Data Protection Guidance in relation to Card Payment Transactions

The processing of payment card transactions involves the processing of information about individuals and, consequently, is subject to regulation under the Data Protection Acts 1988 and 2003 ("**Acts**").

The person who is primarily subject to regulation in this respect is the data controller. The data controller is the person who, either alone or with others, controls the contents and use of the personal data.

The Data Protection Commissioner issued guidance in January 2008 for data controllers who process payment card transactions[1]. The guidance focuses on what is required, from a practical perspective, by a number of the data protection principles in relation to the processing of credit/debit/charge or other relevant card payments.

In the context of payment card transactions, there can be a number of data controllers. This is due to the complexity of the events which unfold in the course of a payment card transaction and the number of different organisations involved in initiating and completing the transaction and who, consequently, store or handle the cardholder's personal data. For instance, the merchant, the cardholder's bank and the credit card company could process a cardholder's personal data, as a data controller, in the context of a single payment card transaction.

Data Protection Principles

Data controllers are required to comply with the data protection principles set out in section 2(1) of the Acts. The data protection principles are:

1. the data must be obtained and processed fairly;

2. the data must be accurate and complete and, where necessary, kept up to date;

3. the data must have been obtained only for one or more specified, explicit and legitimate purposes;

4. the data must not be further processed in a manner incompatible with that purpose or those purposes;

5. the data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed;

6. the data must not be kept for longer than is necessary for that purpose or those purposes; and

7. appropriate security measures must be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, and against all other unlawful forms of processing.

The Commissioner's guidance seeks to provide some practical insight in relation to the application of some of the above principles.

[1] http://www.dataprotection.ie/viewdoc.asp?DocID=581&m=f

1. **Personal data should be obtained for one or more specified, explicit and lawful purposes**

The data subject must know the reason(s) for which his or her information will be used. In the context of a payment card transaction, this will normally be clear provided the data is to be used simply for processing the transaction in question.

The Commissioner is of the view that it can be assumed that once the payment for the product or service for which personal data was collected is completed, the purpose of such collection ends. The consequences of this can be seen, in particular, from the application of the next data protection principle below.

2. **Personal data should not be further processed in a manner incompatible with that/those purposes**

Personal data may not be kept and used for purposes which are not consistent with the purpose for which the information was originally collected.

Consequently, if personal data is collected for a particular transaction, that data cannot subsequently be used for another transaction or purpose unless, according to the Commissioner, the cardholder expressly consents to such further use.

The Commissioner recommends that data controllers put in place data deletion procedures and security measures to ensure that information obtained for one transaction may not be accessed and used for another transaction or another purpose.

If it is proposed to get the customer's consent to use his card details for further purposes, the consent, according to the Commissioner, must be given by the customer positively agreeing to such further use (i.e. by 'opting-in') as opposed to simply not having objected (i.e. opting-out) to such use. Therefore, it seems that it may be possible to keep a customer's data for the purposes of facilitating future card transactions, provided the customer's clear and informed consent is obtained in this respect. This consent should ideally be obtained at the time the information is initially collected.

3. **Personal data should be adequate, relevant and not excessive**

The personal data collected should be restricted to that which is required for the purposes for which it is to be collected. Therefore, in the context of a card transaction, only data which is necessary to complete the transaction (and, if the cardholder has explicitly consented, to complete future transactions) should be collected.

The Commissioner stresses in this respect that personal data cannot in any case be retained on the 'off-chance' that it might be of use again at a future date.

4. **Personal data should not be kept longer than necessary for that/those purposes**

Personal data can only be kept for the duration for which it is needed and no longer.

The Commissioner, in his guidance, stresses the need to be clear about both the length of time personal data can be retained and the reasons for such retention. Once that time is up, the data must be deleted.

The Commissioner takes the view that personal data collected from a card would only need to be retained for a maximum of thirteen months to allow for copy voucher requests, and this only in the case of transactions which involve the signature of a receipt. In such cases, the Commissioner suggests that the information should be retained separately and solely for the

purpose of previous payment queries and for use for future transactions / further purposes. This, it would seem, is on the assumption that consent to future uses has not been obtained.

The Commissioner is of the view that where the transaction is completed using chip and PIN, personal data need not be retained by vendors as the card issuer will have retained an electronic record of the transaction.

Once the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.

Article to be attributed to Robert McDonagh, senior associate & Brian Harley, solicitor in Mason Hayes+Curran's commercial department.

Robert is a senior associate in the commercial department of Mason Hayes+Curran. For more information, please contact Robert atrmcdonagh@mhc.ie or + 353 1 614 5077.