Papers

The impact of the General Data Protection Regulation on the banking sector: Data subjects' rights, conflicts of laws and Brexit

Received: 17th August, 2016

Lori Baker

Until her recent relocation to Dubai, UAE, Lori Baker was a Senior Associate at Fieldfisher LLP in London, in the Privacy, Security and Information team led by Hazel Grant. Her primary areas of focus over the past 11 years have been in Data Protection and Regulatory Compliance and her strengths are in the areas of global/EU data protection, anti-corruption and ethics, IT and telecoms outsourcing, as well as global telecoms regulation and commercial contract negotiation. Lori has been admitted to the bar in two jurisdictions in the US (Pennsylvania (1998) and New Jersey (2002)), and has been a qualified Solicitor of England and Wales since 2012. Her certifications include ISEB certification in data protection and until April 2016 she held a certification as a Certified Compliance and Ethics Professional – International (CCEP-I) with the Society of Corporate Compliance and Ethics. Lori is now based in Dubai and is continuing her work as a Legal and Compliance professional.

Tel: +971 567 901218; E-mail: baker.lori@gmail.com

Abstract The General Data Protection Regulation (GDPR) will undoubtedly have an impact on how businesses manage compliance in the coming years. The banking and finance sector is not immune. It does however already operate in a heavily regulated environment, because the type of personal data banks receive, while not generally fitting the definition of 'sensitive personal data' in the EU, is still highly vulnerable data that could see the data subject becoming a victim of fraud or other financial crime. Between the NIS Directive and the GDPR, what then will be the impact of additional toothy, large-scale regulations requiring databases full of documentation for auditability, transparency and accountability on an industry already (presumably) running a very tight compliance ship? This paper will address:

- the key changes of the GDPR (and for completeness, the NIS);
- what happens when these laws conflict with other applicable regulations;
- other changes in the banking in general, including the end to banking secrecy in light of certain elements of the GDPR around sharing of personal data; and
- the impact Brexit will have in the context of regulating privacy in a non-GDPR environment.

KEYWORDS: banking, GDPR, banking secrecy, NIS Directive, financial crime

INTRODUCTION

Banking as an industry is subject to several strict, documentation-heavy, often cumbersome regulations that seem to keep coming in waves from all jurisdictions around the world. On top of that, outside of the industry regulations, there are general regulations that apply across the board and they are only getting stricter as well.

The General Data Protection Regulation (GDPR), the EU's revised data protection

law that applies to all EU member states, is one such regulation. It may seem fairly innocuous in an industry already flooded with compliance requirements, but this is not necessarily the case.

The GDPR applies to industries in all EU jurisdictions in a uniform, harmonised way (with limited exceptions). It will undoubtedly have an impact on how businesses manage compliance in the coming years. Written very much to strengthen data subjects' rights and the consistency of the direct relationship between the data controller (as in any EU or non-EU business active in the EU market which handles personal data) and the data subject, the GDPR imposes more administrative requirements, as well as more auditability and accountability. In retail banking, and potentially other areas of the banking and finance sector, the biggest impact will be on data subjects' rights and transparency around them. Businesses must step up and fundamentally reform their approach to handling personal data largely as a commodity.

The banking and finance sector is not immune. It does however already operate in a heavily regulated environment, because the type of personal data banks receive, while not generally fitting the definition of 'sensitive personal data' in the EU, is still highly vulnerable data that could see the data subject becoming a victim of fraud or other financial crime. Banks must already submit to scrutiny by several different regulators and supervisors, including:

- the European System of Financial Supervision (ESFS), made up of the European Securities and Markets Authorities (ESMA), the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA), as well as the European Systemic Risk Board (ESRB) and the Joint Committee of the European Supervisory Authorities and the national supervisory authorities;
- individual member state laws and the authorities that implement them; in the UK for example by the Financial Conduct Authority and the Prudential Regulation Authority — both carrying extraordinary powers to scrutinise how banks conduct themselves as a profitable business as well as whether they are behaving ethically and in a compliant manner; and the Financial Ombudsman Service, established by the Financial Services and Markets Act 2000; and
- anti-financial crime and other anti-corruption regulations, forcing banks to obtain and hold extra, sometimes very sensitive data about their customers to demonstrate client suitability and for reporting to fraud and tax evasion prevention authorities.

Note also that the sector is caught by the Network and Information Security Directive (NIS Directive) as banks are considered to be operators of an essential service. Between the NIS Directive and the GDPR, what then will be the impact of additional toothy, large-scale regulations requiring databases full of documentation for auditability, transparency and accountability on an industry already (presumably) running a very tight compliance ship?

This article will address:

- the key changes of the GDPR (and for completeness, the NIS);
- what happens when these laws conflict with other applicable regulations;
- other changes in banking in general, including the end to banking secrecy in light of certain elements of the GDPR around the sharing of personal data; and
- the impact that Brexit will have in the context of regulating privacy in a non-GDPR environment.

KEY CHANGES FROM THE GDPR AND THE NIS

For all businesses that the GDPR affects, the key changes pertain largely to protecting

the rights of data subjects. The GDPR is meant to ensure the availability of easy, understandable information about how a data subject's information is processed; who may have his or her data at any one time; how to access said data; how the data can be amended/destroyed; and how the data can be easily moved around. It has an extremely wide extra-territorial reach, as non-EU businesses offering services or 'targeting' EU citizens are also caught, and must declare an established headquarters entity in Europe for culpability within the EU. Fines under the GDPR can be massive, depending on the severity of the violation. There are more stringent breach notification requirements not only in what needs to be informed to a regulator and even the data subject in certain cases, but with respect to timing as well — 72 hours to report a data breach under the GDPR. The NIS adds to this as it imposes security and network requirements on essential services operators and digital service providers (DSPs), as well as reporting obligations where there is a serious security breach or incident. Security measures and notification requirements include:[1]

- *preventing risks*: technical and organisational measures that are appropriate and proportionate to the risk;
- *ensuring security of network and information systems*: the measures should ensure a level of security of network and information systems appropriate to the risks; and
- *handling incidents*: the measures should prevent and minimise the impact of incidents on the IT systems used to provide the services.

In the banking sector, credit institutions will have to abide by the requirements implemented by the relevant member state under the Directive.

There is overlap between the two, and discussing the merits of either or both laws misses the point. It is worth noting, however, that several key requirements have changed for the banking sector: there is yet another overlay of regulation on the data banks process for customers and clients; the security of IT systems must be thoroughly reviewed and upgraded; breach notification requirements impose a double-whammy effect (and careful contingencies for which one wins must be prepared);[2] and fines under either law could mean a serious impact on the industry's overall bottom line, noting in particular that the banking sector handles such enormous amounts of personal data that its neck may well be first on the block.

WHICH REGULATIONS WIN: GDPR OR FINANCIAL CRIME AND TERRORISM PREVENTION REGULATIONS?

Among other regulations, banks must comply with an array of financial crime, corruption and fraud prevention laws both domestic and international, some of which are in direct contradiction with the principles of the GDPR. Simple compliance checking/due diligence products are a good example of how the laws supporting their existence may conflict and even may lead to further unchecked fraudulent and corrupt activities. On the one hand, laws curbing financial crime require certain disclosures of personal information, including knowledge about one's location, family and other relationships, and often, criminal records information. Banks and financial institutions must comply in order to investigate properly and ultimately provide personal and business loans and mortgages, trade stocks and commodities, or for something as simple as dispensing money to the rightful current or savings account owner.

From another angle, it is clear that financial industry regulators in EU jurisdictions support the use of compliance checking and due diligence products to go towards ensuring the businesses they have authorised are doing the right things, fitting the ethical business profile they expect, and

running a solid, profitable yet fair business that serves consumers properly. Compliance checking and due diligence products contain personal information and the businesses that develop such products are subject to the GDPR as well.

What happens then, when a data subject who is a money launderer requests that his data be altered or fully removed from the product developer's database? In the UK, for example, does a law applicable to the money launderer, the Proceeds of Crime Act 2002 (POCA), win or is the GDPR sufficiently powerful and broad to fully protect *any* data subjects' rights with respect to processing their personal data?

Conflict of laws?

The GDPR touches on these kinds of conflicts in both the recitals and in the main text. Recital 96 and corresponding Article 36(4) on consultation with supervisory authorities, along with Recitals 111 and 112 on international data transfers and finally limitations in Articles 17 and 23 can be helpful in understanding the impact of a conflict of law and the required next steps.

Recital 96 and Article 36(4) explain that where processing of personal data is high-risk, the supervisory authority should be consulted. Member states should check with the supervisory authority when drafting new legislation that would require the processing of personal data to facilitate compliance with the GDPR. It is slightly unclear as to whether this means that each member state should check with the each other's supervisory authority's for these purposes, as the GDPR covers all member states; however, checking with one is presumably tantamount to checking with all, as the regulator's GDPR interpretation should in theory be the same in each member state. The end result is that any new law drafted that could evoke privacy concerns would have addressed to the extent possible those concerns to ensure data subjects are not subject to onerous laws encroaching on their right to privacy. (Cue the UK's soon to be adopted Investigatory Powers Act — perhaps a discussion for another time.)

Recitals 111 and 112 on international data transfers goes further to clarifying whether personal data may be processed abroad for potentially conflicting regulatory purposes. The GDPR sets out derogations that allow for processing of personal data required for procedures before regulatory bodies. Recital 112 explains:

> 'Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport'.[3]

Regarding sensitive personal data, it further states:

> 'In the absence of an adequacy decision, Union or member state law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. member states should notify such provisions to the Commission.'[4]

Article 23(1)(e) and (h) specifically address restrictions on data subjects' rights outlined in Articles 12–22 where requirements of a conflicting member state law or other important objectives of public interest 'of the Union or of a member state' must be considered, including taxation matters such as evasion and secrecy, financial crime, public health and social security.

Finally, according to Article 17, there are exceptions to the rule around 'the right to be forgotten', as this is not an absolute right.

Article 17.3(b) states that the right to be forgotten:

> 'does not apply where the processing is necessary for compliance with a legal obligation which requires processing by Union or member state law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.[5]

Open door to financial crime heaven

In the run-up to the adoption of the GDPR, many in the EU data protection professional community were (and some still are) concerned that the new regulation would be a fraudster's sanctuary.

While not completely explicit in the recitals and articles noted above, there is perhaps enough information in these GDPR references to argue that at least Union or member state interests, when in conflict with GDPR, should be measured against and where necessary prevail in order to prevent financial crime or to enhance public safety and welfare. A data controller such as a bank will in any case have to prepare a very solid playbook for reacting to requests such as the right to erasure where doing so would create a huge gap capable of being filled with fraudulent and possibly other criminal activity, so the money launderer in the example above does not get away with money laundering under the POCA, or even funding of terrorism with laundered money.

Reflecting on the recitals and articles noted above, banks and the financial sector will also have to consider how best to approach and document a process for legitimising international data transfers where, for example, the Foreign Corrupt Practices Act 1977 or other international fraud prevention law comes into play. It is well known how the PATRIOT Act 2001, a US law principally aimed at preventing terrorism, has affected international data transfers currently, in that the EU generally is reluctant to transfer personal data to the USA due to the reach and perceived invasiveness of the PATRIOT Act. Safe Harbor collapsed in part because of perceptions of the PATRIOT Act (rightly or wrongly). Again, banks must engage in thoughtful consideration and well-defined procedures for responding to requests from persons who, by expunging or altering their data upon their request, would wreak havoc in a variety of ways should they be able to hide behind conflicting laws meant to protect and enhance the rights of the general public, bearing in mind that it is the general public the laws are written to protect rather than the criminals seeking to take advantage of them.

Returning to the example of compliance-checking products and information, what further obligations will the credit reference agency/product developer have to inform the bank, its customer, about the removal of the data, or otherwise, how trustworthy would the data in the compliance product be if the data must ultimately be removed? Article 19 of the GDPR instructs that where any changes, updates or removals occur under Articles 16, 17 and 18, the data controller has an obligation to inform all recipients of the personal data unless it would be overly burdensome or impossible to do so, both terms being somewhat subjective. The data subject also has a right to know who the recipients are should he or she request such information.[6]

Where to find the data

Overall, it is critical for businesses, especially banks, not only to determine their compliance position as above, but in line with the Article 19 obligations, they must understand — and document — the information providers in the supply chain. They must also tend to a comprehensive understanding of all resulting data flows and what data will be available in said

flows, as well as any rights or requirements applicable to them in sharing information altered or removing personal information appropriately. The availability of data going forward may be lacking for the reasons outlined above, at least temporarily until a suitable response is coordinated, and business must go on. Slowdowns and lack of data protection compliance knowhow in the supply chain could cost banks and other businesses working with them a great deal of time, resources and money, which may yet be felt in the economy generally. It is also especially important to know all suppliers and choose wisely — their compliance sophistication and approach is as important as any other piece of this puzzle.

END OF BANKING SECRECY/ INCREASED DATA PROTECTION: WHAT IS THE DIFFERENCE?

Another area of interest in the changing data protection law and how it works (or not) with other EU principles, therefore affecting the banking industry, is the end of banking secrecy in order to prevent tax evasion. As banking secrecy comes to an end, and clients' personal data become more readily available as a result, the GDPR has been adopted and is due to be implemented. One means more unencumbered access to personal data, and possibly more data on the third-party market and available especially to regulators, and the other means less data potentially available without consent or some other tenable reason for processing the personal data without consent. What really then is the difference between the two concepts, and does anything under GDPR really slow the progress and compliance of banks cooperating with banking transparency efforts?

Banking secrecy developed following a public scandal in France regarding prominent public figures called out for hiding their money outside of France, primarily Switzerland.[7] Swiss bank secrecy is based on a statutory right to privacy that significantly limits sharing of personal and banking information with anyone, including tax authorities and foreign governments except generally where severe crimes such as terrorism or tax fraud may be involved and then the information could only be shared under court order. Incidentally, Swiss bank secrecy is the forerunner of pseudonymisation, requiring replacement of the account holder's name and other private information with numbers.

Switzerland distinguished between tax fraud and tax evasion, which, combined with secrecy laws, created a haven for anyone interested in hiding income from tax authorities. With changing times, though, the international regulatory and political community eventually pressured the Swiss government into updating bank secrecy laws. In March 2009, the Swiss government stated that it will no longer distinguish between tax fraud and tax evasion in dealings with foreign clients. There was also pressure to end banking secrecy to prevent terrorism, as Swiss bank accounts were one of the key places terrorist groups and individuals hid their funding. This allowed US laws like the PATRIOT Act, as discussed above, as well as the Foreign Account Tax Compliance Act (FATCA 2010) to be as highly effective as they are controversial with respect to privacy concerns.

FATCA is currently one of the most widely known tax fraud and evasion prevention regulations. Its main purpose is to reclaim foreign funds hidden in offshore accounts that should have been subject to income and potentially other taxes. EU countries attempted the same with their own individual member state laws. Under such laws, personal information may be shared with the relevant tax authorities at home and abroad.

Are they not the same thing?

Turning back to data protection, banking secrecy, with its inherent right to privacy,

has a lot of similarities. Some may therefore ask why it is ending at such a time that data protection compliance is to become even more necessary and enforceable. The answer appears to be that while the GDPR as is geared toward enhancing data subjects' rights, as a data subject, if current guidance is any indicator, there is very little room to object to a bank or other relevant financial institution sharing personal data either within the member state or internationally as required under applicable banking transparency related laws.

Just as GDPR negotiations were concluding and a final draft text was ready in December 2015, the Article 29 Working Party clarified the necessity of compliance with banking secrecy laws and explained a basis for processing personal data in accordance with them that does not contradict or impair the enhancements in data protection.

The Article 29 Working Party Paper 234 175/16/EN, entitled 'Guidelines for member states on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes',[8] while pertinent to the EU Directive 95/46/EC (the Directive), elaborates on the importance of sharing data for the prevention of tax evasion and fraud, leading governments to create the laws described above as 'information exchange tools'. The paper states that there are comparative conditions applicable to intra-EU transfers of personal data and transfers to third countries with data protection adequacy findings. However, none of the Directive's Article 26 derogations would legitimise the international transfer of personal data to the USA. The Article 29 Working Party has suggested instead that Article 7(e) of the Directive applies to legitimise the processing of personal banking data for taxation purposes. It states:

> 'member states shall provide that personal data may be processed only if:
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.'[9]

The Article 29 Working Party has further suggested that certain safeguards must be in place to ensure that personal data are protected adequately in these circumstances. One such proposed safeguard is to ensure a firm legal basis for such processing is in place:

> '*Legal basis*
>
> The exchange of personal data shall be regulated by a clear legal basis, whether a legislative act or an international agreement. It is essential that any law or agreement is accessible by citizens and foreseeable in its application, in accordance with the requirements of Article 8 ECHR. Such instruments shall contain substantive provisions that implement (and not just merely refer to) the Directive and/or the national data protection law that implement it. It is also important that national procedures, providing for the involvement of respective Parliaments — and eventually DPAs — are fully respected in order to create a democratic, clear and foreseeable legal basis.'[8]

Thus, EU member states and the USA have in place tax treaties, an example of which is the UK–US Automatic Exchange of Information Agreement and corresponding regulations and guidance notes. The Article 29 Working Party Paper 234, along with other similar guidance, renders data protection enhancements in this specific area all but moot to a degree, provided its recommendations on safeguards such as a sound legal basis and adherence to data protection principles including purpose limitation, necessity, retention, transparency and onward transfers are respected and employed.

The GDPR impact for banks and financial institutions is successful, structured implementation of these safeguards, especially in making the transition from the similar areas of banking secrecy (and its demise) and enhanced data protection.

BREXIT

London is a centre for banking and finance. Brexit threatens London's position in this regard, and on top of it, the UK will have its own privacy regulations that, if incompatible with GDPR, will impact the industry even further. If the UK is leaving the EU, one might question why it is worth worrying about the impact of the GDPR on banking and finance at all. It may be concluded, however, that precisely *because* of Brexit, the sector's preparations for the impact of the GDPR will be just as important for the following, non-exhaustive list of reasons:

- The GDPR is current law — it is good law *now*, so UK businesses should be aiming to comply with it.
- Nobody knows exactly what the future of UK data protection law will look like, but it is probably going to be the GDPR (or the UK equivalent), at least to allow the free flow of data between the EU and UK (and globally).
- Organisations must have implemented the GDPR by 2018, so unless there is complete legislative departure from the EU before then, GDPR will apply until Brexit actually happens. Theresa May, the present UK Prime Minister, has made it clear to her EU counterparts that she is not interested in discussing Article 50 of the Lisbon Treaty, with respect to triggering EU exiting proceedings, until early 2017.[10] Furthermore, Article 50 procedures themselves will take up to two years to complete.
- If a bank or other financial institution has EU operations, the whole organisation will need to comply anyway. It is therefore highly important to comply in the UK.
- Linked to EU operations, the GDPR has an element of extra-territoriality such that any UK entity products aimed at EU citizens require compliance with the GDPR.

In short, it appears there that while Britain has voted to leave the EU, there is no escaping the GDPR. As above, banks and financial institutions will have to prepare accordingly.

CONCLUSION

The GDPR is but one of many regulations that banks and the finance sector must abide by, but at least banking is not in the boat alone. In some cases, the GDPR is entirely compatible with other regulations, and in others, it creates at best uncertainty that while resolvable, if unprepared will cost businesses, including banks, lost profits and potentially reputational damage, among other possible pitfalls. Banks and those in the finance business will have to spend significant time sorting out how best to manage fraud prevention and financial crime regulatory compliance against compliance with GDPR. Many pundits have asserted that banks' necks will be first on the block for investigation into compliance or lack thereof. As nearly every business in any industry must rely on banking and finance sector businesses, banks can respond by supporting a strong, clear compliance position, considering well in advance the potential pitfalls such as consistency with requirements under other laws. The players with the sophisticated, insightful approach will save themselves and their customers a lot of hassle, while succeeding in an otherwise rocky regulatory terrain that is only getting bumpier.

ACKNOWLEDGEMENT

Thank you to Hazel Grant, Partner, Fieldfisher LLP for her kind assistance with this paper.

References

1. Scanlon, L. (2016) 'The Network and Information Security Directive — who is in and who is out?', *The Register*. Available at: https://www.theregister.co.uk/2016/01/07/the_network_and_information_security_directive_who_is_in_and_who_is_out/ (accessed July/August, 2016).
2. European Commission (2016) 'Directive on Security of Network and Information Systems', available at: http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm (accessed 2nd January, 2017).

3. European Commission (2016) 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)', *Official Journal of the European Union*, Vol. 59. Available at: http://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed July/August, 2016).
4. *Ibid*.
5. *Ibid*.
6. *Ibid*.
7. Komisar, L. (2003) 'Offshore banking, the secret threat to America', *Dissent Magazine*, Spring. Available at: http://www.thekomisarscoop.com/2003/04/offshore-banking-the-secret-threat-to-america/ (accessed July/August, 2016).
8. Article 29 Working Party (2015) 'Guidelines for member states on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes', (175/16/EN). Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp234_en.pdf (accessed July/August, 2016).
9. *Ibid*.
10. Mason, R. and Oltermann, P. (2016) 'Angela Merkel backs Theresa May's plan not to trigger Brexit this year', *Guardian*, 20th July. Available at: https://www.theguardian.com/politics/2016/jul/20/angela-merkel-backs-theresa-mays-plan-not-to-trigger-brexit-this-year (accessed July/August, 2016).