Opinion of the European Data Protection Supervisor

on a proposal for a Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2], and in particular Article 28(2) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 27 July 2013, the Commission adopted a draft proposal for a Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC (the proposed Directive), and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions.[3] These proposals were sent to the EDPS for consultation on 28 July 2013.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM (2013) 547 final and COM (2013) 550 final.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

2. The EDPS welcomes the fact that he is consulted by the Commission and welcomes that a reference to this Opinion has been included in the preamble of the instruments.

3. Before the adoption of the proposed Regulation, the EDPS was given the possibility to provide informal comments to the Commission. Some of these comments have been taken into account. As a result, the data protections safeguards in the proposed Regulation have been strengthened.

4. As the proposal for a Regulation does not raise any issues from a data protection point of view, the EDPS will concentrate his comments on the proposed Directive.

1.2. Objectives and scope of the proposed Directive

5. The aim of the proposed Directive is to help develop further an EU-wide market for electronic payments, which will enable consumers, retailers and other market players to enjoy the full benefits of the EU internal market, in line with Europe 2020 and the Digital Agenda. To achieve this and promote more competition, efficiency and innovation in the field of e-payments, the Commission states that there should be legal clarity and a level playing field, leading to downward convergence of costs and prices for payment services users, more choice and transparency of payment services, facilitating the provision of innovative payment services, and to ensure secure and transparent payment services.

6. The Commission claims that these objectives will be achieved by updating and complementing the current framework on payments services, providing for rules that enhance transparency, innovation and security in the field of retail payments and improving consistency between national rules, with an emphasis on the legitimate needs of consumers.

2. Specific comments on the proposed Directive

2.1. General reference to data protection law

7. The EDPS notes that the provision of payment services requires the processing by different stakeholders of personal data: names, bank account numbers and content of contracts need to be exchanged between payers and payees and through their respective payment service providers in order to guarantee a smooth functioning of the transfers.

8. The EDPS welcomes the introduction in Article 84 of a substantive provision stating that *any* processing of personal data taking place in the frame of the proposed Directive should be done in full respect of the national laws implementing Directive 95/46/EC and Directive 2002/58/EC, and of Regulation EC No 45/2001.

9. However, the EDPS recalls that clarifying the applicable data protection legislation is essential but not sufficient. The references to applicable data protection law should be specified in concrete safeguards that will apply to any situation in which personal data processing is envisaged.

10. In his letter in response to the Commission´s public consultation on the Green Paper entitled "Towards an integrated European market for card, internet and mobile payments"[4], the EDPS underlined that the full respect of EU data protection rules requires specific safeguards to be applied. In particular, he indicated that the exchange and processing of personal data related to payers and payees and with the various payments service providers must respect the principles of necessity, proportionality and purpose limitation, as well as the obligation not to keep the data for longer than it is necessary. The EDPS also highlighted the crucial importance of transparency as a means of ensuring the effective exercise by individuals of their data protection rights. The EDPS therefore recommends that specific safeguards are explicitly included in the text of the proposed Directive, as detailed further below.

2.2. The legal basis for the processing of personal data

11. As to the processing of personal data by payment systems and payment service providers, it should be made clear in the proposed Directive that the provision of payment services entails the processing of personal data. Currently the proposed Directive envisages the processing of personal data solely in the context of the prevention, investigation and detection of payment fraud according to Recital 71, without taking into account the fact that the provision of the payment service itself may imply the processing of personal data. As to the legal basis justifying such processing, it should be clarified expressly in the proposed Directive that the processing of personal data may be carried out insofar it is necessary for the performance of payment services.

12. As regards the processing of personal data for the prevention, investigation and detection of payment fraud, the EDPS considers that Article 84 of the proposed Directive is not precise enough to be considered as a valid legal ground for such processing. The provisions regulating fraud prevention should - at least in main lines - define more precisely the purpose(s) of the processing, the personal data concerned and the modalities of the processing. When defining these elements for the processing of personal data, due account should be taken of the principle of proportionality (only those personal data that are necessary for the purpose of the processing may be processed). The EDPS therefore recommends inserting a more precise provision in the proposed Directive.

[4] See EDPS letter of 11 April 2012 in response to DG MARKT public consultation on the Green Paper entitled "Towards an integrated European market for card, internet and mobile payments", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-04-11_Mobile_Payments_EN.pdf

2.3. Proportionality of the processing

13. It should be ensured that the different actors only access and process the data that are necessary for the performance of their services (see for instance Recital 26). As an illustration, in principle mobile operators responsible for the transmission of the transaction order should not have access to content information on the details of payments. This should be expressly stated in a substantive provision of the proposed Directive.

14. In the same way, the provisions on third party access (see below under 2.7.) in Articles 58 and 59 of the proposed Directive should make clear that information about 'availability of sufficient funds' should consist in a simple 'yes' or 'no' answer to the question if there are sufficient funds available – not in for example a statement of the account balance.

15. The EDPS underlines the importance of implementing the principles of "privacy by design" and "privacy by default" in all data processing systems developed and used under the proposed Directive. These concepts have emerged under the current data protection Directive 95/46/EC and are expected to receive legal recognition under the proposed General Data Protection Regulation (see Article 23)[5]. "Privacy by design" refers to the integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data, while "privacy by default" refers to the selection of the most privacy friendly configuration by default.

16. "Privacy by design" implies *inter alia* – that it is ensured that data processing systems are designed to process as little personal data as possible (data minimization); that "privacy by default" settings are implemented; that access to individual's information is limited to what is strictly needed in order to provide the service; and that tools enabling users to better protect their personal data (e.g. access controls, encryption) and exercise their rights are implemented.

17. The EDPS has repeatedly underlined the importance of appropriately taking into account these concepts in the implementation of the Digital Agenda[6], in anticipation of the adoption of the proposed General data protection Regulation. He therefore recommends adding in a substantive provision of the proposed Directive stating the obligation that "privacy by design/privacy by default" be embedded in all data processing systems developed and used in the frame of the proposed Directive.

[5] COM (2012) 11 final.

[6] See EDPS Opinion of 18 March 2010 on 'Promoting Trust in the Information Society by Fostering Data Protection and Privacy' and EDPS Opinion of 10 April 2013 on the Communication from the Commission on 'The Digital Agenda for Europe - Driving European growth digitally', available on the Consultation section of the EDPS website: www.edps.europa.eu

.

2.4. Supervision by competent authorities

18. The EDPS welcomes that the proposed Directive in Recital 32 introduces a duty for competent authorities to exercise their powers "with respect to fundamental rights, including the right to privacy" when supervising the compliance of payment institutions. The recital also states that for the exercise of those powers which may amount to serious interferences with the right to respect private and family life, home and communications, Member States should have in place adequate and effective safeguards against any abuse or arbitrariness, for instance, where appropriate through prior authorisation from the judicial authority of the Member State concerned. The EDPS recalls that these requirements are without prejudice to the control of an independent authority (national Data protection authority) under Article 8 (3) of the Charter of fundamental rights of the European Union.

19. The EDPS would, however, like to see the concretisation of such requirements in a substantive provision of the proposed Directive. He therefore recommends introducing in Article 22 of the requirement for competent authorities to request documents and information by formal decision, specifying the legal basis and the purpose of the request and what information is required, as well as the time-limit within which the information is to be provided.

2.5. Exchange of information

20. Article 25 of the proposed Directive requires competent authorities to exchange information between them and with the European Central Bank, and with the national central banks of the Member States, EBA or other relevant competent authorities designated under national or EU legislation applicable to payment service providers.

21. Article 26(3) provides that competent authorities shall exchange all essential and/or relevant information, in particular in the case of infringements or suspected infringements by an agent, a branch or an entity to which activities are outsourced. In some cases these exchanges of information will undoubtedly relate to identified or identifiable individuals, for example to an agent, a payment service user or a consumer.

22. The EDPS considers that both provisions are too vague and, consequently, do not provide adequate legal basis for the required processing of personal data. As regards purpose limitation, the proposed Directive fails to specify the purposes of the exchange of information and the kind of data that will be exchanged, including any personal data. Furthermore, the EDPS notes that the proposed Directive does not lay down any concrete limitation of the period for the retention of the personal data potentially processed. This is likely to lead to uncertainty and undue diversity in national implementation and/or practice.

23. On the basis of the foregoing, the EDPS recommends (i) mentioning the purposes for which personal data can be processed by national competent authorities, the EU central bank, the national central banks and the other authorities referred to in Article 25, (ii) specifying the kind of personal information that can be processed under the proposed Directive, and (iii) fixing a proportionate data retention period for the above processing (or at least introducing precise criteria for its establishment at national level).

2.6. Transparency and information of individuals

24. The EDPS takes note that several provisions[7] set forth a number of requirements to increase transparency towards users. He believes that the requirement of transparency as regards payment services should also include the obligation of transparency in respect of the processing of personal data of individuals. Data subjects should know who processes what data for which purpose, for how long, and how they can exercise their rights, including those related to the access to their data and to their rectification or erasure.

25. The EDPS therefore recommends including in a substantive provision of the proposed Directive a specific reference to the obligation to provide individuals with appropriate information about the processing of personal data in accordance with national provisions implementing Articles 10 and 11 of Directive 95/46/EC and to Article 11 of Regulation EC No 45/2001.

26. Furthermore, Recital 35 should also be amended to require the provision of all information required under the Directive "*as well as under Directive 95/46/EC and Regulation EC No 45/2001"* (also, the word "*only*" should be deleted, as the information requirements laid down in the Directive are not the only ones that need to be complied with).

27. The provision of information about the processing of personal data in due time before requiring the payment service is all the more important as consent of the user is meant to play a central role and authorisation of payment transactions would only be considered to be given if the payer has given his consent. Before providing his/her consent to the transaction, the payer should not only be informed about the price and fee calculations but also of the modalities of the processing of his/her personal data so that he can take an informed decision about such payment and the implications on the processing of his/her personal data.

28. The EDPS welcomes that the provisions on transparency provide clear rules on the means of providing information to users and on the necessity that such information remains available at all times. He recommends that it is expressly stated in the provisions concerning transparency that the modalities set forth as regards the provision of information to users also

[7] For instance, Articles 37- 42, 44-46, 49-51 and Recitals 32, 35, 39-42

apply to the provision of information about the processing of personal data pursuant to Articles 10 and 11 of Directive 95/46/EC.

2.7. Third party access

29. Articles 58 and 59 of the proposed Directive introduce rules governing the access to and use of payment account information by third party service providers and third party payment instrument issuers.

30. The EDPS notes that the Commission has paid attention to data protection when drafting these Articles, especially the principle of data minimisation. However, in the view of the EDPS the relevant provisions leave too much margin for interpretation. For example, the terms 'availability of sufficient funds' and 'sensitive payment data' are not defined anywhere in the text of the proposed Directive. This could lead to divergent transposition in Member States with the possibility of data protection risks involved with third party access if these undefined terms are given a broad interpretation in national legislation.

31. In the case of 'availability of sufficient funds' the EDPS recommends that it should be made clear that the information transmitted to the third party should consist in a simple 'yes' or 'no' answer to the question if there are sufficient funds available – not in for example a statement of the account balance.

32. The term 'sensitive payment data' does not exist in data protection law. Article 8 of Directive 95/46/EC lists the special categories of sensitive data that are granted a higher level of protection. Payment data is not among the categories listed. This does not mean that personal data concerning payments is not protected by data protection law, but it is not characterised as 'sensitive data'. The EDPS therefore recommends that the word 'sensitive' is deleted and that the term 'payment data' is used instead.

2.8. Security requirements

33. The EDPS welcomes the obligation for payment institutions in Article 5(j) to provide the competent authorities with a security policy document, a detailed risk assessment in relation to its payment services and a description of security control and mitigation measures taken to adequately protect the payment services against the risks identified including fraud and illegal use of sensitive and personal data.

34. As security is of crucial importance in the field of payment services, it must be ensured that the processing of personal data, and their passing along through the various intermediaries, respect the principles of confidentiality and security in compliance with Articles 16 and 17 of Directive 95/46/EC. The EDPS recommends adding in recital 6 and Article 85 that the processing of personal data must respect the security requirements laid down in Articles 16 and 17 of Directive 95/46/EC.

35. Recital 6 and Article 85 provide for an obligation to report within undue delay major security incidents to the European Banking Authority. The EDPS wishes to underline that similar notification requirements are also set forth under Directive 2002/58/EC, as revised by Directive 2009/136/EC, for the telecoms sector whenever personal data of individuals have been compromised, pursuant to which the responsible entity must notify the competent authority of that breach (i.e. the data protection authority or the telecommunication regulator) as well as the individuals concerned where relevant.

36. Consistency must therefore be ensured with the personal data breach requirements that are already applicable to telecom providers under Directive 2002/58/EC, as revised by Directive 2009/136/EC, and with the planned personal data breach provisions of the proposed General Data Protection Regulation that would apply to all data controllers (Articles 31 and 32). It should be clarified in a recital of the proposed Directive that the security incidents reporting obligations are without prejudice to other incident reporting obligations set forth in other legislation, in particular the personal data breaches requirements set forth under data protection law (in Directive 2002/58/EC and in the proposed General Data Protection Regulation) and the security incidents notification requirements planned under the proposed Directive on network and information security[8], a proposal on which the EDPS has published an Opinion[9] on 14 June 2013. The EDPS would also like to stress that the fact that the Proposed Directive in Article 85 refers to the proposed Directive on network and information security, which is still under negotiation, creates an ambiguous situation which further strengthens the need for clarification.

37. Article 87 of the proposed Directive states that Member States shall ensure that a payment service provider applies third party authentication. The Article also states that the European Banking Authority (EBA) in cooperation with the European Central Bank (ECB) shall issue guidelines addressed to payment service providers on state of the art customer authentication and any exemption of the use of strong customer authentication. The EDPS recommends including references in the proposed Directive to the need to consult the EDPS in so far as the guidelines concern the processing of personal data.

[8] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final.

[9] EDPS Opinion of 14 June 2013 on the `Cyber Security Strategy of the European Union´, available on the Consultation section of the EDPS website: www.edps.europa.eu

2.9. Standardisation and interoperability

38. The proposed Directive stresses the need to develop and to reinforce standardisation and interoperability. As underlined in our response to the public consultation, we believe that the development of these standards should be preceded by privacy impact assessments that would analyse the implications of new technologies available on the privacy and data protection of individuals. This process should allow identifying which are the risks associated to each of the technical options available and which are the remedies that could be put in place to minimize data protection threats. We therefore suggest adding in a substantive provision of the proposed Directive the obligation that these standards are developed on the basis of, and after having conducted, privacy impact assessments.

3. CONCLUSIONS

The EDPS welcomes the introduction in Article 84 of a substantive provision stating that *any* processing of personal data taking place in the frame of the proposed Directive should be done in full respect of the national laws implementing Directive 95/46/EC and Directive 2002/58/EC, and of Regulation EC No 45/2001.

The EDPS recommends that:

- references to applicable data protection law should be specified in concrete safeguards that will apply to any situation in which personal data processing is envisaged.

- it should be made clear in the draft Directive that the provision of payment services might entail the processing of personal data.

- it should be clarified expressly in the proposed Directive that the processing of personal data may be carried out insofar that it is necessary for the performance of payment services.

- a substantive provision is added stating the obligation that "privacy by design/privacy by default" be embedded in all data processing systems developed and used in the frame of the proposed Directive.

- regarding exchanges of information: (i) mentioning the purposes for which personal data can be processed by national competent authorities, the EU central bank, the national central banks and the other authorities referred to in Article 25, (ii) specifying the kind of personal information that can be processed under the proposed Directive and (iii) fixing a proportionate data retention period for the processing or at least introducing precise criteria for its establishment.

- a requirement should be introduced in Article 22 for competent authorities to request documents and information by formal decision, specifying the legal basis and the purpose of the request and what information is required

should be introduced, as well as the time-limit within which the information is to be provided.

- it is introduced in Article 31 that the modalities set forth as regards the provision of information to users also apply to the provision of information about the processing of personal data pursuant to Articles 10 and 11 of Directive 95/46/EC.

- in the case of the term 'availability of sufficient funds' in Articles 58 and 59 it is made clear that the information transmitted to the third party should consist in a simple 'yes' or 'no' answer to the question if there are sufficient funds available – not in for example a statement of the account balance.

- in the case of the term 'sensitive payment data' in Article 58 that the word 'sensitive' is deleted and that the term 'payment data' is used instead.

- it should be clarified in a recital that the security incidents reporting obligations are without prejudice to other incident reporting obligations set forth in other legislation, in particular the personal data breaches requirements set forth under data protection law (in Directive 2002/58/EC and in the proposed General Data Protection Regulation) and the security incidents notification requirements planned under the proposed Directive on network and information security.

- it must be ensured that the processing of personal data, and their passing along through the various intermediaries, respect the principles of confidentiality and security in compliance with Articles 16 and 17 of Directive 95/46/EC.

- a substantive provision is added to the proposed Directive with the obligation that standards are developed on the basis of, and after having conducted, privacy impact assessments.

- a reference should be included in the proposed Directive to the need to consult the EDPS in so far as the EBA guidelines on state of the art customer authentication and any exemption of the use of strong customer authentication concern the processing of personal data.

Done in Brussels, 5 December 2013

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor