RS2

Squaring the Circle: PSD2 and GDPR One Year On

It's been a year since the EU launched the second Personal Services Directive (PSD2), designed to open up retail banking to greater competition. This legislation was followed by the General Data Protection Regulation, or GDPR, which aims to better protect customer data from exploitation. **Ulrike Schaffter - Group Chief Product Officer** from **RS2** looks at what's happened since PSD2 and GDPR were introduced, and why financial services firms across Europe need to get involved in Open Banking, despite the apparent conflict between PSD2's commitment to open sharing of banks' customer data, and GDPR's aim to protect that data.

Recent developments in the regulation of financial services in the EU represent a profound change – and financial institutions, as well as their partners, need to be doing more to shape their strategies relating to these developments. Although Swiss management consultants Roland Berger estimate that up to 40 percent of banks' revenues could be at risk from changes introduced under PSD2 and GDPR, less than half of Europe's financial institutions currently have coherent plans in place to address the threats and opportunities emerging from this new legislation. If your business hasn't planned for PSD2 or is not yet GDPR compliant, it's time to determine your approach before competitors using new open software protocols and shared customer data threaten your products, services and profitability.

Squaring the Circle: PSD2 and GDPR One Year On

PSD2: All Change

The introduction of the EU's Second Payments Services Directive (PSD2) in January 2018 forced all financial services companies to make their customer data freely available for use by competitors, and to open customer channels to competitors by sharing application programming interfaces, or APIs. The new regulations mean that, for the first time, it's possible for mobile phone companies, technology firms, utility companies and retailers – any business with customer relationships – to offer financial services products.

PSD2 represents just part of a wider global shift to introduce more competition into the financial services market, offering consumers wider choice and, it's argued, greater convenience. The EU's move follows a separate, independent initiative from the UK's Competition and Markets Authority (CMA), launched in 2016, to open up that country's retail banking market to more competition. PSD2 also mirrors similar measures underway in India, China, Brazil, Australia and many other major markets around the world. The message that PSD2 should send to the financial services sector is that the previous regime, which saw regulation protect many customer channels and business areas from outside competition, is disappearing fast.

GDPR: Consumer Rights in the Digital Age

Shortly after the introduction of PSD2, the EU also brought its General Data Protection Regulation, or GDPR, into effect. Designed to protect consumers from the exploitation of their electronic data without explicit consent, GDPR demands that those using consumer data receive their approval to do so – and places strict technical and organisational requirements on companies when using that data for any purpose, from marketing to product development or even AML and KYC regulations.

As with PSD2, the EU's GDPR legislation should be seen in the context of a global move to protect consumers from having their data used without their prior knowledge. Canada, Singapore, Australia and most recently certain states in the US have all launched similar legislative packages: furthermore, the EU's legislation explicitly includes companies based outside the EU that deal with EU consumers.

The EU has not been slow to demonstrate that it means business with its new data protection measures, either: in late 2018, fines were imposed on organisations operating in Germany, Portugal and Austria under GDPR legislation enacted in those countries. In January 2019, France imposed the biggest fine to date (US$57 million) on Google for the misuse of customer data when targeting advertising based on customer's search histories.

With member states allowed to charge up to 4 percent of a company's total world-wide turnover as a fine – in Google's case, this would amount to US$ 975 million in 2018 – these fines show that financial services firms should be taking GDPR compliance very seriously.

> **"EU fines of up to 4 percent of turnover show financial services firms should take GDPR very seriously."**

Taken together, these two pieces of legislation represent a huge change in the financial services market, potentially increasing competition on the one hand, while also adding to regulatory demands and restricting certain marketing practices in the case of GDPR. There's also a conundrum at the heart of these legislative moves: while PSD2 levels the playing field for non-financial actors to get involved by opening up customer data for use by competitors, GDPR makes accessing consumer data and reaching consumers more of a challenge by mandating explicit consent when gathering and manipulating customer records.

That's why financial services firms, service providers and non-financial firms looking to get involved need to have strategies in place to address these changes – or risk being left behind by the better prepared.

What's Happened So Far?

GDPR has transformed the rules of marketing and data management. Under GDPR, consent must often be obtained more than once to use customer data from consumers. Thus, if a bank has approval to acquire a customer's records, either that bank or its partners must seek approval again if they wish to offer the data to a third party for marketing purposes. Despite this dramatic change, a recent survey from TrustArc says only 20 percent of firms doing business in Europe are currently GDPR compliant – and that a further 27 percent had not begun compliance strategies as of January 2019.

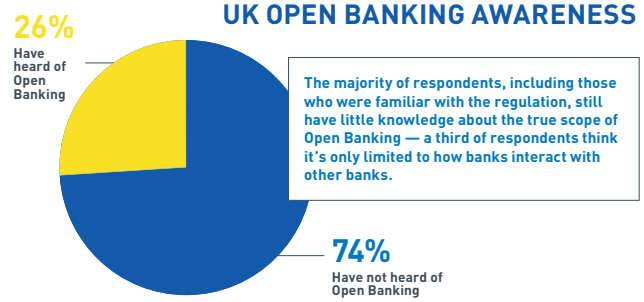
Likewise, companies across Europe have been slow to take up the opportunities offered by PSD2. Although these regulations came into force a year ago, only the UK, Germany, Italy and France have

published "national guidance" frameworks relating to it. Of these four, Germany and the UK are most advanced, with 40 German banks and PSPs, the so-called "Berlin Group", publishing operating guidance on 21 December last year. The UK is further ahead, with a full legislative framework and guidance, 88 PSD2 applications created in 2018 by non-financial companies to provide financial products, and 13 products from third party providers now live.

Despite these signs of apparent readiness, the pan-European **Fintech Disruptors 2019** study from MagnaCarta revealed that 56 percent of financial services companies across the continent had yet to finalise their approach to PSD2.

Don't Delay

Part of the problem facing financial services companies looking at PSD2 stems from a perceived lack of consumer interest in Open Banking. Although most consumers don't trust their banks when it comes to value for money, this doesn't mean they are ready for change. Ernst & Young's 2018 Consumer Trust study suggests around one in three European consumers trust their bank – yet this low figure is still better than Europeans' views of their mobile phone service providers or utilities companies. In late 2018, US firm Cardlytics undertook a study of consumer awareness of Open Banking in the UK and found that fully 74 percent of consumers had never heard of Open Banking – and that's in the world's most advanced Open Banking market.



Source: Cardlytics Report - Open Banking in the UK - December 2018

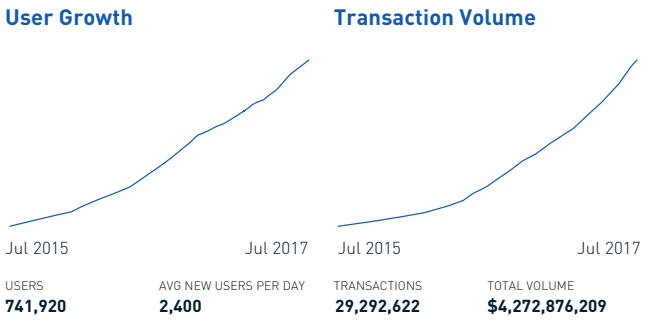
As a forward-thinking financial services firm, you should be getting on the front foot with both GDPR and PSD2 to protect yourself against the risk of regulatory non-compliance and prepare your company for the opportunities Open Banking will present.

> **"Forward-thinking financial companies should get on the front foot with GDPR and PSD2 to prepare for emerging opportunities and protect themselves against regulatory breaches."**

A January 2019 study from PwC, **The Future of Banking is Open**, identified £7.2 billion of opportunities for early movers into Open Banking. While the management consultancy recognised a current lack of consumer interest in the changes brought about by PSD2, it nonetheless claims that consolidating consumer's business to fewer providers, reducing friction for consumers and combining multiple accounts on a single digital platform will enable early movers to attract customers with higher rates of interest and attractive offers, all made possible by the cost savings represented by managing customer accounts via a single platform.

The Risk of Inertia

So much for the opportunities. As is so often the case in business, the biggest risks come from not taking action. Consider the rise of digital-only banks such as Revolut and Monzo in the UK, which now have more than two million customers between them after a period of stratospheric growth in recent years.



Source: Crowdfundinsider and Revolut

New digital-only banks are appearing across Europe, from N26 in Germany to Ditto in France and Klarna in Sweden. All of these players are hungry for market share, and ready to co-platform with mobile companies to attract customers. No financial institution with an eye on the future can afford to ignore its strategy regarding PSD2 and Open Banking any longer.

Across the payments value chain, increasing activity by "Big Tech" firms such as Apple and Amazon make the situation no less secure for Payment Service Providers (PSPs). Apple has recently announced the world's first digital-only credit card with Mastercard, while global PSP Finablr recently inked a deal to enable WeChat transactions at point of sale across tens of thousands of US merchants. As these transactions are offered at zero cost to merchants, the threat to traditional PSPs unprepared for PSD2 becomes clear. The market is changing, and tomorrow's winners need to be ready for the next wave of innovation. In fact, the PwC study referenced above anticipates no fewer than three waves of new products as a result of PSD2 in European markets over the next decade.

Data: The 21st Century's Oil

The link between the opportunities offered by PSD2 and the apparent regulatory burdens proposed by the EU's GDPR legislation is data. As **The Economist** noted in a late 2018 editorial, it's becoming increasingly clear that customer data will be as important to this century as crude oil was to the twentieth century. And just as the activities of oil companies came under increasing public scrutiny and suspicion as the last century unfolded, so we

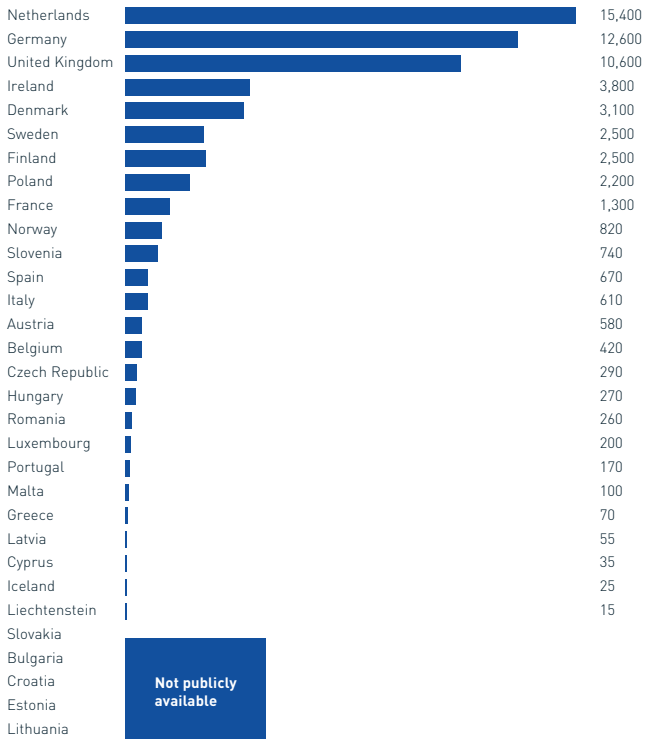
can expect the corporate sector's treatment of customer data to be closely watched in the next few years.

> **"CUSTOMER DATA WILL BE AS IMPORTANT TO THE 2020s AS OIL WAS TO THE 1920s."**

The signs are already there: Google is under examination for three separate anti-trust violations relating to data management in the EU, while US Presidential Candidate Elizabeth Warren has openly called for the "big tech" giants, all of which thrive on data harvesting, to be broken up into smaller companies. **Forbes** magazine recently credited Amazon with being "ingenious" for having avoided anti-trust suits related to its own data management practices.

Used correctly, consumer data can revolutionise a company's customer service, marketing and product development functions, creating new products and services based on consumer interests. However, as the recent groundswell of political activity against big tech firms and the rise in GDPR-related legislation around the world demonstrates, the wrongful use of consumer data can be disasterous. In the twelve months since GDPR was introduced, there have been more than 59,000 reported breaches of GDPR rules, with 75 percent of large organisations suffering a breach and 91 fines imposed, according to research published in February 2019 by law firm DLA Piper.

Number of Data Breaches notified
from 25 May 2018 to 28th January 2019*



* Not all of the countries covered by this report make breach notification statistics publicly available and many only provided data for part of the period covered by this report. We have therefore extrapolated the data to cover the full period. It is also possible that some fo the breaches reported relate to the regime pre-dating GDPR.

Source: DLA Piper GDPR Data Breach Survey February 2019

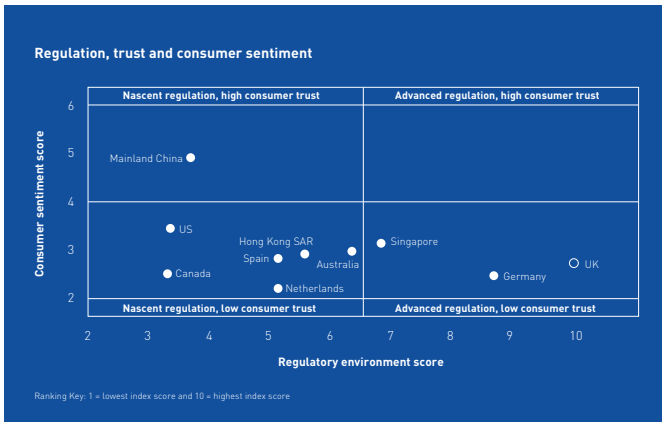
Secure Customer Authentication: Creating Friction?

As well as opening up financial services to a wide range of competitors, PSD2 also introduces new challenges and potential pain points for all players in the retail financial services market. Not least among these is Secure Customer Authentication (SCA), which mandates two-factor authentication for all companies offering digital and mobile financial services products. While this provision will no doubt improve security for consumers, doubts persist about its viability – especially when it comes to payments.

Given that a recent study in the US estimated two-factor authentication, and the need to repeat authentication at check-out, is responsible for US$130 billion a year in abandoned sales, your organisation should be thinking about its approach to SCA as a matter of urgency. If you are an established or emerging financial institution, your business is particularly at risk, especially since those telecommunications and technology firms interested in your customers have long experience of multi-factor on-line, mobile and hybrid authentication technologies.

The Future: Trends Towards PSD2 and GDPR

Looking ahead, financial services firms can expect legislation similar to GDPR and PSD2 to be implemented in other countries globally. As noted earlier, countries outside Europe such as Canada, Australia, Singapore, Brazil and Mexico have all either implemented data protection legislation similar to GDPR, or have plans for implementation underway. As regards PSD2 and Open Banking, Germany, Spain, Canada and China are all making plans to legislate in favour of open APIs and the sharing of customer data, which are the essential elements of PSD2. Even the US, champion of allowing markets to decide outcomes, is considering mandating open APIs as a means of enhancing competition.



Source: Ernst and Young Open Banking Opportunity Index

Aside from these regulatory drivers, we can expect further developments – such as the data breaches experienced by British Airways in the UK and India's Aadhaar – to increase consumer demands for data protection. And with Ernst & Young's Open Banking Barometer revealing that nearly half of negative consumer sentiment regarding Open Banking linked to data security concerns, the message is clear – make sure you're GDPR compliant, not just for compliance's sake, but because it's good for your business.

What's more, complying with GDPR in Europe will prepare you for similar legislation underway in other regions. And best of all, GDPR compliance will allow you to adopt Artificial Intelligence (AI) and Machine Learning techniques for the data your business generates, developing new products and services for your customers and giving your business a competitive edge while remaining compliant.

The EU has published a full GDPR compliance checklist at www.gdpr.eu for companies looking to enhance their compliance. Clear steps which need to be taken, including a data processing audit, legal privacy policy and public statement of that policy, are listed on this site. If you haven't already undertaken a GDPR compliance audit, we encourage you to do so at the earliest opportunity.

What It Means for Your Business

As PSD2 and GDPR permeate the financial services industry over the next year to eighteen months, we can expect to see more direct-to-account solutions emerge from telecommunications companies, utilities companies and others. Examples would include life insurance offered by a telecoms company on a direct debit basis from within its customer platform, or a utilities company offering a digital wallet for online payments. Offering these services from their own platforms reduces the number of times customers are required to undergo two-factor authentication. It also means these new entrants can offer incentives, such as money-off deals on mobile phone packages for customers taking up their financial products.

The arrival of new competitors in the market isn't all bad news for financial services firms: for PSPs and other intermediaries, new players like telcos and utilities companies will need to partner with firms that have specialist experience in processing, acquiring and compliance. Equally, established financial institutions now have the opportunity to shore up their customer relationships and partner with dynamic FinTech start-ups to offer new, compelling products to their existing customers.

Prepare to Perform

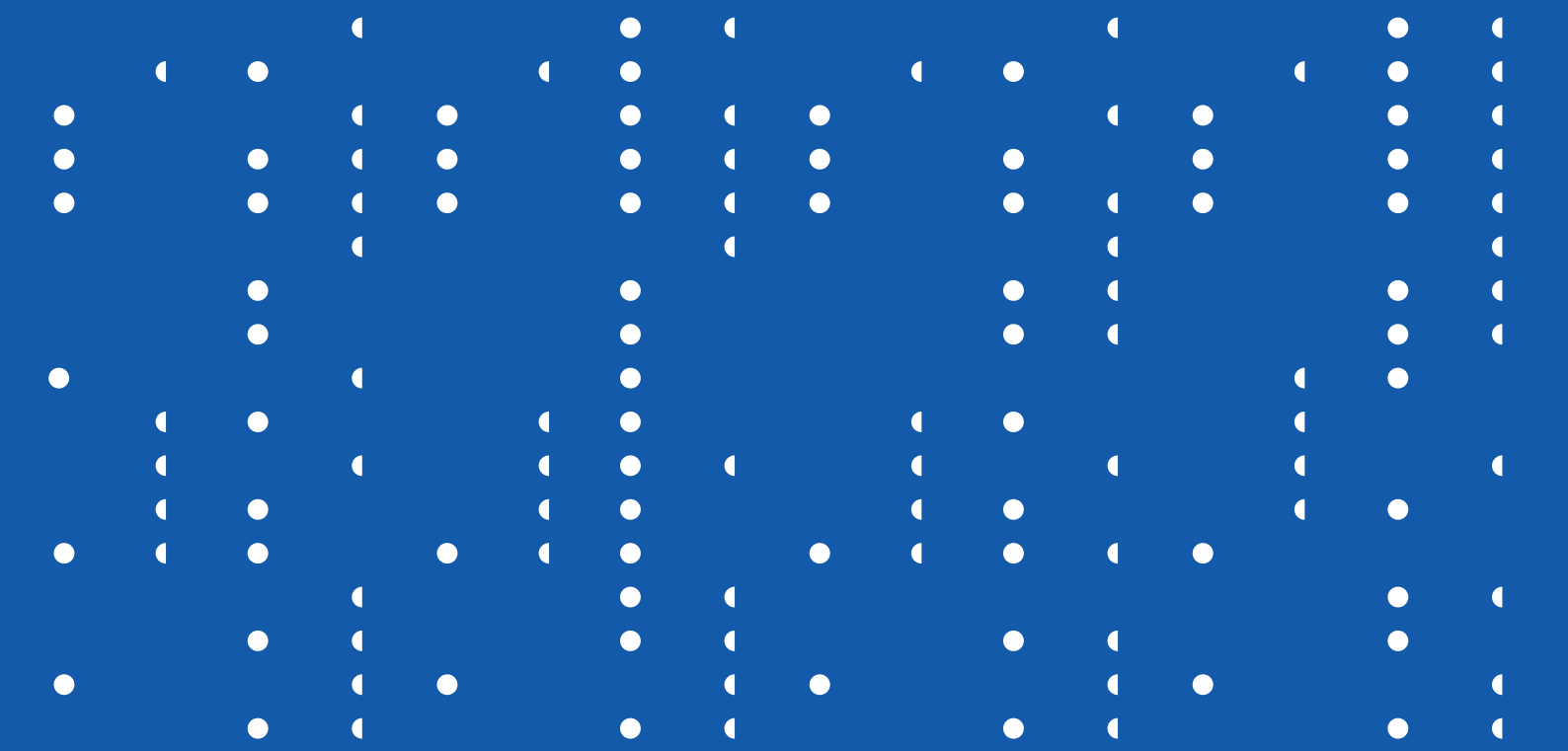
Despite the challenges presented by PSD2 and GDPR from both the compliance and operational perspectives, the good news is that there's still time to act. As Nick Middleton, Head of Payments Strategy at the UK's Nationwide Building Society says, "Despite the hype, the fact is that most of the public don't adopt rapid innovations all that well." Put another way, the current state of consumer inertia has bought time for financial services firms that have yet to define their strategic approach to PSD2. Furthermore, as a financial services firm, you have the experience and know-how to succeed in this market: your challenge is to translate that knowledge and experience into a new, more competitive, environment in the next few years.

All the signs are that the impact of PSD2 will be slower to make itself felt than GDPR, which has already seen a number of immediate sanctions for non-compliance and regulatory breaches, including large fines, levied against financial and technology companies. That said, we recommend the following three concrete steps:

1. **Define your approach to PSD2.** Based on the information in this white paper, how is PSD2 going to affect your business in the next 18 to 24 months? What steps do you need to take from the perspective of your operations, marketing, customer relationship management and technology functions? This could include upgrading your customer login software to be SCA compliant, ensuring your APIs are open and consistent with PSD2 standards, and others.

2. **Consider Partnerships and Collaborations.** Dependent on your sector of activity and strategic approach, you may be looking to partner with a secure authentication specialist or a fintech with a promising new product. Alternatively, you may be approached by a Third Party Provider (TPP) such as a telecommunications firm with a partnership proposal for your customer base. Successful partnerships are likely to be a fruitful approach after PSD2, and your company should be actively seeking meaningful partnerships where there is a defined purpose, and a clear business opportunity with measurable, bottom-line results.

3. **Pilot new products and partnerships.** New partnerships, such as Apple and Mastercard's recent announcement of the world's first digital credit card, are fraught with potential risks and need careful planning and testing before being launched to market. We recommend working with experienced advisors on pilot projects before moving to full roll-out. Too often, companies announce partnerships for the press release value, only to experience challenges at the implementation stage. This is particularly true when working to new regulatory guidelines such as those introduced by PSD2 and GDPR.



RS2

Get in touch

RS2 is working with customers around the world on strategic implementations related to PSD2 and has experience of working directly in GDPR-compliant payments solutions. We'd love to hear from you with any questions about your organisation's optimal approach to Open Banking and data management.

www.rs2.com