The GDPR, Guernsey and the financial sector

November 2017

In the seventh of a series of regulatory columns in Compliance Matters by experts in Guernsey's legal sector, Collas Crill Senior Associate Nin Ritchie considers the effect that the EU's General Data Protection Regulation is going to have on financial firms and the steps that they should think of taking when gearing up for it.

You don't need a lawyer to tell you that the General Data Protection Regulation (GDPR) juggernaut is steadily chuntering towards any organisation who operates or wants to operate in or with the EU, and there is nothing you can do about it other than to be prepared and ready for the impact when it hits on 25 May 2018. On that cheery note, maybe I should stop there, but I won't!

Guernsey is on track to introduce the *Data Protection (Bailiwick of Guernsey) Law 2017* (DPGL) in conjunction with the coming into force of the GDPR. It will do two things. It will make Guernsey an 'equivalent' jurisdiction (being one of only 11 non-EU jurisdictions to have this status); and, in doing so, it will extend GDPR-type obligations to Guernsey organisations regardless of where they are in the world and with whom they chose to do business. The cost of getting it wrong is high and, depending on the seriousness of the mistake, the fine may well be too much for some organisations to bear.

William Mason, the director general of the Guernsey Financial Services Commission (GFSC), told a recent meeting that the GFSC employed interns in the summer to sort through, scan and shred more than five million pages (1,750 archive boxes) to make sure that, by spring next year, it would be complying with the GDPR. I have a few points to make about this. Firstly, what happened to students spending their summer as surf instructors? Secondly (and more importantly), the GFSC will no doubt expect the entities it licenses to follow suit and take their obligations seriously. Thirdly, that volume of documents and data is probably a drop in the ocean compared with the data that some of the regulator's larger globally operating licensees are holding. Mason noted that although the GFSC's clean-up exercise had been a bureaucratic chore (not least for the sun-deprived interns), it would save money on archive space in the long term.

It is that 'bureaucratic chore', the process to get complaint with GDPR/*DPGL*, that compliance teams ought to be focusing on now. That is not a choice – it has to happen – but why should an organisation go through the cost and disruption of such a major overhaul without getting some commercial value from it?

Have no doubt, unless an organisation is in the unique and fortunate position of opening for business with GDRP/*DPGL*-compliant systems and processes on the date when the GDPR/*DPGL* become effective, it will have to make some organisational, technical and legal changes to get up to scratch.

So where is the good news? Many organisations in Guernsey have been operating in a healthy and compliant way for years, maybe even decades. The need to work towards GDPR/*DPGL* compliance presents such firms with a unique opportunity to take stock of the data they hold and have a good peer through the looking glass at (i) how it flows, (ii) where it is stored, (iii) who has access to it, and (iv) how it can be managed more effectively.

Some firms have grown quickly and/or been acquisitive in recent years. The GDPR/*DPGL* might inspire them to consider, as appropriate, whether and how to centralise systems and resources. Now may be the right time on the data mapping journey (if it hasn't happened already) for them to consider how to get the best use out of the data they hold and set up a system to make that operational.

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.

Think about Big Data at its most basic level. For example, if one's firm has a central resource for holding "client due diligence" (CDD) data that streamlines the client take-on process, that only retains what it needs but still helps it assess business risks, set its risk appetite, do its target marketing and even price its products and services.

We must take other considerations into account. In view of recent case law and regulatory developments, here are four points that a financial firm ought to consider when gearing up for GDPR.

Privilege

Decisions in the recent cases of *Re the RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch) (08 December 2016) and *Serious Fraud Office v Eurasian Natural Resources Corporation Ltd* [2017] EWHC 1017 (QB), which have caused a huge stir amongst dispute lawyers, show that data flows and the identities of the people who may have access to data are vexed subjects. These cases focus on privilege, thankfully only something to which organisations need to turn if they find themselves on the unwelcome end of a regulatory or law enforcement investigation or some form of litigation. The documents protected by privilege are those an organisation can hold back from producing to the other side.

The current position (pending the appeal of the SFO in its case) is that legal advice privilege will only cover confidential communications between an organisation's lawyers and people charged with obtaining that legal advice. Communications with anyone else in the organisation, even if they originally had the job of providing the lawyers with the facts and figures they needed to provide their advice, will not be protected by privilege. With that in mind, and in the hope that the organisation never finds itself at the receiving end of such unpleasantries, organisations might think about imposing appropriate checks and balances in line with principles of the GDPR to ensure that the processing of data, including legal advice, is streamlined to be what is necessary and accessible to only its intended recipients.

Trustee disclosure

Turning to the rights of the beneficiaries of trusts to information under the UK's existing data protection regime, the decision in *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74 shows that Guernsey trustees should ensure that information relating to their deliberations and exercise of their discretion (including any legal advice they seek) remains in Guernsey in order to avoid the danger that the information may be disclosable under another jurisdiction's data protection legislation.

That English decision confirmed two important principles:

- that English law firms are not exempt from the scope of the English data protection regime and, when faced with a subject access request, English lawyers must comply with the request by disclosing any personal information they hold that is not privileged; and, arguably more importantly for trustees,
- the question of interplay between the English data protection regime and a beneficiary of a trust's rights to information has been firmly resolved in favour of the statutory entitlement to information created by England's *Data Protection Act 1998*.

Here the laws differ between England and Guernsey. The current Guernsey data protection laws include specific subject access request exemptions that mirror its trust law provisions restricting disclosure, whereas the English regime does not. Therefore, as long as those exist (and fingers crossed the exemption carries over to the DPGL) Guernsey trustees, if advised by their Guernsey lawyers, should be exempt from complying with a beneficiary's subject access request. It is timely for a trustee to use this opportunity to ensure that it is confident in its data flows and, to the extent possible, in order to limit the risk exposing its data to others who have access to it, implement controls to limit sharing beneficiary data with other parties, particularly those outside of Guernsey.

The Common Reporting Standard

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.

The Organisation for Economic Co-operation and Development's CRS is another data protection minefield. Many know that Guernsey as an early CRS 'adopter' was faced with its first reporting deadline on 30 June 2017, with hefty sanctions possible for non-compliance. Guernsey's reporting 'financial institutions' were and are obliged to complete 'due diligence' on reportable persons: a heady task with new data being collected continually as new clients come on board and old clients' circumstances change. Given the tight timeframe for the first reports, many organisations found themselves pulling data together from various sources in order to have something to report. This cannot have been effective in terms of time or money and certainly cannot be the model for future reporting. Each organisation now has to streamline its processes to obey CRS while also adhering to the principles of the GDPR.

The bottom line

William Mason certainly had a point about saving money on archive space; why pay for space to store data that one's organisation simply should not be holding? How can an organisation know what personal data it holds, let alone whether that data is adequate, relevant, limited to what is necessary, accurate and kept up-to-date (or erased or rectified if it is wrong) when it is in a brown box under lock and key in a warehouse offsite? The simple answer is that it can't.

I'm sorry, future interns, your summers may not be as bright as they used to be! I am certain that you will have many more hours of sorting, scanning and shredding to look forward to. I hope you do it in an intelligent way, with streamlined systems capturing personal data that is only being used for the purposes for which it is being processed.

An original version of this article was first published by Compliance Matters, November 2017.

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.

For more information please contact:

Nin Ritchie

Group Partner // Guernsey

t:+44 (0) 1481 734273 // *e:*nin.ritchie@collascrill.com

Michael Adkins

Partner // Guernsey

t:+44 (0) 1481 734 231 // *e:*michael.adkins@collascrill.com

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.