Italy's new data protection rules for mobile payments

The Italian Data Protection Authority has produced new rules on the protection of users' data when making payments through mobile devices with the publishing of a Resolution in the Official Journal of the Italian Republic on 16 June. This Resolution puts forward several limits to the use of data by participants in the mobile payments market, as Laura Liguori and Federica De Santis of Portolano Cavallo Studio Legale explain.

On 22 May 2014, the Italian Data Protection Authority ('DPA') issued a Resolution ('Resolution') providing new rules on data protection for payments through mobile remote payment services (e.g. smartphone devices and tablets). The Resolution follows a public consultation launched by the DPA in January 2014 and was published in the Official Journal of the Italian Republic on 16 June 2014.

Telecoms operators, merchants and technology aggregators, but also other players involved in the provision of mobile remote payment services, shall comply with the rules and security measures set forth in the Resolution.

Scope of the Resolution

Remote mobile payment services allow users to pay remotely through a mobile device. This kind of mobile payment is growing and becoming more popular, with the aim of making the process of ordering and buying goods or services much faster and easier. Undoubtedly, the use of remote mobile payment technologies entails the processing of a large amount of personal data, e.g.:

- phone number;
- information on the product or service purchased by the user (e.g. type, price, date and time of purchase, etc.);
- data relating to the subscription and termination of the service, or to the charge of the relevant price on the invoice or to the prepaid card;
- sensitive data relating to the relevant product or service (e.g., information relating to a user's political or religious beliefs or sexual preference); and
- the IP address of the user.

The purpose of the Resolution is to offer greater protection to users who purchase goods or subscribe to services (e.g. online newspapers, e-books, games, communities, multimedia content, etc.) accessible via smartphone, tablets or PC, through mobile remote payment services.

The Resolution does not concern other types of mobile payment technologies such as mobile proximity payment services (e.g. Near Field Communication - 'NFC'), which will be addressed by the Italian DPA in a separate resolution.

The Resolution is particularly addressed to the following players:

- operators or providers of publicly available electronic communications services (e.g. telecoms operators), which provide their customers with a payment service by mobile phone to purchase digital content through the use of a rechargeable phone card, or on the basis of a phone subscription;
- merchants (i.e. companies offering digital content or services);
- technology aggregators or hubs (i.e. companies providing the technological platform through which digital content or services are made available and that usually perform activities such as management of the purchase path, creation of the customer relationship management interface, keeping the SMS for the activation and deactivation of the service, etc.).

The Resolution also applies to other players acting within the remote mobile payment market, e.g. app providers that enable users to buy digital content, games or software by using phone credit.

Having regard to the role performed by the relevant players from a data protection perspective, the Resolution notes that operators and merchants could qualify as data controllers or joint controllers, depending on the concrete circumstances of the case, while the aggregator, depending on its degree of autonomy, could act either as a data processor or as an autonomous controller. For instance, according to the Resolution, aggregators qualify as controllers if, based on specific agreements with operators and merchants, they are engaged in the offering of goods or services and perform activities such as the organisation and the offering of digital content to the user, the offering of customer services, the carrying out of promotional activities relating to the relevant content, etc.

The main data protection obligations set forth by the Resolution relate to information and consent requirements, security measures and data retention.

Information requirements

Users must receive complete information on how their personal data is processed, in compliance with the Italian Data Protection Code (Legislative Decree no. 196/2003).

In particular, the information notice must separate the different purposes of the data processing, specifying whether users' data will be processed for marketing purposes and if automated

modalities of contact will be used (e.g., fax, email, MMS and SMS). If the data are going to be used to profile users or used within loyalty programs, this must be clearly specified as well.

Notice shall be provided at the moment of subscription to the relevant services accessible through mobile remote payments, and shall be provided in a layered way, by displaying a short information notice including a link to a more detailed notice.

The information duty will be fulfilled by both operators and merchants, acting as data controllers, and also by the aggregators in those cases where they act as autonomous controllers.

If the aggregators act as data processors, the information notice provided by operators and merchants must also contain their details.

Consent requirements

Users' consent will not be obtained to process personal data for the provision of the relevant services; however, specific consent is required if data are used for other purposes, such as marketing or profiling, or if data are communicated to third parties.

Security measures

Operators, aggregators and merchants must adopt the minimum security measures required under the Italian Data Protection Code as well as the appropriate security measures provided by the Resolution to ensure the confidentiality of personal data. These measures shall include strong authentication mechanisms for accessing data, procedures for tracking operations and cryptographic systems to protect data.

The Resolution prescribes additional measures to prevent the combination of the data used for the relevant transaction with different sets of data collected by operators (e.g. consumption data), in order to avoid cross profiling of users based on their habits and preferences.

Merchants can only disclose to operators the category of the relevant digital content purchased by users. Details relating to the specific item purchased must not be provided to the operators

Specific measures must also be adopted for services intended for an adult audience, including the attribution to the relevant user of an access code, univocally and exclusively associated to the particular type of product or service requested by the user. Further, technical measures shall be set to ensure that such services can always be deactivated by the user.

Merchants can only disclose to operators the category of the relevant digital content purchased by users. Details relating to the specific item purchased must not be provided to the operators. Users' IP addresses shall be used by merchants solely for the purpose of user navigation on their websites, as well as to route the relevant digital content purchased by the user.

The message sent by operators to merchants when checking whether the user has sufficient phone credit to purchase the relevant digital content will not include codes disclosing the economic reasons for which the operation was not successful. Therefore, the Resolution prescribes that the 'K.O.' signal that operators send to merchants must only be accompanied by a code which allows a distinction between the different causes of error: those that give rise to a retry from those which, instead, do not allow the repetition of the transaction.

Data retention

Personal data processed by operators, aggregators and merchants can be kept for a maximum of six months; once this period has elapsed, data must be erased. Users' IP addresses must be erased by the merchants once the purchase process is complete.

Other provisions

The other data protection obligations set forth by the Italian Data Protection Code will apply (e.g., operators' data breach obligations and notification requirements, e.g. in case of profiling, etc.).

The measures set forth by the Resolution must be adopted within 180 days of publication in the Official Journal.

Failure to comply with the measures prescribed by the Italian DPA may entail sanctions ranging from €30,000 to €180,000. Additional sanctions may apply in case of failure to comply with other provisions of the Italian Data Protection Code.

Comments

The Resolution sets forth several limits to the use of data by remote mobile payment players. Whether the measures identified by the Resolution will be effective to ensure the protection of users' personal data or will prove to be an obstacle to the development of new payment services will be seen following the implementation of the Resolution. In any case, it is expected that the Italian DPA will look much closer at these evolving services and will enforce rules in case of breach.

Laura Liguori Partner
Federica De Santis Associate
Portolano Cavallo Studio Legale, Italy
lliguori@portolano.itf
desantis@portolano.it