European Payment Institutions Federation aisbl

24 SEPTEMBER 2015

EPIF'S POSITION PAPER ON THE GENERAL DATA PROTECTION REGULATION

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 250 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. EPIF thus represents roughly one third of all authorized Payment Institutions in Europe.[1] Our diverse membership includes the broad range of business models including:

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

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers 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 a 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 payment users (e.g. via mobile and internet).

[1] According to the European Commission, there were 568 authorized Payment Institutions in Europe as per end 2012.

W: www.paymentinstitutions.eu E: info@paymentinstitutions.eu T: 0032 (0)2 588 1303

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. We share the view that data flows are an indispensable component of a thriving and expanding digital economy. At the same time, we also recognize that the protection of personal data is essential to maintain consumer confidence and the integrity of the system. Given the importance of this file, EPIF has been monitoring the debates and positioning of the European Parliament and Council on the reform of the Data Protection package and noted agreement among the institutions to reach a final political agreement by the end of 2015.

Among our primary reactions to the draft reform, EPIF highlights four areas of particular importance from the payments industry perspective: (1) We welcome efforts to ensure that the EU's data protection regime is applied consistently across the whole of the EU, which should be the benefit of a regulation over the present directive; (2) Any new data protection regulation should conform with the requirements of other applicable EU policies to avoid conflicts and ensure legal certainty to the greatest extent possible; (3) Existing procedures that facilitate the transfer of data should be recognized in the new regulation and continued; and (4) While the intention of new provisions such as impact assessments, data portability and data subject notification is clear, we encourage EU institutions to bear in mind the unintended consequences a greater administrative burden could have on business operations to the detriment of meeting consumer expectations for a growing number of rapid and secure payment options. We encourage policy-makers to ensure these aspects and principles are reflected in the final version of the regulation.

A number of provisions, 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**

[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).

W: www.paymentinstitutions.eu E: info@paymentinstitutions.eu T: 0032 (0)2 588 1303

the obliged entities to conduct their business in a lawful and compliant manner. EPIF supports the Council's proposal introducing an exception for the consent on profiling when the latter is conducted for the purposes of fraud prevention. However, it is not clear whether this would include profiling for AML/CFT purposes[3].

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. EPIF welcomes the Council's position on enhancing the provisions on 'legitimate interest' for processing data but remains concerned about the need for further clarity on this matter.

Also, some provisions significantly increase the costs and bureaucracy for companies. The Regulation should therefore focus on genuine and substantive privacy risks, rather than providing prescriptive governance. However, EPIF is satisfied with the provisions on the one-stop-shop mechanism and supports the simplification of the supervisory framework. Furthermore, streamlining international data transfer provisions is a positive step towards harmonising the data protection rules.

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

1. PSEUDONYMIZATION (ARTICLE 4)

Under the proposed new rules, the process to remove a personal identifier of personal data or to encode personal data is not addressed and therefore should be incorporated. We encourage the Council's effort to include this in its General Approach. 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. In order for pseudonymization to be effective, the Proposed Regulation must provide incentives for data controller in particular as pseudonymized data will present much reduced privacy risks to an individual. A requirement for consent for the processing of pseudonymized data would not achieve this aim; in fact, it could discourage its use.

[3] See amendment 33, page 91and 92 of DAPIX document 10391/15, dated 8 July 2015

W: www.paymentinstitutions.eu E: info@paymentinstitutions.eu T: 0032 (0)2 588 1303

2. INFORMATION TO BE PROVIDED WHEN THE DATA ARE COLLECTED FROM THE DATA SUBJECT (ARTICLE 14)

Information requirements in Article 14 contain additional requirements compared with the current 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. We remain concerned that the Proposed Regulation will increase the amount of information that data controllers are required to provide to data subjects. This is not in the interest of data subjects. The focus should be on providing helpful, useful and clear information that will improve data subjects' understanding of data processing operations. Overly prescriptive rules on the provision of information risk make privacy notices longer, less clear and less valuable to data subjects.

3. RIGHT TO ERASURE '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.

4. RIGHT TO 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 the legal and regulatory requirements, such as AML and tax. EPIF is concerned that having the right to transfer personal data from one service provider to the other could cause issues as often this information would include confidential and commercially sensitive information.

5. AUTOMATED INDIVIDUAL DECISION MAKING (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

W: www.paymentinstitutions.eu E: info@paymentinstitutions.eu T: 0032 (0)2 588 1303

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 as well as justified business needs of data controllers do not conflict with the new data protection rules.

6. CONTROLLER/PROCESSOR OBLIGATIONS (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 therefore be revisited and better defined.

EPIF welcomes the Council's proposal on mandating the lead authority in the Member State where the processor or controller is established. However the recent developments regarding the One-Stop-Shop (OSS) undermine the original aim of the European Commission. Council proposals to enable local data protection matters to be handled by the local data protection authority, combined with greater involvement of local data protection authorities in cross-border cases, means the original benefits of dealing with a single authority would not be achieved. In addition, EPIF is concerned that for cases that are handled by the OSS mechanism there is currently no right for the data controller to present itself during the discussions between the various impacted data protection authorities and the European Data Protection Board (EDPB) and there is no basis to appeal a decision of the EDPB. These gaps need to be addressed in order to avoid undermining the OSS mechanism through decisions reached without the involvement of the parties to the case.

EPIF welcomes all efforts to promote the consistent application of data protection regulation across all Member States and, therefore, supports the advisory role for the European Data Protection Board as proposed by the Commission. At the same time, however, we believe a more empowered EDPB could create ambiguities among the roles and responsibilities of that body relative to existing competent national data protection authorities and also add a further level of administrative process rather than streamline the current regulatory regime. The final text of the data protection regulation should ensure the respective authorities and mandate of EU- and national-level bodies remain clearly defined.

W: www.paymentinstitutions.eu E: info@paymentinstitutions.eu T: 0032 (0)2 588 1303

7. 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 welcomes the Council's and European Parliament's position where the security breach notification is more targeted. However, EPIF recommends that breach notifications should be issued without undue delay, but only after a comprehensive analysis and investigation of the data breach. Data breaches can take time to investigate properly which must be recognized in the Proposed Regulation.

8. IMPACT ASSESSMENT (ARTICLE 33)

The proposal on data protection impact assessments is commercially resource intensive and more likely to be difficult to implement in practice. We understand the desired objective, but assess the unintended resource implications of adherence to this requirement could include increased costs and impediments to meeting consumer expectations for versatile, near real-time payment options. In particular, the obligation for consultation with stakeholders (Article 33 paragraph 4) may not be realizable because of the risk of disclosing confidential business information. EPIF recommends 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.

9. BINDING CORPORATE RULES AND DATA TRANSFERS (ARTICLE 43)

Binding Corporate Rules will simplify data-transfers, while protecting personal information. EPIF is satisfied with the Council's position on the international data transfers where a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country or territory processing one or more specified sectors within that third country or the international organisation in question ensures an adequate level of protection. EPIF finds that this could simplify the international and inter-company transfers.

Additionally however, where an organisation has implemented BCRs, they should be excluded from participating in proposed EU Privacy Seal Schemes (Article 39 – Certification), as organisations with approved BCRs have gone through an intensive application process, which should be acknowledged as an equivalent (or enhanced level) to privacy seals.

W: www.paymentinstitutions.eu E: info@paymentinstitutions.eu T: 0032 (0)2 588 1303

EPIF welcomes proposals to remove the need for data protection authority approval for the use of standard contractual clauses. As DPA approval is not always required in each Member State under the current framework, this development will align the requirements across the EU, significantly simplifying the use of such clauses and incentivize their use further.

10. HOME REGULATOR PRINCIPLE (ARTICLE 49)

EPIF welcomes the proposal on the 'Home Regulator' which 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 provided the respective roles and jurisdiction of a future European Data Protection Board and national Data Protection Authorities are clearly delineated for service providers seeking to comply with both overarching EU and Member State requirements.

11. 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. This would increase the costs for companies 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. In the end consumers and companies will have to bear these additional costs. Furthermore there is no real business need for this kind of sanctions. If sanctions are introduced, those public bodies processing personal data should be included. It is vital that any sanctions are targeted at genuinely serious cases and that data protection authorities have discretion over whether and at what level to issue fines.

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.

W: www.paymentinstitutions.eu E: info@paymentinstitutions.eu T: 0032 (0)2 588 1303