EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

DG MARKT
European Commission

Via e-mail: markt-sepa@ec.europa.eu

Brussels, 11 April, 2012
GB/PDL **C2012-0034**

Dear Sir,
Dear Madam,

I am writing to you in response to DG MARKT's public consultation on the Green Paper entitled "Towards an integrated European market for card, internet and mobile payments".

The objective of the Green paper is to launch a broad-scale consultation with the stakeholders in order to validate or contribute to the Commission's analysis in identifying potential barriers to a European integration in the card, internet and mobile payments markets. The results of the consultation should help the Commission in identifying the best way to foster such integration.

The EDPS supports any initiative to make electronic payments secure, efficient, competitive and innovative but would like to remind that the introduction and emergence of a European integrated market for electronic retail payments must respect fundamental rights like the right to protection of personal data.

The development of new pan-European payment services will probably result in increasing the number and nature of actors involved in retail payments domestically, abroad and across borders. In particular, the development of mobile payments but also the suggestion mentioned in the Paper (see question 13) to give non-banks access to information on the availability of funds in bank accounts will involve new intermediaries. It will also increase the number of transactions and therefore the amount of collected and exchanged data. Furthermore, new categories of data such as location data may enter in the financial circuit (eg. payment of parking meter through a mobile phone). This poses new challenges and risks with regard to data protection.

Therefore, it is essential to consider data protection as one of the perspectives of the future single market and to integrate it from the earliest stage of the process.

The EDPS welcomes that data protection is addressed in the Green Paper. Indeed, all electronic retail payments referred to in the Paper (payments cards, e-payments and mobile

payments) imply the processing of significant amount of personal data by different stakeholders: names, bank account numbers and content of contract 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.

However, the EDPS notes that data protection is only mentioned under the Chapter on security payments in the Green paper. Security is of course a major issue and the passing along through the various intermediaries must respect the principles of confidentiality and security of the processing in compliance with Articles 16 and 17 of Directive 95/46/EC. Data protection implies that additional safeguards should be included also in other areas than just security. 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 and respect the obligation not to keep the data for longer than it is necessary. Besides, transparency is also a crucial part of data protection, not only because of its inherent value but also because it enables other data protection principles to be exercised.

Data protection requirements

When developing a strategy and/or instruments for the integration of the markets for payments by card, internet or mobile phone, it is essential that from the early start the following data protection aspects are taken into account:

- Transparency: it is important to clearly specify the role of each player in the transactions. Data subjects should be allowed to 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.

- Identification of the controller/processor: it is also crucial to define the role of each player in order to identify the responsibility of each, especially with regard to new payment service providers and intermediaries such as telecommunication operators. It should be assessed who should be considered as a data controller and for which data processing activities.

- Accountability: the principle of 'accountability' should be considered in any initiative involving the processing of personal data. This principle requires the controller to put in place appropriate and effective measures to ensure that data protection principles and obligations are complied with and to demonstrate so to supervisory authorities upon request.

- Proportionality: it should be ensured that the different actors only access and process the data that are necessary for the performance of their services. 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.

- Rights of the data subject: effective mechanisms should be put in place to enable the data subject to exercise his/her rights of access, rectification and erasure of his/her personal data, also in a complex, cross border context.

Technical implementation of data protection requirements

The Green Paper questions the need to develop and/or reinforce standardisation and interoperability. On these issues, the EDPS stresses that the development and/or adoption of technical standards should be based on a prior in depth analysis of the different technologies available and a subsequent privacy impact assessment of the implications. 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.

It is worth mentioning the principle of "Privacy by design/privacy by default". 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. The EDPS is pleased to note that - to some extent - the Green Paper refers to these notions when mentioning that "*it is crucial that authentication mechanisms for payment transactions are designed from the outset to conclude the necessary measures to ensure compliance with data protection requirements*". Notwithstanding the above, the EDPS is of the opinion that the scope of applicability of the concept should be extended beyond authentication mechanisms and security safeguards. Privacy by design also requires - inter alia - ensuring that data processing systems are designed to process as little personal data as possible (data minimization), to implement privacy by default settings, to limit the access to individual's information to what is strictly needed to provide the service and to implement tools enabling users to better protect their personal data (e.g. access controls, encryption) and exercise their rights.

Finally, the EDPS stresses that the issues identified in his contribution call for further developments and data protection will be taken up as an integral element of the further activities relating to the integrated European market for card, internet and mobile payments. In this light, it would also be good to ensure that the developments relating to the proposed new framework for data protection[1] will be taken into account. He is of course willing to contribute further in the next steps following the public consultation.

Yours sincerely,

(**signed**)

Giovanni BUTTARELLI

Contact person: P. de Locht, tel: 02 283 19 99

[1] In particular, the proposal for a new general data protection regulation, COM (2012) 11 final.