

Customer centric banking

Aligning the GDPR and PSD II

Spring 2017



Content

The Challenge	1
The GDPR	2
Individual ownership of data	2
Key elements of the GDPR	2
Demanding timelines	2
Stiff penalties for failure to comply	2
The UK is behind	2
The Payment Service Directive II (PSD II)	3
Open third party access to data	3
The value of payments is in the data	3
Context and metadata	3
Digital transformation	4
Dumb pipes	4
Platforms and marketplaces	4
APIs are the pathway to digital transformation	4
Connecting PSD II and GDPR	5
Consent, purpose and duration	5
Consent	5
Purpose	5
Consent must be informed consent	5
The right to be forgotten	5
Audit trail	5
Successful implementation of PSD II and GDPR	6
1) First of all, stop resisting	6
2) Take a risk based approach	6
3) Become stewards of your customer data	6
4) Get good at data governance	6
5) Remove silos	7
6) Integrate regulatory and innovation initiatives	7
7) Automate onboarding and offboarding of partners	7
8) Monitor your audit trail	7
Conclusion: get ahead of the game	7

The challenge: GDPR v's PSD II

Managing a large book of regulatory projects alongside a growing book of digital and simplification initiatives is already a considerable challenge for most Financial Services organisations. This challenge is now made even steeper by two regulations, the Payment Services Directive II (PSD II) and the General Data Protection Regulation (GDPR) that appear to be pulling in opposite directions. While the PSD II requires banks to open customer account and transaction data to third parties via open APIs, the GDPR imposes rigorous requirements for them to protect customer data as well as stringent penalties for failure to do so.

Actually, these two regulations are closely related. These regulations are expected to be effected into European law within six months of each other i.e. in January and May 2018 respectively. Organisations should be looking to implement these regulations in an integrated manner rather than in silos.

In this paper, we discuss the core elements of a successful implementation strategy for the GDPR and PSD II programmes in the industry.

The GDPR

Individuals ownership of data

The GDPR seeks to achieve two fundamental objectives:

1. Strengthen the rights of the individual over their data.
2. Hold businesses responsible for ensuring a higher standard of privacy.

The GDPR focuses on the individual's right to own their data. Anyone using the individual's data must obtain the individual's consent for a specific purpose and duration.

Key elements of the GDPR

The key elements of the regulation are:



Privacy by design – Solutions must be designed, developed, implemented, operated and maintained with privacy in mind.



Right to be forgotten – Equally solutions need to have the functionality to 'remove' an individual's data.



Data portability – The consumer must be able to retrieve their data in a readable/ logical format (so that they may reuse it with another vendor).

Demanding timelines

Solutions that are launched after the GDPR has been implemented in May 2018 must meet the requirements from day one and existing solutions must be adapted to meet the requirements following a transitional period.

Stiff penalties for failure to comply

To ensure that businesses prioritise GDPR compliance, the regulation introduces potentially hefty fines – up to 4% of global revenue for non-compliance or 20m euros, whichever is higher.

The UK is behind

An update of UK data privacy legislation has been long overdue as the last comprehensive legislation, the 1995 data privacy acts, predates google. Several other EU countries have updated their privacy rules more recently than 1995, so organisations in the UK might find it more demanding to implement the GDPR than their peers in certain EU countries.

The GDPR gives the individual the power to request their data to be handed back to them. Current UK legislation does not require this.



The Payment Service Directive II (PSD II)

Similar to the GDPR, PSD II will strengthen individual ownership of their own data by allowing the individual to choose the third party for payment initiation and account data services. Since the regulation has been designed to foster competition and innovation in payments services.

Open third party access to data

With a PSD II licence, the external providers (including other banks) can:

1. Initiate payment transactions on accounts held by the bank's customers using the bank's APIs. The regulation refers to these third parties as Payment Initiation Service Providers (PISP).
2. Use the bank's APIs to analyse a customer's account balance and transactions in order to offer valued added services such as providing financial advice or product recommendations. The regulation refers to these third parties as Account Information Service Providers (AISP).

The key purpose of the PSD II is to allow banks to facilitate third party access to client accounts, it requires non-discrimination. In other words, any third party with a regulatory approval to be a PISP or AISP can use a bank's relevant APIs to provide services to the customer.

Banks cannot refuse to give access to licensed third parties although it remains to be seen whether the regulators may dilute this provision in the future.

The value of payments is in the data

PSD II may be a concern for banks, but it also represents a significant opportunity for banks to establish themselves both as a PISP and an AISP and compete with other banks and players hoping to seize the market.

This may be a good strategy considering no one has more experience handling payments and financing than banks.

What makes 'payments' important is not the capital transaction (the transfer of money). Bank's margins on payments transaction will get thinner and thinner as competition increases. The real opportunity to add value is in harvesting and analysing real consumer data to offer innovative products and services.

For example, Square, a US based payments company started out as a mobile PoS terminal provider but rapidly branched out into working capital loans using sophisticated analytics and prediction.

Context and metadata

Digital marketers and surveillance agencies such as the United States NSA have known for years that while there is information in our emails, phone calls, chats and tweets, there is often even more valuable information in the context in which we communicate. Similarly, when it comes to payments, context information is even more valuable than the information embedded in the transaction itself.

Increasingly, the value of payments information is the ability to understand the context in which the consumer makes the purchase decision and to influence the moment. This context information includes:

- What did they buy;
- Where did they buy it;
- When did they buy it;
- What the weather was like at that moment;
- What mood was the consumer in;
- What did they post on social media before or after the purchase;
- Where had they been right before the purchase;
- Who were they with; and
- What did the others buy at the same time.

The moment where the consumer is about to spend their hard-earned money is important for a few reasons. At the instant that a consumer decides to pay, they are making a commitment, generally with much more focus and attention than when they send an email or post a tweet. The time when a payment is made is also generally, a perfect time to:

1. Direct marketing (preferably via mobile platforms);
2. Offer financing (preferably via mobile platforms);
3. Gather data about consumer's buying behaviour; and
4. Offer valuable advice and transition from a deposit taker to trusted advisor.

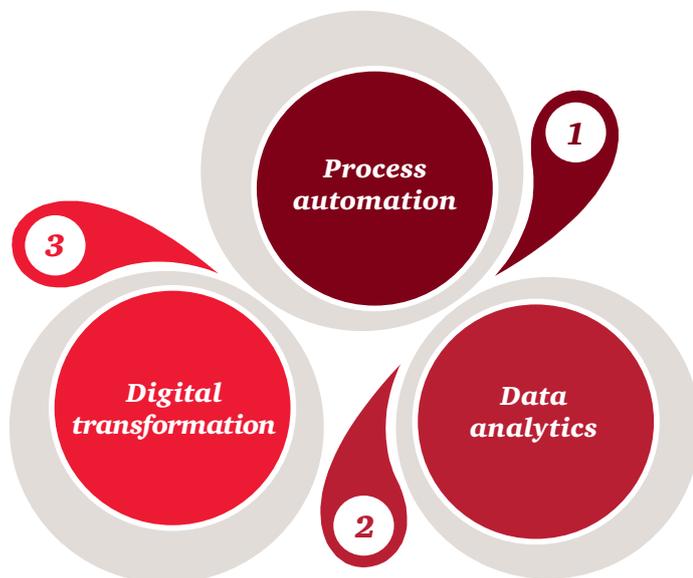
We could infer that the next generation of privacy rules will focus on privacy of context and metadata. The ability to capture, analyse and process vast payments and context information and meta-information will provide all parties in a digital ecosystem one critical source of competitive advantage, as long as they can demonstrate awareness and respect for individual data privacy.

Digital transformation

The scenario of banks turning into dumb pipes is often overstated and there is a historical reason for that. Indeed, digital transformation has always been a steep challenge for most incumbent organisations in any industry. In fact, only so many examples can be found where an incumbent organisation has successfully transformed itself to compete successfully against digital-first disruptors. Even in the capital intensive airline industry that has very high barriers to entry, digital transformation initiatives have taken over a decade to yield results.

Despite the dire predictions, so far incumbent Financial Services organisations have stood their ground well against the disruptors. Outside of China and India, waves upon waves of Fintechs such as P2P lenders, new payments providers like Transferwise and Ripple and now mobile only banks have so far only made a minor dent in the walls of the formidable fortresses that the big banks are. However, with the nimble, innovative and digital-first Fintechs finding progressively greater capital investment and regulatory support in most markets, the threat has continued to grow, and digital transformation is no longer an option for Financial Services organisations.

Financial services firms see **the main potential of FinTech investment** over the next three years to be in:



Source: Q4 2016 CBI/PwC survey

Dumb pipes

It may appear that in a post PSD II environment, Banks (ASPSPs) would be at a risk of essentially functioning as Account and Deposit holders for customers, and mainly providing access to third parties (PISPs and AISPs) that own the customer interaction on the front end. In this scenario, Banks will essentially provide infrastructure similar to utilities whereas TPPs capture the high margins and customer mindshare from owning the user experience of value added services.

For example, the banks' telephone, mobile and internet banking services will face stiff competition from innovative startups, telecoms organisations, retailers, Silicon Valley companies and others. Our latest CBI/PwC survey found that 71% of banks see competition coming from new entrants (the highest since the Survey began in December 2006).

This scenario is bearable only for a small number of sprawling banks that derive their revenue primarily from interest rates on lending. However, for most banks under growing pressure from shareholders to create new revenue and increase their return on equity, becoming a 'dumb pipe' is not an acceptable outcome.

Indeed, banks today are quite concerned about the risk of being reduced to pure infrastructure providers or 'dumb pipes', in the same way that telecoms network providers like AT&T and Sprint were turned into pipes and plumbing for communications by smartphones from Apple.

Platforms and marketplaces

Due to the complexity of transforming critical legal, technology and data infrastructure, recent years have seen the emergence of the bank as a marketplace, or the bank as platform business model. These models generally seek to take advantage of the bank's data, access to customers and strengths in regulatory compliance and resilience while creating a digital system where nimble and agile Fintechs can quickly deliver innovative services to the bank's customers.

Inspired by the stunning success of Apple and Amazon in building content and retail ecosystems, these business models look to transform incumbent financial services organisations from monoliths into thriving financial ecosystems.

Similarly, recent years have seen extensive discussion about the Uberisation of just about everything. Inspired by the rapid market dominance of Uber, Airbnb and Spotify that collect a per transaction fee merely by connecting consumers and service providers using asset-light digital platforms, banks are starting to think beyond merely controlling access to customer data and payments rails and opening these assets up to third parties to increase ROE by reducing the asset base and improving their asset turnover (sales/assets).

APIs, the pathway to digital transformation

An API based architecture, essentially mandated by PSD II provides the simplest pathway to transforming a sprawling legacy bank first into a platform (like Facebook), and then into a marketplace (like Amazon). While varying widely in their quality and scope of implementation, almost all major banks currently have open API initiatives that will allow third party developers to use APIs to build innovative consumer facing applications. Many banks state that they have had internal API platforms for years, that the technology and controls surrounding these APIs are mature and well understood and that opening up APIs to third parties in a careful and considered manner is the logical next step.

Connecting PSD II and GDPR

Consent, purpose and duration

These three concepts form the core of a GDPR compliant PSD II implementation. While digital marketers will naturally be excited about the opportunity to cross-sell services to consumers by capturing data and context metadata, the GDPR essentially forbids doing so without clear consumer consent limited by both a clear purpose and duration. Above all, a consumer can withdraw consent they provided earlier, and thereby request the removal of all personal data in the possession of a bank or a third party.

This is especially critical so that the accountability for any misuse can be assigned correctly, for example, when a third party may be at fault. Let's go through these concepts in turn.

Consent

The key to being able to collect and leverage consumer data requires making sure that the organisation and its third parties have specific consent from the consumer for their data used in a transparent manner.

Purpose

The consent should capture the broad parameters of how the data may be used. If such data is to be shared with third parties, consumer agreements must capture with whom the data may be shared and how it may be used by third parties.

Consent must be informed consent

Any legal agreements or T&Cs must be adequately clear and specific so that the consent of the user can be characterised as informed consent. Further, if the user journeys involving the capture of consent information obscure what the customer needs to know e.g. through unusually long agreements or too many clicks, a privacy lawyer can in theory even argue that the consent was not really informed consent.

The right to be forgotten

The GDPR gives every individual the right to revoke their consent. Businesses must be able to stop using the consumer's data for which the consent has been revoked and in some cases remove the data altogether from the organisation.

Open Banking increases probability of incidents, GDPR increases severity of impact

PSD II allows third party actors to provide the public with access to financial data and services that traditionally the bank directly controlled. Given the objective of creating fair and open access for third parties, the regulation does not provide a framework to have contractual liabilities in place, so the bank has little control over how these 3rd parties will operate or behave. Some of the potential exposure scenarios are:

1. A third party uses the bank's data to engage in misselling (potential Conduct Risk implications)
2. A third party violates the terms of a customer's consent for the use of data
3. A third party enables hackers to bypass the bank's cybersecurity controls
4. A third party aggregates and sells customer data to other third parties, potentially even in sanctioned jurisdictions
5. A third party combines a customer's social and transaction data to mine their identity information and engages in identity fraud, or worse
6. A third party exposes the bank's API to denial of service attacks, leading to severe difficulty for customers who need access to payment services

In all of these scenarios, the main risk exposure to the bank comes from their role as the custodian of the customer's data and the owner of the customer relationship. Even if it is a third party that fails to manage their GDPR obligations, the reputational risk may lie predominantly with the incumbent banks because they have the reputation to lose in the first place, as opposed to let's say a startup using the API. Even if the banks can position themselves to avoid actual direct financial liability under GDPR (and without taking adequate/reasonable measures as per GDPR, that might be difficult), the Customers/public perception is that the bank should have protected my data and the bank is damaged by association. Even where consent is given the general public may not fully understand the consequences of their action in a complex open banking ecosystem which puts the responsibility ultimately back with banks.

Indeed, in the extreme scenario, we could witness a sequel to the industry wide prepayment insurance disaster of yesteryears, or worse. This means a bank's first line of defence is now extended and it is now they who must ensure they have robust risk management processes and structures in place.

Maintaining an audit trail of consent

Consent, purpose and duration form key elements of the audit trail required to protect the bank in case of a dispute, or in case of misuse of customer data by third parties using the bank's APIs.

Similarly, where the right to be forgotten can not be implemented due to other competing regulations requiring the data to be retained (e.g. suitability, market abuse or financial crime rules), appropriate controls will need to be designed and implemented so that the reasons for retaining customer data must be captured and evidenced to regulators upon request.

Successful implementation of PSD II and GDPR

So what makes a successful implementation strategy for the GDPR and PSD II programmes?

1) Stop resisting

The process of authoring PSD II technical standards has seen extensive debate and even resistance from some banks. Similarly, the gap between the current and target data infrastructures required to comply with the GDPR has led to some institutions focusing on what is 'good enough', rather than what good actually looks like.

While some incumbent institutions continue to resist the openness that the PSD II represents, frequently citing cyber security, resilience and customer data privacy as concerns, other institutions are speeding ahead by recognising the opportunity and taking this dual challenge head on.

The institutions that turn this dual threat into opportunities for digital transformation will out-compete the institutions that resist, irrespective of whether some of the provisions of PSD II get diluted, or how aggressive the courts are in interpreting the GDPR.

2) Take a risk based approach

We acknowledge the concern that a riskless implementation of either of these regulations is very difficult, if at all possible. The GDPR will be interpreted by the law surrounding the regulation, which will define the minimum standards that organisations must comply with.

Similarly, in the PSD II space, there is no current minimum standard for open APIs and each bank is left to create their own definitions. This will change as regulators recognise the need for third parties to aggregate customer data across their banking relationships, without incurring excessive cost or risk. There is considerable debate around the precise form of strong customer authentication, assigning liabilities, the ability of banks to onboard or offboard third parties and incident reporting.

For GDPR or for PSD II, it is not sufficient to have a vision and a strategy unless there is a clear understanding of the variety of risks at each stage of execution.

3) Become stewards of your customer data

We believe that the regulators' appetite for violations of the GDPR will be relatively low, and we acknowledge that many organisations may find it challenging to achieve effective compliance within the next 18 months.

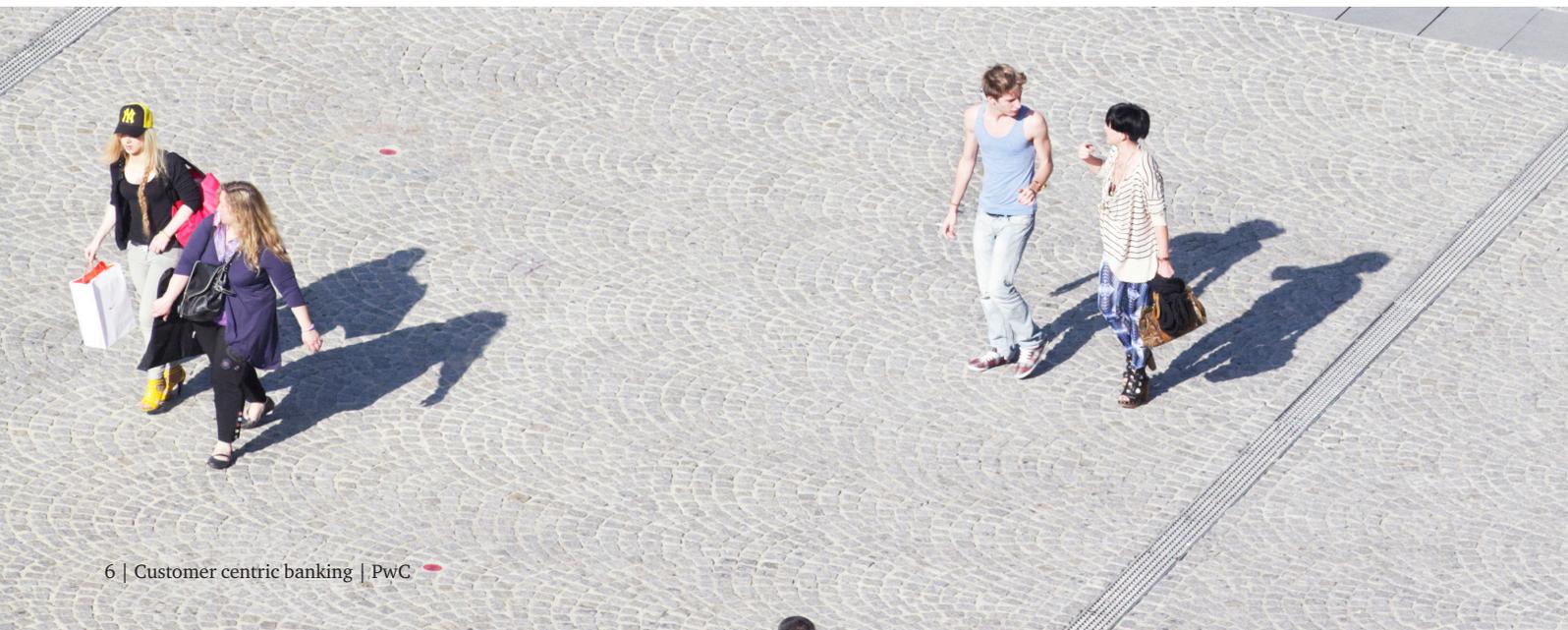
That said, based on enforcement actions surrounding other regulations such as Financial Crime rules, we anticipate that systemic or particularly egregious violations will attract steep penalties, particularly when regulators deem that the organisation in question does not demonstrate adequate steps to mitigate the relevant risks.

The most important protection against risk is a culture of privacy i.e. an environment where employees across the organisation see themselves as stewards of customer data and understand the requirements of the regulation for their particular roles.

4) Get good at data governance

Recently, regulators have recognised the need for transforming banks' data infrastructure and governance. Aside from the steep potential for fines, the GDPR is also industry or function independent, as well as much more specific and quite rigorous in its definitions and requirements.

'The GDPR provides banks with an unprecedented opportunity to transform their data governance and infrastructure. Chief Data Officers can now demand that the business and control functions understand in detail how data flows through their processes and systems, how private information is identified, what the entry points for private information are, what controls exist around these processes and how the IT infrastructure automatically ensures that the risks are identified, measured and managed.'



5) Remove silos

It is now quite clear that data privacy cannot be handled in silos but requires a combination of experts from different domains, business strategy, legal, data governance, technology, cybersecurity and alliances.

The key foundations for responding to the three requirements as set out above include having a solid grasp of what data is in scope for the GDPR, where this data is held, who has access to it and why as well as what it is being used for. Having that insight at the organisation's fingertips will go a long way toward implementing and managing compliance.

6) Integrate regulatory and innovation initiatives

Most banks have innovation initiatives designed for speed and control functions designed to minimise risk. Going forward, the innovation and transformation teams at banks must be well informed about the privacy rules and work in close partnership with control functions to achieve effective outcomes.

If you want to establish digital ecosystems based on the opportunities created by the PSD II, the solutions must be adapted to the GDPR, especially the right to be forgotten and the right to data portability. Any business model that includes consumer data must take into account the requirements of the new data protection regulation.

7) Automate onboarding and offboarding of partners

When looking for third party partners, understanding your own unique role and value proposition is key to building the right shape ecosystem with good governance structure.

Customers must be protected but any actions against third parties that are perceived as anti-competitive may expose a bank to regulatory risk. This is why capturing and monitoring the behaviour of third parties e.g. via complaint management systems, automated monitoring and machine learning techniques, will be important.

8) Monitor your audit trail

Since banks own the customer relationships today and many third parties may be small entities with limited capital or reputational risk, monitoring the audit trail of consent and using it to assess and manage the corresponding operational and legal risk may be essential.

Conclusion: get ahead of the game

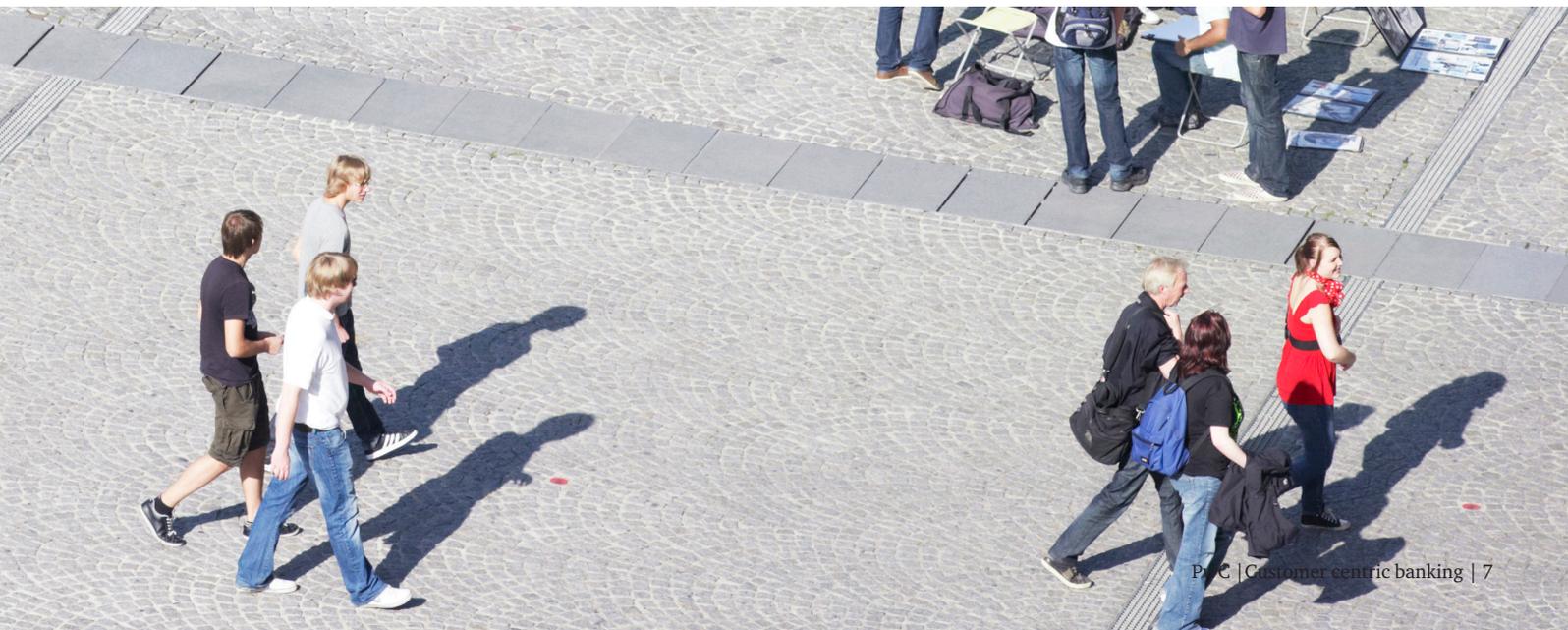
At a superficial level, the GDPR and PSD II seem to conflict. PSD II technical standards are still being defined and the industry's still waiting to see how the data protection authorities across Europe will interpret the provisions of the GDPR.

The new digital banking world

This uncertainty means you should respond with a sense of urgency. A wait and see approach could put you at a serious competitive disadvantage compared to banks that are gearing up to meet this dual challenge head on and transforming their infrastructure, data governance, culture and ways of working for the impending digital era of banking.

The trend towards open APIs creates new threats from competitors in other industries but it also creates new possibilities for banks to compete and succeed in the digital era. Many banks are following successful Silicon Valley organisations and reshaping themselves as platforms and marketplaces rather than the monolithic, closed companies of the past. The emergence of these open business models acknowledges that success depends on creating an ecosystem of partners, which in turn requires sharing data in a safe and controlled manner.

We recommend an integrated approach to implementing both the GDPR and PSD II. At a minimum, banks must consider the GDPR upfront in their PSD II programmes and other data and digital initiatives.



Contacts



Rav Hayer

Partner and Risk Assurance Digital Leader

T: +44 (0)20 7213 3451

E: rav.hayer@pwc.com



Jonathan Turner

Partner, Technology UK and EMEA

Technology Lead

T: +44 (0)20 7213 5565

E: jonathan.v.turner@pwc.com



Ajit Tripathi

Director, Fintech and Digital Banking

T: +44 (0)20 7804 4827

E: ajit.tripathi@pwc.com



Tayyaba Arif

Director, Data Management and GDPR

T: +44 (0)20 7804 6148

E: tayyaba.arif@pwc.com

Join the conversation



#regulationQnA



This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2017 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

170518-122230-LM-OS