
AFME feedback on the European Commission's Roadmap on the report on the application of the General Data Protection Regulation

29th April 2020

The Association for Financial Markets in Europe (AFME)¹ is pleased to provide feedback to the European Commission's roadmap on the upcoming report on the application of the General Data Protection Regulation ('GDPR')².

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

The GDPR is intended to give individuals more control over their personal data, to provide a greater level of transparency as to what is being processed and why, and to ensure that data controllers can demonstrate that their companies comply with the requirements. It also aims to improve business opportunities by facilitating the free flow of personal data in the European Digital Single Market. AFME believes that the GDPR has been an important milestone and we set out below some brief comments we hope the European Commission finds useful in the drafting of its report on the application of the GDPR.

Scope of the review:

Article 97 GDPR requires the European Commission to submit a report on the evaluation and review of the GDPR. Article 97(2) requires the Commission to examine, in particular, the application and functioning of Chapter V on the transfer of personal data to third countries, and Chapter VII on cooperation and consistency. The Commission may choose also to consider other aspects of the GDPR in its review.

We note that the European Council in its position and findings on the application of the General Data Protection Regulation "encourages the Commission to evaluate and review in its upcoming report the application and functioning of the GDPR beyond what is specifically mentioned in that article"³.

Given the importance and the impact of the GDPR, AFME is of the opinion that the European Commission should not limit its review to the issue of international transfer of personal data to third countries and the cooperation and consistency mechanism between national data protection authorities.

In this note, we set out our comments on the following aspects of the GDPR

- Firms in the financial sector, in particular with regard to data sharing for the purposes of AML/CFT;
- International transfers (in particular Standard Contractual Clauses);
- Geographic scope (Article 3 GDPR);
- Cooperation and consistency.

¹ AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia. AFME is registered on the EU Transparency Register, registration number 65110063986-76.

² [Report on the application of the General Data Protection Regulation - Roadmap.](#)

³ [Council position and findings on the application of the General Data Protection Regulation \(GDPR\), paragraph \(6\).](#)

Association for Financial Markets in Europe

London Office: 39th Floor, 25 Canada Square, London E14 5LQ, United Kingdom T: +44 (0)20 3828 2700

Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 788 3971

Frankfurt Office: Bürohaus an der Alten Oper, Neue Mainzer Straße 75, 60311 Frankfurt am Main, Germany

T: +49 (0)69 153 258 967

www.afme.eu

Firms in the financial sector:

The GDPR is intended to give individuals more control over their personal data, to provide a greater level of transparency as to what is being processed and why, and to ensure that data controllers can demonstrate that their companies comply with the requirements.

Firms are however required to obtain, analyse, and retain large amounts of personal data in order to meet their wider regulatory obligations, including responding to requests from financial regulators and from law enforcement.

So, on the face of it, there could be a conflict between the GDPR and the financial regulatory framework, unless there is a clear lawful basis for processing.

Firms may need to process personal data for the following purposes:

- (1) Compliance with a legal obligation under EU or Member State law
- (2) Compliance with guidance from regulatory authorities
- (3) Compliance with a non-EU legal obligation
- (4) Regulatory cooperation with financial conduct regulators and law enforcement (where not mandated by EU law)
- (5) Protection, e.g. protecting the firm against legal claims, or protecting the firm, customers and others against fraud and other crimes

The key point in each situation is for firms to establish a lawful basis for processing, and to be able to demonstrate that they have done so.

There are specific rules for certain cases, such as processing of special categories of personal data (Article 9 GDPR), processing of personal data relating to criminal convictions and offences (Article 10 GDPR), and international transfers (Chapter V GDPR). In these cases, in addition to establishing a lawful basis for processing as described above, it is necessary to meet further conditions.

While there is a potential conflict in certain cases between the GDPR and the financial regulatory framework, our analysis is that the GDPR has anticipated most of the problems, and that firms should generally be able to continue processing data to meet their wider obligations to regulators.

We would nevertheless encourage the European Commission to ask, as part of its review, whether there are any areas of potential conflict, and we would be pleased to seek input from the industry in this regard.

For instance, in the context of financial crime and the fight against money laundering, it is important to ensure that obliged entities are able to access information which may be relevant to carry out customer due diligence. National competent authorities have also expressed some questions about their abilities to exchange information between them, including outside of the EU.

International transfers:

AFME would welcome further legal certainty as regards international data transfers, notably considering the current legal challenges to the European Commission Standard Contractual Clauses (SCCs)⁴, the EU-US Privacy Shield⁵, as well as the uncertainty surrounding Brexit. Guidance on how best to deal with international transfers involving EEA-based processors acting on the instructions of a non-EEA entity would for instance be particularly helpful.

⁴ [Case C-311/18](#).

⁵ [Case T-738/16](#).

Furthermore, with regards to SCCs, we would encourage the Commission to focus on specific improvements needed to the SCCs, namely as it relates to a data processor in the EU transferring personal data to its sub-processors outside of the EU, in order to provide services to the data controller with whom a service agreement is in force. In these cases, the SCCs provided in Decision 2010/87⁶ cannot be used. The Commission could, for instance, make reference to or take into account the former WP29 working document on “Draft Ad hoc contractual clauses EU data processor to non-EU sub-processor” (WP214 of 21 March 2014)⁷ which provide different options to regulate the transfers to third countries.

Moreover, we believe that the European Commission, in order to ensure that data subjects have an effective protection *vis-à-vis* a cross border transfer, should make reference to, and take into consideration, the application of article 50 GDPR. It would be advisable that the European Data Protection Authorities (DPAs), the EDPB and the European Commission actively work to implement an effective international cooperation system, in compliance with article 50 GDPR. The international cooperation system provided for by Article 50 should also aim at supporting the DPAs of non-EU countries in the application of the rules laid down in the matter of privacy, which in turn, would provide data subjects with an effective protection of their rights in the third country of destination or in the various non-EU countries which are part of a chain of transfers.

Geographical scope of the GDPR:

Our members would welcome further clarification on the scope of the GDPR, notably as it concerns multinational organisations with cross-border activities which may pose challenges in determining the applicability of Article 3 GDPR. For instance, this could include guidance on whether non-EU organisations captured by Article 3(2) should be considered as ‘adequate’ for international transfer purposes.

We would thus encourage the European Commission to pay particular attention to these issues when conducting its review of the application of the GDPR.

Consistency and cooperation among authorities:

AFME encourages the European Commission to assess the level of consistency and cooperation amongst data protection authorities within the EEA. Although, and as stated in Article 52 of the Regulation, data protection authorities are independent supervisory authorities responsible for monitoring the application of the GDPR, and for issuing guidance at national level, our members have noticed that authorities within the EU may in some cases have a different interpretation of the legislative requirements provided for by the GDPR. For instance, we have noted some differences in interpretations with regard to Article 9 (on the conditions for processing special categories of personal data) and with regard to Article 33 (on the notification threshold of a personal data breach to the supervisory authorities). This creates additional complexity for companies operating cross-border.

AFME looks forward to continue exchanging on this important topic and stands ready to support the European Commission’s review of the GDPR.

AFME Contacts

Richard Middleton
Richard.Middleton@afme.eu
+44 (0)20 3828 2709

Aleksandra (Ola) Wojcik
Aleksandra.Wojcik@afme.eu
+44 (0)20 3828 2734

Hélène Benoist
Helene.Benoist@afme.eu
+32 (0)2 788 39 76

⁶ [European Commission Standard contractual clauses for the transfer of personal data to processors established in third countries, Recital 23](#)

⁷ [WP29 Draft Ad-hoc contractual clauses “EU data processor to non-EU sub-processor.”](#)