Know Your Customer

White Paper

European KYC regulations and their impact on the compliance function

knowyourcustomer.com

Foreword*

When thinking of the world of financial regulations over the past few years, one of the first things that come to mind is the series of scandals of alleged money laundering that have dominated newspaper headlines around the world.

For many financial institutions, the last couple of years of the decade represented a reality check about the penetration of laundered money in their operations, brought about by extensive investigations by regulatory bodies.

With this white paper, we aim to take a closer look at each of the main anti-money laundering regulations that either came into force before 2020 or are currently on the horizon in the European Union.

Our objective was to analyse what all of these pieces of regulation had in common and how they are collectively changing the compliance function as we know it. Additionally, in light of the recent coronavirus pandemic, we have no doubt that a new wave of regulations – which will include clear indications regarding digital and remote onboarding best practices – is just around the corner.

Happy Reading!

Claus Christensen
CEO, Co-Founder
Know Your Customer

* A version of this white paper was first released in 2019. The current version has been updated to reflect some of the effects of COVID-19.

Index

1. Introduction

1.1 Introduction to the white paper

Global attention to money laundering and financing of terrorism has grown exponentially in recent years. As criminals find new tactics, global financial regulations constantly evolve to try and keep up. In this new environment, businesses face **increased risks of penalties and reputational damage** if they are not equipped to replace their long-established manual processes and adapt their internal procedures to the new status quo.

At the same time, the world has become a much more interconnected place where companies that want to expand beyond their home market can do so without needing a physical presence on the ground. However, with every new jurisdiction come different regulatory requirements which no financial institution can afford to overlook. In this new, ever-evolving landscape, European regulations have played a key role in leading the way for the rest of the world to follow.

Over the past few years, high-profile cases of alleged money laundering at banks have increased the general public's and the regulators' attention on the penetration of illicit funds and fraud into European societies, so it is likely that the existing requirements will be continuously adjusted as the institutions' knowledge of these criminal practices deepens. To add a further level of complexity, not only the evolution of customer expectations is adding new pressure on organisations to deliver seamless, fully digital and mobile experiences, but the unprecedented situation determined by the coronavirus pandemic is also accelerating the pace of digital transformation in KYC compliance.

In this white paper, we take a closer look at the key financial regulations that came into force in the European Union in the last few years, focusing in particular on the impact of such regulations on **customer onboarding**, **Know Your Customer (KYC)** and **anti-money laundering (AML)** requirements for financial institutions either based or operating in Europe.

Readers will gain a better understanding of the key trends underpinning the evolution of KYC regulations in Europe as well as be presented with tangible examples of how a digital-first approach can foster international growth while ensuring full KYC regulatory compliance across multiple jurisdictions.

1.2 The rising tide of regulations

To truly understand the rise of financial regulations in Europe, it is important to consider the macro-economic and geopolitical context that preceded their introduction.

The decade from 2007 saw the world – and the European region in particular – being swept by what later became known as the **Global Financial Crisis** and the **Great Recession** that followed it. As countries got into a recession with tangible economic consequences, a large part of the general population struggled to understand the mechanisms that got their national financial systems in trouble in the first place. As a corollary to the growing mistrust in corporations, people started to feel the need for more transparency on how their personal data was being stored and used by companies.

At the same time, news stories such as the Panama and Paradise Papers propelled general awareness about the extensive penetration of money laundering practices in our societies. Finally, tragic terrorist attacks renewed the urgency of introducing extensive strategies to prevent terrorism financing across jurisdictions.

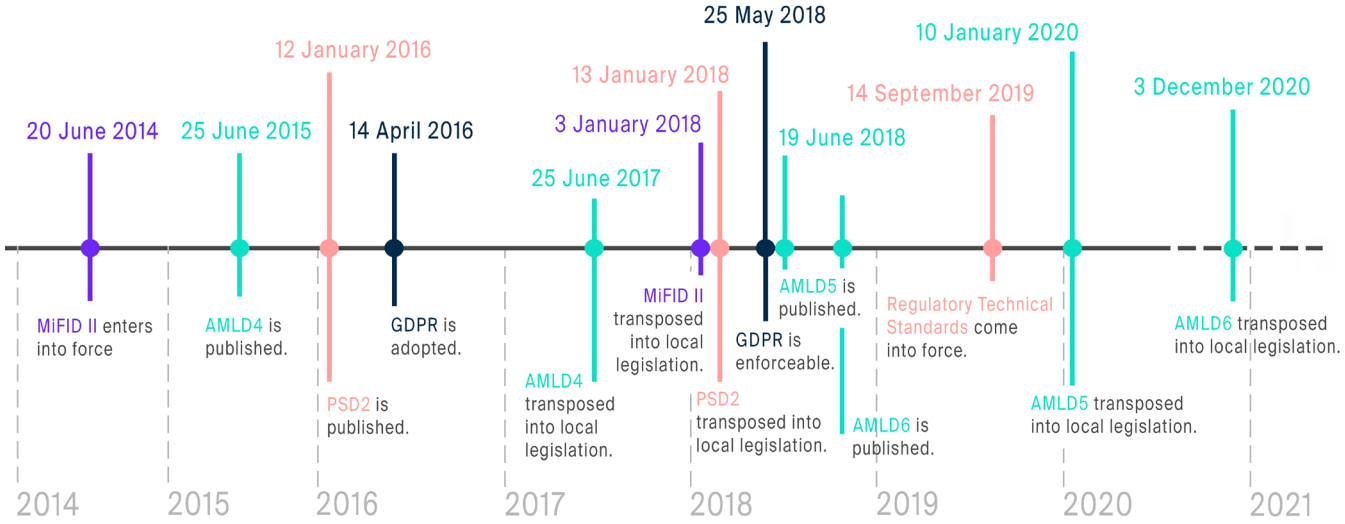
The regulations analysed in this white paper were all introduced to address one or more of the general issues the financial sector has been facing for the past ten years. In particular:

- The **Fourth, Fifth & Sixth Anti-Money Laundering Directive (AMLD4, 5 & 6)** are aimed at counteracting the extensive penetration of money laundering in our societies by introducing more thorough checks and better cooperation between countries, as well as harsher criminal liabilities;

- The **Payments Services Directive (PSD2)** was introduced to stimulate customer-centric innovation in banking, with a focus on preventing payment fraud and misuse of electronic financial tools;

- The updated **Markets in Financial Instruments Directive (MiFID II**) was primarily driven by the need for more transparency in financial investment operations;

- The **General Data Protection Regulation (GDPR)** was the EU's response to the general public's request to regain control over personal data.



The timeline above showcases at a glance how the European regulatory landscape has changed over the past few years, with a growing number of regulations coming into force in quick succession.

1.3 The new role of compliance

Historically, the role of **risk and compliance professionals** has always been the one of the **gatekeepers** who would put processes in place to protect the organisation against damaging individual behaviour, hefty regulatory fines and reputational consequences. In this new, stricter regulatory environment, this role has become even more fundamental.

In particular, the growing risk of economic and reputational repercussions has been pushing the compliance function closer to the **centre of the business structure**. The approach to compliance is ceasing to be an afterthought or a "tick the box" exercise, becoming more proactive and strategic.

With multiple regulations coming into force in quick succession, compliance professionals have found themselves in need of a **more flexible and dynamic approach to their function**, one that would allow for prompt changes to adapt to the new requirements as they are introduced.

The sheer scope of the new regulations has also made it mandatory for compliance teams to work with a variety of departments at their organisation. In particular, **a close collaboration with the IT function** is necessary to ensure that existing company policies are reflected by the procedures in place and respected by all team members. In 2020, the coronavirus crisis has further increased the need for collaboration between these two departments. To ensure business continuity for financial institutions, it is essential that compliance ceases to be a primarily office- and paper-based function to become a digital and remote activity.

In the following chapters, we will conduct **an analysis of the most important financial regulations introduced in Europe over the past few years**. We will take a closer look at how legal and risk teams have been driving change across their organisations working with multiple stakeholders to review operational workflows, update technological infrastructures and propose a new approach to compliance.

2. Anti-money laundering

2.1 An overview of AMLD4, 5 & 6

AMLD4 IN EUROPE AND BEYOND

When the **Fourth Anti-Money Laundering Directive** came into force on 26 June 2017, it had been 12 years since the introduction of its previous iteration, back in 2005. With the AMLD4, which puts in place a comprehensive regulatory framework, the EU confirmed its role as a global leader in anti-money laundering requirements. The key innovations of the AMLD4 included the **institution of a central registry for beneficial owners** as well as changes to customer due diligence requirements. Additionally, special emphasis was given to the so-called "risk-based approach", with financial institutions being required to put in place and start following comprehensive risk-based policies.

AMLD4 at a glance

Official Name: Directive (EU) 2015/849

Published on: 25 June 2015

Deadline for transposition into local legislation: 26 June 2017

Who AMLD4 applies to: Financial Services, Real Estate, Lawyers, Trusts, Accountants & Tax Advisors

The impact of AMLD4 was felt well beyond the European Union's borders. For instance, the directive clearly states that firms with majority-owned subsidiaries located in countries where the minimum AML requirements are less strict than the EU ones should implement the EU requirements at those subsidiaries as well.

THE INTRODUCTION OF AMLD5

Roughly a year after the enactment of AMLD4, the EU released its successor, AMLD5 (the 5th Anti-Money Laundering Directive). Published on **19 June 2018**, the directive should have been transposed into local legislation by **10 January 2020**. However, a few member states were behind in implementing the new measures even before the outbreak of COVID-19, which is bound to delay the process even further.

AMLD5 mostly adds to the earlier iterations of the directive, instead of overhauling them. In particular, AMLD4's framework for identity verification, AML and KYC procedures for financial institutions is mostly untouched. Its scope is extended (art dealers, for instance, are required to run AML and KYC checks on any customers buying or selling items with a value of €10K or more), but its **real targets** appear to be the **governments of member states**.

For instance, AMLD5 mandates that **access to public beneficial ownership registers** – which were first introduced by AMLD4 – should be **extended to members of the public** across the EU, with the declared aim of allowing for "greater scrutiny of information by civil society, including by the press or civil society organisations".

AMLD5 at a glance

Official Name: Directive (EU) 2018/843

Published on: 19 June 2018

Deadline for transposition into local legislation: 10 January 2020

Who AMLD5 applies to: Same as AMLD4 + Gambling, Virtual Currencies, Art Dealers

Following the same spirit, AMLD5 requires countries to **set up national beneficial ownership registers for trusts**, which have historically been a popular place to hide beneficial ownership from prying eyes thanks to their very opaque nature. Information about trusts should only be publicly accessible when there is a "legitimate reason" for requesting it, but nonetheless this is a big step and a clear sign of the EU's commitment to better transparency.

MORE CLARITY ON PEPs

Another measure introduced by AMLD5, and aimed at governments more than financial institutions, is the requirement for European countries to **specify what they mean by a 'PEP' (Politically Exposed Person)** in a centralised register. One possible outcome of this requirement is a reflection by governments on their criteria for including certain people in their PEP lists. For instance, should the mayor of a small town in Germany be considered a PEP in the same way as the husband of German Chancellor Angela Merkel? The objective of AMLD5 is to force governments to clear up this haziness.

MORE ATTENTION TO DIGITAL

Other areas AMLD5 touches upon are the **threshold** for identifying the holders of **prepaid cards** (lowered to EUR 50 in the case of payment transactions from outside the EU) and the extension of the directive's scope to include **virtual currencies**, to be monitored by competent authorities.

Finally, what can arguably be considered the most revolutionary aspect introduced by AMLD5 is that it explicitly allows for **eIDAS**, the electronic signature standard in the EU. Up until now, the uncertainty around the need for physical signatures has represented one of the biggest blockers to a full digitisation of the customer onboarding process for financial institutions.

Once the directive is transposed into law across all member states, financial institutions will be able to fully **digitise all the KYC forms** of their onboarding processes.

THE LAST PIECE OF THE PUZZLE: AMLD6

Only four months after the publication of AMLD5, the European Parliament published the 6th iteration of its Anti-Money Laundering directive to complete the legislative framework and strengthen member states' ability to fight financial crime.

In particular, the latest directive extends the scope of criminal liabilities and entities with an updated list of predicate offences (e.g. crimes that are a component of a more serious crime) and introduces tougher penalties for legal persons found guilty of money laundering offences. It also provides a harmonised definition of money laundering offences, with the objective of removing loopholes across the bloc's member states.

AMLD6 at a glance

Official Name: Directive (EU) 2018/1673

Published on: 23 October 2018

Deadline for transposition into local legislation: 3 December 2020

Who AMLD6 applies to: Same as AMLD4 & 5

More specifically, the fourth article of the AMLD6 indicates that aiding, abetting, inciting or attempting a money laundering offense will all be punishable crimes under the new rules.

Explicitly including the role played by "enablers" among the punishable offences will allow European legislators and law enforcement to combat the spread of money laundering and terrorism financing more effectively.

2.2 The impact of AMLD4, 5 and 6 on compliance

COMPLIANCE TEAMS & AMLD4

The introduction of AMLD4 forced most financial organisations to review their existing risk policies and internal procedures to ensure compliance with the new requirements. By introducing greater administrative sanctions for breaches, **AMLD4 increased the pressure on risk & compliance teams** to design and implement internal processes that would meet all the new criteria. In particular, under the new directive, companies could be **fined twice the amount of the benefit generated**[1] by a specific money laundering breach, which puts the company at great risk from both a financial and a reputational point of view. With the introduction of tougher punishments and the extension of criminal liability to legal persons, AMLD6 further increased the pressure on compliance professionals to tighten company policies and procedures.

The new **risk-based approach** requirements forced many organisations to introduce different rules and journeys – during and after onboarding – for low vs high risk customers. The use of a **simplified vs enhanced due diligence framework**, at least initially, increased the workload of compliance teams across Europe, especially when they found themselves tackling new challenges through legacy strategies. When done manually or through disparate systems, the implementation of a risk-based strategy consumes an extreme amount of time and resources. To address this challenge, numerous organisations chose to introduce a technology solution during or right after reviewing their internal procedures, to lighten the burden of manual work on compliance teams.

WHAT TO EXPECT FROM AMLD5 AND 6

Most changes introduced by AMLD5 refer to the Member States' governments more than to individual organisations. However, the clear guidance provided by the directive on the use of **electronic signature** – together with the current focus on digital procedures in light of social distancing measures - is likely to boost a further digitisation of contract signing and due diligence steps for the financial sector. Additionally, the fact that **virtual currency exchanges** will now be under closer scrutiny is likely to have a **stabilising impact** on this kind of companies.

In the case of AMLD6, the key impact will probably be felt in relation to the new risks for compliance staff and individual executives determined by financial instutions' AML oversight. It is to be expected that explicitly including the role played by "enablers" among the punishable offences will drive numerous financial institutions to pay even more attention to compliance policies and procedures at every level of the organisation, introducing **"compliance by design" technologies and processes** and conducting more frequent and thorough internal audits.

3. Payment services and open banking

3.1 An overview of PSD2

NEW LANDSCAPE, NEW NEEDS

The original **Payments Services Directive (PSD)** was created in **2007** by the European Commission with the aim to create a single market for payments in the European Economic Area. After ten years, the needs and capabilities of the market had changed so much that it was time for an update on the existing regulations. The process wasn't an easy one; the proposal for review, made in 2013, was accepted in late 2015 and the final directive was published only in 2017.

FOSTERING INNOVATION & COMPETITION

Although regulations might rarely be associated with innovation, that is not the case for PSD2. In fact the directive's objective was to **drive competition** between European banks and new payment service providers.

Numerous new FinTech players[2] are taking the banking and payments world by storm, disrupting the industry by focusing on **customer-centric services and seamless experiences** delivered through mobile devices. If, before PSD2, larger banks could retain a critical competitive advantage as the only ones able to view or process payments information on their customers' accounts, that is not the case anymore.

PSD2 at a glance

Official Name: Directive (EU) 2015/2366

Date of entry into force: 12 January 2016

Deadline for transposition into local legislation: 13 January 2018

Date of entry into force of the Regulatory Technical Standards: 14 September 2019

Who PSD2 applies to: banks, payment service providers

THIRD-PARTY PROVIDERS

More specifically, under PSD2 bank customers can choose to use **third-party providers** to manage their finances and banks are obligated to provide access to their customers' accounts through open Application Program Interfaces (APIs). Each third-party provider is classified as either an **AISP (Account Information Service Provider)** or a **PISP (Payment Initiation Service Provider)**.

As the quite self-explanatory names imply, AISPs have access to the account information of bank customers, which, for example, they can use to analyse spending behaviours and help with budgeting. PISPs, on the other hand, initiate a payment on behalf of the user without the need to provide credit card details with each transaction. PISPs are able to withdraw the money directly from a user's account if they had previously given their consent.

STRONG CUSTOMER AUTHENTICATION

One of the most important changes for organisations' compliance processes refers to **Strong Customer Authentication (SCA)**, which came into force on 14 September 2019, as stated in the European Banking Authority's Regulatory Technical Standards (RTS)[3].

To comply with the SCA rule, payment transactions processed within the EU – excluding a restricted number of exceptions to allow for "frictionless flow" – require the customer's identity to be verified using at least 2 of the following:

Something the user KNOWS

- **Password**
- **Passphrase**
- **Pin**
- **Secret fact**

Something the user HAS

- **Mobile phone**
- **Wearable device**
- **Smart card**
- **Badge**

Something the user IS

- **Fingerprints**
- **Facial features**
- **Voice patterns**
- **Iris format**

3.2 The impact of PSD2 on compliance

THE ADVANCEMENT OF OPEN BANKING

PSD2 has the potential to have a **sensible impact on the payments sector** as a whole. By advancing open banking across Europe, it is likely to create an environment where banking as we know it might change drastically. According to a PwC study[4], 2 out of 3 European banks intend to use PSD2 to change their strategy, with the majority of European banking executives saying that PSD2 will impact all of their core banking operations.

The first and most immediate steps banks have taken is to build their APIs and provide useful resources – such as API Developer Portals or API Landing Pages – to help developers at third-party companies build new applications as stated under the regulation.

RISING COMPLIANCE COSTS

The consequences of the regulation for banks' compliance teams are not to be underestimated. As an example, a large European bank with a global presence recently estimated its **PSD2 compliance costs** at around **€35 million**[5], plus another €15 million for expenses not related to compliance specifically, such as the ones connected to gaining third party provider status.

IMPLEMENTING SCA REQUIREMENTS

One of the specific requirements that has certainly kept compliance teams – and their IT departments – busy is the one of Strong Customer Authentication. Any organisation in the e-commerce and payments space had to review their existing systems to include SCA methods, but without sacrificing the smooth digital experience that customers had now come to expect.

The new requirements also have clear **implications for the KYC process**. More and more organisations have started combining the traditional collection of KYC information and the set-up of **multi-factor authentication credentials** within the same digital journey. This helps ensure optimal customer experiences and reduce the risk of drop-offs which occurs when the customer onboarding journey is divided into multiple steps, at different times.

Those payment service providers that have been able to find the least intrusive formula for SCA are likely to reap huge benefits going forward. At the same time, although it might take a while for consumers to get used to multi-factor authentication, the need for measures to prevent card fraud – which isw estimated to reach $31.67 billion in 2020 from $16.31 billion in 2015[6] – is hard to deny.

4. Investing and trading

4.1 An overview of MiFID II

MiFID & MiFID II

The original **Markets in Financial Instruments Directive (MiFID I)** was introduced on 1 November 2007 with the aim of creating a level playing-field for firms to compete in the European Union's financial markets and to ensure consistent consumer protection across the board. Eleven years later, on **3 January 2018**, it was replaced by a revised regulation, aka MiFID II. The MiFID II legislative package includes the **MiFID II Directive** and the **Markets in Financial Instruments Regulation (MiFIR)** together with related delegated acts and guidance, all of which must be read together.

ONE GUIDING PRINCIPLE: TRANSPARENCY

To reinforce the integrity of the financial system and restore confidence by preventing some of the abuses emerged during the Global Financial Crisis, the MiFID II is centred on the key **principle of transparency**.

It applies to all investment firms, wealth managers, broker dealers, product manufacturers and credit institutions within the EU as well as third-country firms providing investment services in Europe.

Under MiFID II, financial institutions are required to **keep their investors much more informed**, whether that is about pricing, product or process.

MiFID II at a glance

Official Name: Directive 2014/65/EU

Date of entry into force: 20 June 2014

Deadline for transposition into local legislation: 3 January 2018

Who MiFID II applies to: : investment firms, market operators and data reporting service providers, credit institutions

At the same time, organisations are now expected to know a lot more about their prospective clients and their assets than they used to. There is now a need for extensive documentation around **suitability and appropriateness checks** and **client assets management**, which introduces new KYC requirements for companies' compliance teams.

In fact, under MiFID II financial institutions are required to take into consideration **clients' risk tolerance** and **ability to bear losses** before entering into a business contract with them.

As such, organisations are now expected to collect a much larger amount of KYC information during customer onboarding, which translates into **a lot more data to process** and **specific customer journeys** to devise to reflect the new criteria.

UNDERSTANDING YOUR DATA

One of the defining elements of the global financial crisis was the **lack of understanding** from financial institutions of the **financial products** that were being sold to their clients, as the subprime mortgage crisis so tragically exemplified. To prevent history from repeating itself, MiFID II requires companies to better understand their data, analyse it, report on it and track the decision process to ensure that the available information has been taken into consideration every step of the way.

As a related consequence, under MiFID II **algorithmic and high frequency trading** is much more regulated, and firms are expected to have resilient systems and appropriate risk controls in place. At the same time, MiFID II requires **more comprehensive transaction reporting** for a much wider range of financial instruments.

A LARGER SCOPE

Similarly to AMLD5 extending its scope to more sectors such as art dealers, MiFID II **expands the range of commodity derivatives** under its scope, while significantly narrowing exemptions for firms dealing in this type of derivatives.

4.2 The impact of MiFID II on compliance

FAR-REACHING CONSEQUENCES

The impact of MiFID II is as widespread as it is deep, ranging from the overall functioning of European financial markets to the internal processes of organisations.

To put things into perspective, a report by Expand - a Boston Consulting Group company - and IHS Markit[7] revealed that financial organisations spent an estimated total of $2.1 billion on MiFID II preparations.

A NEW NEED FOR INNOVATION

As previously noted, the introduction of major pieces of regulation brings opportunities for review and innovation across financial institutions.

In particular, to meet the transparency requirements of MiFID II, most organisations found themselves in need of replacing legacy technology solutions with more powerful end-to-end alternatives able to deal with the complexities of the new regime.

Under MiFID II, every stage of a transaction, from front-office order-taking to back-office reconciliation, should be consistently recorded and explained, as well as be clearly accessible by the customer.

NEAR-REAL TIME REPORTING

Under MiFID II, the National Competent Authority (NCA) must be informed of any transaction no later than one day after it occurred. In the case of trades conducted at a trading venue, MiFID II mandates near-real time reporting, a requirement which could not be met without the use of technology.

NEW KYC REQUIREMENTS

When devising Know Your Customer procedures under MiFID II, compliance teams should pay particular attention to the new criteria for the suitability & appropriateness assessments of both existing and perspective clients as well as the ones for client classification. Dealing with such a large amount of diversified data becomes an almost impossible feat if approached with a traditional strategy.

Risk professionals that are successfully protecting their organisations from the risk of non-compliance tend to walk away from multiple, disconnected systems to embrace a more harmonised approach powered by innovative solutions.

5. Data privacy

5.1 An overview of GDPR

UNPRECEDENTED MEDIA ATTENTION

Few legislations have gained as much media attention as the **General Data Protection Regulation (GDPR)** has in 2017 and 2018. People who would usually not be involved in compliance matters – such as small business owners sending out a monthly newsletter – found themselves having to navigate the seemingly impenetrable world of EU regulations while the GDPR was heralded as the **most important change in data privacy regulation in twenty years**[8].

Compared to the rest of the directives analysed in this white paper, GDPR is a Regulation and, as such, it did not need to be transposed into local legislation before becoming applicable from **25 May 2018**. Its scope is also extensive, as it applies to all organisations located within the EU as well as any organisations located outside of the EU which collects or processes the data of individuals within the European Economic Area.

REGAINING CONTROL OF PERSONAL DATA

The Regulation was primarily introduced to help individuals **regain control over their personal data**, following the exponential growth of data-driven applications introduced by organisations over the last few years.

GDPR at a glance

Official Name: REGULATION (EU) 2016/679

Adopted on: 14 April 2016

Enforcable from 25 May 2018

Who GDPR applies to: : Any organisation collecting or processing data from EU residents

Once again, the principle underpinning the new rules is **transparency**; this translates into more straight-forward conditions for consent (it should made clear what exactly individuals are consenting to when sharing their data) as well as the ability to withdraw consent swiftly; at the same time, the GDPR gives citizens the **right to access** their personal data and request details about how it is being processed by a specific organisation, as well as the **right to be forgotten**, which means requesting the complete erasure of personal data related to them.

THE NEW ROLE OF THE DPO

Under the GDPR, those organisations where data processing involves regular and systematic monitoring of individuals on a large scale should appoint a **Data Protection Officer (DPO)**.

The selected DPO, whether a member of staff or an external consultant, should not only have **extensive**

knowledge and experience of data protection laws but also possess a **good understanding of current IT processes and data security**.

Organisations based **outside the European Union** are also required to appoint an EU-based individual as a point of contact for their GDPR obligations.

HOW TO DEAL WITH DATA BREACHES

Last but not least, any data breaches should be reported to the supervisory authority within **72 hours** of when the organisation became aware that they occurred.

If the data breach involves personal data that could have a negative impact on individuals, this should be **promptly communicated to the affected parties**.

5.2 The impact of GDPR on compliance

THE IMPORTANCE OF DATA MAPPING

Because of the **pervasive nature of data** in the operations of today's organisations, ensuring compliance with the GDPR requires **extensive collaboration** between different departments, including – but not limited to - legal/risk, IT and marketing.

In particular, when first reviewing existing internal operations, the involvement of the IT team was absolutely necessary as they typically have the most comprehensive and technical understanding of the data infrastructure of their company. It is essential to **map in detail** when and what kind of data is collected from customers, where it is stored, who has access to it (including external data processors), and how it can be shared or erased with the interested party might the need arise.

REVIEW AND CENTRALISATION

Once the data was mapped, IT teams worked with their colleagues in compliance to **review the existing flow of information** and, where needed, **centralise different data sources**. For instance, avoiding duplications of personal data helps organisations act efficiently when a customer requests for their data to be erased from their system.

Such implementations do not come at a small price, especially for large organisations. An analysis from Sia Partners[9], for examples, estimates the cost of GDPR compliance for FTSE 100 at €16.7 million (£15 million), with banks being the group with the highest expected spend.

PSD2 AND GDPR SYNERGIES

This process of review, centralisation and updating of systems was an extremely onerous process which involved a variety of stakeholders. This is especially true for those organisations in the banking and payments space that are also subject to PSD2, which came into force in early 2018 as well.

Both regulations are aimed at giving customers more control over their personal data and compliance teams often reviewed the two in tandem, devising new internal processes that would meet all requirements.

KYC/AML AND THE GDPR

From a KYC, AML and customer onboarding point of view, the key concern for relating to the GDPR for compliance teams include the ability to r**etrieve and share all the information** that their company holds on a specific user, the execution of customers' right to be forgotten, as well as the **encryption of information** and the **compliance of their data processing** when using third party solutions.

For those organisations already using an external system for their KYC and AML checks, this meant working closely with their vendor to ensure that all GDPR requirements were taken into consideration. For companies still relying heavily on a **manual or semi-manual approach**, that often meant starting to bring their procedures into the digital realm.

GDPR DURING THE COVID-19 CRISIS

During the COVID-19 crisis, legislation has slightly expanded businesses' ability to process customers' and employees' personal data in the name of **health and safety**, but this is not a limitless ability and defined boundaries are still in place. More specifically, organisations that limit the collection of information to what is **strictly necessary** for the purpose at hand will reduce the risk of incurring in non-compliance fines once the storm has passed.

6. Conclusions

6.1 A new compliance status quo

UPDATING THE 19TH CENTURY APPROACH TO COMPLIANCE

Over the last few years, we have witnessed the first phase of a much needed **transition in the approach to financial regulations** in Europe. Thanks to the newly introduced requirements, the financial sector has finally started moving from a 19th Century, paper-based understanding of the compliance function to one better suited to address the challenges of the 21st Century.

Specifically, the new regulations take into consideration the **commodity value** that **data** has in today's world. Information in the digital realm isn't simply a virtual note of something that exists in the physical world, but it has become something completely different.

MANY REGULATIONS, SAME PRINCIPLES

Although different in their scope and application details, all the regulations that we have analysed in this white paper appear to be underpinned by a few key principles. First, most of them aim to tackle the historic **power imbalance** between consumers and companies. In practice, this translates into new rules that give customers more power over who gets to access their data and how that data can be used, including to manage their finances and investments.

Information in the digital realm isn't simply a virtual note of something that exists in the physical world.

Another fundamental principle is **transparency**. Whether it's a matter of providing clearer information about financial investments to clients, creating official registries to better understand companies' ownership structures, or giving access to the data that a certain company holds about us, the efforts of the new regulations towards transparency is unequivocal.

WHAT TO EXPECT

The times we live in are undoubtedly characterised by **incremental and unstoppable change** in our approach to compliance, partially fostered by rapid advancements in technology and closer cooperation between regulators. In this environment, it isn't easy to venture predictions. However, there are some key trends we expect to see confirmed in the near future:

- The **EU** has been **leading the way** regarding AML and customer onboarding requirements in the financial sector. In the immediate future, we expect more jurisdictions – especially in Asia – to introduce similar regulations.

- As exemplified by PSD2 and AMLD5 in particular, we expect the **scope of AML/KYC requirements** to be **extended** to a greater variety of businesses and sectors, well beyond the realm of traditional regulated industries.

- The **role of compliance** will become even more **strategic**, as their knowledge of regulatory requirements will be sought after to ensure business processes and IT implementations are compliant and cost-effective. To maintain organisations' **competitive advantage** in a world of growing operational costs, compliance teams' expertise is increasingly fundamental to shape business processes from the very beginning, finding solutions that are both efficient and fully compliant.

- Increased user expectations will lead more and more financial institutions and, as the requirements expand to more sectors, organisations in general to **turn to automation**. Automation's strength is its ability to quickly and consistently scale the efforts needed to enforce compliance procedures across different organisations and geographies in a way that limits frictions in the user journey. This is a fundamental ingredient for **commercial and operational success** in the era of growing financial regulations and demanding customer expectations.

- Finally, the recent and unprecedented situation caused by the **COVID-19 outbreak** has accelerated existing **digital transformation trends** of the compliance function. For reasons of public safety as much as business continuity, financial institutions need to swiftly implement effective and secure **RegTech solutions** to empower their teams to work remotely and continue to onboard new customers safely.

6.2 Embracing the power of automation

THE TIME FOR AUTOMATION IS NOW

Embracing the power of technology and automation is a process that always takes time and effort, whichever department or organisation it involves. When the **digital transformation journey** is embarked on by multiple stakeholders working remotely in the midst of a global pandemic, the complexities increase.

As the analysis conducted in this white paper highlights, the recent changes in regulations, together with the steep penalties and reputational damage caused by non-compliance and the additional hurdles to paper-based procedures determined by the COVID-19 emergency, make the **traditional manual approach** to KYC/AML and customer onboarding **not financially viable** anymore.

As daunting as the implementation journey may seem, compliance technology and automation solutions have the potential to rapidly scale compliance teams' efforts while future-proofing the overall business against new potential emergencies.

THE GROWING REGTECH MARKET

For the past few years, the RegTech industry has been specialising in providing regulatory technology solutions to organisations looking to reap the benefits of compliance automation.

According to a Forrester report[10], global investment in RegTech companies reached **$4.6 billion** in the first three quarters of 2019. This represents a year-over-year **growth rate of 103%**.

Global investment in RegTech companies reached $4.6 billion in the first three quarters of 2019.

Evidently there was no lack of awareness among investors regarding the potential of the RegTech sector. However, the coronavirus pandemic has further demonstrated the strategic importance of remote onboarding solutions to ensure business continuity in times of crisis. As a result, investment in RegTech is likely to increase even further in 2020.

As the number of available options grows, compliance teams should thoroughly investigate which vendors offer the solutions that are best-suited to address their specific challenges, while also providing the following:

- **Regulatory compliance** – Compliance expertise and deep knowledge of local financial regulations should be built into the system's workflows to accelerate implementation.

- **Flexibility** – This is key to adapt to new regulations as they are introduced or as the organisation expands into new markets.

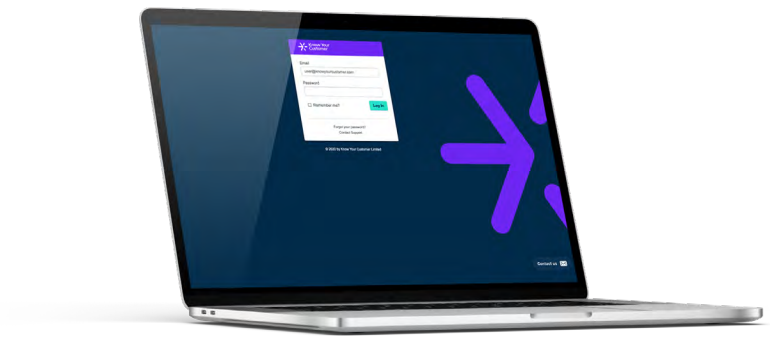
- **Seamless customer experiences** – As consumers' expectations evolve, so should the customer onboarding experience that organisations are able to deliver.

- **Ability to integrate multiple legacy systems** – Harmonising multiple systems through a dynamic solution is fundamental to ensure the success of any digital compliance strategy.

Times of transitions rarely come without challenges, but by partnering with the right RegTech provider financial institutions can start reaping the numerous benefits of automation before their competitors.

KNOW YOUR CUSTOMER'S TECHNOLOGY

At Know Your Customer, we specialise in providing scalable, flexible and dynamic onboarding solutions for financial institutions that are serious about compliance. Our technology enables organisations to ensure **on-going AML compliance**, replacing time-consuming manual processes and disconnected systems that put their business at risk with a centralised and more efficient approach to client onboarding.



Our horizontal, end-to-end digital solutions empower compliance teams to centralise the four pillars of client onboarding within one solution. These include:

1. Document Collection
2. Data Extraction and Assessment
3. On-Going Monitoring
4. Reporting & Analysis

Through a unique combination of Machine Learning, Optical Character Recognition and Automation, our system – which can be quickly integrated with existing infrastructures through robust APIs – revolutionises the essence of customer onboarding, making it better, faster and stronger.

ABOUT KNOW YOUR CUSTOMER

Established in 2015, Know Your Customer is a global RegTech company with offices in **Hong Kong**, **Dublin**, **Singapore**, and **Shanghai**. Our clients span across 11 sectors – including banking, FinTech, insurance, payments, real estate, asset management, legal, among others – and 18 jurisdictions and are using our technology to verify and onboard customers from more than 180 countries.

Our digital solutions help global financial institutions meet regulatory requirements in Europe as well as comply with monetary authorities' and central banks' guidelines all over the world. To find out more about Know Your Customer, visit knowyourcustomer.com or request a demo here.

Know Your Customer

info@knowyourcustomer.com
knowyourcustomer.com

Know Your Customer
@KYC_ltd

Endnotes

1 https://www.consilium.europa.eu/en/press/press-releases/2015/04/20/money-laundering-strengthened-rules/

2 https://www.nytimes.com/2018/11/20/technology/finance-start-ups-neo-banks.html

3 https://eba.europa.eu/-/eba-publishes-final-draft-technical-standards-on-the-specification-of-an-economic-downturn

4 https://www.pwc.com/gx/en/financial-services/assets/pdf/waiting-until-the-eleventh-hour.pdf

5 https://www.bankingtech.com/2018/11/the-psd2-compliance-clock-is-ticking-but-help-is-at-hand/

6 https://nilsonreport.com/

7 https://www.expandresearch.com/studies/mifid-ii-industry-cost-analysis/

8 https://www.bbc.com/news/technology-43657546

9 https://www.consultancy.uk/news/15101/gdpr-compliance-to-cost-ftse100-firms-15-million-banks-face-largest-bill

10 https://go.forrester.com/predictions-2020