Data portability under EU GDPR: A financial services perspective

The right to portability is perhaps the least understood concept in the GDPR. **Philip Woolfson** and **Daniella Terruso** discuss challenges with this requirement.

A new aspect of data protection law will be introduced when the European Union General Data Protection Regulation (GDPR) applies on 25 May 2018: Data subjects have acquired a right to data portability (RDP) and data controllers will be bound to provide the personal data that they process from that data subject "in a structured, commonly used and machine-readable format". The data subject must be able to "transmit those data to another controller without hindrance" from the initial controller[1].

Limited restrictions apply. The right will only apply to electronic (automated) processing based on consent or a contract. Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller is exempt. Importantly, and in common with the related right to access, data subjects have the right to personal data which concerns them, not another data subject[2].

RDP raises many implementation questions as controllers prepare to respond to portability requests. The Article 29 Working Party[3] (WP29) is expected to deliver guidance on this and three other aspects of GDPR before the end of the year[4]. In parallel, some national supervisors have initiated consultations[5].

This article examines developments in a selected regulated sector, namely financial services, to explore how RDP may be successfully implemented and where difficulties may arise.

Financial services as a regulated sector

In recent years there has been growing interest by financial institutions in the consumer data they hold. Data gathered from consumer use[6], combined with additional contextual data[7], and lower processing costs have boosted financial product and service development, as outlined in further detail below. New market entrants, from start-up financial technology (FinTech) companies to large digital services providers seeking new avenues, are also using consumer data to offer services such as price comparison or data aggregation which may transform all manner of financial markets. Finance is, however, not a new regulatory frontier. In addition to restrictions which will be placed on controllers through the GDPR, the way firms, including banks, insurers and payment services providers, conduct business is highly regulated. These rules preventing market manipulation, conflicts of interest and other shortcomings are also in flux as regulators continue to address the long-term effects of the 2008 financial crash. So, as regulators grapple with new market developments, to what extent does this regulatory focus dovetail, or could there be conflicts or omissions which will impede successful implementation of RDP?

The benefits and risks of increased data sharing?

Financial institutions already share customer personal data with each other, with outsourcing companies, and selected third parties. There is some evidence in insurance[8] and in banking[9] that firms are starting to share that data with consumers themselves. Our question is whether such initiatives would be sufficient for RDP purposes, or whether more must be done before the GDPR applies.

In the best case scenario, data exchange initiatives in banking and insurance should bring substantial benefits to customers by assisting them to shop around for the products and services that are most suitable for them. It should also lead to better quality, consumer-targeted products. There is evidence that this is already happening in insurance: in a recent call for input on Big Data in retail general insurance (private motor insurance and home / contents insurance)[10], the UK's Financial Conduct Authority (FCA) found that insurers are indeed developing more personalised products based on their access to consumer data. Technology, such as car-based telematics devices, provides continuous feedback to consumers on their habits and the FCA suggests this helps them manage their risk; it also reports evidence that sharing this data with insurers can lower costs (see *PL&B UK* July 2015 pp.14-15). The FCA did not find any evidence that consumers using telematics experience difficulties in switching providers, which may indicate that UK consumers are already using their data to shop around. The FCA also reports there are no particular difficulties regarding portability of telematics data. Firms may, therefore, have found solutions in this segment of the market which could help them fulfill their future duty to provide personal data to customers "in a structured, commonly used and machine-readable format" as per GDPR requirements.

Other regulators are monitoring developments closely. The European Banking Authority (EBA) for instance, recently noted the risks from increased use of consumer data: potential for information asymmetries — where one party has greater access to information than another — between provider and consumer, misuse of data, security risks as well as reputational risks to providers. It is in mid-consultation on the matter and may suggest revising existing legislation or issuing guidance, if it considers that the risks in the banking sector are not adequately addressed[11].

UK initiatives

However, the financial sector is not waiting for the GDPR before embarking on data sharing. In fact,

RDP is probably not the primary concern, but there can be RDP side benefits. The UK government's midata initiative (*PL&B UK* October 2014 p.18), introduced primarily to implement the UK's current account switch guarantee[12], was recently used in an overview report on the GDPR[13], published by the Information Commissioner's Office (ICO) as an example of the state of the art. The public/private scheme, set up in 2011, helps consumers manage their personal finances by providing access to their historical transaction data. Since 2015, all big banks in the UK provide the option for customers to download account information from their on-line banking platforms. Customers can then use this data on a comparison website, Gocompare, to shop around for suitable alternative payment account providers. In time, midata promoters suggest the initiative could cover credit card, utilities and mobile phone contracts.

More generally, following the Competition and Markets Authority (CMA) investigation into the UK retail banking market, which published its final report in August, the largest banks have been ordered to develop and adopt open access standards to enable third party providers (TPPs), i.e. companies offering services based on consumers' payment account information, to expand.

REFERENCES

1 Article 20, GDPR.
2 The Article states that exercise of the right must not adversely affect the rights and freedoms of others.
3 An advisory body set up under Directive 95/46/EC comprising representatives of national supervisory authorities; the European Data Protection Supervisor and the European Commission.
4 The other aspects are: data protection impact assessments; certification; and the role of the data protection officer.
5 For example the recent consultation by the French DP authority, the CNIL, launched in June 2016.
6 For example, in-car telematics devices or payment accounts and payment cards transaction data. The European Banking Authority in a recent discussion paper on innovative uses of consumer data stated that payment data gives banks extensive insight into their customers' purchasing habits and preferences which can bring both benefits and risks to those data subjects.
7 Such data is increasingly harvested from social media sources.
8 Such as the use of in-car telematics for motor insurance or fitness trackers for health insurance.
9 See below the example of midata in the UK for payment account information.
10 The feedback statement from the FCA (FS16/5) was published on 21 September 2016.
11 The deadline for comments to the EBA discussion paper on innovative uses of consumer data was 4 August 2016.
12 This was introduced in the UK following multiple investigations into retail banking practices.
13 Overview of the General Data Protection Regulation (GDPR), published by the ICO on 12 July 2016.
14 A consultation paper is open for comments until 12 October 2016.
15 Article 290 TFEU: a legislative act may delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act.
16 Article 291 TFEU: where uniform conditions for implementing legally binding Union acts are needed, implementing powers may be conferred on the Commission (and in some cases the Council).
17 Responses are available on the CNIL website (in French).
18 A fab lab is the short term of art for fabrication laboratory, usually describing a small-scale workshop offering digital fabrication.
19 In some sectors, such as insurance, it would be unfortunate if the consumer could edit the data to present himself in a more favourable light. It could have an effect on the insurer's ability to fully identify the risk before concluding a contract. The consumer would be making a deliberate representation which would render the contract void.
20 Currently, the ICO provides guidance with respect to requests made on behalf of others. Given the changes under the GDPR, controllers will probably need to review (and tighten) current practices.
21 e.g. IaaS cloud providers may not have access to their clients' personal data but to what extent could they have a duty to ensure the infrastructure is in place to enable their clients to provide the data "without hindrance").
22 Such as the CMA order to large UK banks on open access standards and PSD2 requirements on common and secure open standards.

The revised Payment Services Directive (PSD2)

A key concern for controllers in finance is security and interoperability. Part of the solution may lie in the revised EU Payment Services Directive (2015/2366), which applies from 13 January 2018 and will regulate TPPs. Currently EBA is drafting regulatory technical standards. These include common and secure open standards of communication between payment account providers and TPPs[14]. Focusing on secure data exchange between regulated entities (banks, TPPs, etc.), could help such firms to fulfil their duty under Article 20(2) GDPR whereby the data subject has the right to have their personal data transmitted directly from one controller to another, where technically feasible.

The standards do not, however, cover the format or content of any data exchange direct to consumers, and thus do not fulfill all RDP requirements.

Data protection authorities' guidance

Drafts of the GDPR text reveal that the Commission had intended to set criteria and conditions for the exercise of RDP by "delegated act[15]". Standard forms and procedures, including e-formats would have been set by way of "implementing act[16]". Both powers were deleted during the negotiation process, leaving WP29 to fill the gap. Guidance on RDP, covering format, scope and practical implementation, is due before the end of the year.

The process of developing guidance was launched over the summer. By way of example, France's data protection authority, the CNIL, initiated a consultation, which ended on 19 July, asking respondents to give their views[17] on: the anticipated benefits for data subjects and controllers; the limits to RDP; the format of the data exchange (controller to data subject and controller to new controller); and how respondents saw RDP applying to their sector.

On 26 July, members of WP29 met civil society representatives, professional associations and academics at a "FabLab[18]" event in Brussels.

From the responses to the consultation and informal feedback received from the FabLab, we can see that

controllers require the following clarifications:

1. the exact scope of RDP;
2. the exact scope of the limitations;
3. how controllers can protect IP rights and potentially conflicting duties (e.g. the confidentiality and professional secrecy regimes under banking legislation);
4. whether data will have to be provided in full or whether a summarized form would be acceptable;
5. whether data should be provided in a form that allows consumers to edit what they wish to send to the new controller[19];
6. whether, as in responding to a subject access request, a fee could be charged, particularly for requests that could be justifiably deemed unreasonable or repetitive;
7. bearing in mind the duty under RDP and also for access requests, not to provide data that would adversely affect the rights and freedoms of another person, how to successfully balance the data subject's right of access/RDP against the other individual's rights[20];
8. the impact RDP could have on relations between controllers and processors[21];
9. the potential impact of RDP on data retention – should limits be imposed on the number of years of data to be provided; and
10. to what extent professional associations (e.g. in insurance or recruitment) will be required to develop common standards.

Concluding remarks

From our brief survey of the financial services sector, we can see evidence that insurers and banks have taken useful steps towards fulfilling their duties under RDP, even if this may not have been the initial impetus for data exchange. Security and interoperability are being addressed through standard-setting requirements[22] and the regulators are monitoring the situation closely. Is it sufficient? It is a strong basis from which to start, particularly for controller-to-controller data exchange, which will benefit from the standards that are being currently developed, but it seems more effort is required before controller-to-data-subject exchange is fully operational. This may be understandable given the uncertainties at this stage surrounding WP29 guidance. We await the end of the year with great interest.

AUTHORS

Philip Woolfson is a Partner, and Daniella Terruso, EU Policy Advisor at Steptoe & Johnson, LLP.
Emails: DTerruso@steptoe.com
Pwoolfson@steptoe.com

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory 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 help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

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

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

Subscription Fees

Single User Access

International Edition **£500 + VAT***

UK Edition **£400 + 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 United Kingdom Report.
www.privacylaws.com/UK

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

EU-US Privacy Shield put into practice – first experiences

Some 200 companies had been certified towards the end of September. **Axel Spies** discusses the challenges already encountered and also what lies ahead of us.

The US Department of Commerce launched its self-certification system of the Privacy Shield (PS) on 1 August. The Commerce Department's PS website[1] provides information and assistance for US and European companies. Whoever expected long lines of registrants in front of the Department of Commerce building may be disappointed. Despite the publicity and huge expectations particularly in Europe, the enthusiasm among US companies has been lackluster. After

Continued on p.3

Privacy issues on the radar of competition authorities

How can regulators empower consumers and fight unfair user terms when they review mergers? **Laura Linkomies** reports from Brussels on the EU's Big Data challenge.

The EU Google antitrust case in 2014 set the alarm bells ringing: as Google has 90% of the European search market, has it abused its position? The answer from the European Commission was no, but Google had to make some concessions. In 2015, Disconnect, a US firm that designs privacy-enhancing technologies, filed a complaint against Google for violating privacy rights – Disconnect argued that

Continued on p.6

Issue 143 **October 2016**

NEWS

2 - Comment: World of privacy shrinks
8 - European Cyber Security Month

ANALYSIS

10 - Norway's Consumer Council wins revised app privacy terms
29 - The role of genetic data in personalized medicine

LEGISLATION

19 - Philippines puts key privacy rules in place but NPC faces pressure
22 - Data localisation in China and other APEC jurisdictions

MANAGEMENT

5 - Q&A on EU-US Privacy Shield
11 - Book Review: DP and Privacy
12 - Data portability under EU GDPR: A financial services perspective
15 - 3rd parties under the Privacy Shield
27 - Russia's DPA raises its profile
31 - Ashley Madison: Lessons for all
31 - Events Diary

NEWS IN BRIEF

9 - South Africa to appoint regulator
9 - US issues self-driving car guidance
14 - Privacy and trade agreements
14 - Senegal enters DP arena
18 - EU advice on Privacy Shield
21 - Israel's DPA issues guidance on audio recordings and CCTV
21 - Ecuador introduces privacy bill
26 - EU e-Privacy revision on its way
26 - US Cyber-Insurance Bill proposed
28 - Germany: GDPR Act leaked
28 - Bavaria issues GDPR guidance
28 - Ireland's hearing on Standard Contractual Clauses in February
31 - Ashley Madison: DPAs' report

INTERNATIONAL report

ISSUE NO 143 OCTOBER 2016

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

SUB EDITOR
Tom Cooper

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

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

CONTRIBUTORS
Axel Spies
Morgan Lewis LLP, US

Anna Romanou
Eurofins, Belgium

Stefania Tonutti
PhD in Law and New Technologies, Italy

Scott Livingston
SIPS Asia, Hong Kong

Philip Woolfson and Daniella Terruso
Steptoe & Johnson LLP, Belgium

Rena Mears, Ryan Sulkin, Eric Roth and Jim Halpert,
DLA Piper LLP, US

Merrill Dresner
PL&B Correspondent

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* International 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 2046-844X

comment

World of privacy shrinks as we share the same issues

Large mergers affect not only people as workers or consumers but also in terms of privacy protection – read on p.1 what the European Data Protection Supervisor and BEUC, the European Consumer Organisation, are trying to do about it. Data localisation laws, the requirement to process personal data in a country, are becoming better known now. It is not only an issue in Russia, but also in China and to some extent, also in some other APEC countries (p.22).

EU-US Privacy Shield work continues – the US Commerce Deputy Assistant Secretary, Ted Dean, has been talking to EU Data Protection Commissioners on how to make the Shield work the best possible way. Part of its success depends on a favourable view by the DPAs, part on the understanding and awareness of consumers (p.18) and part on the take-up and compliance by US business (p.1). On p.15, take a detailed look at how Privacy Shield obligations affect vendor management.

An additional important point, specifically for banks and telcos that cannot take advantage of the Shield, is the future of EU model contractual clauses. The case on their legality will now be heard in February next year (p.28). The EU may consider expanding the scope of the Privacy Shield, but for now, companies that do not want to apply for the Shield for one reason or another are in a limbo.

The right to data portability under the GDPR is still not well understood. Read on p.12 a financial services perspective on this new concept.

Organisations now have until September next year to organise compliance with the data protection law in the Philippines. Implementing regulations have been issued, and those processing data of at least 1,000 individuals must notify (p.19).

Genetic privacy poses many questions that are not governed by existing laws. Also the GDPR's approach in this field is somewhat unclear. While there are some guidelines on genetic data, genetic enhancement and personalized medicine, sufficient rules are lacking (p.29).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.