Legal Information Management, 18 (2018), pp. 76–79

doi:10.1017/S1472669618000178

Practical Privacy: Report from the GDPR World

Abstract: In this article Susan Doe reports from the perspective of the law firm sector on the progress towards the introduction of the General Data Protection Regulation that became automatically 'live' on 25 May 2018. She provides an introduction to the Regulation, highlights some practicalities for law firms when considering compliance with GDPR and offers a 'to do' list with reference to the record of data processing, training needs, security, and contracts and documentation. She also provides advice on what should be considered especially in respect of client demands.
Keywords: law firms; privacy; data protection; General Data Protection Regulation; GDPR

INTRODCTION

Take a moment to consider how much of your personal data is out there in the world. Who, however legitimately, has access to your name, contact details, bank account details, photos, videos, CCTV footage? Also, consider how the world has changed since the last Data Protection Act in 1998. The European Union has thought long and hard about how to protect the individual's right to control how their data is used. Then they made sure the world noticed by putting in some potential fines that make eyes blink, if not water. The top end is four per cent of global turnover, or 20 million euro, whichever is greater. The General Data Protection Regulation (GDPR) will become 'live' on 25 May 2018. I hesitate to say it will come into force to you, dear readers, because of course this is a Regulation and it does not need to be brought into force.

What about Brexit, I hear you cry? It is not a magic wand to make it disappear. The UK government has made it very clear that its provisions will survive the UK's exit, and even if they had not, its scope is so wide that any organisation that has international reach will be caught.

Law firms have limited personal data on their systems compared to the social media giants, public authorities and even major retailers. Those of you in the field of information, knowledge and libraries will have an even more limited pool. However, it still applies and while I am well aware that I am adding to the not inconsiderable amount of literature out there on the GDPR, I will target this at law firms and where possible, to the legal information profession.

COMPLIANCE UNDER GDPR

The aim of any compliance programme under the GDPR is to understand what personal data you have and what happens to it, where it goes and how secure it is. And, to be transparent about it to the data subjects, so that they are in a position to assert their rights over it. The rights under the GDPR are the rights of access (under a subject access request); to erasure (the so called 'right to be forgotten'); restriction of or objection to processing; data portability (to be able to easily move your data from one vendor to another for example). These are all subject to country-specific requirements. Even though this is a Regulation, each country in the EU can make specific requirements, for example, under the UK's Data Protection Bill.

Personal data is defined as any information that directly or indirectly identifies an individual. Obviously, this is a wide definition and does not need to include a name. As long as the information can be used to identify someone, it is personal data. It could be a mobile phone number or an email address. Email addresses are particularly interesting for those of you (all of you?) who subscribe to databases that use email addresses as part of a login. The vendor of that database will therefore hold personal information and will be processing it, and therefore must make sure it is treated correctly under all the data protection principles. That includes not to use it for a purpose incompatible with the reason for which it was originally collected. If it is collected for the purpose of accessing a database, using that email to contact the individual for a marketing purpose is unlikely to be legal. Contacting them to say that the service is currently unavailable probably would be.

FURTHER GUIDANCE AWAITED

At the time of writing further guidance on GDPR is still awaited from the Information Commissioner's Office (and

other European data protection regulators), the EU's WP29 Working Group and various professional bodies such as the Law Society. That guidance will be invaluable in determining your priorities on what needs to be done and what position you will take on issues such as whether you should appoint a Data Protection Officer (DPO) or whether you are ever likely to be a data processor as well as a controller. Processors have wider responsibilities under the GDPR than they did under previous legislation and provisions need to be made should any of your work fall under that of a processor.

GDPR: A 'TO DO' LIST

The Processing record

Having a written record of data processing is a requirement under the GDPR for both data controllers and data processors, with some exceptions; for example, if the organisation employs less than 250 people (though this is balanced against whether the processing carries a high risk to the data subject).

Data controllers are those who determine the manner in which the data is processed. Processors process on another's behalf and in accordance with the controller's instructions.

The record should be available on request to the relevant supervisory authority (in the UK, the Information Commissioner's Office). This should apply firm-wide, but each area, including Library, Information & Knowledge, should consider their own circumstances.

You need to document the:

a. **purpose/s** for which you process personal data (eg administration of personnel; supervision at work; customer relationship management ; fight against fraud)

Supervision at work would include procedures such as operating database usage recording software. Be careful even if you anonymise names of users; if you can effectively still identify individuals using other information such as job title/department then you could still be using personal data. GDPR has specific rules about anonymisation and pseudonymisation so you will need to carefully consider those in relation to how you are operating.

b. Decide whether you are the **controller or processor** for this purpose.
c. The **type of data** processed, ie. that which is personal data, such as, email address, bank details.
d. What is your **legal basis** for processing?

These are listed under Article 6 of the GDPR. In most law firm cases these would either be performance of a contract, legal obligation or legitimate interest. Legitimate interest reasons will need to be balanced against the rights of the data subjects. Each case will need to be assessed and the reasons documented.

Consent is also listed as a potential basis, but the guidance is clear; consent will be virtually impossible to justify in an employment context. Essentially, anything you currently have as an 'opt out' tick box – remove and replace. Consent, in any case, needs to be active and deliberate, it cannot be by default. It also cannot be bundled into a group, each purpose must be able to be consented to (or not) individually.

Also, note that you should not have more than one lawful basis for each process.

e. The **recipients of the data** – where does it go? Third parties? Internally? Outside the EU?

For third parties, check the agreements or contracts. What are they contracted to do? Do you have the right to audit them? For international firms, what is your method of safe transfer to countries deemed unsafe by the EU? Model contracts? Binding corporate rules? Privacy shield? Are they up to date? Keep an eye on the various challenges to these methods currently going through the courts.

f. The **security** measures implemented to protect the data.

These would include security policies and training of personnel as well as technological protections.

g. The period of data **retention**

Is there a policy? Statutory periods? Professional standards guidance? Does the data actually get deleted after this period or is the retention policy really hypothetical?

How long you keep data in defiance of what is written in a retention policy is particularly important when it comes to Subject Access Requests (SARs). If the data is there, even if it should not be, it will need to be disclosed. If it isn't there simply because it was destroyed in the normal course of events under retention, then there is no longer a requirement to search. However, suddenly deleting something in accordance with a retention period simply because you have received a SAR will be frowned upon by the regulator.

h. Have there been any previous **security breaches** of this data?

It is imperative that the processing record is treated as a 'live' document. It is not meant to capture a moment in time but to be updated as and when necessary.

Behind all this record keeping is good business practice. Data subjects have increased rights and you need to be on top of them. If you know where your data is, why you keep it and for how long, and where it is going - you have the essentials to be able to deal with issues such as breach notifications and subject access requests.

Training

These two areas, breach notifications and subject access requests, strongly show the need for training of all

https://doi.org/10.1017/S1472669618000178 Published online by Cambridge University Press

personnel, so that they are at least aware of the issues and know how to recognise what a breach and a SAR is.

Breaches need to be notified within 72 hours of being spotted. This could mean something like a laptop going missing, or an email with personal data being sent to the wrong recipient. You have to weigh up the risk to data subjects, but at the very least it is important to let those in your privacy/risk team know that something has happened.

SARs, ie. requests for a copy of an individual's personal data, can be sent to anyone at the firm, there is no requirement for them to go to the privacy/risk team or to HR, for example. They could be in the middle of an email from a client. It is necessary that all staff should know how to spot a SAR and where to send it. Under the GDPR these requests must be met 'without undue delay' and within 'one month'.

I would suggest that it would be a very useful exercise to run a dummy SARs exercise, and make it as awkward a request as possible. This will give you a good idea of whether you are ready to deal with the real thing in the allotted timescale.

Include the lawyers in the training. There seems to be some tendency for SARs to be used to try and circumvent legal privilege. SARs are strictly 'purpose blind', but anything provided to the individual should be carefully considered and redacted where possible (remember that what they are entitled to is personal data regarding themselves) to avoid giving out information that it is not necessary to give. They also need to be aware of any possible personal data issues regarding using ancillary services such as translators.

Training should also make people aware that they need to inform the relevant people when there is a new process or piece of software that will process personal data and therefore make sure the processing record is kept up to date. They also need to know that it is a requirement to run a privacy impact assessment (PIA) in certain cases – eg. under the GDPR, high risk processing. (For guidelines see the WP29 Working Group's report from October 2017).

A privacy impact assessment seems at first glance to be yet another burdensome document. However, they are a very useful tool to assess the data protection implications of processing and they are key in demonstrating compliance with the GDPR. They should describe the envisaged processing and the purposes; an assessment of necessity and proportionality of the processing in relation to its purpose; an assessment of the risk to the data subject's rights and measures to address the risks and demonstrate compliance with the GDPR. Be aware that you will be asked to complete a PIA if you wish to use a new system that includes personal data, so look on it positively. These, like the processing record, should be live documents and updated regularly.

Training needs to be ongoing. Existing staff and lawyers and any new joiners need to be covered. Ideally the induction programme should include a piece on data protection, and either a live workshop/seminar or a webinar where people's attendance can be tracked. This is on a par with the anti-money laundering and anti-bribery training that you should already be requiring your staff and lawyers to undergo.

Security

This covers physical security (eg building access cards; CCTV monitoring) and information technology security. Law firms have been considered for some time to be a weak link in the chain in cybersecurity issues. Even if this were not the case, frankly, this can and does happen to anyone.

Law firms hold a vast amount of both competitive and privileged information (trade secrets, undisclosed deal information) as well as any private client personal data. This makes them very attractive to would-be hackers. Even if the main reason behind a hack is not personal data, there is still a risk to it if anyone breaches your systems.

Part of the issue is that in many cases breaches are not spotted until sometime after illegal access has been gained. Your IT security people should be aware of dark web monitoring solutions, so that they can be alerted to leaks and breaches far sooner. The dark web is where most of the information gained from cyberattacks ends up.

Again, the detail in your processing record should assist your efforts in detecting where the breach has occurred and what has potentially been lost.

Contracts and documentation

Engagement letters, employment contracts, privacy policies, notices – anything that covers data protection rights and obligations needs to be reviewed and updated.

[I have deliberately kept issues to do with marketing and business development to the side in this article since most of the issues they deal with, especially in business to business marketing, will be governed by the E-Privacy Regulations that has been delayed at the time of writing and will need to be assessed once it is in its final form. However, any online privacy policies or consent functionality on public websites should be reviewed in light of GDPR.]

Vendor contracts need to be prioritised regarding the level of personal data that they encompass in the service provided. The GDPR provides prescriptive wording for updating contracts. It may well be the case that there are a lot of vendor contracts to assess and you will need to prioritise according to the amount and type of data processed under the contract. You might even find running a PIA a useful exercise to determine priorities. Due to the tight deadline accepting and mitigating risk may be your best option for now rather than any chance of totally avoiding it.

Database contracts seem to be low priority in most cases – ie those that have personal data in the form of email addresses which form part of a login. As mentioned

https://doi.org/10.1017/S1472669618000178 Published online by Cambridge University Press

earlier in the article, the fact that this is personal data in itself means the vendor is a processor of personal data. It may be that vendors review this policy in order to avoid being a processor and thereby being subject to the increased responsibilities of processors under the GDPR.

In the meantime be careful about what the contract terms say about them using the email address for anything other than the login.

GDPR: A 'TO CONSIDER' LIST

This section could easily be headed 'client demands'. Each firm will need to make a call depending on their own circumstances and come to a decision appropriate to their business. Make sure it, and the reasons behind it, are documented.

1. Data Protection Officers (DPO)
   The GDPR states strict conditions for when a DPO is necessary. It may be that law firms, especially the smaller ones, decide that they do not actually HAVE to appoint one. However, it may be that your clients would expect that your firm would have one. Whichever you decide, make sure you document your reasoning and are able to explain clearly to your clients why you came to that decision.
2. Processor or controller? In the normal course of events a law firm would be a data controller. However there may well be cases, depending on the type of clients and work that you do, where you are acting as processor for an amount of personal data on behalf of your clients, eg. in a TUPE case or an M&A dealroom situation.

   Make sure you are clear in your engagement terms as to what you consider to be the situation. You may need to follow up with further terms if your role has a processor element.
3. Pitches and proposals
   If clients are not asking already about your data protection compliance programme as part of the due diligence and assessment process, they will. Be prepared, especially regarding what you will need to and what you would be prepared to, hand over.

Two final issues. It would be a very useful exercise to push the whole mantra of data minimisation at everyone in your firm. Simply, do not keep it, if you don't need it.

The rights of data subjects to erasure/be forgotten and portability are, currently at least, difficult to envision in a law firm setting. The right of erasure for example cannot override retention rules, whether employment based or client records regulated by the SRA.

FINAL THOUGHTS

This has been a whistle-stop tour of the practicalities regarding a potentially worrying piece of legislation. I would only advise you to keep in mind your own data; what would you want done with it? In most cases, I think that we would be happy for the GDPR to exist.

Biography

Susan Doe is Director of Compliance & Data Protection – Europe at Sidley Austin LLP. She was a former Director of Information & Research at Sidley Austin and has many years' experience in law libraries. She obtained a law degree from LSE and followed a career in law firm libraries from 1989 onwards, firstly at Nabarro Nathanson, then at Winckworth Sherwood, before moving to the US law firm, Sidley Austin in 1999. Susan moved away from libraries and information and into her current role regarding compliance and data protection in May 2017. She held the position of BIALL Chair in 2004-2005, the first person elected to the post from a US firm.

N.B. The views expressed in this article are the author's own and do not represent the views of Sidley Austin LLP. This article should not be seen as providing legal advice.

https://doi.org/10.1017/S1472669618000178 Published online by Cambridge University Press