Comments by **Jonathan Sewell, Director of Risk and Compliance at Payne Hicks Beach** first published by The Law Society Gazette online on 26 March 2018 and reproduced with kind permission
https://www.lawgazette.co.uk/roundtables/gdpr-a-data-minefield/5065408.article


Jonathan Sewell
Director of Risk and Compliance

GDPR: a data minefield

By Eduardo Reyes 26 March 2018

As solicitors and their clients gear up for May's implementation of the GDPR, the *Gazette*'s latest roundtable hears that many appear to have left their preparations to the 11th hour. Eduardo Reyes reports.

Roundtable participants:

Emma O'Connor, Boyes Turner, **Brett Warburton-Smith**, Lockton, **Nicola Fulford**, Kemp Little, **Akber Datoo**, D2LT, **Frank Jennings**, Wallace, **Jonathan Sewell**, Payne Hicks Beach, **Gregor Kleinknecht**, Hunters, **Eduardo Reyes**, Law Society Gazette, **Adam Rose**, Mishcon de Reya, **Rowena Herdman-Smith**, Mishcon de Reya, **Laura Devine**, Laura Devine Solicitors, **Peter Wright**, DigitalLawUK, **Timothy Hill**, The Law Society, **Philip Giles**, Giles Wilson, **Patrick Wheeler**, Collyer Bristow.

'I'm sure everyone else around the table has found that there's so much misinformation and snake oil out there at the moment.'

So declares Peter Wright, managing director of DigitalLawUK and chair of the Law Society's GDPR committee. Reflecting on the 'cottage industry' spawned by the General Data Protection Regulation, Wright warns of 'people who suddenly say they are GDPR experts and will give you help and guidance'. A bit like the 'millennium bug', then – be aware.

On 25 May, GDPR introduces new laws on holding and 'processing' data. It requires transparency in respect of an organisation's possession and use of data, which must be for a 'legitimate process'. And if a result can be achieved without processing the data, an alternative method should be deployed.

Once the regulation takes effect, the maximum amount the Information Commissioner's Office (ICO) can fine for a breach will rise from the current £500,000 to £17m (€20m), or 4% of global turnover – whichever is higher. That would seem to reflect the fact that, as Payne Hicks Beach director of risk and compliance Jonathan Sewell puts it: 'Data is the new oil… so we are under a duty to drill responsibly.'

Lawyers have been advising clients on the GDPR while also getting their own house in order. Kemp Little partner Nicola Fulford notes: 'In many ways, law firms are ahead of many other sectors because of the overriding obligations of client confidentiality, which should have led to firms as businesses taking security and cybersecurity seriously long before now.' Commercial firms should have learned lessons, she says, following incidents where M&A due diligence has been conducted by firms with IT systems that were hacked for the market intelligence contained in the data.

Even for a well-run firm that is on its guard about such things, preparing for GDPR has been a significant task. 'We've been trying to train all members of the firm, from support teams through to client-facing lawyers,'

Mishcon de Reya partner Adam Rose says. 'I've done 13 sessions so far with 50-60 people in each one. It's been quite an exercise.'

As with most compliance tasks, Mishcon's training aims to be more than a box-ticking exercise, Rose adds: 'It has been quite useful in terms of opening people's eyes to business development opportunities, as well as their own personal practices [where] they assumed everyone was always doing [something] and therefore it was OK.' Many are also engaged by the link to their personal lives: 'When they come out they say, "I didn't realise I had data subject rights".'

The GDPR has been a particular headache for some smaller firms, observes Philip Giles, partner at Giles Wilson and a committee member of the Law Society's Small Firms Division. 'For small firms there is perhaps a lack of practical guidance about how to implement it,' he says. 'You see a level of paranoia at one end of the scale, where absolutely everything seems to be broken down into minute detail, and then inaction at the other end. There's no complacency [on GDPR] but it's on a very long list of things that need to be done in terms of compliance and risk. I think most firms will feel that they're ready, but we're all waiting to see if we actually are.'

Laura Devine, principal of five-partner niche immigration firm Laura Devine Solicitors, says compliance with GDPR has recently taken up to a third of the time of her firm's compliance officer: 'It's very time-consuming and costly for a small firm. Think how complex it is and how many areas it touches – current employees, past employees, clients, clients with criminal records, information on personal devices.' An added complication for Devine is that her firm has a US office, with which, of course, data is often shared.

She and colleagues have, at least, begun work on GDPR compliance in good time. Elsewhere, preparation has suddenly become frantic, some suggest, because the non-experts have only

recently been willing to focus on GPDR. As Wallace partner Frank Jennings says: 'I've been talking about GDPR for the last three years, but it's only over the last six months that clients have actually started taking me seriously.

'Some of the people I've been speaking to are amazed that there is a Data Protection Act 1998, let alone GDPR. I explain to them that if you look back far enough, we've had data protection obligations in the UK since 1984. Brexit's not going to change that. In fact, [the UK] started this after the second world war when we helped write the European Convention on Human Rights. Then, we led the way with the Data Protection Act. So those people for whom GDPR is proving to be a shock are the ones who need to be most worried.'

Fulford notes in this context that the ICO will have expectations based on data laws already in place. 'The data protection principles, fundamentally, are very similar under GDPR,' she points out.

'In terms of enforcement and risk, regulators are saying "if you're not doing some of the new things around… data [management]… or your transparency [is not] quite as good as it might be, then we will give you a bit of time and a bit of leeway'. However, Fulford warns: 'If you're not doing the fundamental basics that you should have been doing for the last 20 years under the Data Protection Act, I don't think they will be holding back in terms of compliance and enforcement. These are not new obligations.'

In that respect, says Rose, law firms are probably on the ICO's radar: 'One of the things that I think the ICO has reported on is that the legal sector is one of the top areas of complaint. There's health, local government, education and then legal. [Given] it's been an area where people have complaints, it's quite possible that the ICO would look at a sectoral approach – and at large firms, small firms and medium-sized firms as well.'

Hunters partner Gregor Kleinknecht says that this degree of scrutiny is justified by the sensitivity of the data law firms hold: 'A medium-sized firm like Hunters obviously doesn't manage and process as much data as a Clifford Chance would do, but we're still about 50% private client. So we're holding a lot of what would be described as special personal data, which relates to potentially vulnerable clients. The risk there is higher than if we were purely a commercial firm dealing with commercial clients.'

Suppliers and other law firms, the latter dealt with in the context of transactions, are also relevant to GDPR compliance, Mishcon de Reya partner Rowena Herdman-Smith reminds the group. 'In the world of business, you share data with suppliers to help you deliver your services.' Mishcon found it has had to educate these suppliers: 'Some of them really don't know that they are also going to be asked to be compliant with GDPR. Some of them don't know that they are actually processing data.'

Emma O'Connor, associate at Boyes Turner, expands on the 'vast amounts of data that we hold not just as data controllers, but also as data processors', adding: 'You think about litigation where we're not [just] receiving information about our client, but maybe about our client's employees. So, we have to think not only about our own privacy notices, but also about what the client has told their employees about what's going to happen to that data.' Equally, a firm acting for an employee (or ex-employee) will hold data about the employer and other employees.

While O'Connor notes that 'there shouldn't be any bombshells here about people's data – it should be pretty obvious to most people,' she adds: 'The difficulty will come in scenarios where we're transferring data to third parties, [or] outside of the European Union.' Global organisations and international law firms need to find ways to be 'transparent about what we're doing with the data, so we don't have people up in arms'.

There are challenges, too, even in law firms where data has always been treated with consistency and transparency. Herdman-Smith explains: 'We have collected data for many years, for very good and proper reasons, but we have data in lots of legacy systems… when you start looking, you start finding things that you then have to address.'

Part of the misinformation surrounding GDPR relates to activities it is claimed must stop. The information commissioner uses the example of a bogus claim that dentists will not be able to remind patients when a check-up is due. As O'Connor notes: 'GDPR doesn't stop people doing what they've always been doing with data… we've had data protection laws for some years. But what it does mean is we have to be much smarter and much more open about what we do with data.'

How harsh?

As Fulford notes, the ICO's attitude to a breach – specifically the level of a fine, reprimand or remedy – may depend on the strength of an organisation's pre-GDPR data law compliance.

But this is an area where there are many unknowns. As Collyer Bristow partner Patrick Wheeler says, the ICO has said the new regime will be 'evolution not revolution'. This, though, is less straightforward than it sounds; somehow the expectation is 'evolution, not revolution, but total compliance from day one'.

'I think for the vast majority of clients and, certainly in my experience the vast majority of law firms, it is a revolution,' Wheeler argues. There are 'people who are nowhere near compliant with the 1998 [Data Protection] Act… To read and understand the ICO guidance you have to have a base grounding in what data protection is about. If you pass on the small business guidance notes to clients, they come back and say, "Well, that's all very well, but I haven't got a clue what any of this means". So, there is a very big education job still to be done and you have to start further back from where the ICO is starting.'

Sewell picks up the point: 'I think there are a lot of legal resource providers who are hedging their bets and waiting to see how things develop. What I've noticed speaking to other firms of solicitors generally and reading the press, is that there tends to be… a correlation between risky practices and non-DPA compliance.'

Covered?

That leads the discussion to the relevance of insurance. Brokerage Lockton's Brett Warburton-Smith notes that opinion in the insurance market is divided over the relevance and validity of insurance related to data breaches.

'There's a place for insurance and what it can provide in terms of protection,' he says. 'However, I certainly wouldn't say it's a replacement for having to comply with GDPR by any stretch of the imagination.

‘You’d be surprised. A lot of the profession are turning round and saying, “Well, OK, let’s just buy some specialist insurance, or even rely on our existing PII insurance and we’ll go ahead on that basis”.’

But what can insurance cover? ‘The other question which is probably more talked about than anything else at the moment in our world is whether the fines and penalties might be insurable,’ Warburton-Smith reveals. Unlike the Financial Conduct Authority, ‘the ICO hasn’t come out and said, “fines are not insurable”’. Hence the grey area, he adds: ‘We, and no doubt others, have taken advice from other parties and looked into it quite carefully. Despite some brokers sadly going out and saying that fines probably are insurable, we don’t believe they will be.’

Cybersecurity insurance may cover some data breaches, but specialist cover is not purchased to cover loss but rather to support a firm’s response to a breach: ‘That will help you deal with the relevant 72-hour time period to notify affected individuals and give you access to specialist forensics security people to come in and try and establish what the problem is.’

With GDPR looming, is data management part of the narrative law firms must address in PII proposal forms to gain good cover at the best rates? ‘[That’s not] coming into proposal forms yet,’ Warburton-Smith replies. ‘We’ve taken a view with our proprietary policy wording that there’s absolutely no pull in highlighting GDPR in there. Because if you do that, then potentially you don’t have cover for any other regulation, in whatever jurisdiction. So, we’re keeping silent on it.’

All present have considered various high-profile incidents of data loss and the consequences for the organisations concerned. ICO fines aside, Fulford notes, ‘reputation, and share price, and customer loss’ are all jeopardised in the corporate world and the stakes are similar for a law firm. ‘There’s been the odd company that’s managed it very well, and done excellent customer communications, and not really suffered much downside,’ she says. ‘Then, conversely, there are others who made a complete hash of it. They’ve tried to cover it up. It’s come out later and the costs have increased dramatically.’

These are events that a firm and its clients must plan for, stresses Fulford. The time frame within which a crisis can be properly dealt with is very short: ‘You need to know within your organisation who’s responding, who needs to be involved in the discussions, who’s doing what communications.’

She adds: ‘If you’ve looked again at your disaster recovery, your business continuity, then you’re going to have a much “better breach” – albeit it’s going to be awful. The alternative is it just happens and… no one knows what to do, or someone makes the wrong statement, or nobody closes things down.’

As Jennings says, this is ‘just another part of your GDPR preparation’.

O’Connor observes that creating the right culture around data in an organisation is critical. Staff must realise how grave poor data management or a data breach are, yet feel able to come forward swiftly when an incident occurs. ‘The first priority has to be, tell somebody,’ she says. ‘That’s where the training and the awareness comes in. You’ve got to have the confidence and the courage to be able to speak up and say “Look, I’ve clicked the wrong button”.’

Fines

Clearly, there are many sound reasons to treat the GDPR seriously that do not relate to the level of fine that could be imposed for a breach. Yet, the eye-catching size of the penalties available will always make fines a talking point.

How, specifically, will the ICO's stated goal of 'evolution, not revolution' be reflected in punishments? And, over time, will Brexit bring about divergence in practice from the EU27?

'I think the UK is in an interesting position at the moment,' Rose says. 'You've got the information commissioner being quite clear that she believes more in the carrot than the stick.' But if 'mainstream European practice' moves towards higher fines, the UK may lose its 'finding of adequacy', making it more difficult for data to pass between the UK and EU member states.

Fulford observes: 'In terms of enforcement and attitude, I've found that the information commissioner has moved towards Europe in the last year or so… it always used to be that Spain was fining all of the time, but actually I think the UK is a significant finer under the directive. In the last few years there have been a lot more fines in the UK than most of the other countries.'

The question, Rose notes, is whether raising the maxima fine will actually see a rise. Will fines for breaches now issued at £100,000 be £200,000 for similar breaches in the future, 'or do they translate as £4m?'

'I think they will build,' Fulford concludes. 'I think if you look at ICO guidance, they will start fairly low, but they will increase.' Wheeler agrees, adding that an EU finding of adequacy will be a key priority for the ICO: 'I think the only direction is up, frankly – in some ways to set an example to show that we are taking this seriously. Fines are one of the eye-catching ways to make that happen.'

That will not be the only regulatory response, O'Connor predicts: '[We're] moving to the new course of "naming and shaming". Most rules now – gender pay, national minimum wage – reflect a naming and shaming culture. I think that's what we'll start to see with the data protection as well, in the hope that fear of reputation damage will spur people to comply.'

For these reasons, Wright reflects as the discussion comes to an end, all organisations need to take GDPR extremely seriously. He recounts some of the worrying reasons for inaction he has encountered: 'You do still get the most bizarre excuses… [such as] "Oh, we don't have a website".' There is 'misinformation that's swirling around online' and '[people] get the weirdest misconceptions about what GDPR actually means'. The EU referendum result, he notes, made it more difficult to get attention for GDPR: 'It went quiet for about six to 12 months. It was only towards the end of last year that we've really seen people coming to us for help. People have left it until the 11th hour.'