Payment service providers face even tougher DP requirements

Processing personal data for open banking initiatives, covered by Payment Services Directives or the Open Banking Standard, will always require explicit consent. By **Jane Finlayson-Brown**.

Access to data is a fundamental part of unlocking value from new business models in financial services. It allows emerging players to scale quickly and test their products in real world environments; it also offers incumbents the insights needed to reach new customers and explore new business lines. Standardisation and interoperability are essential building blocks for those looking to work with data.

Application Programming Interfaces (APIs) are one of the technologies at the centre of bringing both standardisation and interoperability to the market. For example, APIs can facilitate the quick and efficient aggregation of information to make comparison of different services (and potentially account swapping) much simpler. APIs may also allow lenders to access transaction data to speed up credit availability and facilitate fraud checks. Combined with developments in robotics and biometrics, the potential for innovation is enormous.

APIs are already widely in use in financial services, and particularly by some of the more tech-savvy players. Indeed for some banks, digital technology and agile ways of working are already at the heart of their offering. The head of APIs at German-based Fidor Bank, for example, has described Fidor as "not only a technology company that always tried to be ahead of all developments and try out new things, but we're also a bank". For incumbents, open APIs may provide a rich source of ideas and technology to spark innovation within their own businesses as well as the opportunity to collaborate with emerging players.

The rise in API use, and particularly the interest in open APIs[1], is not just market driven. There is pressure from regulators and policy makers to encourage open banking to bring greater competition through the development of new services and the market entry of new payment service providers. With data sitting at the heart of the open banking equation, an appreciation of data protection frameworks in the context of APIs will be at the heart of any API strategy.

The incoming legislation

The General Data Protection Regulation (GDPR) is of course dominating many companies' privacy initiatives and would be quite enough to contend with on its own. However, spare a thought for those seeking to exploit the new opportunities or mandated to make room for new entrants. They will need to consider the revised Payment Services Directive[2] (PSD2), the 2016 Open Banking Standard[3] (the Standard) and in some cases, the requirements flowing from the Competition and Markets Authority's (CMA's) Market Investigation into Retail Banking (the CMA RBMI)[4].

PSD2, to be implemented in national legislation by 13 January 2018, among other matters, seeks to remove barriers to entry for third parties, such as "payment initiation services providers" (PISPs) and "account information services providers" (AISPs). PISPs are involved in facilitating the use of Internet payments through online banking, such as payments from consumers to merchants. AISPs are information aggregators; for instance, they could allow customers to review data about a number of their bank accounts in one place.

The Standard is a UK initiative prompted by HM Treasury, aiming to optimise data usage to facilitate banking transactions and encourage innovation. The Standard is to serve as a guide as to how data can be created, shared and used, through the use of open APIs. Examples of the types of services that could be possible are very similar to those envisaged under PSD2, such as enabling reconciliation of different bank accounts, comparing mortgage products or obtaining a tailored loan offer based on historic data demonstrating credit-worthiness.

The CMA RBMI was published on 9 August 2016 as the conclusion of a market investigation into the supply of retail banking services to personal current account customers and to small and medium sized enterprises in the UK. The CMA considered that currently there are too few incentives for banks to compete on price or innovation. They conclude that this has also led to difficulty for new entrants, especially regarding their ability to challenge banks with large customer bases.

As a result, the CMA has announced a number of measures. Pertinently, these include the development and adoption of an open API banking standard by the largest retail banks[5] in Great Britain and Northern Ireland, by early 2018 "at the latest", with certain sharing of information by the end of March 2017.

Common to all of these initiatives is therefore the sharing of information, including personal data, to facilitate provision of the new services. These new regimes stretch beyond the policy aspirations for new market entrants and products into practical realities, addressing security standards, obligations, liability and breach notification.

Is there is an alignment of regulatory stars?

Faced with a range of regulatory initiatives reliant on big data techniques and aiming to foster innovation as well as the requirements of the GDPR, it is not surprising that a number of familiar issues and themes appear and reappear, but yet not quite as anticipated when viewed through GDPR-sensitive eyes.

While many would regard the GDPR as a (perhaps appropriately) demanding set of standards, the requirements of the new initiatives show a further tightening of approach.

New requirements for consent and privacy notices

At the heart of PSD2, the Standard and the CMA RBMI is an assumption that not only will data protection be respected, but that "explicit consent" to the data sharing will be obtained from the relevant customer. There may, of course, be a number of different new service providers to whom data could be transferred. The Standard calls for explicit consent to be provided "each and every time" data is shared and, consistent with the GDPR, provides that consent should be as easy to revoke as it is to be given. Interestingly, the term "explicit consent" is reserved in the GDPR for consents required for special categories of data (i.e. a defined class of what is considered to be highly sensitive data, and which would generally not encompass banking information).

This consent driven approach may be well intentioned but it seems somewhat at odds with policy makers in the GDPR world, who are concerned that often the consent that is obtained is not true consent and who seem to lean towards use of other mechanisms for legitimising use of data rather than what they see as an over-reliance on consent. These include processing necessary for the performance of a contract or for the purpose of legitimate interests which are not overridden by the interests, rights and freedoms of the data subject.

While traditional banking confidentiality consents to disclosure are often found in account terms and conditions, this is no longer sufficient from a data protection perspective. The newly published ICO guidance on privacy notices (ICO Privacy Notices Code of Practice)[6] sets out the ICO's latest thinking on its expectations both for obtaining consents and for the related compliance action of providing fair processing information to data subjects.

In an example that focuses on sharing data via apps and social network sites, the ICO emphasises the need for each data controller involved to provide information about its own use of data, as well as acknowledging the possibility of a joint end-to-end privacy notice or resource that brings together all of the relevant information, for instance, through a dashboard. Going forward under the GDPR, the information required to be provided in a privacy notice is more extensive than data controllers have been used to, but a "layered" approach is possible to aid digestibility.

The ICO Privacy Notices Code of Practice requires that consents should be clear and prominently displayed, accompanied by a positive opt-in and sufficient information to enable a choice to be made. There is also an obligation on the part of the provider to explain the different types of processing if relevant, with good practice suggesting that separate unticked opt-in boxes should be provided.

In an open banking context, a combination of layering of notices and information, just-in-time notifications and approvals and a dashboard approach may be the most practicable way forward. Given the GDPR requirement that a controller must be able to evidence a consent, it will be essential for banks allowing access to customers' data and providers of these new services to build such a facility into their systems.

Purpose limitation

The very essence of Big Data has thrilled and scared the privacy world in equal measure.

Infamous instances of big data techniques overstepping what society would regard as acceptable have prompted opinions from the Article 29 Working Party and the European Data Protection Supervisor. There was considerable debate at the time of the drafting of the GDPR as to whether the provisions on purpose limitation should be more or less restrictive than those in the existing Directive.

In the end, a compromise position was reached and the GDPR allows for further processing of personal data where that processing is "not incompatible" with the purpose for which the data was originally collected. The GDPR gives some broad guidance on factors that determine compatibility, such as the link between the two purposes.

The approach taken in both PSD2 and the Standard is, as outlined above, that explicit consent must be granted. PSD2 provides that a PISP shall "not use, access or store any data for any purpose other than the provision of the payment initiation service as explicitly requested by the payer". The Standard states, "where customers grant consent for… use of their data… there should be no ambiguity under law as to what data was supplied and what it was to be used for."

Accordingly, any further processing will require the user's explicit consent. Players in this market will therefore need to frame their consents and notices carefully.

Security, security and yet more security…

The authors of new regulatory initiatives are acutely aware of the need for strong security, without which the new services will likely fail. As we know, the concepts of security standards, privacy by design, privacy impact assessment, breach notifications and responses are all critical to compliance under the GDPR.

PSD2 echoes these sentiments but introduces requirements for further regulatory reporting. An annual comprehensive assessment is required, detailing operational and security risks relating to the payment services provided and the adequacy of the mitigation measures and control mechanisms. PISPs and AISPs are subject to specific obligations to ensure that the personalised security credentials they process are not accessible to other parties and are transmitted through safe and efficient channels. In addition, "major operational or security" incident reporting to the relevant competent authority "without undue delay" is required. Guidance is to be issued as to the content and format of this, as well as standard notification templates.

Strong customer authentication (SCA) is a key feature of PSD2. PISPs will be required to use SCA when, for example, a customer initiates an electronic payment transaction. SCA as defined in PSD2 requires the use of two or more of: something the customer knows (such as a PIN); something the customer has (such as a token); and/or something the customer is (such as biometrics).

Action points

The adoption of these new initiatives marks an exciting new era for Fintech

products. The new requirements are challenging and generally tougher than the requirements under the GDPR. Accordingly, action points for those firms seeking or obliged to comply include:

1. When considering GDPR grounds for processing data, remember that there is no choice when it comes to data processed for open banking initiatives covered by PSD2 or the Standard. It is always consent and indeed explicit consent.
2. The new standards and guidance will no doubt be helpful in assisting players to work out how best to communicate with customers, but consider layering, just-in-time notices and consents and dashboards.
3. Beware of joint and several liability. Ensure that notices are carefully constructed to ensure this does not arise and to differentiate between each party's activities
4. There is no expansion of scope of processing via purpose limitation principles. To avoid re-issuing notices or the need for new consents, think carefully about their terms.
5. Consider the security requirements across the various initiatives and whether it is easiest to build to the highest common denominator.
6. Ensure that your breach notification policies take into account PSD2 notifications as well as GDPR (and, for that matter, other regulations outside the scope of this article, such as the NIS directive[7]!) (see *PL&B International* February 2016 p.1 on NIS Directive).

AUTHOR

Jane Finlayson-Brown is a Partner at Allen & Overy LLP
Email:
Jane.Finlayson-Brown@AllenOvery.com
www.allenovery.com

REFERENCES

1 An open API is a means of accessing data based on a standard that can be accessed and used by anyone.
2 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance). PSD2 applies to payment services in the EU, with a particular focus on electronic payments.
3 Introducing the Open Banking Standard (Open Data Institute ODI-WP-2016-001: theodi.org/open-banking-standard)
4 Final report published on 9 August 2016: assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf
5 RBSG, LBG, Barclays, HSBCCG, Santander, Nationwide, Danske, BoI and AIBG.
6 ICO publication: 'Privacy notices, transparency and control' dated 7 October 2016
7 Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures to ensure a high common level of network and information security across the Union

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Elizabeth Denham: A bigger, bolder, brighter ICO

In an exclusive interview with *PL&B*, Elizabeth Denham talks about her plans for the ICO, including the enforcement regime, GDPR compliance advice and personal liability for directors.

By **Laura Linkomies**.

Settling in her new position, Denham said that her office is extremely busy trying to keep up with its normal work whilst preparing for the GDPR. She said that in addition to guidance that it is preparing for organisations in the UK, the Information Commissioner's Office (ICO) itself has to change its way of working and prepare for its new responsibilities under the GDPR.

She said that the office would issue an update in the coming weeks on upcoming guidance on the GDPR. This will include guidance on the role of the Data Protection Officer and the new standard for consent. Denham said that the office would not be issuing sectoral guidance but would be ready to advise and assist industry associations in developing their own codes. She said that the ICO does not have resources to do this work for all the sectors that might want industry-specific guidance.

"As a regulator we want to work with companies as we always have and provide advice – we try to be helpful. That is the 'ICO way' – working closely with different sectors. I will continue this type of cooperation."

She said that the EU Art. 29 WP will be making decisions on guidance with regards to Data Protection Officer qualifications in December. The ICO will then issue guidance to organisations in the UK.

Future UK DP regime

Denham said that she would not wish to speculate on what form the future UK DP regime will take in the long term – it is a decision for the

Continued on p.3

Issue 88 **November 2016**

UNITED KINGDOM
report

ISSUE NO 88 **NOVEMBER 2016**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

SUB EDITOR
Tom Cooper

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS

Alison Deighton and Jenai Nissim
TLT LLP

Ellen Temperton
Lewis Silkin LLP

Jane Finlayson-Brown
Allen & Overy LLP

Ellie Hurst
Advent IM Ltd

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

Companies see benefits from ethical stance on DP

Companies are dedicating time and money just now into GDPR compliance. There is no choice as we now have confirmation from government that the new Regulation will apply in the UK from May 2018 (p.5 and p.18). Compliance programmes are needed to make sure you stay within the letter of the law (p.6) but the trend of unhappy consumers taking action perhaps suggests that a more holistic, ethical way of dealing with personal data is called for.

When we visited the ICO to conduct an interview with Elizabeth Denham earlier this month, she told us that some individuals had expressed dissatisfaction at the level of the fine issued to TalkTalk (which they regarded as too low) and expressed concern, directly to the ICO, regarding WhatsApp's and Facebook's planned data sharing.

Denham's opinion piece on the WhatsApp question was published recently in the *Guardian*. She declared: "The difficulty with digital services is that because we're so invested in them, we become dependent on a service that we can't always easily extricate ourselves from. As big companies buy up their competitors, are there realistic alternative services out there? And even if I can find an alternative messaging service to WhatsApp, that only works for me if my friends and family move service too. In those situations, we need to have better protections for consumers."

"It's a problem that overlaps data protection and competition law. We need to start thinking more about the obligations that follow personal data, and how people are being protected. If a company makes a promise, then that promise needs to be honoured, irrespective of corporate manoeuvres."

In October, *PL&B International Report* covered the synergy between data protection, consumer and competition law within the EU framework. I am sure this is a topic that will feature on many national DPAs' agendas in the future.

In the UK, organisations are busy dealing with Data Subject Access Requests. Read on p.9 how the courts interpret law in this area. New data protection challenges arise for open banking (p.11) and body worn cameras (p.15).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the *PL&B UK Report* back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and *PL&B Annual International Conferences*, in July, Cambridge.

6. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"I particularly like the short and concise nature of the *Privacy Laws & Business Reports*. I never leave home without a copy, and value the printed copies, as I like to read them whilst on my daily train journey into work. **Steve Wright, Chief Privacy Officer, Unilever**"

Subscription Fees

Single User Access

UK Edition **£400 + VAT***

International Edition **£500 + VAT***

UK & International Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the International Report.
www.privacylaws.com/int