threats at an all-time high, legal firms have been identified as a prime target for cyber threats. Accesspoint speaks to many firms that have found that their current IT provider does not have the level of skill or competence to implement and maintain robust cybersecurity.

Cyber Essentials is a great way of demonstrating your organisation's commitment to cyber security. This government-backed certification scheme is one of only a few visible ways you can demonstrate to clients and suppliers that you take data security seriously.

However, it isn't just cybersecurity. How you handle physical data should also be considered. For legal firms this can be a significant challenge. Files left on desks, poor storage, third-party engagement and mobile device management (MDM) to mention but a few, are all areas where firms can experience data breaches.

Once you have collected a subject's data, they'll be able to exercise a number of rights under the GDPR. Not only should you become familiar with them but also ensure that you have the policies and procedures to handle them. Subject access requests (SARs) have been around for a long time. In a recent survey, over 30% of interviewees said they will use their rights to SARs under the regulation. Note: with the exception of some circumstances, you can no longer charge for these requests and unless your systems and procedures are established they could become quite onerous.

Legal firms have been identified as high risk and so it makes sense for them to build a robust framework of data protection and security. Mishandling data or suffering breaches can be costly, not just in terms of large fines and potential compensation claims but in recovery costs and, perhaps more importantly in the longer term, reputational damage.

With new rights, obligations and threats it makes commercial sense to ensure your data protection stance is ready for this new information age. Do it well and you can join other law firms that are using it to their commercial and competitive advantage. [LPM](#)



AFTER THE FINISH LINE



Nick Hayne, head of professional services at Quiss, says firms need to remember that compliance isn't an end-all ... it's ongoing and it'll change

It's unlikely anyone will check your compliance on 25 May. So, forget the deadline and worry instead about achieving and then maintaining compliance in the future.

Because if your business suffers a data breach and you are not compliant, a big fine, adverse publicity and reputational damage could follow.

The first thing you should do is get some answers and be assessed. There are simple-to-use portals with probing questions, all designed to interrogate you, your business and your approach to compliance.

These will assess you on data protection and information security compliance. Your approach to data sharing and subject access requests will be assessed, along with an appraisal of your records management. There will also be practical

measures to help with your direct marketing questions.

The answers you provide will help create a detailed RAG report, which will highlight critical issues (red), urgent issues (amber) and less-important issues (green).

These simple online assessments will help you decide what aspects of GDPR will impact your business most and this useful gap analysis will help identify your immediate priorities. If you are satisfied you are compliant or well on the way, it might just be worth a quick check.

THINK BEYOND THE DEADLINE

You must ensure the people in your business who are trusted with personal data understand their obligations under GDPR. Take appropriate steps

and if that means posters on walls, notes on desks and regular progress updates, with tips to help compliance, then get it done; then keep doing it.

Regular training for specific groups within your business will help and show you are committed to ongoing compliance. Make it relevant with good examples.

Post-deadline, consider adding GDPR compliance to your firm's risk register and sign up for email updates from the Information Commissioner's Office (ICO) to ensure you are aware of best practice advice.

Understand you are accountable – in future you must demonstrate you understand and comply with the concept of accountability, a key principle under the GDPR. This will typically involve creating more policies and procedures or updating your existing ones. It will be important that you keep a paper trail and not just tick boxes.

Using data protection impact assessments (DPIAs) where appropriate can be helpful in showing ongoing compliance. The ICO requires these to be undertaken before any type of processing which might result in a high risk.

Basically, if you're processing any form of personal data, do the assessment and keep records which will satisfy the authorities should they audit your business. The ICO also requires you to undertake a DPIA when deploying new technologies.

DECIDE AND DOCUMENT

Certain organisations will be required to appoint a data protection officer (DPO), others may decide it is best practice to appoint one, but most will not require one. If you decide not to appoint one, ensure you document the process used to reach your decision.

Data protection should be considered in commercial contracts applying to data processing and if you outsource it, only use processors that meet the requirements of GDPR.

Your contract will be large and comprehensive hopefully, allowing the processor to act only on the documented instructions of your data controller – this is very important and mitigates your risk.

Among a host of terms covered, you must make sure the processor can prove they have appropriate measures in place to ensure the security of processing personal data and delete or return it all at the end of the contract.

REVIEW AND RENEW

If you haven't already done so, review all internal policies and create new ones if appropriate

policies are missing. Under the GDPR, you must be able to demonstrate you have integrated data protection into your data processing activities.

You must ensure you collect only the personal data you need for the activities you have specified and ensure it is limited to only what is necessary. The less data you hold, the less the risk, but also consider use of pseudonymisation or encryption to protect personal data.

YOU WILL BE TESTED

You must be prepared, with written and documented procedures for dealing with subject access requests (SAR) from data subjects.

Ensure you understand the timeframes needed for a response and can complete without delay, including data subjects' rights to be forgotten, move their data, and so on. Prepare communications templates in advance to ensure a quickly compiled email doesn't reveal other sensitive data.

And prepare for lots of requests in the first few months as data subjects flex their new rights, knowing you cannot charge a fee or refuse to comply except in exceptional circumstances.

It's critical all your employees understand what a personal data breach looks like, even those not normally working with personal data. To be safe, create and use an internal breach reporting procedure, documenting the detection and investigation process.

You must understand what to do if there is a breach, who you have to notify, and how long you have to do it. The clock is ticking from the moment you become aware and it's not the time to develop new procedures.

The final note is that the GDPR is designed to change the way you think about how you protect, use and manage personal data. While it's unlikely you will instil the required culture change by deadline day, GDPR compliance must become second-nature, or your business could pay a high price – literally.

Help is at hand. Quiss provides a range of services to toughen up your IT system and infrastructure security to lessen the risk of a data breach.

We can proactively phish your people to ensure they remain aware of cyberattack threats and attempt to force our way into your network to test its ability to resist criminals.

Also, we provide GDPR gap analysis, help with achieving the Cyber Essentials Plus standard and a range of technical solutions backed by a Security Operations Centre (SOC) running 24/7/365, if necessary. If security threats worry you more than GDPR, and they should, please get in touch today. [LPM](#)

ABOUT THE SPONSOR

Quiss provides a range of innovative business support solutions for law firms of every size across the UK – shaping technology to help them achieve more.

www.quiss.co.uk

Quiss
Excellence through experience

HERE IT COMES

Natasha Rawley, the file queen at Archive Document Data Storage (ADDS), gives firms the GDPR breakdown for improving data management processes

Although many law firms in the SME market have been adopting cloud technologies in different forms, moving fully away from the traditionally paper-heavy industry is quite the task – that’s a lot of data being recorded and passed around on physical and digital files.

And with the General Data Protection Regulation (GDPR) ‘doomed’ to hit businesses at the end of May, SME firms need to know how to manage all of their data – wherever it may be.

The file queen, Natasha Rawley at ADDS, says: “SME firms should focus on getting the right processes in place to fully prepare for the GDPR. There are some simple steps you can take to ensure the precious client data you hold is being managed carefully.”

LISTEN AND UNDERSTAND

Step one on the journey to being GDPR compliant, Rawley says, is the information asset register. Firms should register anything and everything within the organisation that contains and controls information.

“For example, if they have laptops, a practice management software, hardcopy files, mobile phones that contain email attachments and other contact information, we encourage firms to put everything on an information asset register – this defines exactly what they have and will make it much easier to be GDPR-compliant.”

Once firms know what they have, the next step is to control that information, she says. ADDS uses a physical and electronic record management system called ActiveWeb, which allows firms to barcode all of their physical information and electronic equipment – it allows you to barcode and track matter files, deeds, wills as well as the tech used by staff such as mobile phones, USB sticks, hard drives, and so on.

Rawley says: “You can run a monthly audit to make sure that everyone still has their tech hardware and there haven’t been any data breaches.

“It also means that if you have a file room onsite, you can keep track of all of those devices and physical files. They can be signed in and out to fee earners or wills can be sent out to clients if requested.”

ADDS allows its clients to use ActiveWeb software as part of their service when they store files offsite, and they can implement it in house as well. Regardless of what EDRM system a firm uses, control in this way is an absolute necessity, you need to know where your data is, who’s touched it and audit it accountable she says.

After firms know and control the information they store, step three is to ensure it is secure. Rawley says that a good factor in security is to put different access levels in place so that people have to request files and only get access to information relevant to that person – both inside and outside of the business.

“Wherever information is held, on a document or practice management system, firms need to have the right security standards set in stone. And fee earners of certain departments should only access certain files and at certain security levels. Outsourcing this records management to someone like ADDS takes the burden away from the firm,” she says.

The final step is accountability – a data protection officer is a must, Rawley says. If the firm can’t spend the resource to hire one, then they need to put the practice manager in charge, or a personal assistant or secretary.

“You need to have a gatekeeper – someone needs to take charge of the firm’s records and information management in correspondence to GDPR.”

HASTA LA VISTA, BABY

Rawley says another thing ADDS encourages, which is a massive part of GDPR, is a record retention policy – it’s there to make sure that the firm is destroying the information it should, at any given time.

“One of the biggest improvements brought out



from the GDPR is that it forces firms to take better care of the personal information they hold, and to ensure that it isn't being held onto any longer than necessary."

This not only covers their client files and information but also internal information - things like HR records, she points out.

"At the moment, everyone is so busy concentrating on the external information that they store, they're not looking into internal information. They shouldn't be hanging onto internal HR information for longer than they should after employees leave the practice. Firms need to record and destroy any electronic or physical documents pertaining to internal data as well," Rawley says.

And when it comes to the point where things are ready to be destroyed - whether they're destroying hardcopy files, hard drives, or USBs - firms need to make sure they're destroyed by a reputable company.

She says: "Firms shouldn't close their eyes when it comes to the actual destruction part. Hard drives can be shredded as well, rather

“Firms need to record and destroy any electronic or physical documents pertaining to internal data as well.”

than just being recycled or wiped."

And, obviously, Rawley adds, firms need to ensure they hold someone accountable - whether that person sits in the firm itself or they outsource these services. Firms should confirm that the companies they work with are aware and compliant with the GDPR and have the right ISO certifications in place.

It's all very daunting, yes, but the GDPR can be broken down into component parts and attacked subsequently. Rawley says that there's more information and tools provided for free on the ADDS website that SME law firms can follow to prepare. **LPM**

ABOUT THE SPONSOR

ADDS has provided record data management services since 1987. As a legal sector specialist, it's helped firms of all sizes streamline and improve record and information processes.

www.archivestorage.net



Don't get caught

-  Accredited GDPR consultants who are qualified solicitors
-  Sophisticated GDPR workflow software developed 'exclusively for legal'
-  Secure GDPR platform with 14 work modules
-  On-site consultation and training
-  Full risk assessments and gap analysis
-  Breach and contract management features



Visit our website and download our free PDF information booklets now

Contact us on: 0203 189 2645
www.theaccesspoint.co.uk/gdpr

Accesspoint

Your gateway to more informative IT solutions