SIMONT BRAUN

MOBILE WALLETS AND MOBILE CONTACTLESS PAYMENTS – A CLOSER LOOK AT DATA PROTECTION

Brussels, May 2015.

INTRODUCTION

In our first memo on mobile wallets and mobile contactless payments, we focused on the technical aspects of such payments and noticed that the mobile payment ecosystem is complex. It constitutes a wide variety of different actors that are involved when a mobile contactless payment is executed: payment service providers (PSP), merchants, Trusted Service Managers (TSM), Mobile Network Operators (MNO), app developers, etc.

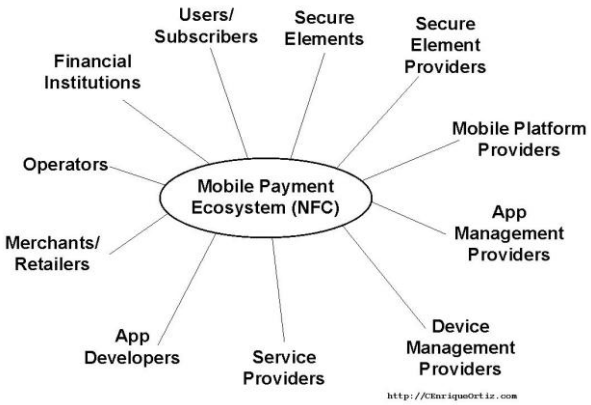
Within that ecosystem, personal data are being processed by various operators at different stages. How to assess the role of these entities when they process personal data, and in particular are they accountable, and to what extent, for the processing of the personal data?

MAKING A MOBILE CONTACTLESS PAYMENT: WHICH PERSONAL DATA IS PROCESSED?

The legal framework on data protection and privacy is defined in the first place by the European Data Protection Directive of 24 October 1995, implemented in Belgian law by the Act of 8 December 1992 ("BDPA"). Further, as mobile payments involve electronic communications, the so-called "ePrivacy" Directive of 12 July 2002, implemented in Belgian law by the Act of 13 June 2015 on electronic communications, is also applicable.

The legislation applies to the '*processing* of *personal data'*. The scope of both notions ('*processing*' and '*personal data*') is very broad.

'*Processing*' is in fact each operation performed on personal data: a merchant registering a payment transaction, an issuing bank executing payment instructions, a MNO transmitting



payment credentials, a mobile wallet developer collecting details on the purchaser. These are all acts of 'processing' under data protection legislation.

Only the processing of 'personal' shall fall under the scope of the BDPA. '*Personal data*' is all data by which a natural person (i.e. the data subject) can, directly or indirectly, be identified. Regarding a mobile contactless payment transaction, such personal data can *inter alia* be: a bank account number, payment credentials, a phone number, a smartphone ID number but also details on the shops visited and the products bought, all of which can be seen as personal data as long as they (in)directly relate to an individual.

The fact that the processed data would be encrypted (for example by a TSM) has no influence on this qualification. It remains personal data as it contains data that, indirectly (i.e. via decryption), relates to an identified or identifiable person.

DATA PROCESSOR AND/OR DATA CONTROLLER?

The main question is to know who acts as a mere 'data processor' and who acts as the 'data

controller' and is personally held by all the obligations under the BDPA.

According to the legislation, the 'controller' is he who determines the means and purposes of the processing. The processor acts only on behalf of the data controller. His obligations are more accurate, i.e. essentially to comply with the instructions given by the controller and to abide by jointly defined security and confidentiality measures.

However, if the processor decides to make further use of the data for his own purposes, he will then be regarded as a controller himself in that respect. It is thus likely that a single operator can qualify both as a controller for the processing of one set of personal data and as a processor with regard to another data set.

A few examples related to a mobile contactless payment transaction can clarify this:

- A merchant can be qualified as a data controller with regard to the purchase details (description, date, time, etc.) that he processes for the execution of the sales agreement as well as for his administration purposes.
- A Trusted Service Manager is likely to act only as a processor as he operates on behalf of a PSP and/or MNO to ensure the customer's payment credentials are transmitted in an encrypted and secured way.
- A mobile wallet developer can act in both capacities. On the one hand, as a processor, in case his app is developed at the request and on behalf of a bank to facilitate the contactless payments of the bank's customers. On the other hand, if the developer retains access to personal data (e.g. phone numbers or browsing history) for providing additional services, such as personalized advertisements, he is to be qualified as a 'controller' too. The same goes when the provider of the mobile wallet app is the developer itself (e.g. Apple or SixDots).

Both notions are thus functional concepts. The factual circumstances are therefore crucial to make an assessment on the specific role of an operator: which sets of data are processed, for which purposes, and which entity determines these purposes and decides on the technical and organizational measures? The existence and content of the contracts concluded between the different parties will often contain relevant provisions allowing to identify these roles and responsibilities.

DATA PROCESSING REQUIRES A LEGAL GROUND

Any processing of personal data must rely on a legal basis, which in the case at hand may be either the necessity to perform a contract, or the consent of the data subject.

Many of the operations carried out while executing a mobile contactless payment, are "*necessary for the performance of a contract*", pursuant to article 5.f) BDPA and therefore pose no problem. But most frequently, the data will also be processed for other purposes than for the strict performance of the payment instructions. In such cases, the customer's consent is required. A bank which provides a mobile wallet app to its customers may wish not only to install the application on the smartphone and to process payment details, but also to use the data for secondary services, such as insurance or investments products for instance. Therefore, it will have to obtain the customer's permission for each of these purposes, unless those are compatible with the purposes initially announced, taking into account the customer's legitimate expectations.

When requesting a client's initial permission, it is therefore advisable that data controllers quite accurately describe such potential 'other purposes' for which they might make secondary uses of the data at a later stage. In so doing, they will mitigate the risks associated with data protection rules.

* * *

Do you want to find out more about mobile wallets and mobile payments in a Belgian or more general context, how it can be used and what the consequences may be for your activity?

Please contact Simont Braun's Digital Finance Team:

Catherine.Houssa@SimontBraun.eu

Benjamin.Docquir@SimontBraun.eu

Philippe.DePrez@SimontBraun.eu

Jan.Clinck@SimontBraun.eu

Or by telephone via +32 (0)2 543 70 80