The fight against tax avoidance and other financial crimes *vs* the right of data protection

A regulatory tug-of-war for Financial Services?

How an increasingly transparent regulatory landscape favoring the prevention of financial crime and exchange of tax information interacts with, and at times conflicts with, GDPR and the public view of the need for increased personal data protection

April 2020

pwc

1. Executive Summary

Introduction

When we hear the phrase "GDPR" we usually think of either our social media privacy (need to check those settings) or those annoying "Please agree to share your information with us" popups we now have to agree to every time we visit nearly any website. But what about our financial data privacy? Do most of us consider what our banks and other financial business partners are doing with our information when we do business with them? While much of the public appears to understand their rights under the General Data Protection Regulation ("**GDPR**") with regards to their social media presence (thanks to Cambridge Analytica and other scandals) there is more bubbling under the surface with regards to individual rights under GDPR and their relationship with the financial services industry. Of particular interest for this paper is where the individual rights under GDPR may at times conflict with the regulatory requirements imposed on the financial services industry.

In the last decade the European Union ("**EU**"), the Organization for Economic Cooperation and Development ("**OECD**"), and the United States ("**US**") have empowered tax administrations and other government units to improve tax compliance, fight tax evasion, and tackle certain financial crimes through new regulations/directives which are aimed at a global sharing of tax information and combating money laundering. Concurrently the exponential rise in new digital technologies continued finding innovative ways to improve our lives. However, as the EU data protection framework could not keep up, it was proposed that a new regime was necessary to cope with the digital revolution. Now GDPR systematizes individual rights and establishes the fundamental '*right to data protection*'[1]. This paper explores the rights of EU individuals in respect to EU anti-money laundering and tax transparency regulations. It thereby proposes a metaphorical tug-of-war that the financial services industry faces, highlighting topics of discussion and risk for regulatory compliance program owners to explore with their legal department while monitoring or adjusting these programs. GDPR means that customers are asking more questions, and with the next big viral news story always looming on the horizon financial services organizations are going to need more answers.

Bigger Trend - Increased Transparency

Following a push by the G20 in 2009 when the global economy was suffering the effects of the global financial crisis and in the wake of revelations such as the UBS tax evasion scandal, the Lux Leaks, and the Panama Papers, the world has seen increased public scrutiny and new compliance requirements from a number of tax and regulatory reforms to counter tax evasion and money laundering. As a result, the number of Tax Information Exchange Agreements ("**TIEA**") in place around the world increased significantly in order to boost tax transparency.

In 2010, the US enacted the Foreign Account Tax Compliance Act ("**FATCA**") with the objective to combat tax evasion by US citizens and residents with undeclared offshore financial accounts. In doing so, the US sought to enhance information exchange between tax authorities. FATCA also acted as a catalyst for the Common Reporting Standard ("**CRS**"), which was introduced by the OECD in 2014, with the objective to disclose financial account balances and income earned by individuals and entities outside of their country of tax residence by mandating an automatic exchange of financial account information between tax authorities in reportable jurisdictions.[2] FATCA and CRS are collectively referred to as the Automatic Exchange of Information ("**AEoI**").

In 2015, the EU adopted the 4th Anti-Money Laundering Directive ("**AMLD4**") to strengthen transparency rules in the financial system to tackle terrorism financing and money laundering. However, the scandal surrounding the Panama Papers and the financing of terrorist groups involved in the terrorist attacks in Paris and Brussels in 2016 and 2017, respectively, has led to amendments, which are part of the EU Commission's "Action Plan for strengthening the fight against terrorist financing". The new Directive issued in 2018 is the fifth revision of the EU anti-money laundering law and is generally referred to as the 5th Anti-Money Laundering Directive ("**AMLD5**"). AMLD5 is not a comprehensive overhaul of the existing legislative framework but rather an amendment of AMLD4 to better counter the financing of terrorism and to ensure increased transparency of financial transactions.

1 General Data Protection Regulation (EU) 2016/679, Article 17

2 A Reportable Jurisdiction is defined as a jurisdiction with which an agreement on Automatic Exchange under CRS is in place.

In doing so, it increased transparency on company ownership by improving the accuracy of Ultimate Beneficial Owner ("**UBO**") registers, which require that financial institutions obtain, validate and store more personal information about their customers. Certain other OECD jurisdictions continue recent implementations of UBO registers to align themselves with the goals of the Global Forum [3] (e.g. the UK Crown Dependencies and Overseas Territories, such as the British Virgin Islands, Bermuda and the Cayman Islands).

In order to prevent the financial services industry from being exploited as a means of laundering money and committing financial crimes, the tax transparency identification rules under CRS are linked – via the 2012 Financial Action Task Force ("**FATF**") Recommendations – to AML and counter financing of terrorism ("**CFT**") regulations, including Know Your Customer ("**KYC**") requirements. Due to the implementation of AML and CFT requirements, the tax transparency rules also apply to related parties. For example, the identification and disclosure of a natural person, who holds the position of senior managing official of a certain type of entity is impacted.[4] In addition, the release of the Panama Papers in April 2016 added some further sense of urgency to tighten tax transparency requirements to align them to stricter local AML and CFT regulations. This can be seen in the Cayman Islands, which reduced the ownership threshold for Controlling Persons under CRS from 25% down to 10% as of December 2017.[5]

Furthermore, the continued development of international trade and multinational corporations ("**MNCs**") has increased the need to scrutinize relief from double taxation. Many countries sign Double Tax Agreements ("**DTA**") with each other to address the issue of double taxation. In practice, this has led to a world where investments may be channeled through 'special purpose vehicles' set up in convenient jurisdictions to take advantage of 'treaty shopping', which helps them to structure low-tax pathways through the international tax system. This practice can result in the undesirable outcome that income is not being taxed in any jurisdiction. In order to combat this, local tax authorities are increasing their efforts to seek documentation of underlying ownership on entities that are seeking withholding tax relief at source or tax reclaims in order to demonstrate that the entire structure is truly eligible for deductions from statutory tax rates. The financial services industry generally has a duty to their customers to seek the best return on investment which will involve taking the necessary measures to minimize withholding tax leakage where allowed by law.

Though not a primary focus of this paper, there are emerging players in the tug-of-war that will have significant impact on regulatory compliance programs in the coming months and years as clarity is sought and received by the financial services industry. Continuing demands by the public for privacy has contributed to increased demand for cryptocurrencies. While some tax authorities have issued views as to the treatment of virtual currencies under the regulations discussed in this paper, many are taking a 'wait and see approach' and will follow suit with guidance from financial regulatory bodies. The emergence of new rules on mandatory disclosure and exchange of cross-border tax arrangements such as the DAC6 Directive[6] will lead to exponentially more personal data being collected and stored by local tax authorities trying to crack down on tax avoidance or abuse of direct taxes. There are many unknowns and uncertainties with DAC6 given that the drafting of primary legislation is still underway in many EU Member State and the financial services industry is still assessing the impacts in those EU Member States that have issued their primary legislation.

3 The Global Forum on Tax Transparency and Exchange of Information for Tax Purposes, founded in 2000 and restructured in September 2009, consists of OECD countries and other jurisdictions that agreed to implement tax related transparency and information exchange

4 In cases, where no natural person(s) directly or indirectly holds a certain percentage of ownership, which exceeds aspecified threshold

5 Cayman Islands Anti-Money Laundering Regulations, 2017, Section 2(1)(a)

6 Council Directive (EU) 2018/822 of May 25, 2018

Summary
There is a global regulatory trend towards transparency to counter tax evasion and money laundering. However, GDPR, and the increased public demand for privacy goes opposite to this trend. Recent scandals, such as the Cambridge Analytica breach in March 2018, have led to increased public scrutiny and a public debate as to whether protection of personal data is more important than tax and financial crime transparency. Though not legally binding, the July 2018 European Parliament resolution on the adverse effects of FATCA[7] suggests a political desire to bring balance to the tug-of-war. GDPR has resulted in increased restrictions on which data financial institutions may obtain, store, process, and grant access to. This presents significant challenges for the financial services industry explored in this paper. GDPR not only places restrictions on how, when and why personal data can be collected, processed and used, but also broadens the definition of personal data, bringing all information collected under the AML/CFT and tax transparency regulations within the jurisdiction of GDPR. Non-compliance by financial institutions under GDPR can attract penalties of up to 4% of annual worldwide turnover or €20 million, whichever is greater. These financial penalties are in addition to potential reputational damage and loss of future business. In addition to privacy concerns, increasing trends towards regulatory transparency result in burdensome and delayed account opening procedures for customers. It is therefore important that the right balance is found.

$20m

Penalty for non-compliance under GDPR or,

4%

of annual worldwide turnover, whichever is greater.

"Annually, we lose billions of euros to money laundering, terrorism financing, tax evasion and avoidance - money that should go to fund our hospitals, schools and infrastructure. With this new legislation, we introduce tougher measures, widening the duty of financial entities to undertake customer due diligence."

Judith Sargentini, Member of the European Parliament

7 5 July 2018 European Parliament resolution 2018/2646(RSP) on "adverse effects of the US Foreign Account Tax Compliance Act

Table of contents:

2. Key Abbreviations

AEoI	Automatic Exchange of Information
AMLD	Anti-Money Laundering Directive
CFT	Counter Financing of Terrorism
CRS	Common Reporting Standard
DAC	EU Directive on Administrative Cooperation
DPA	Data Protection Authority
DTA	Double Tax Agreement
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FFI	Foreign Financial Institution (non-US)
FI	Financial Institution
GDPR	EU General Data Protection Regulation
IRS	Internal Revenue Service
KYC	Know Your Customer
OECD	Organisation for Economic Cooperation and Development
QI	Qualified Intermediary
TIEA	Tax Information Exchange Agreements
UBO	Ultimate Beneficial Owner

3. GDPR - High Level Impact Assessment

Overview

On May 25, 2018, GDPR[8] came into force. It is the biggest change in data protection for 20 years – revolutionizing the way that personal data are used and handled. This presents significant challenges for the financial services industry as controllers and processors of personal data need to adhere to the regulation in order to be compliant. With penalties of up to €20 million, or 4% of worldwide annual turnover of the preceding year,[9] and the opportunity for individuals (data subjects) to sue, data protection and its scope will now become increasingly important - making it a topic at board meetings in the coming years.

After four years of tough negotiations and several draft versions of the GDPR framework, the EU Parliament finally approved it on April 14, 2016. GDPR repealed the pre-existing EU Data Protection Directive[10] and has been described as the "most groundbreaking piece of EU legislation in the digital era", making businesses more accountable for data privacy compliance. It also offers individuals extra rights and more control over their personal data by recognizing that the ownership of data resides with the individual and not with the controllers and processors of personal data.

GDPR contains legal binding rules and must be applied in its entirety across the 28 EU Member States[11]. Unlike a directive, it does not require national governments to pass any enabling legislation, making it directly pertinent and requisite. Thus, GDPR can eliminate inconsistencies in how the data protection law is applied in EU Member States. The introduction of new rights for individuals, such as the '*right to be forgotten*' and the '*right to portability*', as well as the introduction of mandatory breach notification (within 72 hours), are increasing the regulatory burden for financial institutions.

From a jurisdiction perspective, it introduced a lead EU regulator for MNCs in their 'main place' of establishment. There is also an extension of scope of EU data protection rules, applying them not only to controllers established within the EU, but also to non-EU controllers and processors, if that processing relates to offering services or goods to EU citizens and the monitoring of behavior, which takes place within the EU.

Impact on Financial Institutions

Financial institutions[12] have an enormous obligation to protect their customers' data privacy rights while at the same time complying with AML/CFT and tax transparency regulations. As a result, GDPR has a significant impact on financial institutions and service providers to the financial services industry, where billions of financial records and personal data are handled on a daily basis for various activities, such as customer onboarding, relationship management, transaction processing, etc. A reliable risk management approach is therefore critical. Impacted key areas include:

8 See Appendix 1.1 for further background on GDPR

9 In comparison, fines for breaches under the United Kingdom ("UK") Data Protection Act 1998 are capped at £500,000

10 Directive 95/46/EC of the EU Parliament and the Council

11 The UK confirmed its compliance with GDPR will not be affected by Brexit. In August 2017 the UK government proposed a new Data Protection Bill that would transfer GDPR into UK law after it leaves the EU

12 GDPR and other regulations discussed in this paper are applicable across multiple industries. However, the focus of this paper is on the interactions and conflicts for financial institutions and the financial services industry

1) Lawful bases for processing personal data

Under GDPR, financial institutions must process personal data under one of six lawful bases.[13] There are many regulatory obligations that require financial institutions to retain data, for example, provisions on record keeping or AEoI requirements.[14] A financial institution's compliance with such obligations will clearly fall within the scope of the legitimate interests base. However, GDPR emphasizes data minimization. The retention of data for longer periods than required under regulatory rules may give rise to challenges as to what constitutes legitimate interests. Therefore, financial institutions using this base must ensure they maintain a balance between keeping data and erasing it.

2) Customer consent

Under GDPR, personal data refers to anything that could be used to identify an individual, either directly or indirectly. Identifiers include online data such as names, email addresses, IP addresses, or location data, which track user behavior. Financial institutions need to consider what grounds they are relying on to process this kind of data, and if they are relying on consent, how they are obtaining it, storing it, whether it covers online data, and the uses to which it can be put. Consent also triggers data subject rights such as *'data portability'*[15] rights and the *'right to be forgotten'*. Financial institutions may keep some data to ensure compliance with AML/CFT and tax transparency regulations, but in all other circumstances where there is no valid justification, the individual's right to be forgotten applies.

3) Third party data sharing

The volume of data processed by financial institutions, combined with the increase in outsourcing back office functions, means that financial institutions have numerous flows of data to external vendors. In a global operations environment this can also mean that financial institutions are using external vendors located in jurisdictions outside of the EU, which are therefore not required to comply with GDPR. Third party data sharing represents a key risk for financial institutions. Therefore, financial institutions must ensure that their vendors are complying with their GDPR obligations and that this is reflected in the contractual documentation.[16] Furthermore, financial institutions must have data protection safeguards in place that ensure that the data is not used for other purposes.

4) Consequences of a breach

GDPR imposes a 72-hour window for data protection officers to report a breach to the Data Protection Authority ("**DPA**"). The notification should contain details regarding the nature of the breach, consequences of the breach, the categories and approximate number of individuals impacted, measures already taken to rectify, and contact information of the Data Protection Officer ("**DPO**"). Notification of the breach to individuals may be avoided if that breach is "unlikely to result in a risk to the right and freedom of natural persons". The mandatory reporting requirements for breach both to regulators and in some cases affected customers also adds a new element of risk: reputational damage.

---

13 General Data Protection Regulation (EU) 2016/679, Article 6(1)

14 E.g. account holder identifying information, including underlying documentation, which is required to be reported under FATCA/CRS

15 The individual's' right to request access to, or the removal of, their own personal data from financial institutions without the need for any outside authorization.

16 Financial institutions should consider allowing three to six months to get the third party terms and conditions in place, additional lead-time may be necessary for vendors located outside of the EU to allow them to bring their compliance programs up to GDPR standards.

As mentioned above, liability in the event of any breach is significant. For serious violations, such as failing to gain consent to process data or a breach of privacy by design, financial institutions will be fined up to €20 million, or 4% of their global turnover, whichever is greater. Lesser violations, such as records not being in order or failure to notify the DPA, will incur fines of up to €10 million, or 2% of global turnover. In this regard, 'privacy by design' requirements mean that data controllers must consider the privacy risks and data protection compliance from the start of a project involving personal data which could include developing new financial products or drafting new policies. Furthermore, following a breach, regulators will also examine the measures a financial institution took to safeguard personal data in order to determine fines. The activities of the DPO and the breach response solution are therefore critical.

In the fiercely competitive financial services industry the consequences of a breach under GDPR go far beyond the fines imposed by the new regulation. Financial institutions, which are found non-compliant under GDPR, will not only face the stark glare of media and customer scrutiny but also run the risk of losing their customers trust. There can be a devastating reaction from customers when trust in a financial institution is violated. A 2016 survey[17] found that 28% of respondents left their banks and 22.4% left their credit card companies as a result of unauthorized activity on their accounts. Therefore, in order to maintain trust, financial institutions need to assure customers that they are GDPR compliant and their customers' data will not be stolen or abused.

The following discussion of scenarios of potential conflict highlights topics of risk for regulatory compliance program owners to explore with their legal department while developing or adjusting their GDPR programs. Tax departments have historically been viewed as areas of low volume for processing of personally identifying information ("**PII**") as the expectation is that corporate level tax filings are the primary function of such departments, which generally only contain details of Directors or other key personnel. However, as this paper will highlight, tax departments can process high volumes of PII, which may be outside the attention of legal departments. As such, tax departments should proactively seek out consultation with their legal teams rather than assuming that their programs that process PII have been considered.

"The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation."

– UK's Information Commissioner Elizabeth Denham on 'GDPR and accountability'.

---

17 Identity Theft: The Aftermath 2016, Identity Theft Resource Center (ITRC), 2016

4. Scenarios of Potential Conflict

Overview

Global tax transparency initiatives are trending towards alignment with KYC processes for customer identification purposes. At the same time, GDPR restricts which data financial institutions may obtain, store, process, and grant access to. This increases the need for financial institutions to be accountable for all information they collect. Therefore, we discuss in this chapter the challenges financial institutions face when aligning GDPR rules with tax transparency and AML/CFT requirements. The appendices include additional background information on the regulations/directives discussed in this chapter.

AML & AEoI (FATCA & CRS)

Regulators across multiple jurisdictions are increasing their focus on customer due diligence ("**CDD**") with respect to AML and CFT, and more recently, tax evasion. Though AML/CFT and KYC requirements have been in place for over 15 years, recent transparency rules, such as the EU Directive AMLD5 adopted by the EU Parliament in April 2018[18] and the increased KYC complexity, continue to raise compliance standards across the financial services industry.

These new AML/CFT requirements and the increase of penalties[19] for failing to comply coincide with the issuance of new KYC-like requirements from multiple tax authorities around the world. The enactment of provisions related to FATCA, designed to detect and deter tax evasion by leveraging and supplementing KYC and other customer information collected by financial institutions, was followed by the OECD's introduction of CRS. The recent media attention on offshore banking customer account and tax-related documentation, resulted from scandals such as the Panama Papers, further emphasized financial institutions' need to monitor relationships and transactions for potential tax evasion and other suspicious activity.

Financial institutions attempting to respond to these trends will need to enhance their onboarding ecosystems to ensure compliance with the convergence of emerging tax transparency requirements and increasing AML/CFT requirements. Regulatory and process enhancements are becoming paramount for any financial institution looking to remain compliant and reduce risk and cost, while minimizing any negative impact to customer experience.

Both FATCA and CRS[20] have been implemented by all EU Member States through local laws, which enable comprehensive cross-border transfers of sensitive financial account information between jurisdictions - raising important privacy and data protection concerns. Therefore, GDPR contains a provision that the collection and exchange of tax related information is allowed, even if it contains PII, if it is based on the law(s) of an EU Member State. Therefore, all AEoI related actions, such as obtaining customer documentation[21], storing PII, and submitting information reports to tax authorities (processing) should be permissible under GDPR.

The focus of this discussion is on the considerations that a Financial Institution ("**FI**")[22] for both FATCA and CRS purposes should make in regards to GDPR. However, entities that are classified as a Passive Non-Financial Foreign Entity ("**PNFFE**") under FATCA and/or Passive Non-Financial Entity ("**PNFE**") for CRS purposes and therefore required to disclose certain PII of related parties must also consider how they may be impacted.

---

18 EU Member States are tasked with implementing AMLD5 by January 10, 2020

19 In September 2018, Dutch bank ING was fined €775 million for failing to spot money laundering

20 See Appendix 1.4 for further background on AEoI (FATCA & CRS)

21 Including Controlling Person(s) information under CRS and Substantial US Owner(s) information for FATCA purposes

22 Though FATCA makes reference to Foreign Financial Institution ("FFI"), we refer to such FFIs as FIs throughout this paper as a collective FATCA and CRS term for ease of reading.

While FATCA introduced the concept of 'substantial US owner', CRS broadened that approach to require information on any Controlling Person ("**CP**").[23] In contrast, from an AML/KYC perspective, AMLD5 requires financial institutions to identify and take reasonable measures to verify the identities of the 'beneficial owner(s)' in relation to a customer.

Conflicts and challenges for financial institutions arising out of GDPR requirements may include, but are not limited to:

- Reviewing FATCA and CRS entity classifications to ensure that each entity in their group has the appropriate status in order to avoid 'over reporting', which could be a possible violation of GDPR. Historically, many entities have taken a conservative and practical approach to pre-emptively treat their entities as FIs although it may have been reasonable to classify them as PNFFEs under FATCA and/or PNFEs for CRS purposes. Therefore, consideration should be given in this instance as to whether the entity has a 'lawful basis' to collect and report PII under the FI classification as the processing of data under GDPR in the absence of a clear 'lawful basis' is a violation that can attract penalties of up to €20 million or 4% of global revenue.[24] Consultation with tax advisers may be appropriate where a conservative approach has been taken and the entity was preemptively treated as a FI.

- An entity that has classified itself as a PNFE is required to disclose its CPs when opening bank or other financial accounts. In practice, CPs are generally aware of the disclosure of their identity either through ownership or other means of control (such as being a senior managing official). FIs should confirm that they have policies and procedures in place to inform and receive consent from such CPs, where required. This point becomes particularly relevant for FIs that are incorporated or otherwise tax resident in the United States as US FIs may be effectively treated as PNFEs under CRS when opening bank or other financial accounts outside of the US[25].

- FIs may have policies and procedures in place to collect certain PII on account holders in an effort to 'future proof' their AML/CFT and AEoI compliance program. Generally, FIs are hesitant to request new information from customers so they may have established procedures, which collect information about an account holder in the interest of not having to request it again in the future. This may be seen, for example, where FIs request AML/CFT information, required under a newly proposed legislation such as AMLD5, which has not been implemented at the time of the request; or where a customer opens an account with a FI that is an excluded financial account and therefore not reportable but the customer has the ability to open new accounts in the future that would be reportable. In an effort to reduce follow up data collection, and the challenges with setting 'trigger points' to request that information, FIs may collect AEoI related certifications at initial onboarding of the excluded financial account.[26] This could potentially result in the FI holding information that is not currently required in order to meet its FATCA and CRS reporting obligations if and when the customer opens a reportable account type. Explicit consent to collect and store that excessive data may need to be considered.

- Individual customers do not tend to be well versed on AEoI matters. As such, if they call a customer service representative to ask about certain tax information that has been shared with their local tax authority or the US Internal Revenue Service ("**IRS**"), it may not be immediately apparent that it is AEoI related. FIs may face challenges in educating customer service representatives about these calls and how to redirect them to the appropriate parties (which may be the tax department in certain cases rather than a transfer agent, administrator, or other service provider) in order to meet the response timelines required under GDPR.

---

23 Who in some cases may have no financial interest in the entity
24 General Data Protection Regulation (EU) 2016/679, Article 6
25 Though the US was the catalyst for CRS through the passage of FATCA, the US is not itself a regarded as a participating jurisdiction for CRS purposes for all countries
26 Categories of excluded financial accounts can vary between jurisdictions but are generally seen as accounts that are at a low risk of tax evasion such as certain retirement or pension accounts regardless of who holds the account

- Consideration should be given to how PII is handled for substantial US owner(s) or CP(s) disclosed on a PNFFE/PNFE customer self-certification forms. For example, where a FI has an account holder that returns a self-certification claiming a classification of a PNFFE/PNFE, which discloses the identity of the substantial US owner, or CP(s), the FI should consider whether they have a customer relationship with such related parties. In practice, if a substantial US owner or CP calls a FI requesting details of how that individual's data was collected and shared with local tax authorities or the IRS, the FI would not likely be able to undertake their usual customer level security verification procedures before offering information back to the related party. As the substantial US owner or CP is not likely treated as a customer of the FI, it would be difficult (or even impossible) to verify the related party's identity before providing back the data being requested. The FI would then be a position where it is unable to comply with data requests from the customer.

- It is yet to be seen how the European Commission, the European Data Protection Board, and EU Members States will react to or incorporate the July 2018 recommendations of the European Parliament resolution on the adverse effects of FATCA[27]. Though the resolution covers a number of topics related to the rights of EU citizens, one point that should receive particular attention is with regards to the call on EU Member States to "review their IGAs and to amend them, if necessary, in order to align with the rights and principles of the GDPR [...and for the EU to...] initiate infringement procedures against EU Member States that fail to adequately enforce EU data protection rules". Certain Model 1 IGA jurisdictions that did not originally contain the Sponsoring arrangements in the Annex II to the IGA (e.g. Republic of Ireland, United Kingdom, Germany, Spain, etc.) allowed FIs to utilize the Sponsoring regulations of the US Internal Revenue Code ("**IRC**") instead. Historically, such FIs have completed their FATCA due diligence procedures under the local IGA and submitted annual reporting to the local tax authority. The IRS recently made an informal statement that FIs using the Sponsoring arrangement under the IRC are expected (and required by the IRC) to be completing their annual reporting directly to the IRS rather than through their local tax authority. This news came as a surprise to the financial services industry as well as the local tax authorities involved in implementing the operation of the IGAs. FIs that report directly to the IRS rather than through their local tax authority could likely be in violation of GDPR. The European Commission may also view this oversight on the part of the IGAs to be a violation of GDPR at the EU Member State level. Many of the impacted EU Member States were able to negotiate retroactive amendments to their IGA which resolved this issue. However, a number of the impacted EU Member States mentioned above are still working to address this issue by consulting with the IRS or by amending the Annex II to their IGA to include Sponsoring arrangements. As such, many Sponsored or Sponsoring FIs using the IRC (rather than the IGA) were required to submit certain certifications to the IRS about their FATCA compliance programs in March of 2019 which should not otherwise have been required. Many impacted FIs needed to consider whether they must submit a "qualified certification" given that they have not complied with the reporting that is required to have been made directly to the IRS (even though in principle the IRS would have received the reporting through the data exchange with the local tax authorities). If Sponsored or Sponsoring FIs that are caught by this failed to make required certifications to the IRS, their FFI agreement and GIIN could be cancelled and they would be subject to 30% FATCA withholding on the receipt certain payments of US source income going forward.

There are operational challenges and conflicts arising out of GDPR requirements in connection with CDD measures. Similar to AML/CFT procedures, AEoI CDD does not end once the account is opened. Processes must be implemented to identify any "change in circumstance" in customer's FATCA or CRS status. This illustrates that compliance is an ongoing responsibility requiring proper governance, procedures, and internal controls strategies, FIs should review these challenges and conflicts with their legal department and GDPR advisor. This can also be seen as an opportunity for FIs to streamline GDPR compliance by leveraging processes required pursuant to AML/CFT and AEoI to design a fully compliant, effective, and sustainable business model around CDD. Financial institutions have historically struggled to find the right balance and harmony between their AML/CFT, KYC, and AEoI customer due diligence processes. The risk of penalty exposure with GDPR presents an opportunity to escalate the business case for process integration. FIs utilizing Sponsoring arrangements through the IRC but are domiciled in one of EU Member States that does not including Sponsoring arrangements in the Annex II of the IGA should actively engage with their local tax authority for a resolution.

---

27 July 5, 2018 European Parliament resolution 2018/2646(RSP) on "adverse effects of the US Foreign Account Tax Compliance Act (FATCA) on EU citizens and in particular 'accidental Americans'"

Double Tax Treaties, Tax Relief at Source & Tax Reclaims

The continued development of international trade and MNCs has increased the need to scrutinize relief from double taxation. As a result, many countries entered into DTAs with other countries to avoid or mitigate double taxation. However, since this has led to investments being channeled through 'special purpose vehicles' set up in convenient jurisdictions to take advantage of 'treaty shopping', many local tax authorities are increasing their efforts to seek documentation of underlying ownership on entities that are seeking withholding tax relief at source or tax reclaims in order to demonstrate that the entire structure is truly eligible for deductions from statutory tax rates. In the case of such tax transparent entities that have EU resident individuals as investors, it may - without consent - no longer be possible to make certain claims of relief at source from withholding taxes on portfolio dividends and interest in jurisdictions outside the EU. It may also prove more difficult to file tax reclaims in some jurisdictions where relief at source is not granted or generally not available.

Conflicts and challenges for tax transparent investment vehicles arising out of GDPR requirements may include, but are not limited to:

- Is there a legal basis for transmitting PII to a third party in the case of reductions of withholding taxes (such as under a DTA)? It does not appear that it is a legal requirement to apply relief at source, especially in cases where an underlying investor may file a reclaim of taxes independent of the investment vehicle (such as through filing a self-assessment tax return). That being said, an investment vehicle has a general obligation to its direct and indirect investors to maximize the return on investment which means that it cannot ignore the pursuit of legally allowable (though perhaps not required) reductions in withholding taxes.

- Where an EU tax transparent investment vehicle intends to share PII with non-EU third parties for relief at source or tax reclaim purposes, and there is no legal basis for such sharing (as discussed in the previous point), is the investment vehicle required to allow each investor to individually opt in / opt out (obtain consent)? And does such opt in / opt out jeopardize the ability of the entire investment vehicle to claim relief at source or to file a tax reclaim where a number of investors opt out (i.e. consent to facing the higher headline rates of tax withholding)?

- Can an EU tax transparent investment vehicle share underlying investor PII with non-EU withholding agents such as US transfer agents? If so, how does the investment vehicle document or gain comfort that the non-EU withholding agent has optionally become GDPR compliant? Is such confirmation required or is there any allowance for providing the information with specific consent? How frequent would such consent be required to be obtained and are processes in place to obtain and monitor that consent? How would an investor revoke that consent?

- If an EU tax transparent investment vehicle is limited by the above, for example, by investing into the US and being unable to transmit underlying withholding certificates as part of a Form W-8IMY package, would this make it more attractive to invest into US securities via a Qualified Intermediary ("**QI**") instead? The QI will only provide its entity level Form W-8IMY with no detail of underlying investors in its self-certification to non-GDPR compliant US withholding agents. Note that there may challenges to the QI itself from a GDPR perspective (discussed later in this paper).

It is clear that financial institutions face a different set of GDPR challenges under AML/CFT and AEoI requirements than those faced under tax relief at source and tax reclaim filing procedures. AML/CFT and AEoI CDD and reporting requirements and procedures are formed on a legal basis and therefore the challenges and conflicts faced correspond to consent, data retention, and general security protocols for indirect customers. Tax relief at source and tax reclaim filing procedures face slightly different challenges and conflicts which correspond to documenting the existence of a legal basis for collecting, storing, and processing the data in contrast to obligations to maximize investor returns through legally allowable (though optional) reductions in withholding taxes.

Qualified Intermediary Regimes

QI is a term that can have varied meanings depending on its context. In the context of this paper, it is generally viewed as an entity that is an intermediary acting on behalf of customers, and has applied for a special status with a tax authority to act as a tax withholding and/or reporting agent in a chain of parties. In general, an intermediary is usually not the tax withholding or reporting agent for its account holders and a tax withholding or reporting agent upstream would hold the primary responsibility for such obligations. With a QI status, an intermediary can take on certain responsibilities that would normally be held by the upstream agent. The most well known QI status is that of the US QI which is administered by the IRS. Other jurisdictions may also have QI regimes (e.g. Republic of Ireland). For the purposes of this paper, we focus the discussion on the US QI status and program though the issues outlined here may be extrapolated out to those other regimes.

US QI Agreement

The US QI Agreement[28] ("**QI agreement**") is not law of one of the EU Member States and as such does not supersede GDPR. As discussed in the appendix, the QI agreement is an optional status that a non-US intermediary may seek to conform to their business and operational goals and create a more customer friendly experience.

Though there are a number of obligations that a QI must meet under the QI agreement, as discussed in the appendix, the focus of this discussion can be split into two distinct processes:

1. Onboarding of account holders (e.g. investor subscription documents, etc.) and self- certification due diligence (e.g. Form W-8 reviews/checks including claims of treaty benefits, etc.)

2. Year-end annual tax reporting to the IRS (e.g. Forms 1099 or 1042-S)

Conflicts and challenges for QIs arising out of GDPR requirements may include, but are not limited to:

- QIs should review their account holder self-certification and year-end annual tax reporting processes to determine which parts have a legal basis for which no voluntary consent is required, and which other parts do not have an EU legal basis and may require voluntary consent. Processes should be reviewed to understand how the QI may obtain voluntary consent as well how to allow an account holder to revoke such consent.
- QIs should review their account holder subscription documents to ensure they adequately cover any necessary consents. Existing subscription consents may cover self-certification data collection, which is not necessarily shared with third parties (such as in the case where the QI assumes primary tax withholding and reporting, including Forms 1099 reporting). Are any additional consents required where self-certifications must be passed along to third parties such as in the case of a QI that does not assume certain Form 1099 reporting obligations? Is such consent required one time or on a recurring/transactional basis?
- The QI agreement contains a provision that indirect account holders that are non-US need to be reported annually on Form 1042-S as payee specific (as opposed to pooled reporting applicable to many pools of direct payees). An example is a Netherlands QI with an account holder that is a tax transparent Netherlands mutual fund for joint account (closed FGR) that has Netherlands individuals as participants / account holders. Without prior, voluntary, consent this payee specific Form 1042-S reporting to the IRS may not be possible under Dutch law as the reporting to the IRS is not a requirement under EU law. In this case, would the QI refuse customers that have indirect account holders (i.e. a customer of the QI, which is itself a non-qualified intermediary or other flow-through entity)? This may result primarily where local banking secrecy laws prohibit the dissemination of this information. Alternatively, the so-called Joint Account option is applied for direct account holders with indirect account holders. The QI may also consider that rather than refusing the customer with indirect account holders, whether they may act as a Non-Qualified Intermediary ("**NQI**") for those accounts instead which would require the NQI to pass along the indirect account holder information to the upstream withholding agent instead (where tax withholding and reporting would occur rather than at the level of the QI). As mentioned in the points above, existing account holder subscription documents may already contain consent to pass indirect account holder self-certification documentation to third parties as part of a Form W-8IMY package.

---

28 See appendix for further background on US QI agreement

- Similarly to the previous point about payee specific Form 1042-S reporting for indirect payees, a QI should consider if they would be prohibited under GDPR or other local law from reporting such payees on Form 1099 to the IRS. In certain circumstances, a QI may elect to not be a primary Form 1099 reporting agent. In this case, the QI would pass along any Forms W-9 (i.e. US resident self-certification) to the upstream withholding agent who would perform the Form 1099 reporting instead. This could potentially eliminate the possibility that the QI is reporting information to a tax authority without consent, where previous consent was obtained to share the self-certification documentation. However, even in these cases a QI (and even an NQI) is ultimately responsible for Forms 1099 and 1042-S reporting where it has reason to know that the upstream agent has not met the reporting obligations.

- Payee specific Form 1042-S reporting is effectively eliminated in the case of a QI making a payment to another QI. As a result, there may be an increase in NQIs seeking QI status. In the absence of an NQI seeking QI status, the payment from a withholding agent to a QI may need to default back to the previously mentioned scenario where the QI cannot act as QI for other NQIs which results in all indirect account holder self-certification documentation passing upstream to the withholding agent (which may be a US withholding agent outside the purview of EU GDPR requirements).

QI programs add significant layers of complexity to the GDPR compliance program. QIs must develop a governance and compliance program that contemplates each intricate movement of direct and indirect account holder self-certification information and tax data to third parties and to local tax authorities. Unwinding and scrutinizing these layers can be challenging without the appropriate resources involved to understand the requirements and processes involved for each party to the layers. Engagement with third parties is crucial to understand where one process changes how it will impact the upstream and downstream parties.

US QI Certification

One of the obligations of a QI, as discussed in the appendix of this paper, is to submit recurring certifications to the IRS regarding its QI compliance program. Where a QI has identified material failures or events of default, these must be disclosed to the IRS. A QI should understand how GDPR will impact its existing compliance program (i.e. reporting due currently for historic transactions) as well as any modifications it may need to make to the future of the QI compliance program.

Challenges or questions that QIs could face during their IRS certification process may include, but are not limited to:

- QIs that previously failed to obtain consent from indirect account holders to include them in the QI payee specific 1042-S reporting, may have an issue that requires resolution. Consent to be reported to the IRS on Form 1042-S (or 1099), if required, can still be obtained from such indirect account holders, but may need to be voluntary. Therefore, account closure or terminating QI services as a consequence is not an option in the case of historic transactions.
- For those customers that do not (or cannot) provide consent, the QI may not be able to report the indirect account holders to the IRS on Form 1042-S or 1099, under local law restrictions (i.e. banking secrecy, etc.). This would very likely constitute a material failure / event of default that would need to be disclosed to the IRS during the certification process.
- Where a QI identifies to the IRS a material failure / event of default in its compliance program (from historic transactions / events), it will need to disclose a satisfactory remediation plan. QIs would need to consider whether they can continue to act as a QI for certain account holders (e.g. look through / transparent account holders on Form W-8IMY where the intermediary does not act as a primary withholding and reporting QI, etc.). In such cases, the QI may need to consider a plan to act as an NQI for that specific subset of account holders and disclose this future plan to the IRS. In the case that the QI may need to act as NQI for account holders with indirect account holders, the QI should consider the required consents (if not already contained in subscription documents) for this process of passing account holder (direct and indirect) to upstream agents (which may be outside of the EU).

A voluntary consent process should also consider opt out procedures such that each payee may decide to suffer the highest statutory rate of withholding on their allocable share of income as an "unknown payee" rather than have their PII shared outside of the EU. A QI acting as an NQI in this regard may need to consider if such approach would jeopardize their FATCA status (where applicable).

QIs in certain cases will face a unique set of conflicts and challenges as a result of GDPR. On the one hand, QIs have signed up for a QI agreement with the IRS to comply with US QI regulations in order to better serve their customer base. GDPR and other domestic laws may result in such QIs being unable to satisfy the requirements of the QI agreement. These QIs are effectively faced with deciding which penalties to face those resulting from GDPR or banking secrecy law violations or those resulting from non-compliance with the QI agreement. QIs have significant work to undertake to ensure they find the balance that allows them to comply with all of these requirements while still meeting their business and operational goals.

Emerging Issues - Cryptocurrency and DAC6

The DAC6 was adopted on May 25, 2018 by the European and Financial Affairs Council ("**ECOFIN**") which requires the mandatory disclosure for certain cross-border arrangements[29]. The main goals of DAC6 are to strengthen tax transparency and to fight against what is regarded as aggressive cross-border tax planning. Each EU Member State has until December 31, 2019 to transpose DAC6 into domestic law. While the provisions of the Directive will apply from July 1, 2020, transitional measures mean that the first reportable transactions will be those where the first implementation step of a cross-border arrangement occurs from June 25, 2018. DAC6 does not define "aggressive cross-border tax planning" but instead offers five hallmarks (lettered A through E).

Where an arrangement meets any of the hallmarks and is cross-border, it will be reportable under DAC6. Arrangements are reportable by any and all parties that meet the definition of an "intermediary", but unlike other regulations discussed in this paper where there is no intermediary with a reporting obligation (e.g. US intermediary or a law firm claiming attorney client privilege) then the reporting obligations rests with the taxpayer (both individual and corporate level). A number of hallmarks contain a "main benefit" test in order to be reportable while others do not. DAC6 is broadly written and does not always contain any exclusions for ordinary, day-to-day, routine tax advice and planning (depending on the local implementation). As such, even though a large amount of uncertainty and confusion surrounds DAC6, it is expected to have profound impacts across the both financial and non-financial industries. Tax authorities will collect and store PII as part of reporting submitted by intermediaries and taxpayers of reportable cross-border arrangements. It is understood that the EU may create a central repository of the data collected to allow each EU tax authority access to scrutinize the data for aggressive cross-border tax planning. Taxpayers, their advisors, their counterparties, and their service providers should begin understanding DAC6 now given the transitional measures that may require reporting in the future of arrangements they are undertaking today. Organizations may need to discuss with their legal departments where to strike a balance between collecting PII now in anticipation of local implementation of DAC6 with the 'right to privacy'. Though DAC6 is adopted by ECOFIN, domestic legislation does not exist in every EU member state as of the issuance of this paper and as such a view should be formed as to whether there currently exists a 'legal basis' to collect and store PII for DAC6 purposes given the uncertainty as to whether an arrangement will be reportable or not.

Of particular relation to this paper are the hallmarks concerning AEoI and UBOs. Under DAC6, cross border arrangements may be reportable where they:

- may undermine reporting obligations on the automatic exchange of financial account information
- involve a non-transparent legal or beneficial ownership chain with interposed entities that carry on no economic activity and whose beneficial owners are not identifiable

29 More information on DAC6 can be found at https://www.pwc.com/gx/en/services/tax/tax-policy-administration/dac6-eu-directive-on-cross-border-tax-arrangements.html

From an AEoI perspective, cross-border arrangements that might be captured under CRS avoidance arrangements include types of accounts that have features of financial accounts but that do not fall within the definition of a financial account, such as cryptocurrencies for example. It also appears that the simple movement from a trust to a company could be captured here as well as the movement of financial accounts from a CRS participating jurisdiction (such as EU Member States) to a non-participating jurisdiction (for example the US). In the context of opaque offshore structures, DAC6 seeks to address arrangements that are designed to shelter UBOs in non-transparent (opaque) structures, e.g. transactions where beneficial owners in CRS participating jurisdictions establish an entity in a non CRS participating jurisdiction, that makes them unidentifiable (e.g. occasionally the US).

Cryptocurrency and Distributed Ledger Technology ("DLT" sometimes referred to as "blockchain") were first conceived in the late 1980s but did not gain functional popularity until around 2009. Their popularity has continued skyrocketing year on year since then and financial regulators have found it challenging to keep up in order to both protect investors and the financial market as well as ensure proper taxation of the transactions involved. Virtual currencies were defined by the European Central Bank ("**ECB"**) in 2012 as "digital money in an unregulated environment, issued and controlled by its developers and used as a payment method among members of a specific virtual community". Cryptocurrency is a form of virtual currency that keeps transactions secure, manages creation of new units, and are transacted over DLT networks. Cryptocurrency may be used as a payment method but many buyers also actively trade them as a financial investment. Ownership of cryptocurrency is not anonymous but is more "pseudo-anonymous" given that the currency is not identifiable to a person but is instead identifiable to a specific electronic key. Though not the primary driver behind the popularity of cryptocurrency, the privacy and pseudo-anonymity afforded to users is very attractive in the public view.

A fundamental question that financial regulators and tax authorities are struggling with around the world is whether cryptocurrency is classified as money or is more appropriately classified as a commodity, security, or other type of asset. The answer to this question is paramount to regulation and taxation of cryptocurrency though very few jurisdictions have issued guidance or regulation in this area.

Challenges or questions that FIs may face with cryptocurrency include, but are not limited to:

- Does cryptocurrency meet the definition of a "Financial Account" for AEoI purposes subject to account opening due diligence and self-certification requirements? If so, how do you perform such procedures on a pseudo-anonymous account holder?

- Is holding or investing in cryptocurrency a "Financial Asset" for purposes of classifying an entity as an FI for AEoI purposes?

- How will you perform other CDD procedures on a pseudo-anonymous account holder such as those outlined in AMLD5?

- In the case, that cryptocurrency is a Financial Account then it would be reportable under FATCA and CRS and subject to the due diligence challenges previously mentioned. In the case that is not viewed as a Financial Account, it may be viewed as having "features similar to that of a financial account" under DAC6. Where there is a cross-border arrangement involving such cryptocurrency then you may have a transaction into or out of a non-reportable account under hallmark D subject to DAC6 reporting.

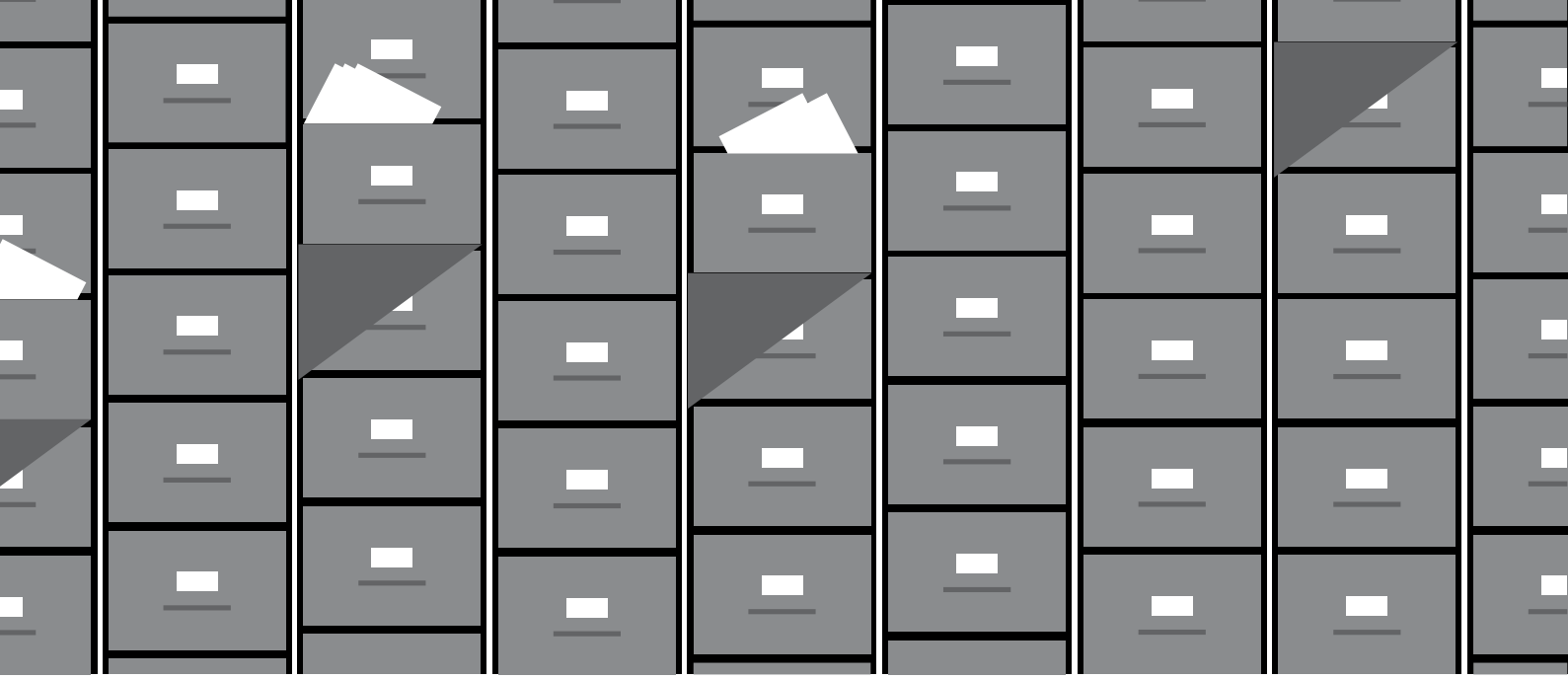
Though DAC6 has far broader implications than those discussed here related to cryptocurrency, it is an illustrative example of the continuing privacy tug-of-war and resulting challenges that the financial services industry will face far into the future.

5. Conclusion - Next Step

This paper set out to explore the proposed metaphorical tug-of-war that the financial services industry faces between GDPR rights of EU individuals and the AML directives, tax relief at source, tax reclaims, Qualified Intermediary programs, and AEoI. Throughout the discussion, we have proposed a number of challenges and conflicts by raising questions or providing examples. Though we have proposed a number of approaches that may be considered as part of this exploration, it will be up to each financial institution to consider each issue discussed as part of a holistic view of their operations and risk profile. In this regard, this paper should serve as a tool to assist in prioritizing operational tax programs with the Board and GDPR implementation teams. Financial institutions should consider:

- Do you have the right subject matter experts involved?
- Have the legal and GDPR experts in your organisation considered and documented the results all of the operational tax issues raised in this paper? Or do you need to build their awareness of the volume of PII that your operational tax programs process? Will you use this paper to build that awareness?
- Have you engaged with the different service providers (i.e. custodian, administrator, transfer agent, counterparty, withholding agent, vendors, etc.) that may be a component to different processes and documented the results?
- How have you documented comfort that service providers themselves are GDPR compliant, particularly when they are located outside of the EU?
- Where you operate as a QI, or are considering applying to be a QI, are you engaging with client relationship teams to educate them on the issues and how it may impact the services you provide? Will you consider approaching your customers to receive their feedback on how to best serve them? Is your Responsible Officer informed of any qualified certifications that need to be made to the IRS?
- Where your CDD processes are not fully integrated with each other, how will you leverage GDPR as a way to prioritize your business case for such improved integration?
- Will you engage with Portfolio Managers and other investment teams to discuss the impact to their yield as a result of changes to relief at source or tax reclaim filings where reductions in the tax rate may no longer be possible?
- Are you engaging in DAC6 discussions?
- How will your organisation modify its GDPR compliance program as the relief at source and tax reclaim processes continue their move away from paper/PDF based and into the digital/electronic world?

Operational taxes is increasingly an area of exposure to financial penalties but also non-financial penalties such as damage to reputation and brand. GDPR has brought to light opportunities for financial institutions to reduce these risks while enhancing customer and business partner trust.



Appendix 1 - Background Information

Appendix 1.1 - GDPR

1.1.1) Key Changes

Although the key principles of data privacy still hold true to the previous directive, GDPR takes a farmore rigorous approach to the protection of data privacy than its predecessor. It introduced considerable updates to align data protection laws with the technological advances made as well as the increased number of tax and regulatory reforms enacted over the last decade. The most relevant changes of the GDPR are described below.

Expanded scope

The biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of GDPR, as it applies to all organizations processing the personal data of data subjects residing in the EU, regardless of the organizations' location. Previously, territorial applicability of the directive was ambiguous and referred to data processing 'in context of an establishment'. This concept has arisen in a number of high profile court cases. The Court of Justice of the European Union ("**CJEU**") has been developing jurisprudence on this concept, finding that Google Inc. with EU based sales and advertising operations was established within the EU.[30] Under Article 3, the GDPR makes its applicability very clear – it applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.

30 Case C-131/12, Google Spain SL, Google Inc. v AEPD, Mario Costeja Gonzalez, 2012

Consent
Under Article 7 of GDPR, the conditions for consent have been strengthened, and organizations are no longer able to use long illegible terms and conditions full of legalese. The request for consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent, as it is to give it. In addition, consent must be freely given and for specific purposes.

Penalties
As mentioned before, fines for a breach of GDPR are substantial. Regulators can impose fines of up to 4% of annual worldwide turnover or €20 million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements. For example, not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines. This means an organisation can be fined 2% for not having their records in order, not notifying the supervising authority and data subject about a breach or not conducting impact assessment.[31] It is important to note that these rules apply to both controllers and processors – meaning 'clouds' are not exempt from enforcement under GDPR.

Privacy Impact Assessments
Article 35 of the GDPR introduced the duty for organizations to undertake Privacy Impact Assessments when conducting risky or large scale processing of personal data.

Data Protection Officers ("DPOs")
Under GDPR it is not necessary to submit notifications to each local Data Protection Act ("**DPA**") of data processing activities, nor is it a requirement to notify or obtain approval for transfers based on the Model Contract Clauses ("MCCs"). Instead, there are internal record keeping requirements and a DPO appointment is mandatory only for those controllers and processors whose core activities consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

Mandatory breach notification
Organizations must notify supervisory authority of data breaches 'without undue delay' or within 72 hours, unless the breach is unlikely to be a risk to individuals. If there is a high risk to individuals, those individuals must be informed as well.

New rights of individuals (data subjects)
Although these rights already exist under the pre-existing EU Data Protection Directive, GDPR enhanced existing rights and introduced new rights such as the 'right to data portability'. This implies additional obligations for data controllers.

1) **The right of access (Article 15)**
Information requested by data subjects must be provided within one month as a default with a limited right for the controller to extend this period for up to three months.

2) **The right to rectify (Article 16)**
Data subjects continue to enjoy a right to require inaccurate or incomplete personal data to be corrected or completed without undue delay.

3) **The right to erasure ('right to be forgotten') (Article 17)**
The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay. However, the right only arises in a certain circumstances

31 General Data Protection Regulation (EU) 2016/679, Article 28, 33 and 35

notably where the controller has no legal ground for processing the information.

4) **The right to restriction of processing (Article 18)**
Data subjects enjoys a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data is no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller and whether these override those of the data subject are contested.

5) **The right to data portability (Article 20)**
This is an entirely new right in GDPR and has no equivalent in the pre-existing Directive. Where the processing of personal data is justified either on the basis that the data subject has given their consent to processing or where processing is necessary for the performance of a contract, or where the processing is carried out be automated means, then the data subject has the right to receive or have transmitted to another controller all personal data concerning them in a structured, commonly used and machine-readable format.

6) **The right to object (Article 21)**
The pre-existing Directive's right to object to the processing of personal data for direct marketing purposes at any time is retained. In addition, data subjects have the right to object to processing which is legitimized on the grounds either of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate "compelling legitimate grounds" for processing which override the rights of the data subject or that the processing is for the establishment, exercise or defense of legal claims.

7) **The right not to be subject to automated decision taking, including profiling (Article 22)** This right expands the pre-existing Directive right not to be subject to automated decision making. GDPR expressly refers to profiling as an example of automated decision-making. Automated decision making and profiling "which produces legal effects concerning [the data subject] ... or similarly significantly affects him or her" are only permitted where

a) necessary for entering into or performing a contract
b) authorized by EU or Member State law, or
c) the data subject has given their explicit (ie opt-in) consent.

The scope of this right is potentially extremely broad and may throw into question legitimate profiling for example to detect fraud and cybercrime. It also presents challenges for the online advertising industry and website operators who will need to revisit consenting mechanics to justify online profiling for behavioral advertising. This is an area where further guidance is needed on how Article 22 will be applied to specific types of profiling.

Accountability
Accountability is a recurring theme of GDPR. Data governance is no longer just a case of doing the right thing; organizations need to be able to prove that they have done the right thing to regulators, to data subjects and potentially to shareholders and the media often years after a decision was taken. GDPR requires each controller to demonstrate compliance with the data protection principles.

---

32 General Data Protection Regulation (EU) 2016/679, Article 28, 33 and 35

Privacy by Design
Organizations should design data protection into the development of business processes and new systems. Since privacy can no longer be an afterthought when developing new products. Privacy settings are set at a high level by default.

Obligations on Processors
New obligations on data processors — processors become an officially regulated entity.

Appendix 1.2 - EU AML Directives

1.2.1) AML Directives Overview

The EU has implemented AMLD5 as it sought to drive financial transparency across the continent. A provisional agreement on AMLD5 was published in December 2017. On April 19, 2018, the new directive was formally adopted by the EU Parliament, amending AMLD4, which was issued in 2015, which had to be transposed into local law by the EU Member States by June 26, 2017. The quick succession of these amendments was the result of scandals surrounding the Panama Papers and the financing of terrorist groups involved in the attacks in Paris and Brussels. In light of this, AMLD5 aims to ensure a significant tightening of the EU regulations for the prevention of money laundering and terrorism financing. The EU Member States are now tasked with implementing the Directive by January 10, 2020. The aim of the amendments is to set out measures to better counter the financing of terrorism and to ensure increased transparency of financial transactions. It will do so by:

- preventing risks associated with the anonymous use of virtual currencies for terrorist financing and limiting the use of pre-paid cards;
- increasing transparency on company ownership by improving the accuracy of beneficial ownership registers;
- strengthening the monitoring of financial transactions to and from high-risk third countries;
- enhancing the powers of EU Financial Intelligence Units and their access to information, including centralised bank account registers;
- ensuring centralised national bank and payment account registers or central data retrieval systems in all EU Member States.

The rules will now apply to entities which provide services that are in charge of holding, storing and transferring virtual currencies, to persons who provide similar kinds of services to those provided by auditors, external accountants and tax advisors which are already subject to the AMLD4 directive and to persons trading in works of art.

For the first time, the obligations are to be imposed on exchange platforms for virtual currencies such as Bitcoins and the providers of digital wallets for virtual currencies. The objective of the Directive was to design a definition, which would cover as many tokens as possible and to cover all the potential uses of virtual currencies.

1.2.2) Enhancement of transparency of the beneficial ownership

The beneficial ownership registers for legal entities, such as companies, will be public. The access to the beneficial ownership registers for trusts is limited to competent authorities, professional sectors and persons who can demonstrate legitimate interest. This wider access to part of the beneficial ownership information will enhance public scrutiny and will contribute to preventing the misuse of legal entities for money laundering and terrorist financing purposes.

The national registers on beneficial ownership information will be interconnected directly to facilitate cooperation and exchange of information between EU Member States. In addition, EU Member States will have to put in place verification mechanisms of the beneficial ownership information collected by the registers to help improve the accuracy of the information and the reliability of these registers.

Appendix 1.3 - QI

1.3.1) QI Program Background

The Qualified Intermediary ("**QI**") program was created by the US Internal Revenue Service ("**IRS**") in 2001 under 26 U.S.C. § 1441. The introduction of this program, which is optional to participate in but requires an application and IRS approval for a QI status, required participating Foreign Financial Institutions ("**FFIs**") to maintain records of their direct and indirect US and foreign account holders, withhold and remit tax from payments, and to annually report income paid to them and related withholding taxes (if any). These requirements imposed on FFIs in the QI program were closely aligned to the existing tax withholding and requirements imposed on US financial institutions. As such, an intermediary that successfully applied for and received QI status could take on certain responsibilities that would normally be held by the upstream US financial institution tax withholding and reporting agent. This program was attractive to FFIs for many reasons, including privacy for their account holders.

Generally speaking, the IRS requires any entity or person, US or non-US, making a payment of US source fixed or determinable, annual or periodical income ("**FDAP**") to a non-US person to withhold tax ("**WHT**") at the US statutory rate of 30% on such payment of income. In the regular instances of a non-US intermediary that is not the beneficial owner and is in receipt of US source income, such intermediary must pass along to the withholding agent (generally a US withholding agent) a Form W-8IMY and the underlying documentation of each investor or account holder that the intermediary represents ("**Form W-8IMY package**"). In this instance, the withholding agent (generally a US withholding agent) will perform tax withholding based on the allocations of income and applicable withholding tax rates claimed in this Form W-8IMY package of the intermediary. The underlying account holders may be making claims of reductions in withholding taxes under double tax treaty claims but they may be making of claims of exemption from withholding taxes under US domestic laws, etc. At the close of each calendar year, the withholding agent (generally a US withholding agent) will issue Forms 1099 to any indirect US account holders disclosed in the Form W-8IMY package and Forms 1042-S to any indirect non-US account holders disclosed in the package. The Forms 1099 and 1042-S are an information return to the underlying account holders of their allocable share of income from distributions passed through to them via the non-US intermediary, the character of such income, any taxes withheld on such income, and the reasons for any reduction in withholding from the headline WHT rate in the case of non-US account holders. Where an underlying account holder is due a refund of tax due to overwithholding by the upstream withholding agent, that account holder would need to file its own tax return to make such claim. An alternative to this process is that a non-US intermediary may form a US withholding and reporting compliance program for its customers, and apply to the IRS for QI status and thereby avoid passing tax documentation of beneficial owners to upstream withholding agents via the Form W-8IMY package mentioned earlier.

Similar concepts to QI exist in the case of other tax transparent vehicles such as partnerships and trusts. These are known by their IRS names of Withholding Foreign Partnerships ("**WFP**") and Withholding Foreign Trust ("**WFT**"), though are frequently known with the Qualified Intermediary status collectively as "QIs". As such, references to the QI program can be broadly applicable to WFP and WFT status as well.

1.3.2) Key Highlights of QI Obligations

A few highlights of the QI status:

- QIs generally take responsibility for calculating withholding tax allocations and either performing the withholding themselves or providing the blended withholding rates applicable to each type of income to the upstream withholding agent (generally a US withholding agent).

- QIs will also generally perform Forms 1099 and 1042-S reporting to its customers at the end of each calendar year. The upstream withholding agent will not report to the indirect account holders of the intermediary in this case and instead will issue one Form 1042-S directly to the QI. There are exceptions to this where the QI does not take primary reporting responsibility for certain account holders.

- QI status allows reporting to the IRS on a pooled basis rather than a payee specific basis in certain circumstances. Pooled reporting is not allowed by the QI in the case of payments to a non-qualified intermediary or another flow-through entity.

- The primary overall benefit of QI status is to provide privacy for both QI and its customers and reduce the burden of payee specific reporting. This privacy is between the customer of the QI and the upstream withholding agent. Such privacy is not generally between the customer and the IRS.

- Collective refunds claims, which allow QIs to seek a refund on behalf of its direct customers. As a result, the direct customers are not required to file tax returns with the IRS to obtain refunds, but rather may obtain such refund directly from the QI.

- A QI is generally also a Financial Institution for purposes of FATCA (discussed elsewhere in this document). Therefore, a QI would be considering the interaction of its US due diligence, withholding tax, and reporting processes (Forms 1099 / 1042-S) with their FATCA processes.

- The QI must establish a compliance program with the following key features:

    - Written policies and procedures for fulfilling QI requirements
    - Training for documenting customers, calculating and remitting tax withholding, and preparation and submission of annual payee reporting (Forms 1099 / 1042-S)
    - Systems and processes for collecting and reporting data.
    - Monitoring and implementing business changes and developments/changes in QI requirements, including FATCA requirements.
    - Designation of a Responsible Officer ("RO") to make recurring certifications of the QI compliance program to the IRS.

1.3.3) Information Collected and Reported to the IRS by a QI

The below list is a non-exhaustive example of information that may be collected about direct and indirect account holders on IRS Forms W-8 or W-9 as well as information that may be reported to the IRS on Form 1099 or 1042-S at calendar year end:

- Name;
- Country of incorporation or citizenship;
- Residence and mailing address;
- Taxpayer identification number ("TIN") in jurisdiction(s) of tax residence;
- Date of Birth (of an individual);
- Account Number;
- US tax classification (of an entity);
- FATCA classification and GIIN (of an entity, where applicable);
- Details of eligibility for certain reductions in withholding tax rates (such as a claim of DTT benefit);
- Payments of US source income made to the account during the calendar year;
- Details of intermediaries to the payment (such as name, TIN, etc);
- Details of substantial owners of certain entities that are Specified US Persons;

Appendix 1.4 - AEoI

1.4.1) FATCA Background and Overview

As mentioned above, previous to FATCA the IRS instituted the QI program in 2001 under 26 U.S.C. § 1441, which required participating FFIs to maintain records of their direct and indirect US and foreign account holders and to annually report income paid to them and related withholding taxes (if any). One report issued about the program included a statement of a finding that participation in the QI program was too low to have a substantive impact as an enforcement measure and was prone to abuse. An illustration of the weakness in the QI program was in 2008/09 the case of Bradley Birkenfeld, a former UBS employee, which revealed that UBS advised US individuals to open offshore accounts connected to foreign entities, which would receive payments with no withholding tax yet beneficial owners were US residents. Though it is not illegal for a US citizen or resident to open an offshore financial (bank) account, such accounts must be voluntarily disclosed by the taxpayer and US income tax paid on income earned in the account, in most cases. UBS agreed to pay a fine of $780 million, release (through the Swiss government) the names of 250 US holders of offshore accounts, and cease its illegal banking and brokerage activities in the US. Under a separate agreement, UBS also agreed to disclose the names of a vast number of US holders of offshore accounts at UBS.

In 2009, under an offshore voluntary compliance program, almost 15,000 US taxpayers disclosed to the IRS that they held funds in previously unreported offshore accounts. Voluntary self-disclosure requirements (such as the Form TDF-90.22.1 Report to Foreign Bank and Financial Accounts) were proving insufficient to combat tax evasion and thereafter the US added a system aimed at the compulsory disclosure of US taxpayers by FFIs. On March 18, 2010, the Obama Administration signed into law the "Hiring Incentives to Restore Employment Act" (the "**HIRE Act**"), which includes the Foreign Account Tax Compliance Act ("**FATCA**"). FATCA established a basic principle: a FFI is subject to a 30-percent withholding tax on its US sourced income unless it complies with the FATCA reporting duties, in respect of 'Specified US Persons'[33] who are account holders of that institution. The requirements are contained in the relevant US Treasury Regulations ("**US Regulations**"). The result is an extensive third-party monitoring and disclosure regime on financial institutions located outside the US in an effort to expose undeclared foreign assets of Specified US Persons to the IRS. Though FATCA was originally billed, as being somewhat of a voluntary program for FFIs to participate in, non-participation by FFIs would result in effective denial of access to the US financial system through the FATCA penalty tax withholding being applied by US financial institutions on payments of US source income.

FATCA also impacted US financial institutions given they are generally the last point of contact before a payment of US source income leaves the US financial system. As such, US financial institutions may be required to impose FATCA penalty tax withholding to non-compliant FFIs. US financial institutions may also have to submit annual FATCA reports to the IRS (similar to FFIs) such as, for example, when making a payment of US source income to certain entities that have disclosed the identity of substantial owners that are US Persons.

1.4.2) Intergovernmental Agreements

The US recognized that in some jurisdictions there are legal barriers for FFIs to implement FATCA as well as some practical difficulties for FFIs in complying with FATCA. Therefore, two model Intergovernmental Agreements ("**IGAs**") were developed to overcome the legal issues and to reduce some of the burden on FFIs. In cases where governments have not signed an IGA with the US, 'agreements in substance' have been reached instead and are effectively treated as having an IGA in place.

Where an entity is in a jurisdiction, which has signed a Model 1 IGA with the US, this effectively changes the way that FATCA applies to that entity. FFIs resident in Model 1 IGA countries ("**Model 1 IGA FFIs**") will be required to register with the IRS to obtain a Global Intermediary Identification Number ("**GIIN**") but will be governed by local regulations and guidance notes rather than the US Regulations. Such FFIs will report to the local tax authority, who will then share the information with the IRS. FFIs in Model 2 IGA countries ("**Model 2 IGA FFIs**"), or FFIs in countries without an IGA ("**Participating FFIs**"), will also register with the IRS to obtain a GIIN but will instead report directly to the IRS rather than through local tax authorities.

---

33 For a specific definition see US Regulations

Though reports by Model 2 IGA FFIs and Participating FFIs are generally not required where such report is nil, Model 1 IGA FFIs may have nil reporting requirements depending on the local guidance on the IGA of that jurisdiction. The due date for annual reports by a Model 1 IGA FFI varies by jurisdiction while the annual reports by a Model 2 IGA FFI or Participating FFI are due to the IRS by March 31 (with an option to an extend).

1.4.3) Foreign Financial Institutions

FATCA obligations apply to all non-US entities, which fall within the definition of an FFI. These are:

- Custodial Institution
- Depository Institution
- Investment Entity
- Specified Insurance Company
- Treasury Center and Holding Companies (in certain cases such as for Participating FFIs)

The FATCA regime requires FFIs to perform due diligence and reporting obligations with regard to identifying and reporting Specified US Persons to the IRS on an annual basis in respect of financial accounts held by such persons. The regime came into effect on July 1, 2014 and reporting is required in respect of relevant financial accounts from that date.

1.4.4) Reporting by Foreign Financial Institutions

Certain categories of FIs that are regarded as Reporting FIs are obliged to register with the IRS in order to obtain a GIIN and submit annual reports. Certain categories of FIs that are regarded as Non- Reporting FIs generally are not obliged to register with the IRS in order to obtain a GIIN and do not submit reports. Such Non-Reporting FIs may have certain other modified due diligence requirements. The categories and definitions of Reporting FIs and Non-Reporting FIs can vary between US FATCA regulations, and between each IGA jurisdiction. One common form of Non-Reporting FI is a discretionary investment advisor that does not maintain financial accounts for its customers.

Model 2 IGA FIs and Participating FIs are required to have an individual designated as a Responsible Officer who oversees FATCA compliance and submits recurring certifications to the IRS as to the status of such FATCA compliance program. Model 1 IGA FIs, though not required to designate a Responsible Officer nor make regular compliance certifications to the IRS, may still wish to designate an individual with a similar role to that of a Responsible Officer to oversee their compliance program though on an optional basis.

1.4.6) CRS Background and Overview

On July 15, 2014, the council of the OECD approved a new Standard for the Automatic Exchange of Financial Information in Tax Matters ("**AEoI Standard**"). This AEoI Standard comprises the Competent Authority Agreement ("**CAA**") and CRS, and includes Commentaries and various Annexes. Together these are the agreements for automatic exchange of information on taxpayers' financial assets and income outside their country of tax residency (sometimes called 'home country'), including bank accounts. It calls on governments to obtain detailed information from their domestic financial institutions about such accounts and to exchange this automatically with other jurisdictions on an annual basis. The G20 endorsed this AEoI standard and requested all countries to participate.

CRS came into operation on 1 January 2016 in all early adopting jurisdictions including EU Member States. Over 100 jurisdictions have signed up to CRS which imposes obligations on FIs to collect and review information in an effort to identify an account holder's tax residence in a participating country and then in turn, to provide certain specified account information to the home country's tax administration on an annual (or more frequent) basis.

Where the FI is resident in an early adopting jurisdiction, they are required to identify and confirm the tax residence status of all new account holders from January 1, 2016. This requirement operates alongside the current requirement to identify and confirm the status of account holders under FATCA. It is also necessary to undertake due diligence with respect to pre-existing accounts (i.e. accounts opened prior to January 1, 2016) by December 31, 2016 or December 31, 2017 (depending on the type of account holder, and dates occasionally vary by jurisdiction). From January 1, 2016, FIs are required to update account opening documentation to include tax

self-certifications as part of that process. Many jurisdictions have adopted the wider approach under CRS, which means FIs must report all reportable account holders to their local tax authority (not just those located in participating jurisdictions). Depending on the account holder's tax residency and whether it is a participating jurisdiction, the local tax authority will decide which account holders to further report to the relevant jurisdiction.

There is no single source IRS style registration for CRS reporting and, as a result, there are no GIINs or other registration numbers issued to FIs. Each local tax authority may issue its own requirements for obtaining a unique identification number for CRS purposes (as a GIIN may not always be appropriate to use for CRS).

Similar to FATCA, CRS contains a category of Non-Reporting FIs. However, these FIs may receive slightly different treatment than under FATCA resulting in categories of Non-Reporting FIs under FATCA that are Reporting FIs under CRS. Non-Reporting FIs may have certain modified due diligence requirements.

1.4.7) Information Collected, Reported, and Exchanged under AEoI

The below list is a non-exhaustive example of information that may be collected about account holders on their self-certification forms as well as information that may be reported if the account is determined to be a reportable account under FATCA or CRS:

- Name;
- Address;
- Jurisdiction(s) of tax residence;
- TIN in jurisdiction(s) of tax residence;
- Date of Birth;
- Place of Birth;
- Account Number;
- Personal details such as those outlined above for reportable controlling person(s) (or substantial owners in the case of FATCA) in the case of an account held by an entity that is required to disclose those persons;
- The account balance or value at the calendar year end (or other measurement period);
- Payments made to the account in the period must be reported though the types of payments to report depend on the type of FI that is required to report
- Currency in which each amount is denominated;
- Where an account was closed during the year, the closure of the account

About PwC

At PwC, our purpose is to build trust in society and solve important problems. It is this focus which informs the services we provide and the decisions we make. Demonstrating genuine leadership is more important to us than size or short-term revenue growth. To achieve our aim to be recognized as "the leading professional services firm," we must be innovative, responsible and attract outstanding people. Our strategy is therefore built around five priorities: 1. be technology enabled; 2. deliver exceptional value to our clients; 3. empower our people; 4. lead by example; 5. invest in sustainable growth.

As one of the most integrated advisory firms, PwC can assist financial institutions streamlining GDPR compliance by leveraging processes required pursuant to KYC/CFT/AML and AEoI to design a fully compliant, efficient and sustainable business model around customer information.

Contact the Authors

Robert Jan Meindersma – Director, Tax
+31 683608441
robert.jan.meindersma@pwc.com

Jessalyn Dean – Senior Manager, Tax
+31 651123821
jessalyn.d.dean@pwc.com

Saba Ullah – Senior Manager, GDPR / AML
+31 887922848
saba.ullah@pwc.com