European Payment Institutions Federation aisbl

26TH APRIL 2013

EPIF'S POSITION PAPER ON THE EUROPEAN COMMISSION'S PROPOSAL FOR A GENERAL DATA PROTECTION REGULATION

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment institutions ("PI") sector at the European level. We currently represent over 250 PIs offering services in every part of Europe. Our diverse membership includes the broad range of business models covered by the PSD including:

- 3-party Card Network Schemes
- Acquirers
- Money Transfer Operators
- FX Payment Providers
- Mobile Payments
- Payment Processing Service Providers
- Card Issuers

EPIF seeks to represent the voice of the PI industry with EU institutions, policymakers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as an infrastructure provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of society (e.g. via mobile and internet).

INTRODUCTION

EPIF welcomes the European Commission's proposal for greater harmonisation of the EU data protection regime within the internal market with regard to the processing of EU personal data.

A number of provisions, however, lead in their current form to legal uncertainty as they seem to be in conflict with the requirements under applicable Anti-Money Laundering and Counter-Terrorism Financing rules (AML/CFT). Under European AML/CFT rules, i.e. the 3rd AML Directive, customer due diligence measures (CDD) need to be taken in order to effectively fight money laundering, terrorism financing, fraudulent activities as well as other forms of crime.

These CDD requirements foresee the creation of customer profiles as part of the required risk assessment and risk measures[1]. The financial industry is required to keep respective customer data for at least 5 years after the business relationship comes to an end, in some cases Member States request a longer period of time.[2] **Thus, it needs to be clarified that data protection rules, for instance on 'profiling' or 'the right to be forgotten', do not compromise applicable AML/CFT rules in order to allow the obliged entities to conduct their business in a lawful and compliant manner.**

A risk-based approach with regard to the type of data and/or processing purpose (e. g. personal profiling) is strongly recommended. The best approach would be to keep current rules that allow data processing according to 'legitimate interests', including for AML, fraud and risk management purposes. For that purpose, we recommend to clarify this explicitly in the text of the Regulation.

Also, some provisions significantly increase of costs and bureaucracy for companies. The Regulation should therefore focus on genuine and substantive privacy risks, rather than providing prescriptive governance. The Regulation could deliver key benefits, such as simplification of intra-company and international data transfers, enabling companies to deal with one data protection authority, and harmonisation of rules.

[1] See for instance Chapter II (Customer Due Diligence) of Directive 2005/60/EC – the "3rd AML Directive".

[2] See Article 30 of Directive 2005/60/EC. Unfortunately, the 3rd AML Directive is a "minimum harmonisation" Directive, therefore Member States are allowed to go beyond its provisions (cp. Article 5).

Based on the above, EPIF would like to highlight the following issues:

1. PROFILING (ARTICLE 20)

It is unclear what form of profiling is covered by Article 20 as '*legal effects*' and '*significantly affects'* are too general and bear the risk of undue restriction on otherwise legitimate data analysis activity. As mentioned above, it is unclear if, or how, common AML and permitted customer insight analysis would be impacted. Article 20 should focus only on profiling that causes serious and unjustified prejudice, rather than on preventing legitimate and economically important data analysis, such as AML, fraud prevention and customer insight work. For instance fraud prevention in order to protect payment institutions and payers and payees from fraud by third parties (e.g. lost or stolen cards, compromised card numbers) requires the profiling of all card transactions and the matching against certain fraud patterns. For the avoidance of doubt, we recommend adding an explicit statement in the text clarifying that applicable AML/CFT requirements and -rules as well as justified business needs of data controllers do not conflict with the new data protection rules.

2. RIGHT TO BE FORGOTTEN (ARTICLE 17)

The current draft stipulates an obligation to ensure data subjects can delete personal data held on them. However, the retention of some data, for example for AML, tax and risk management purposes, is already a legal requirement under existing law, and should therefore be excluded from the scope of this Article.

3. INFORMATION TO THE DATA SUBJECT (ARTICLE 14)

Information requirements in Article 14 contain additional requirements compared with today's rules. Pursuant to the new regulation, the data subject for example has to be informed about legitimate interests or contractual reasons for data use, retention periods and the basis for international transfers. Many consumer notices have already been criticized for being too detailed. The current proposal will lead to further additions and to even longer provisions, which could greatly add to customer confusion.

4. DATA PORTABILITY (ARTICLE 18)

The proposals on data portability and in particular the requirement to use a prescribed common format would present significant practical difficulties as well as substantial costs for businesses. The data collected and processed by Payment Institutions is largely part of legal and regulatory requirements, such as AML and tax. It is therefore difficult to see what practical benefit data subjects will gain through this right.

5. SECURITY BREACH NOTIFICATION (ARTICLES 31,32)

EPIF recommends a risk-based approach for the data security breach notification requirement. A large number of data security breach notifications could, for example, confuse data subjects. Breach notification should therefore focus on serious breaches. EPIF recommends that breach notifications should be issued without undue delay, but only after a comprehensive analysis and investigation of the data breach.

6. IMPACT ASSESSMENT (ARTICLE 33)

The proposal on data protection impact assessments is commercially unworkable. In particular, the obligation for consultation with stakeholders (Article 33 paragraph 4) is not realizable because of the risk of disclosing confidential business information. We recommend adding a section that includes the possibility to prove that measures can be taken to protect personal data by presenting adequate and established certificates. There is also a need to specify that the primary aim of a PIA is to ensure compliance with data protection law, rather than some wider non-legal policy outcome.

7. PSEUDONYMIZATION

Under the proposed new rules, the process to remove a personal identifier of personal data or to encode personal data is not addressed by the Proposed Regulation and therefore subject in full to the Proposed Regulation. This serves as a disincentive to pseudonymize personal data and is arguably in conflict with the actual developments and efforts of banks, payments institutions, credit card issuers and others to pseudonymize as much personal data as possible in the online environment or on paper bound documents (card numbers, bank account data etc.). Given the requirements for consent and in the absence of additional clarity with respect to the legitimate interest clause, a new legal basis should

be added to the Proposed Regulation to authorize the processing of pseudonymized data without data subject consent.

8. SANCTIONS (ARTICLE 79)

The proposed sanctions of up to € 1 million or 2 % of worldwide annual turnover of the data controller or even data processor also include negligent breaches of the data protection rules. Since it will be supplemented by national penalties the inclusion of a negligent breach as well as the maximum amount of the sanction are exaggerated. This will lead to a considerable increase of processing costs due to much higher insurance coverage costs for the Data Controllers. At the very end consumers and companies will have to bear these additional costs. Furthermore there is no real business need for such kind of sanctions. If sanctions are introduced, than public bodies processing personal data should be included.

Other parts of the European Commission proposal are considered as positive by EPIF and we encourage policy makers to ensure these aspects and principles are reflected in the final outcome of the debate:

A) "Home regulator" principle (Article 49)

The proposal allows a data-controller to deal with a single regulator. This principle may simplify compliance and improve the consistency of rules. It is a key benefit.

B) Binding Corporate Rules (Article 43)

Binding Corporate Rules will simplify data-transfers. Wider simplification of international and inter-company transfers would be helpful.

C) Controller/Processor responsibility to be clearly defined (Article 24)

The controller currently carries the responsibility for all data security risks of its sub-contractors. The proposed new obligation of these entities to keep data secured allows regulators to take actions against sub-contractors and will split data controllers' responsibility. However, the split of obligations between the data controllers on the one hand and respective sub-contractors on the other should be clearly defined. On the other hand the expanded definition of a Data/Joint controller will lead to a re-qualification of many Data Processors into Joint Controllers. This might lead to a joint and several liability of a Data Processor with a Data Controller and increase the costs of data processing. The definition of a Joint Controller should there be revisited and better defined.

For more information about the PI sector, the EPIF organisation and its members or our position papers, please contact us via our website or secretariat.