Are PSD2 & GDPR set on a collision course?
Page 4

What does MiFID II mean for Alternative Finance Platforms?
Page 5

PSD2: Opportunities & Challenges for Alternative Finance
Page 8
The countdown to 25 May 2018 is underway, when the EU General Data Protection Regulation ("GDPR") will come into force. As an EU regulation, it will be directly applicable to all EU member states. And because of Brexit, it will be directly applied in the UK by a new Data Protection Act 2018.

The FinTech team at City law firm Fox Williams has prepared a GDPR action list setting out all pertinent actions FinTechs and finance providers should be taking to get themselves ready for this regulatory change. This special report looks at a couple of critical issues: data breach reporting and privacy notices.

**Data breach reporting**

A “personal data breach” refers to any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It may be as a result of a sophisticated hack, or is more likely to be an everyday issue such as falling for a phishing email, or losing a laptop or storage device containing unencrypted personal data.

What the GDPR says:

You must notify the ICO of a data breach without undue delay and where feasible within 72 hours, unless the data breach is unlikely to result in a risk to individuals.

If the breach is likely to result in high risk to individuals, you must also inform data subjects “without undue delay”, unless an exception applies.

Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Action list:

- Make sure you have the right procedures in place to detect, report and investigate a personal data breach.
- Develop (or update) an Incident Response Plan for managing data breaches.
- Set up a personal data breach register to record the facts relating to any breach, its effects and the remedial action taken.
- Put in place a response team including compliance, tech, marketing, PR, financial, legal.
- “Rehearse” the plan to make sure everyone understands what is required.
- Review data breach / cyber insurance and consider if it needs to be updated.
Privacy notices

GDPR will almost certainly require you to update your privacy notices. This would also be a good time to think about designing the customer journey around privacy, putting the customer’s interests first and allowing them to easily understand how their data will be used.

What the GDPR says:

Much of the information to be supplied is the same as under current law, but some additional information must be provided depending on whether you are collecting the information directly from data subjects or from a third party, including details of:

- the data protection officer;
- the legitimate interests relied on, where applicable;
- transfers to third countries and safeguards;
- data retention periods;
- data subject’s rights, including new rights of portability and erasure (right to be forgotten).

Action list:

- Review privacy notices to make sure they include the required additional information.

While there is a requirement for more detail, privacy notices must also be:

- Concise, transparent, intelligible and easily accessible; and
- Written in clear and plain language.

- Consider use of layering (providing brief summary information with links to more detailed information), just-in-time information, privacy dashboards, use of icons etc. as part of a customer journey built around privacy concerns.

About Fox Williams

We provide clear, commercially pragmatic advice on data protection compliance and preparation for the GDPR. We can carry out a comprehensive GDPR readiness assessment, with gap analysis and recommendations to help determine which business processes you will need to review and implement in preparation for the GDPR. We provide strategic advice on:

- Drafting privacy policies, data retention policies, and incident response plans
- Data processing arrangements, including due diligence on vendors, and drafting and negotiating data processing agreements
- Data protection and HR, including drafting staff data protection policies, communications monitoring, recruitment and selection
- Advising on personal rights, including the right to be forgotten, data portability and subject access requests
- International data transfers, including implementation of Model Clauses, Privacy Shield and Binding Corporate Rules
- Compliance with e-marketing and cookie regulations
- Carrying out a data protection impact assessment or compliance audit
- Provision of data protection training to staff
- Dealings with the ICO and other regulatory authorities, investigations and proceedings
- Second opinions and checking post-implementation changes

In the event of a data security breach incident we provide rapid legal support to mitigate legal risk including compliance with reporting requirements, communications to data subjects, service providers and other stakeholders, and handling legal claims. In the event of such an incident, please contact us.

Nigel Miller is a founder partner of Fox Williams LLP and leads the firm’s data protection, privacy and cyber security work. Nigel is a Certified Information Privacy Professional – Europe (CIPP/E).
Nigel can be contacted at nmiller@foxwilliams.com

Jon Segal is a partner of Fox Williams LLP and leads the FinTech and Alternative Finance team.
Jon can be contacted at jsegal@foxwilliams.com
Experts in FinTech

Fox Williams’ specialist FinTech and Alternative Finance legal team delivers commercially focused legal and regulatory advice to innovative businesses, including:

- peer-to-peer lending and direct lending platforms
- equity crowdfunding platforms
- challenger banks
- RegTech businesses
- cyber-security businesses
- platforms and software businesses utilising blockchain technologies

We work with established businesses, financial institutions and start-ups.

“Well versed in market developments and provides very good regulatory and commercial advice to fintech start-ups”
Legal 500, 2017

“Astute, commercial and extremely effective practice head Jonathan Segal is a fintech guru”
Legal 500, 2017

Contact our partners:
Jonathan Segal - jsegal@foxwilliams.com
Nigel Miller - nmiller@foxwilliams.com
Andrew Woolf - awoolf@foxwilliams.com
Chris Finney - cfinney@foxwilliams.com

10 Finsbury Square
London EC2A 1AF
+44 (0)20 7628 2000
info@foxwilliams.com
www.foxwilliams.com
A SPECIAL REPORT FROM ALTFI

Are PSD2 & GDPR set on a collision course?
by Daniel Lanyon of AltFi

The next 12 months will be a testing one for fintechs and established financial institutions as they co-ordinate two new regulations.

Compliance is one area of the jobs markets that won’t be complaining about a lack of wage growth in 2018. A great surge of European regulation will hit financial firms next year hugely impacting workloads and requiring a fine toothcomb for those picking apart the details.

Two regulations in particular will keep the City’s legions of compliance officers busy in 2018: The Second Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR). Both have been a long time coming, are likely to be adopted around the same time and have the potential to clash terribly making an extra digital dilemma for firms.

“Without further guidance banks may need to take a very risk-averse approach and redact all data that could possibly fall into the sensitive data category” –DELOITTE

Under PSD2 Third Party Providers can access customers’ digital footprint in terms of their payment account data. Crucially this will be direct access, as long as firms have explicit consent from the customer. GDPR meanwhile applies to all organisations processing the data created by citizens of the European Union, emphasising the responsibility of firms to protect customers’ personal data and privacy.

Put another way PSD2 will require institutions to open up their data archives and give access to personal information related to customer accounts to third parties but GDPR forbids sharing information with third parties.

No clear path ahead
Confused? You are no doubt the only one but it is worth remembering that laws can quite often interact with each other, however, there is little guidance from the EU as to how the two regulations should co-exist. Not only this but the two regulations also come at the same time as the Open Banking launch likely prompts another wave of disruption to banking services.

Both GDPR and PSD2 are no doubt built on the same honourable principle: individuals own their data. When the idea becomes a reality, however, things get more complicated and could threaten the benefits of PSD2.

Deloitte’s regulatory team in the UK have issued warnings to this effect saying further guidance is needed. This is particularly so in determining what constitutes “sensitive payment data” and who is responsible for obtaining consent.

“This lack of clarity on what constitutes sensitive payment data creates challenges for interpretation and implementation and increases the risk of non-compliance. Without further guidance banks may need to take a very risk-averse approach and redact all data that could possibly fall into the sensitive data category in order to avoid breaching rules around data protection, both under PSD2 and GDPR,” Deloitte said in blog post earlier in 2017.

There is no reason GDPR and PSD2 cannot live in perfect harmony but the devil is in the detail and the potential ramifications are also enormous. Firms in breach of regulations are liable to huge fines. While PSD2 does not mention specific penalties, GDPR has a maximum €20m or 4 per cent of global turnover for companies.

For alternative finance platforms getting the correct balance is challenging owing to their smaller staffs and less established balance sheets. As PSD2 mandates unfettered access to reams of data using APIs, those with existing strict standards of how they manage such information will be at an advantage while those in growth mode will require urgent action.
What does MiFID II mean for Alternative Finance Platforms?

by James Hogbin of IP Sentinel

With the impending launch of MiFID II looming in January 2018, alternative financial platforms are going to have to adjust to the new regulations rapidly.

For those that are smaller in size, the rules on research payments, data security and monitoring, and marketing regulations could cause significant issues, both in cost and in management time.

In short, the second Markets in Financial Instruments Directive is a revamped version of the original MiFID, a framework of EU legislation that will now apply to all regulated financial firms. The update is designed to foster greater security and transparency around pricing in the European investment market, while offering greater protection for investors.

Primarily, the rules will force asset managers to separate out the cost of paying for the research they use to make investment decisions, a process also known as “ unbundling”, ending the opaque system of managers receiving research at a discount in exchange for trades. Most of the large asset management firms have chosen to absorb the cost of research into their own profits, rather than charge it out as an additional fee to investors, but those that are smaller might find themselves having to raise fees to drum up the extra cash.

The New Data Rules

Going deeper into the Senior Management Systems and Controls (SYSC) rules, which are applicable to all regulated financial firms regardless of size, MiFID II will be placing stricter surveillance requirements on internal and external communications and data management processes. In the first instance, the FCA may require all calls, including mobile and landline, as well as online communications such as webmail, LinkedIn and WhatsApp, to be recorded, monitored and archived for five years, if they could possibly be related to the marketing of a product or service or be part of an investment transaction.

The large majority of firms in the alternative finance sector, whether that’s digital banking, peer-to-peer lending or digital wealth, are now highly automated, utilising chat bots, mobile apps and form interactions to conduct most of their customer communication. Luckily for them, it’s highly likely that all of this information is already being archived, and therefore the expansion of the retention rule from three months to five years isn’t going to prove too costly or difficult to implement.

What’s more important to note is that MiFID II will now require these firms to monitor the data that’s going into those archives. This means that all regulated financial firms will now have to construct systems which require a human who is educated in compliance to sample the data being stored, and confirm that there’s nothing suspicious going on. Any phone calls made will have to be transcribed and monitored before they go in the vault, as well as every email, instant message or chat bot conversation. Before it was good enough just to save the information, but now you have to surveil the contents.

What are three things you should make sure you do tomorrow?

1. Look at how you archive data: You need to be able to hold five years’ worth of information, and for it to be easily retrievable for an investigation.

2. Think about how you’ll surveil your data: noting down potential buzzwords could help shorten your workload, as well as hiring an in-house or virtual compliance officer.

3. What voice calls and web communications should you record, and how will you monitor them? Take a look at where you might get caught out in the new marketing regulations.
Potential Pitfalls in Marketing and Comms

When it comes to web communications, MiFID II’s marketing regulations are going to make things a bit more challenging. It’s always been the rules that all communications relating to a potential sale of a product or service with an outside person should begin with a disclaimer that states the body’s regulatory status and how you can contact them. However in the digital world, this has rarely been implemented outside of an email footer. As the FCA begin to crack down on marketing communications, alternative finance firms are going to have to think about how these disclaimers can be incorporated into a chat bot conversation, a LinkedIn or Facebook message, or even a tweet.

Finally, all of a firm’s internal data is going to become monitored and will require extra security under MiFID II. For example, no plain username and password web-based services for employees, such as webmail, Dropbox or Gmail, will be good enough unless secured with Multi-Factor Authentication.

Few internal conversations will be out of the scope of marketing communications or investment chain regulations. The fact is that unless you can archive the messages your employees are sending over Facebook, Twitter, LinkedIn or using their personal webmail, you will not be allowed to use those systems on site, on a smartphone or at home as a regulated entity. Platforms like Whatsapp and Telegram, even just for personal use, are absolutely forbidden because the messages being sent and received are encrypted, and therefore cannot be archived.

So there you have it, a breakdown of what MiFID II will mean for those in the alternative finance space. Best practice has always been, “if you can’t archive it, you shouldn’t have it”, but now supervision of data has been included to strengthen the rule. In addition, firms are going to have to be more focused on data security, as well as ensuring they meet stringent regulations on sales and marketing. As we enter the next phase of the digital era, compliance is beginning to make its mark.

What are three things you should keep in mind for the future?

1. As the implementation date of the General Data Protection Regulation (GDPR) is fast approaching, you’ll need to make sure you’re protecting data correctly, and that the policies you have around data management are embedded in your day to day.

2. Think about how you’ll go about disclaiming & archiving short form communication messages, like Twitter direct messages, as well as monitoring & preventing your employees’ use of encrypted platforms like Whatsapp.

3. With the arrival of Artificial Intelligence that learns on the job, how will you regulate that AI to make sure it stays compliant? There’s only so much a compliance officer can do to supervise an AI chatbot.

James Hogbin is Director at IP Sentinel
James can be contacted at james@ip-sentinel.com

IP Sentinel have a unique insight into the why’s and how’s of IT Systems, based on their experience in building services and support for a wide variety of firms both in terms of size and strategy. Find out more at www.ip-sentinel.com
Virtual CTO service for start up Firms

Experts in Compliance IT Systems, Policies & Procedures

Fingerprint Service provides eSupervision for all Emails/IM/Voice/Data in one system

Cloud based IT build out, support & voice services for Regulated firms of all sizes

IP Sentinel have a unique insight into the why’s and how’s of IT Systems, based on our experience in building services and support for a wide variety of firms both in terms of size and strategy. We have a partnership with Cordium to provide a breadth of Regulatory and fund services aside from technology.

Our primary focus is securing your Information Technology through robust procedures, systems, support, continual monitoring and regular auditing

www.ip-sentinel.com  james@ip-Sentinel.com  +44 (0)1825 701870
The introduction of the new Payment Services Directive II (PSD2) heralds a potentially disruptive force in the financial services landscape, bringing both opportunities and challenges.

PSD2 is a European Union Directive that will be adopted by the United Kingdom, regardless of the outcome of current Brexit discussions. Of course, some of the detail underlying PSD2 may be influenced by UK’s departure from the EU, for example, passporting rights.

It will be implemented into UK law on 13 January 2018, and will affect firms that provide payment services. The aim is to promote innovation, improve customer protection, make payments safer and more secure and drive down costs. Encouraging competition, PSD2 promises to give consumers more choice on how they manage their payments and their finances in general.

The new rules require payment and e-money institutions to be re-authorised or re-registered, and this process has already started in October 2017.

How will these new rules affect alternative finance providers such as peer-to-peer lenders and crowdfunding platforms, if at all? I explore the regulatory and potential business implications of PSD2 in this article.

PSD2 Under the Microscope

The new regulation could bring widespread change within an industry dominated by the big banks. Revolutionary in its design, PSD2 will allow customers, both businesses and consumers, to use third party providers to help them manage their money better. These third parties will be able to legitimately access bank data from different sources and provide an aggregated view to their customers. They’ll also be able to initiate payments on behalf of their customers, something that could previously only be done through a bank.

The new regulation compels banks to provide data to authorised or registered third parties through an API (application program interface).

PSD2 introduces two new types of third party providers. They may well have existed in the past, however outside the regulatory net. By bringing them into the net, the regulators are assuring greater customer protection.

Account Information Services Providers (AISP) and Payment Initiation Service Providers (PISP) are both a new creation arising from PSD2. Both are likely to create totally new business models that sit above banking data.

AISPs can access banking data from various sources and present a consolidated view to the customer or another party (through consent), allowing them to analyse, for example their spending habits, or total cost of services across all banks. AISPs can also help companies integrate better with banks, as I will explore in more detail below.

CONTINUED ON NEXT PAGE
PISPs will be able to initiate payment on behalf of their customer. For example, a customer could ask a third party to pay their bills from different bank accounts, without having to set up direct debits with each of their banks. Using the services of a PISP, a peer to peer payment is also possible.

In addition to introducing these new third-party providers, PSD2 introduces the following high-level changes:

Change the regulatory authorisation regime for payment services providers (PSP) and e-money issuers that are not banks or building societies. They bring more organisations into scope and allow for a full authorisation and a lighter touch registration process for smaller PSPs, below a certain threshold.

Authorised PSPs can passport their services across the European Union (of course, subject to outcomes of the Brexit negotiations). Registered PSPs don't unfortunately have this privilege.

Narrowing the scope of regulatory exemptions, and requiring a notification process under certain exempt conditions. These changes will bring greater certainty; however, it will also impact the business models of firms currently operating outside PSD1.

Enhancing rules on ensuring greater security on customer authentication and communication. The European Banking Authority (EBA) will develop technical standards for strong customer authentication, requiring a two-factor authentication process to verifying customers. EBA technical standards will extend to protection of confidentiality and integrity of payment service users' personalised security credentials, to protect against risk of fraudulent activities, especially phishing, which has been prominent recently.

Strengthening conduct of business rules and complaints handling process, as well as capping certain fees, such as fees for using credit cards, and fees for unauthorised payment transactions that may exceed an overdraft limit.

So, what are the Implications for Alternative Finance Providers?

Many in the industry, especially peer to peer lenders, are viewing PSD2 as a positive move.

Firstly, the Open Banking initiative is already heralding an era where banks must open data through APIs. PSD2 could accelerate this process. Alternative finance providers can testify to the frustration of obtaining their client money account information in electronic format. They need this data to carry out client money reconciliation daily. Without electronic data, many are left to screen scrape and dump data in an excel spreadsheet. There are progressive banks who are willingly providing an integrated service to P2P lenders, however, this is not common across the board.

“There are progressive banks who are willingly providing an integrated service to P2P lenders, however, this is not common across the board.”

When taking payments from borrowers, fundraisers and investors, many smaller platforms rely on direct debits initiated by their clients. There are third parties who provide a direct debit service, however, the costs are high and eat into already thin margins. PSD2 open the doors for more PISPs into the market, increasing competition and lowering prices, as well as providing platforms with greater choice.

Using AISPs, marketplace lenders can have access to detailed financial data from various sources, to better inform their credit decisioning process. In the absence of data, especially for small businesses, these alternative lenders have had to rely on unconventional sources such as social media and consumer forums to gain better insight on their borrowers.
Many platforms have developed proprietary algorithmic based technologies that enable them to collate and analyse a myriad of data points to turn it into a credit score. A model is however a model and no substitute for a scoring system that relies on actual data, rather than an inference from qualitative sources.

Through third parties’ AISPs, lenders can now tap into months if not years’ worth of bank transactions to inform their underwriting process. Through one channel, they can also interrogate multiple bank accounts and different banks, with the consent of the borrower.

The outcome could lead to a more stable loan book with higher quality and a lower default rate. These alternative lenders could also extend more credit, helping the small business sector to grow and make a bigger contribution to GDP.

Bear in mind however that with more data at hand, comes more responsibility to safeguard it. GDPR is another significant regulatory change programme that will intensify requirements to safeguard this new access to data.

Would Alternative Finance Providers need to be Regulated?

On the face of it, and with a standard peer to peer lending or crowdfunding model using third party payment providers or credit agencies, such alternative finance firms are unlikely to be directly affected by PSD2. In other words, they will not need to extend their scope of permissions. They can enjoy the significant benefits that this new legislation could bring without the added burden of compliance.

However, the devil is always in the detail. Some of your activities may well come within the ambit of PSD2, requiring you to be authorised or registered. Take for example this case study. Imagine if you aggregated borrower data from various sources, using a third party provider. You then provide this data to your investors to help them make a more informed investment decision. You may also develop algorithms using this data to better match lenders to borrowers. Seems harmless, and after all, you are procuring the data through a regulated third party provider, giving you and your Board comfort.

However dig deeper into the requirements of PSD2, and you could be deemed to be carrying out regulated activities carried out by an AISP. This is just one example of possibly many other examples where PSD2 could affect alternative finance lenders.

In my experience, the scope of any new regulation is never clear-cut. Many alternative lenders are likely to respond with an “I won’t be affected by PSD2, so need to do nothing” response. Others may be too busy to go through a lengthy exercise of assessing whether any activities in their business fall within the new regulatory framework. The onus is on you to ensure that your business, at the most granular level of operation, is not caught by PSD2. Don’t ignore it. Get external help if you don’t have bandwidth within the current team. External assurance will also provide your Board with peace of mind.

Apart from the regulatory implications, PSD2 will open up new opportunities for alternative finance providers to expand their offering. A deeper understanding of this new framework will also bring insights into how best the benefits can be leveraged.

Some business may also be under threat by the changes brought about by this new regulation. Like a regulatory assessment, you should carry out a stress and scenario analysis of PSD2 on your long-term business objectives.

Jay Tikam is founder and managing director at Vedanvi. Jay can be contacted at jay.tikam@vedanvi.com

Vedanvi is a professional services firm helping innovative financial services businesses accelerate growth, manage risks and deal with complex regulatory change. Find out more at www.vedanvi.com
Scaling up the Innovative Finance ISA
30th January 2018
Our seminar dedicated to the Innovative Finance ISA returns in 2018 as the P2P and alternative lending industry gears up for its next stage of growth.

London Summit 2018
26th March 2018
The AltFi Summit London returns for the fifth time, in a new venue, with new topics to explore and brand new audience segments. Open Banking and PSD2, each set to go live in early 2018, will form an important part of the discussion, as will the ongoing maturation of the online lending sector.

Australasia Summit 2018
16th April 2018
We are excited to announce that AltFi Australasia Summit is coming back to Sydney for its third edition.

Contact events@altfi.com for more information

Visit ALTFI.COM for market-leading news, insights and data on the rapidly growing alternative finance and fintech world.