afme/
Finance for Europe

Effective flow of personal data post-Brexit

Implications for capital markets

April 2018

Association for Financial Markets in Europe
www.afme.eu

Contents

Executive Summary

The General Data Protection Regulation (GDPR) lays down rules for the protection of individuals with regard to the processing and free flow of personal data. The impending departure of the UK from the EU creates significant uncertainty as to the ability of businesses, including banks and investment firms, to continue to transfer personal data between the EEA and the UK post-Brexit.

This briefing note outlines:

1. The relevant requirements under GDPR for the processing of data and the mechanisms for transferring data between the EEA and third countries;
2. The uncertainty in relation to firms' ability to transfer personal data between the EEA and UK post-Brexit;
3. The importance of personal data sharing in providing an efficient and secure service to corporate and institutional clients; and
4. AFME's proposed solution - that the European Commission (EC) and the UK should, as a matter of priority:
    - Start discussions in preparation for Adequacy Decisions without delay; and
    - Commit to a transitional solution while adequacy assessments are undertaken.

1 GDPR Background

GDPR Background

- The GDPR will apply across the EU (including in the UK) from 25 May 2018. The EC has stated that the GDPR will:

  "strengthen the protection of the individual's right to personal data protection, reflecting the nature of data protection as a fundamental right for the European Union….it will guarantee the free flow of personal data between EU Member States and reinforce trust and security of the consumers…the Regulation will open up new opportunities for businesses and companies, especially the smaller ones, also by making clearer rules for international transfers of data."[1]

- There are two key concepts relevant for this note: the processing of data and Adequacy Decisions.

Data Processing

- Central to GDPR are new rules about how personal data can be "processed", a term used by data professionals which essentially means all forms of collecting, recording, storing, amending, using and transmitting data. Under the GDPR (as under the previous Data Protection Directive) there is a distinction between processing of personal data within and beyond the EEA.

- Processing of personal data within the EEA must meet the conditions in Chapters I to IV of the GDPR, including conditions relating to:

  - Principles relating to processing of personal data
  - Lawfulness of processing
  - Data subject rights

Adequacy Decisions

- Transferring personal data to a country beyond the EEA must, in addition, comply with conditions laid down in Chapter V. The simplest of these – and the only one which we believe to be practicable in a Brexit context - allows for data to be transferred without additional authorisation where EC has made an 'Adequacy Decision', meaning that it considers that the third country in question ensures an 'adequate' level of data protection.

- In the absence of an Adequacy Decision by the EC, data controllers must comply with one of the other tools listed in Chapter V, such as:

  - Standard contractual clauses (for external flows)
  - Binding corporate rules (for intra group transfers)
  - Approved code of conduct
  - Approved certification mechanism

- These are discussed below. Where none of the tools applies, transfers may only be made in specific situations (set out below at 3.1.6)[2].

[1] Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018. Available from: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf [Accessed 15 March 2018], p1.

[2] See Article 49 of GDPR

Uncertainties: can data be transferred between the EEA and UK post-Brexit?

2.1 UK law post-Brexit

The GDPR will apply in EU, including the UK, from 25 May 2018. The UK also intends to transpose the GDPR into UK law with effect from the date of the UK's withdrawal from the EU, under the EU (Withdrawal) Bill. The UK data protection framework will therefore be identical or close to identical to the EU data protection framework upon the UK's departure.

2.2 Consequences for data transfers

- On the assumption that the UK will no longer be a member of the EEA post-Brexit, the question that arises is whether it will continue to be possible for businesses and regulators to transfer personal data between the EEA and the UK. As of today, the EU has not made an Adequacy Decision in respect of the UK (there is no formal mechanism for it to do so, because the UK is not yet a third country).

- There is of course an identical issue in reverse, in relation to the transfer of data from the UK to the EEA, assuming that the UK replicates the GDPR provisions relating to international transfers. That is whether, pre-Brexit, the UK is able to recognise the data protection framework in the EEA.

2.3 Resulting uncertainties

- Firms require clarity on the legal framework that will be in place for cross-border data flows as a matter of urgency, as discussed further below.

- There are several sources of uncertainty:
    - whether the EU could use the existing mechanism pre-Brexit to recognise the UK as adequate
    - whether the EU will (in any case) choose to start an assessment of the adequacy of the UK data protection framework;
    - whether the EU will encounter and resolve any contentious issues in principle to a decision that the UK data protection framework is adequate
    - whether the EU will have time to reach a decision pre-Brexit

- The EC published a notice to stakeholders on 9 January 2018, drawing attention to this potential problem and the 'additional safeguards' that exist in the absence of an adequacy decision (emphasis added):

  "Subject to any transitional arrangement that may be contained in a possible withdrawal agreement, as of the withdrawal date, the EU rules for transfer of personal data to third countries apply. Aside from an "adequacy decision"…the EU's data protection rules…allow a transfer if the controller or processor has provided "appropriate safeguards". These safeguards may be provided for by:
    - **Standard contractual clauses:** the Commission has adopted three sets of model clauses which are available on the Commission's website;
    - **Binding corporate rules:** legally binding data protection rules approved by the competent data protection authority which apply within a corporate group;
    - Approved **Codes of Conduct** together with binding and enforceable commitments of the controller or processor in the third country;
    - Approved **certification mechanisms** together with binding and enforceable commitments of the controller or processor in the third country.

In the absence of an "adequacy decision" or of "appropriate safeguards" a transfer or a set of transfers may take place on the basis of so-called **"derogations"**: they allow transfers in specific cases, such as based on consent, for the performance of a contract, for the exercise of legal claims or for important reasons of public interest.

These tools are well-known to business operators in the Member States, as they are already being used today for the transfers of personal data to non-EU countries."[3]

3 Proposed solution

3.1 Drawbacks of the "additional safeguards"

The notice highlights the various tools that may be used to underpin certain data transfers to countries outside the EEA. While the tools are useful, and some of them are indeed being used today, there are some drawbacks to each of them, as discussed below.

- Standard contractual clauses (SCCs)
    - Setting up a network of SCCs is very complicated for multinational groups, such as banks, which have several legal entities and branch offices dispersed around the world. This requires a complex, slow process which maps data flows and sets up separate SCCs for each intra-company connection.
    - In addition, there are legal uncertainties regarding the ability to rely on SCCs approved by the Commission, because such clauses are currently under judicial challenge.[4] If SCCs were to be invalidated by the CJEU, businesses relying on SCCs would find themselves overnight without a lawful basis for transferring personal data to third countries. This has happened before.

- Binding corporate rules (BCRs)
    - BCRs allow large international organisations to transfer data. However, they are complex and time-consuming to implement. There are several criteria which must be fulfilled in order for multinational companies to put BCRs in place. These include forming intra-group agreements between enterprises that are engaged in joint economic activity, drafting new policies, and entering into a negotiation phase with lead data protection authorities, which may take one to two years. This makes companies reluctant to initiate an application process and puts BCRs out of reach of SMEs, who generally cannot afford it.
    - At present, only 33 entities have been authorised by the UK Information Commissioner to transfer personal data outside of the EEA under BCRs[5]. From the EU27 perspective, only 67 companies have completed the same procedure under BCRs[6]. It is highly unlikely that data protection authorities in the EU27 would be able to respond to an influx of BCR applications on a sufficiently prompt basis to allow ordinary business to continue.

[3] Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection. Available from: https://eubusinesslaw.wordpress.com/2018/01/12/notice-to-stakeholders-withdrawal-of-the-united-kingdom-and-eu-rules-in-the-field-of-data-protection/ [Accessed 15 March 2018].
[4] 2016 No. 4809 P. *The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems*. Available from: https://dataprotection.ie/documents/judgements/DPCvFBSchrems.pdf [Accessed 10 April 2018].
[5] Information Commissioner's Office: Binding Corporate Rules. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/ [Accessed 14 March 2018].
[6] European Commission: Binding corporate rules: Available from: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en [Accessed 15 March 2018].

- Codes of conduct

    - It would be very challenging for the industry to design a code, and have it approved, in the time available. There are no existing examples of codes of conduct being used as the legal basis for the transfer of personal data from the EEA to a third country. Accordingly, it is highly unlikely that codes of conduct will be a viable solution.

- Certification mechanisms

    - As with codes of conduct, certification mechanisms are unprecedented. At present, we are not aware of any accreditation bodies which would administer certification schemes; hence, there is significant uncertainty as to whether certification mechanisms will be available in time.

- Derogations

    - As noted at 2.3 above, in the absence of an adequacy decision or of appropriate safeguards, a transfer or set of transfers may take place on the basis of so-called derogations, which allow transfers in specific cases. The draft guidelines from the Article 29 Working Party state that the derogations must be interpreted restrictively so that the exceptions do not become the rule. Accordingly, derogations do not constitute a broad solution to the problem.

3.2 Importance of data sharing

- Financial conduct regulators expect firms to have a consolidated view of their corporate and institutional clients in order to meet regulatory requirements such as identifying suspicious transactions, assessing suitability, and combating money laundering, terrorist financing and market abuse. In order for firms to serve their clients, it is therefore necessary for firms to share personal data about employees, directors and shareholders of those clients across all their affiliated entities. In particular, a firm headquartered in the EU27 needs to have the ability to share such personal data with its affiliates in the UK, and vice versa. Firms also need to share personal data about their own employees across the firm, for example to ensure consistency of HR processes, or to monitor employee travel and compliance with expenses and entertainment policies.

- Many firms have established centralised processing hubs in multiple locations to support their data collection and analysis, and for reasons of data security and business resilience. There is a two-way communication flow. Affiliates will provide information to the hubs, which will in turn distribute appropriate information around the group. The hubs constitute an efficient and secure way of storing and processing personal data.

- The chief executive of the UK's Financial Conduct Authority (FCA) has identified the importance of solving the data transfer question, stating on 5 February that:

> "EU and UK firms hold and share a very large amount of data about each other's citizens. It is thought that around three quarters of cross-border data flows involving the UK are with EU member states. The UK is a major exporter of digital data services such as data hosting and processing and is the entry point to Europe for many global data-dependent businesses. The FCA itself is a major exporter of data on trading activity, helping other European regulators oversee firms and markets. In fact, in an average month we export over 250 million trade reports, compared with the 12 million we receive. If the UK was to leave the EU without mitigating actions on both sides, holding and sharing each other's data may be in breach of national law[7]."

[7] Financial Conduct Authority. The Future of the City Speech. Available from: https://www.fca.org.uk/news/speeches/future-city [Accessed 09 April 2018].

- For businesses to continue to operate on a cross-border basis, an arrangement is required to ensure the ongoing free flow of personal data post-Brexit. As the European Banking Authority (EBA) has stated, *"risks related to … data transfer and the protection of data with a third country could disrupt financial stability and market confidence."*[8]

3.3 Proposing a solution: towards an Adequacy Decision

- One possibility could be an EU-UK Privacy Shield similar to the one concluded with the US. This would however be open to legal challenge as was the case for the previous Safe Harbour arrangement.

- Another possibility could, in principle, be to insert horizontal provisions for cross-border data flows and personal data protection in the future relationship between the EU27 and the UK. A temporary solution could be achieved through a transitional agreement. We note that the agreement reached at the European Council on 23 March 2018 on the terms of a transition period starting on 29 March 2019 and lasting until the end of 2020 includes the potentially helpful wording "unless otherwise provided in this Agreement, Union law shall be applicable to and in the UK during the transition period", but exactly how that wording will be interpreted in practice is not crystal clear.

- However, in order to have a practical solution in advance of Brexit we consider that the best way to provide legal certainty for firms intending to transfer personal data between the EEA and UK is for Adequacy Decisions to be made by the EC and the UK. These, together with temporary solutions while adequacy assessments are made, need to be in place ahead of the UK's exit to ensure that there is no gap following the UK's withdrawal.

- Taking into account the EC's expertise and experience in reviewing whether a third country has an adequate level of protection, we believe that it could be feasible to complete the assessments within one year, provided that the matter is given sufficient priority.

- Adequacy Decisions are, in our view, feasible because:
    - the GDPR will apply in the UK from 25 May 2018 and the UK has stated the intention to align UK domestic legislation with the GDPR post-Brexit
    - subject to concerns regarding the UK Investigatory Powers Act (see below) the EU and UK data protection frameworks will therefore be at least as closely aligned as the frameworks in the countries for which an Adequacy Decision has already been made (though it is understood that the Commission is proposing to review all previous adequacy decisions to assess whether they meet the test of being "essentially equivalent")
    - the UK data protection authority has a track record of enforcement of data protection law (a key criterion for adequacy)
    - the same is true of data protection authorities across Europe
- Recent statements from the EC have also noted the connection between the UK's application of the GDPR and the decision on adequacy: the European Commissioner for Justice, Consumers and Gender Equality has stated that:

  "having the same data protection rules would make an EU-UK decision on adequacy much easier".[9]

[8] EBA, Risk Assessment of the European Banking System, 24 November 2017, p.17.
[9] Statement made by Commissioner Věra Jourová at a press conference following the publication of the "Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018" on 24 January 2018.

The UK Investigatory Powers Act 2016

- In relation to a possible Adequacy Decision, it should be noted that the UK Investigatory Powers Act 2016 (IPA) is perceived by some as currently incompatible with EU law, as a result of the CJEU judgement of 21 December 201610.

- In response, the UK Government is consulting on an amendment to the IPA, accepting that:

  "…DRIPA (Data [Retention] and Investigatory Powers Act 2014), and consequently some aspects of Part 4 of the IPA, are inconsistent with EU law, in that: a) there is no provision for independent authorisation of requests for access to retained data; and b) the crime purpose for retaining and accessing data is not limited to serious crime.[11]"

- In relation to access to retained data, the Government accepts the CJEU judgement that:

  "It is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime [para. 120]."[12]

  "The draft Regulations amend Part 3 of the IPA to provide for three different regimes for authorisation of communications data requests."[13]

- In relation to the crime purpose, the consultation notes that the CJEU held that:

  "Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure. [para. 102]."[14]

  Consequently, the UK Government is amending the legislation to define 'serious crime' for this purpose.[15]

- The UK Government clearly acknowledges that amendments to the IPA are essential in order to ensure its compatibility with EU law. Therefore, the CJEU's ruling should not prevent the Commission and the UK from starting the adequacy process, which could run in parallel with the implementation of the proposed amendments.

[10] Case-law of the Court of Justice. Judgment of the Court (Grand Chamber) in Joined Cases C-203/15 and C-698/15. Available from: http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EN [Accessed 14 March 2018].
[11] Investigatory Powers Act 2016. Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf [Accessed 15 March 2018], p6.
[12] Ibid. p18.
[13] Ibid. p18.
[14] Ibid. p14.
[15] Ibid. p15.

5 Conclusion and Recommendations

Conclusion and Recommendations

- For the reasons set out above, it is essential that there is clarity as to the ability for businesses, including banking and investment firms, to continue to transfer personal data between the EU and UK post-Brexit.

- Given the alignment of EU and UK data protection frameworks, and the complexities, protracted process and shortcomings of the other solutions, we propose that the EC and the UK should as a matter of priority:

- agree to start discussions in preparation for Adequacy Decisions without delay. We believe that such a process can proceed independently of the wider negotiations on the future relationship between the EU27 and the UK; and

- commit to providing a temporary solution to avoid any gap while adequacy assessments are undertaken, for example in the Withdrawal Agreement, any other bilateral agreement or, if necessary, through unilateral action.

- We would welcome the opportunity to work with all parties involved in this process, including the European Commission, Member States, and national supervisory authorities. We believe that free flow of data is a cross-sectoral issue, not a political issue but one that is vital for Europe's businesses, including Europe's capital markets businesses which we represent.

Contacts

Richard Middleton
Managing Director, Co-Head of Policy Division
Richard.Middleton@afme.eu
+44 (0)20 3828 2709

Will Dennis
Managing Director, Co-Head of Policy Division
Will.Dennis@afme.eu
+44 (0)20 3828 2683

Oliver Moullin
Managing Director, Brexit
General Counsel and Company Secretary
Oliver.Moullin@afme.eu
+44 (0)20 3828 2712

Stevi Iosif
Associate Director, Advocacy
Stevi.Iosif@afme.eu
+32 2 788 39 76

Aleksandra Wojcik
Associate, Policy, Technology and Operations
Aleksandra.Wojcik@afme.eu
+44 (0)203 828 2734