Data Protection and Privacy

By Ryan Pinder, Partner, Graham Thompson

Introduction

The issue of financial privacy and data protection is always in the headlines, and in the financial services practice, something of significant importance. International regulatory standards have evolved to change almost on what seems to be a daily basis that have eroded the financial privacy for clients. Starting from FATCA, CRS, Beneficial Ownership Registries, and matters related to Economic Substance and spontaneous information exchange. Clients have rightfully expressed concern, concern over their safety, commercial viability and fear for victimization.

On top of this, many countries have Data Protection Acts in place in which we as practitioners have to navigate what seem to be conflicting rules. For example, in the face of the assault on client financial privacy, European countries have initiated penal privacy laws such as The EU General Data Protection Regulation (GDPR). We as practitioners are now the ones with the exposure for not complying with client financial transparency regimes, with not complying with our home country data protection laws, and ultimately not complying with other country data protection laws, such as GDPR. We will touch on these issues today and end with some risk mitigation initiatives that we as practitioners should be considering.

Erosion of Client Financial Privacy

We have witnessed a multi-faceted strategy of regulatory and compliance reforms designed to institutionalize the demise of fiscal transparency, not only in the individual private client market, but also in the corporate structuring market. CRS and FATCA as we all know dismantled the value proposition of our region, financial privacy. CRS and FATCA imposed fiscal transparency for individuals by creating a new standard of automatic exchange of fiscal information. Unlike the CRS and the harmful tax practices initiatives of the past, BEPS has a focus not necessarily on the private client, but on the multinational commercial organization. This has imposed an entirely new framework for tax enforcement and fiscal transparency.

These initiatives have added complexity to Governments, private sector and even those

countries that are imposing these measures to combat, from their prospective, tax avoidance and tax evasion. These initiatives not only are obtaining the underlying goal of the major economies, increased fiscal transparency, but are also imposing cost and complexity of compliance that has the ability to force the private sector participants to retrench and consolidate, but also systematically dismantle the financial service industry as we know it for small, island based IFCs.

These tax initiatives have also eliminated the historical value proposition of IFCs such as The Bahamas and other regional IFCs, fiscal transparency and confidentiality. This is particularly important in markets such as throughout Latin America and other countries where citizen intimidation and victimization is the order of the day, removing a market for us that in all reality requires our services for their self-preservation.

We as countries have adjusted to the implementation of fiscal transparency and automatic exchange of information, but as a result, we have all seen the business in our region suffer from it. We have seen deposits and capital leave the jurisdiction, whether going back on shore, or to the United States. We have witnessed client structures being collapsed and simplified. We have witnessed compliance costs continue to climb through the roof in the private sector just to remain competitive. Fiscal transparency has been a difficult adjustment, one we have all paid the price for.

International Data Protection Initiatives

It is often said that data is the new oil. Many countries have either revamped their local data protection laws or created entirely new legislation to keep up with the influx of data that is collected from individuals. We will continue to see increased data governance and a push for data sovereignty in the coming decade as data on the individual or citizen becomes even more valuable. The transfer and storage of data between multiple jurisdictions will, undoubtedly, bring about conflicts of law that have yet to be addressed as some governments have enacted laws that apply extraterritorially. In this regard, the United States now has the CLOUD Act, a federal law that essentially allows US federal law enforcement agencies to view data held on servers inside or outside the US provided they have a warrant to do so and the tech company is based in the United States. China has the China Internet Security Law which came into effect in 2017 which grants the government large access rights to data held within China and includes onsite and remote inspections of computer networks. India and Brazil are expected to enact new legislation next year that will require data to be stored locally in data centers before it can be transferred outside the jurisdiction.

Of all the new data protection laws, however, the EU General Data Protection Regulation (commonly known as the GDPR) is the most groundbreaking. The GDPR came into effect in May 2018 and since its implementation we have seen that it has been a game-changer in the way we view individual cyber- and data-rights.

There are several Articles within the GDPR that may have the greatest potential impact on security operations going forward. Some of them include:-

Articles 23 &30- which requires companies to implement reasonable data protection measures to protect consumers' personal data and privacy against loss or exposure.

Articles 33 & 33a- which requires companies to perform data protection impact assessments to identify risk to consumer data and Data Protection Compliance Reviews to ensure those risks are addressed.

Article 35- requires that certain companies appoint data protection officers. This mirrors the need for financial institutions to appoint anti-money laundering and compliance offers.

Article 45- extends data protection requirements to international companies that collect or process EU citizen's personal data, subjecting them to the same requirements and penalties as EU based companies.

To sum it all up, this means that at the core of GDPR, EU citizens (as data subjects) enjoy:

- The right to be informed in the event of a data breach within 72 hours of the breach;
- Right of access to copies of one's data profile once a written request is submitted;
- Right of rectification if one's data is incorrect or insufficient;
- Right to erasure (aka the right to be forgotten) if one requests that their data be deleted;
- Right to restriction of processing of one's data;
- Right to data portability (meaning data subjects can reuse a data set between multiple companies if desired);
- Right to object to data processing under certain conditions; and,
- Rights in relation to automated decision making and profiling.

The GDPR emphasizes the need for consent on behalf of the data subject and demands transparency from data processors and controllers in the way that data is collected, stored and used. The fines for non-compliance are severe – up to 20 million Euros or up to 4% of total global annual turnover. In July of this year the UK's Information Commissioner's Office (ICO) (the UK's data protection authority) fined British Airways a record £183m for a major data leak. Last year the ICO also handed down an enforcement notice to a Canadian-based data company for collecting the data of British citizens, without their consent or knowledge, in order to assist in the targeting of ads for the Vote-Leave campaign for Brexit. That company eventually complied with the notice and had to erase all of the data that was held by individuals in the UK. Thus, it can be seen that the GDPR has serious bite when it comes to protecting individual data rights within and outside of the EU.

Bahamas Data Protection Act

The Bahamas has The Data Protection Act that sets forth the regulatory regime for the protection of individual data and establishes a Data Protection Commission as the operative agency to regulate. Before we outline the framework for data protection under the Act, it is important to understand certain key terms:

Data Subject is an individual who is the subject of personal data.

Data Controller is a person who, either alone or with others, determines the purpose for which, and the manner in which any personal data are, or are to be, processed.

Data Processor is a person who processes personal information on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his/her employment.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

It is the Data Controller who has the obligation to abide by the requirements of the Act with respect to information of the Data Subject. Generally, there are 8 rules that the Data Controller must follow:

1. Personal data must be collected by means which are lawful and fair.
2. The data must be accurate and, where necessary, kept up to date (except in the case of back-up data).
3. The data shall be kept only for one or more specified and lawful purposes.
4. The data shall not be used or disclosed in any manner incompatible with that purpose or purposes.
5. The data shall be adequate, relevant and not excessive in relation to that purpose or purposes.
6. The data shall not be kept for longer than is necessary, (exceptions - historical, statistical, or research purposes).
7. The data shall be kept secure to avoid unauthorized or unlawful use, accidental loss or damage.
8. The data must not be transferred to another country unless that country has an adequate level of protection.

1. Collect and process information fairly

To fairly obtain data the data subject must, at the time the personal data is being collected, be made aware of:

- the identity of the data controller
- the purpose in collecting the data, and
- the persons or categories of persons to whom the data may be disclosed
- any other information which is necessary so that processing may be fair.

To fairly process personal data, it must have been fairly obtained, and:

- the data subject must have given consent to the processing or
- the processing must be necessary for one of the enumerated reasons in the Act.

2. Keep it accurate, complete and up-to-date

To comply with this rule, you should ensure that:

- your clerical and computer procedures are adequate to ensure high levels of data accuracy.
- the general requirements to keep personal data up-to-date has been fully examined
- appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.

3. Keep it only for one or more specified, explicit and lawful purposes

You may only keep data for a purpose(s) that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with the purpose. An individual has a right to question the purpose for which you hold his/her data and you must be able to identify that purpose.

To comply with this rule:

- in general, the persons whose data you collect should know the reason (s) why you collect and keep it
- the purpose for which you collect and keep the data should be a lawful one
- you should be aware of the different sets of data which you keep and specific purpose of each

4. Use and disclose it only in ways compatible with these purposes

Any use or disclosure must be necessary for the purpose (s) or compatible with the purpose (s) for which you collect and keep the data. You should ask whether the data subject would be surprised to learn that a particular use of a disclosure is taking place.

A key test of compatibility is:

- do you use the data only in ways consistent with the purpose (s) fir which they were obtained?
- do you disclose the data only in ways consistent with that purpose (s)?

5. Ensure that it is adequate, relevant and not excessive

You can fulfill this requirement if you make sure you are keeping only the minimum amount of personal data which you need to keep, to achieve your specified purpose (s). You should set down specific criteria to judge what is adequate, relevant, and not excessive and apply those criteria to each information item and the purpose (s) for which it is held.

To comply with this rule, you should ensure that the information held is:

- adequate in relation to the purpose (s) for which you keep it
- relevant in relation to the purpose (s) for which you keep it
- not excessive in relation to the purpose (s) for which you keep it.

6. Retain it for no longer than is necessary for the purpose or purposes. (Exceptions include data kept for historical, statistical, or research purposes).

This requirement places a responsibility of data controllers to be clear about the length of time data will be kept and the reason why the information is being retained. You should assign specific responsibility for ensuring that files are regularly purged and that personal information is not retained any longer than necessary.

To comply with this rule, you should have:

- a defined policy on retention periods for all items of personal data kept
- management, clerical and computer procedures in place to implement such a policy.

7. Keep it safe and secure

Appropriate security measures must be taken against unauthorized access to, or alteration,

disclosure or destruction of, the data and against their accidental loss or destruction. The security of personal information is all important, but the key word here is appropriate, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorized disclosure. High standards of security are, nevertheless, essential for all personal information. The nature of security used may take in to account what is available, the cost of implementation and the sensitivity of the data in question.

8. Give a copy of his/her personal data to that individual, on request

On making an access request any individual, about whom you keep personal data, is entitled to:

- a copy of the data you are keeping about him/her
- know your purpose/s for processing his/her data
- know the identity of those to whom you disclose the data
- know the source of the data, unless it is contrary to public interest
- know the logic involved in automated decisions
- a copy of any data held in the form of opinions, except where such opinions were given in confidence.

It is important that you have clear co-ordinated procedures in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is being made.

Every individual about whom a data controller keeps personal information has a number of other rights under the Act, in addition to the Right of Access. These include the right to have any inaccurate information rectified or erased, to have personal data taken off a direct marketing or direct mailing list and the right to complain to the Data Protection Commissioner.

Transferring personal data abroad

An area of concern for many data controllers are the requirements necessary for the transfer of data abroad, especially as more and more legislative and regulatory obligations surround the automatic exchange of information, and even the lawful request for information. This also extends to situations in which Group entities seek to share information with other members of the Group worldwide.

Countries need to ensure that our data protection laws are consistent with internationally recognized principles established by the council of Europe, The European Union (EU), The OECD and the United Nations, although these seem to be ever changing. Generally, to be compliant in transferring data abroad, at least one of the following conditions must be met in that the transfer is:

- consented to by the data subject
- required or authorized under an enactment, convention or other instrument imposing an international obligation on the Country
- necessary for the purpose of obtaining legal advice
- necessary to urgently prevent injury or damage to the health of a data subject
- part of the personal data held on a public register

The management of a Data Subject's data is complex, especially in the cross-boarder environment of financial services. Practitioners have to be careful and comprehensive in their management of client's data and ensure that they are adequately protected and have the appropriate authority if the data has to be shared or transferred. In an era where international exchange obligations continue to grow, complying with data protection laws becomes more and more difficult.

Conclusion

Practitioners have to be very aware and careful on how they treat client data. They also have to be very diligent on how they comply with international obligations. Meshing the two responsibilities at times can seem like an impossibility.

In my experience, when onboarding clients, and managing their personal data, your terms and conditions for client accounts should always speak to how you and your institution will deal with client data. When advising clients, I always incorporate specific client consents on the sharing of data. These terms and conditions can speak to consenting to international obligations of sharing client personal data, and can speak to the ability to share client data among the Group. But to not have specific terms and conditions that address these issues is dangerous, and can result in unintended consequences and potential liability.

It is also helpful to have the conversation with client regarding the erosion of personal financial privacy and how their consent is intended to work with the obligations to share information. We are in a new world order and clients need to understand the obligations that we have as service providers in this ever-changing industry of financial services.

This speech, Data Protection and Privacy, was presented by Ryan Pinder on October 9, 2019, at the 8th Annual Anti-Money Laundering / Counter-Financing of Terrorism Conference, hosted by the Jamaica Bankers Association (JBA) and the Jamaica Institute of Financial Services (JIFS) at the Jamaica Pegasus Hotel, Kingston, Jamaica.

L. Ryan Pinder
Partner

GrahamThompson
T: +1-242-322-4130
Email: lrp@gtclaw.com

About the Author

Ryan Pinder is a partner in the law firm of GrahamThompson and member of the firm's Financial Services, Private Client, Trusts and Estates practice group. His private client practice includes representation of high net worth individuals and families with international and domestic planning and structuring, estate planning and wealth management solutions; and advice in the area of trusts, investment funds and securities law and expertise in bespoke financial services solutions.

His institutional practice includes representation of businesses in commercial transactions, structuring and reorganizations, and compliance with Bahamian regulatory obligations and licensing. Ryan has acted for foreign investors in The Bahamas in all elements of regulatory approvals and obligations; and has coordinated regulatory licensing and compliance for global financial services firms looking to do business from within The Bahamas.

A former Minister of Financial Services and Trade in The Bahamas Government (2012 – 2015), he played an integral role in positioning the Bahamas as a leading financial services centre. Ryan is President of the Bahamas Institute of Financial Services (BIFS).